



# **Technology Needs Assessment**

# Table of Contents

[Introduction](#)

[Methodology](#)

[Organization Mission and Goals](#)

[User Behavior](#)

[Technology Infrastructure](#)

[Stakeholder Interviews](#)

[Logistics](#)

[Interviewee List](#)

[UX Evaluation and Site Testing](#)

[Community Survey Summary](#)

[Google Analytics and Moz Content Audit](#)

[Information Architecture](#)

[Design Evaluation](#)

[Heuristic Evaluation](#)

[Peer Analysis](#)

[Information Architecture and Design](#)

[Platform](#)

[Site Metrics](#)

[Summary of UX evaluation and site testing](#)

[Strengths](#)

[Weaknesses](#)

[Back-office tools, project tools and infrastructure assessment](#)

[Salesforce CRM](#)

[Rackspace Cloud Hosting and MediaWiki Application](#)

[Communication Tools](#)

[Project Tools and Workflow](#)

[Summary of Results](#)

[Recommendations](#)

[OWASP Website - Information Architecture, Platform Selection, Site Redesign and Functionality Enhancements](#)

[Platform Selection](#)

[Information Architecture and Site Redesign](#)

[Back-office tools and Infrastructure architecture](#)

[Salesforce](#)

[Rackspace and OWASP website](#)

[Project Workflow and Toolset](#)

[Gamification and Engagement](#)

[Features and Release Roadmap](#)

[Closing Remarks](#)

[Appendix](#)

[List of Current Tools](#)

[Interview Questions](#)[Staff Meeting Questions](#)[IT Meeting Questions](#)[Builders, Breakers, and Defenders Questions](#)[Chapter and Project Leader Questions](#)[Global Board Questions](#)[Interview Summaries](#)[OWASP Staff Meeting](#)[OWASP IT Interview Meeting](#)[OWASP Builders Meeting](#)[OWASP Defenders Meeting](#)[OWASP Chapter and Project Leaders Interview Meeting](#)[OWASP Chapter and Project Leaders Interview Meeting](#)[OWASP Global Board Interview Meeting- Josh Sokol](#)[OWASP Global Board Interview Meeting- Andrew van der Stock](#)[OWASP Global Board Interview Meeting- Michael Coates](#)[OWASP Global Board Interview Meeting- Matt Konda](#)[OWASP IT Follow up Meeting- Matt Tesauro](#)

## Introduction

The OWASP Foundation is a US-based, not-for-profit organization with a global community of over 250+ international chapters. OWASP is an open community dedicated to enabling organizations to develop, acquire, operate and maintain secure and trusted applications and providing unbiased and practical information for application security.

OWASP has grown beyond its initial conception since 2001 into both a renowned haven for security information, research tools and libraries and a respected organization in the security space. As a result, its current infrastructure and website does not fully meet its user's and organization's needs and provide enough room for future development. A similar project was started in 2011 (OWASP Brochureware Website Proposal)<sup>1</sup> but did not gain the traction needed for execution.

The following project, part of the OWASP Global 2016 Strategic Goals<sup>2</sup>, is a Needs Assessment to evaluate OWASP's community-facing website, internal processes and back-office infrastructure and provide expert opinion outlining strengths, weaknesses, and recommendations for solutions. The project timeline and other details were tracked on the current OWASP wikipedia<sup>3</sup>, which serves as the organization's primary public facing site.

## Methodology

The following section details the methodology used for conducting the Needs Assessment. For a holistic approach, the key areas that we are analyzing are 1) Organization Mission and Goals, 2) User Behavior and 3) Technology Infrastructure and Content. The key tasks and actions taken are outlined below:

### 1. Organization mission and strategic goal review

We believe that by better understanding OWASP's mission, short term and long term goals, we can better assess whether the technology infrastructure, website and efforts are aligned to meet those goals. To facilitate this, we conducted a review of the organization content specific to its mission, goals and other details that we could find in the OWASP Dropbox account and the owasp.org website.

### 2. Stakeholder interviews

To establish the current organization and user's needs and shortcomings, we conducted interviews with key stakeholders (Global Board, volunteers, IT and staff) to gauge what their

---

<sup>1</sup> OWASP RFO Web Design: [https://www.owasp.org/index.php/RFO\\_Web\\_Design](https://www.owasp.org/index.php/RFO_Web_Design)

<sup>2</sup> OWASP Global 2016 Strategic Goals: [https://www.owasp.org/index.php/OWASP\\_Strategic\\_Goals](https://www.owasp.org/index.php/OWASP_Strategic_Goals)

<sup>3</sup> OWASP Website Project:  
[https://www.owasp.org/index.php/OWASP\\_Initiatives\\_Global\\_Strategic\\_Focus/website\\_project](https://www.owasp.org/index.php/OWASP_Initiatives_Global_Strategic_Focus/website_project)

pain points are with the website and organization. We offered multiple time slots for volunteers worldwide to participate in the discussion, however, a majority of the participants were US-based. In addition to stakeholder interviews, we hosted the May 2016 monthly meeting with the New Jersey Chapter of OWASP, where approximately 30-40 members and non-members provided feedback for the current project progress and some suggested site redesigns and participated in a card sorting exercise for the website's information architecture.

### 3. Industry research, trends and peer analysis

For the industry trends and research, we compared the current OWASP website, infrastructure and tools to the current best practices and conducted a peer analysis for other organizations similar to the OWASP Foundation.

### 4. UI/UX Evaluation and site testing

For UI/UX evaluation and site testing, we established user behavior for the current OWASP website using both user expectations and quantitative and qualitative data to make informed recommendations on the current state of the site and better enhance user experience.

### 5. Back-office tools, Salesforce and Infrastructure Assessment

In assessing the technology infrastructure, back-office tools and Salesforce, we benchmarked if the technology itself is meeting the organization's current and future needs in both security project development and organization administration.

### 6. Report Delivery

All gathered information is summarized in this report. The Global Board will review the following documentation and provide some feedback; revisions will be made if necessarily. Lastly, a debriefing will be held to discuss the summary of results and address any additional questions the board may have.

## Organization Mission and Goals

In understanding OWASP's mission and 2016 strategic goal, we can better assess if the current infrastructure and website meet their mission and strategic goals as a renowned security non-profit organization. Based on this analysis, we can design a comprehensive solution to fulfill these goals.

### Mission and Core Values

The following is the OWASP mission and core values outlined on both the OWASP Home<sup>4</sup> and About Us pages<sup>5</sup>.

1. **Mission** - To make software security visible to individuals and organizations to make informed decisions based on unbiased and practical information. Everyone is free to participate and all materials are available under a free and open software license.
2. **Core Values**

---

<sup>4</sup> OWASP Home Page: [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)

<sup>5</sup> OWASP About Us Page: [https://www.owasp.org/index.php/About\\_OWASP](https://www.owasp.org/index.php/About_OWASP)

- a. **Open** - Everything at OWASP is radically transparent from our finances to our code.
- b. **Innovation** - OWASP encourages and supports innovation and experiments for solutions to software security challenges.
- c. **Global** - Anyone around the world is encouraged to participate in the OWASP community.
- d. **Integrity** - OWASP is an honest and truthful, vendor neutral, global community.

## Strategic Goals 2016

The following are the strategic goals outlined on the OWASP website<sup>6</sup>:

1. **Education and Training** - Continue to present existing OWASP training materials and content on a global scale. Create a new curriculum and content based on output from projects and key industry trends.
2. **Expand Outreach, specifically to the Developer Community** - Expand contact with developer community to help educate them on OWASP projects, tools and best practices.
3. **Mature the OWASP Projects Platform** - Provide the OWASP project community a mature project platform to encourage senior developers to participate in the various and many OWASP projects.
4. **Community and Chapter Support** - Retain all existing active chapters and stimulate inactive chapters to become an active part of the community. Encourage creation of new chapters in continuing all community engagement efforts by community, staff and community manage.
5. **Enhance the OWASP infrastructure** - Identify current infrastructure requirements and weaknesses to determine where repairs and upgrades are needed to better support the community and strategic goals.

## User Behavior

To establish user behavior, we looked at both quantitative and qualitative data. For a qualitative overview, we conducted interviews with key stakeholders (OWASP employees, Global Board, chapter/project leaders and volunteers) and distributed a community survey via SurveyMonkey. For a quantitative overview, we relied on data points from Google Analytics and Moz Content Audit to see what content and resources users are utilizing the most and what is being shared the most. With well-established user behavior profiles in mind, we conducted design and heuristic evaluations and reviewed the current information architecture. Ultimately, we wanted to establish how users are engaging with the OWASP website and propose a solution to encourage community participation. In addition, we conducted a peer analysis to show how OWASP compares with other similar organizations in the security and technology space.

---

<sup>6</sup> OWASP Strategic Goal 2016:

[https://www.owasp.org/index.php/OWASP\\_Strategic\\_Goals#tab=2016](https://www.owasp.org/index.php/OWASP_Strategic_Goals#tab=2016)

## Technology Infrastructure

To analyze the current technology infrastructure, we separated the listed tools in the initial RFP<sup>7</sup> into four categories. For each, we compared the industry best practices with the current state of OWASP. The four categories are:

- 1) Website and associated infrastructure
- 2) Salesforce CRM
- 3) Communication Tools
- 4) Project Tools and Workflow

## Stakeholder Interviews

### Logistics

Interviews with key stakeholders were scheduled in the first two weeks of the project and interview questions were prepared and distributed prior to the interview. The goal was to help establish the current pain points of each key stakeholder group, their behavior and opinion on the current OWASP website; touch upon any tools being utilized; and get feedback regarding what improvements they may want to see on the OWASP site and infrastructure. In addition to the interviews in scope, we interviewed the Global Board members to speak on the needs of the community as directly elected representatives.

### Interviewee List

#### 1) IT and Staff Interviews

- a) **Staff Interview** [April 28th, 2016]
  - i) **Kelly Santalucia** - Membership and Business liaison
  - ii) **Claudia Casanovas** - Project Coordinator
  - iii) **Laura Grau** - Events Manager
  - iv) **Kate Hartmann** - Operations Director/Salesforce Administrator
  - v) **Alison Shrader** - Accounting
- b) **IT Interview** [April 28th, 2016]
  - i) **Kate Hartmann** - Operations Director/Salesforce Administrator
  - ii) **Matt Tesauro** - IT Administrator
- c) **IT Follow-Up Interview** [May 27th, 2016]
  - i) **Matt Tesauro** - IT Administrator

#### 2) Builder, Breaker and Defender Interviews

- a) **Builder Interview** [May 3rd, 2016]
  - i) **Kate Hartmann** - Operations Director/Salesforce Administrator
  - ii) **Tom Brennan** - Global Board Member
  - iii) **Aaron Weaver** - Project Leader for AppSec Pipeline Project
  - iv) **Kevin W. Wall** - Project Contributor for ESAPI Project

---

<sup>7</sup> OWASP Needs Assessment RFP:

[https://www.owasp.org/images/7/7b/RFP\\_The\\_OWASP\\_Foundation\\_Needs\\_Assessment.pdf](https://www.owasp.org/images/7/7b/RFP_The_OWASP_Foundation_Needs_Assessment.pdf)

- b) **Breaker Interview** - The Breaker interview meeting was canceled, because only one volunteer responded to participate; this would not yield an accurate or comprehensive representation of the Breakers community.
- c) **Defender Interview** [May 10th, 2016]
  - i) **Kate Hartmann** - Operations Director/Salesforce Administrator
  - ii) **Nikola Milosevic** - Project Leader for SeraphimDroid project, OWASP Manchester Chapter Leader
  - iii) **Gabriel Gumbs** - Project Leader for OWASP Application Security Program Quick Start Guide
  - iv) **Haral Tsitsivas** - Chapter Leader for OWASP Orange County, CA
- 3) **Project and Chapter Leader Interviews**
  - a) **Project and Chapter Leader Interview** [May 17th, 2016]
    - i) **Kate Hartmann** - Operations Director/Salesforce Administrator
    - ii) **Aaron Weaver** - Project Leader for AppSec Pipeline Project, Chapter Leader for OWASP Philadelphia, PA
    - iii) **Oana Cornea** - Chapter Leader for OWASP Bucharest, Romania
    - iv) **Haral Tsitsivas** - Chapter Leader for OWASP Orange County, CA
    - v) **Edgar David Salazar** - Chapter Leader for OWASP Venezuela
  - b) **Project and Chapter Leader Interview** [May 19th, 2016]
    - i) **Kate Hartmann** - Operations Director/Salesforce Administrator
    - ii) **Tom Brennan** - Chapter Leader for OWASP New York/New Jersey
    - iii) **Colin Watson** - Project Leader for AppSensor, Cornucopia, Project Threats, and Snakes & Ladders
  - c) **Project and Chapter Leader Interview** [May 28th, 2016]- This was canceled after 20 minutes due to a lack of participants.
- 4) **Global Board Interviews**
  - a) **Tom Brennan** - Tom have been heavily involved with the project overall in participating in various interviews and in helping us organize a working session during the NJ chapter meeting. As we had asked all key questions, consequently, we did not require an additional one-on-one interview.
  - b) **Josh Sokol** [May 24th, 2016]
  - c) **Andrew van der Stock** [May 26th, 2016]
  - d) **Michael Coates** [May 26th, 2016]
  - e) **Matt Konda** [May 27th, 2016]
  - f) **Interviews not completed:** Jim Manico and Tobias Gondrom

Detailed meeting summaries have been attached in the appendix for reference.



## UX Evaluation and Site Testing

The following section is the evaluation of the OWASP website through a multifaceted approach. We first established a qualitative user behavior view through our survey and stakeholder interviews (detailed in the prior section). In conjunction, we established a quantitative view of user behavior in analyzing Google Analytics and Moz Content Auditing, which results in a holistic user behavior perspective. With this in mind, we moved forward in conducting a peer analysis and a design and heuristic evaluation to verify how closely the current site meets user needs and determine what improvements may help encourage user participation. Lastly, we conclude with a summary of the strengths and weaknesses of the OWASP website.

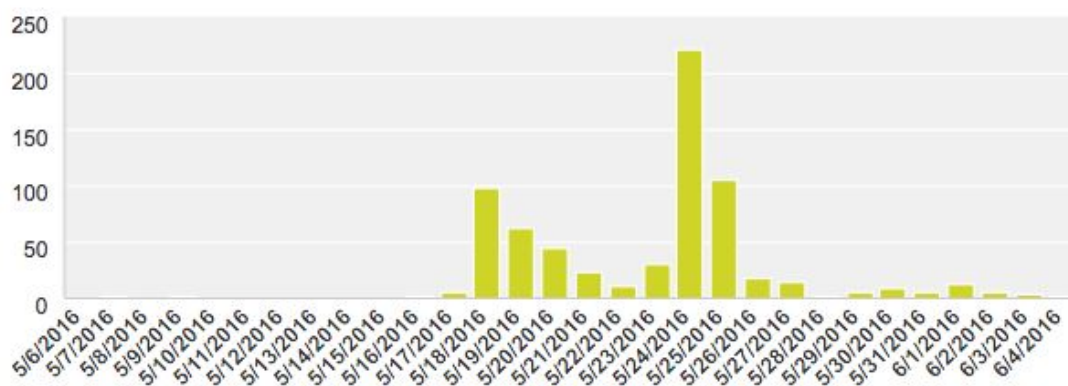
### Community Survey Summary

The following section summarizes the community survey results that was distributed on May 16th, 2016, which yielded 679 responses over the course of 3 weeks. The survey was distributed via email and other social channels (Facebook, Twitter, etc) by Kate Hartmann and were sent in additional reminder notices. The final results were polled on June 5th, 2016 prior to the report draft submission. Of the 679 respondents, 108 were official OWASP members (4.42%<sup>8</sup>), and the remaining respondents chose to remain anonymous and/or were not official OWASP members. Overall, 679 responses out of 45,000 volunteers would be a 1.5% total response rate.

#### Response volume by date:

Responses Volume

5/6/2016 - 6/4/2016



In addition, on the day of the NJ OWASP chapter meeting at Sooryen Technologies Headquarters on May 24, we saw a significant increase in response rate. This may suggest that to drive additional participation from the OWASP community for future surveys and events, chapter leaders should announce requests for participation more often in their chapter meetings

<sup>8</sup> The following percentage was calculated based on email matches between the paid membership list and user supplied emails in the survey. The percentage of OWASP member responses may be higher (up to 16%).

on a global scale; encourage additional in-office work sessions, which may benefit the response rate; and distribute frequent reminder emails.

### Summary of the responses:

#### 1. How often do you visit the OWASP website?

	Responses	Percentage (%)
At least once a week	199	29.31%
At least once a month	230	33.87%
At least once a quarter	167	24.59%
Rarely	82	12.22%

**Key takeaway:** A significant portion of the audience visits the OWASP website at least once a week and month.

#### 2. Have you ever had issues connecting to the OWASP website?

	Responses	Percentage (%)
Yes	76	11.21%
No	602	88.79%

**Key takeaway:** A majority of people connect to the OWASP website without any issues. However, an alarming amount of people from the sample set (11.21%) experienced issues. This may have to do with the Fail2ban settings in place and other contributing factors.

#### 3. On a scale of 1-5 with 5 being the best and 1 being the worst, please rate the OWASP website on the following parameters.

	1	2	3	4	5	Total Response	Weighted Average
Usability	4.90% 33	18.84% 127	37.69% 254	29.23% 197	9.35% 63	674	3.19
Design/ Appearance	8.61% 58	29.67% 200	36.05% 243	20.77% 140	4.90% 33	674	2.84
Mobile use	11.05% 64	27.29% 158	42.31% 245	15.37% 89	3.97% 23	579	2.74
Speed	1.05% 7	6.73% 45	26.76% 179	45.89% 307	19.58% 131	669	3.76

Ability to find information	8.23% 55	23.35% 156	34.13% 228	25.45% 170	8.83% 59	668	3.03
Navigation	7.60% 51	27.72% 186	35.92% 241	23.55% 158	5.22% 35	671	2.91
Quality of material	1.93% 13	5.95% 40	10.42% 70	42.71% 287	38.99% 262	672	4.11

**Key takeaway:** OWASP provides a wealth of high quality security information, projects and tools as indicated by its above average score of 4.11. The website is usable and fast. However, a majority of the other scores highlighted in red indicates that there is room for improvement - particularly in design and appearance, mobile use, navigation and content organization. Recursively, these elements have been stressed upon during the stakeholder interviews as well.

#### 4. Do you find that the OWASP website has redundant and/or unnecessary information?

Never	Rarely	Sometimes	Often	Always	N/A	Total Response	Weighted Average
4.90% 33	28.04% 189	46.29% 312	11.42% 77	3.41% 23	5.93% 40	674	2.79

**Key takeaway:** Unsurprisingly, a good portion of response shows that there is redundant or unnecessary information on the OWASP website. Without a content strategy or moderators, redundant material and pages can be prevalent as there is currently no formal process.

#### 5. Have you had trouble navigating and/or downloading resources you were looking for (such as code repositories and/or documentation)?

Never	Rarely	Sometimes	Often	Always	N/A	Total Response	Weighted Average
14.88% 100	27.08% 182	36.01% 242	12.95% 87	3.13% 21	5.95% 40	672	2.6

**Key takeaway:** Navigation and locating resources have been issues that have been brought up consistently.

#### 6. How often are you able to locate the information you were looking for on the site?

Never	Rarely	Sometimes	Often	Always	N/A	Total Response	Weighted Average
0.15% 1	3.86% 26	19.02% 128	52.90% 356	22.14% 149	1.93% 13	673	3.95

**Key takeaway:** Despite the current site layout and navigation, people are still able to locate information they are looking for whether through internal or external search.

7. How often does the OWASP search engine deliver expected results?

Never	Rarely	Sometimes	Often	Always	N/A	Total Response	Weighted Average
1.05%	8.67%	23.17%	37.07%	7.92%	22.12%	669	3.54
7	58	155	248	53	148		

**Key takeaway:** Despite several complaints regarding site search, it is surprising to find that the OWASP search engine delivers expected results based on other users - this may be from one-time users who have yet to familiarize themselves with other available content.

8. Are you able to find relevant content on the website by searching directly on Google or another search engine?

	Responses	Percentage
Yes	446	66.77%
No	33	4.94%
Sometimes	189	28.29%
Total	668	

**Key takeaway:** When content can't be found via internal search as some survey respondents suggested, Google or other search engines deliver relevant content for the OWASP site.

9. On average, how long does it take for you to locate relevant information to you?

	Responses	Percentage (%)
Less than two minutes	196	29.34%
Two to five minutes	367	54.94%
More than five minutes	105	15.72%
Total	668	

**Key takeaway:** Although users are able to locate content they are searching for, 70.66% of respondents indicated that the typical duration of search time to find relevant information was greater than the optimal less than 2+ minutes, which is alarming in that

10. Is the layout of information easy to understand?

Never	Rarely	Sometimes	Often	Always	N/A	Total Response	Weighted Average
4.48%	24.03%	31.49%	31.34%	6.72%	1.94%	670	3.12

30	161	211	210	45	13		
----	-----	-----	-----	----	----	--	--

**Key takeaway:** As the MediaWiki layout is, to a degree, consistent with the arrangement of the navigation to the left, users have indicated that they are often able to locate information on a page.

11. To what extend do you agree or disagree with the following statement: As a contributor to the wiki, I find it easy to edit existing documentations and/or assets.

Never	Rarely	Sometimes	Often	Always	N/A	Total Response	Weighted Average
1.20% 8	5.85% 39	19.49% 130	14.24% 95	4.80% 32	54.42% 363	667	3.34

**Key takeaway:** Editing documentation/contributing to the wiki is not as complicated as initially hypothesized, however, there may still be a learning curve for new users.

12. What changes or additional features would you suggest for this website? (Open-end question - Summary of top five key points)

- Better navigation, search and advanced filters - Navigation is cluttered with too many links. Including breadcrumbs and a sitemap would help users.
- Organize and keep content up to date - This includes trimming and removing old documents or abandoned projects, removing duplicate content, and standardizing a more consistent format across articles and information layout throughout the site.
- More modern design that works across all devices especially mobile.
- Integration with various sources (AppSec feed, blog, etc.).
- Personalization for members.

13. What existing features about this site would you like to see improved or removed? (Open-end question - Summary of top four key points)

- Improvement - Navigation and Search
- Improvement - Content Updates and Rating System
- Improvement - Polish the design
- Improvement - Better coverage of chapters and projects
- Improvement - More training material

**Key takeaway (Q12-13):** Most, if not all, users agree that the OWASP website needs a facelift and needs to accommodate mobile use, content curation, more personalization and improved information architecture.

14. What is your primary use of the site?

	Responses	Percentage
Contribute to an OWASP project	41	6.27%

Research about OWASP projects	165	25.23%
Read about OWASP best practices	387	59.17%
Locate information about OWASP events	24	3.67%
Purchase OWASP merchandise	1	0.15%
Other	36	5.50%

**Key takeaway:** Most users are here for the content such as best security practices.

#### 15. How would you classify yourself?

	Responses	Percentage (%)
Builder	189	37.50%
Breaker	148	29.37%
Defender	262	51.98%
OWASP Community Member	209	41.47%
Chapter Leader	55	10.91%
Project Leader	35	6.94%
Nonmember	70	13.89%
Other	36	7.14%

**Key takeaway:** Most users classify themselves as Defenders and community members.

#### 16. Which of the following best describes your profession?

	Responses	Percentage (%)
Cyber Security Professional	383	58.47%
Developer/ Solution Architect	139	21.22%
Systems Engineer/ Architect	50	7.63%
IT Project Management	27	4.12%
IT Executive Management	41	6.26%
Outside of IT industry	15	2.29%

**Key takeaway:** As expected, most users are Cyber Security professionals followed by developers and solution architects.

## Google Analytics and Moz Content Audit

The following section outlines the Google Analytics and Moz Content Audit we conducted to establish a qualitative view of user behavior.

### Google Analytics

In analyzing OWASP’s Google Analytics account, we establish a quantitative overview of user behaviors. The key areas of interests are the following:

1. New vs. Returning Visitors
2. Desktop vs. Mobile Visitors
3. Channels

We analyzed the top 10 resources per each segments and the associated user behaviors and engagements for the following time intervals of one month and one year.

### One Month - May 1st, 2016 - May 31st, 2016

#### New vs. Old Visitors



#### Desktop vs. Mobile Visitors

Device Category	Sessions	Pages / Session	Avg. Session Duration	% New Sessions	Bounce Rate
<b>New Users</b>	513,010 <small>% of Total: 53.87% (952,260)</small>	1.75 <small>Avg for View: 1.96 (-10.54%)</small>	00:01:52 <small>Avg for View: 00:02:38 (-28.69%)</small>	100.00% <small>Avg for View: 53.87% (85.62%)</small>	72.43% <small>Avg for View: 68.13% (6.30%)</small>
<b>Returning Users</b>	439,251 <small>% of Total: 46.13% (952,260)</small>	2.20 <small>Avg for View: 1.96 (12.31%)</small>	00:03:30 <small>Avg for View: 00:02:38 (33.51%)</small>	0.00% <small>Avg for View: 53.87% (-100.00%)</small>	63.12% <small>Avg for View: 68.13% (-7.36%)</small>
1. desktop					
New Users	462,219 (90.10%)	1.76	00:01:55	100.00%	72.14%
Returning Users	414,921 (94.46%)	2.22	00:03:35	0.00%	62.46%
2. mobile					
New Users	43,450 (8.47%)	1.65	00:01:23	100.00%	75.55%
Returning Users	20,032 (4.56%)	1.78	00:02:05	0.00%	74.09%
3. tablet					
New Users	7,341 (1.43%)	1.87	00:01:50	100.00%	72.25%
Returning Users	4,298 (0.98%)	1.83	00:02:21	0.00%	75.06%

### Channels

Social Network	Sessions	% Sessions
1. <a href="#">Stack Overflow</a>	12,297	37.23%
2. <a href="#">Stack Exchange</a>	5,542	16.78%
3. <a href="#">Facebook</a>	4,046	12.25%
4. <a href="#">LinkedIn</a>	2,147	6.50%
5. <a href="#">Twitter</a>	1,951	5.91%
6. <a href="#">Blogger</a>	1,417	4.29%
7. <a href="#">Quora</a>	944	2.86%
8. <a href="#">reddit</a>	897	2.72%
9. <a href="#">YouTube</a>	480	1.45%
10. <a href="#">WordPress</a>	474	1.44%

Default Channel Grouping	Acquisition			Behavior		
	Sessions ? ↓	% New Sessions ?	New Users ?	Pages / Session ?	Avg. Session Duration ?	Bounce Rate ?
	5.00% ↑ 952,260 vs 906,920	3.01% ↑ 54.15% vs 52.56%	8.16% ↑ 515,630 vs 476,708	38.47% ↓ 1.95 vs 3.17	23.62% ↓ 00:02:36 vs 00:03:24	33.58% ↓ 68.11% vs 50.99%
1. Organic Search	89.20% ↑ 723,565 vs 382,428	-9.56% ↓ 51.08% vs 56.48%	71.11% ↑ 369,566 vs 215,981	-36.26% ↓ 1.99 vs 3.13	-16.87% ↓ 00:02:50 vs 00:03:24	30.27% ↑ 66.99% vs 51.43%
2. Social	27.48% ↑ 33,030 vs 25,909	32.70% ↑ 59.80% vs 45.07%	69.17% ↑ 19,752 vs 11,676	-39.72% ↓ 1.57 vs 2.61	-48.12% ↓ 00:01:21 vs 00:02:37	34.21% ↑ 76.69% vs 57.14%
3. Referral	-26.97% ↓ 90,383 vs 123,758	35.64% ↑ 56.58% vs 41.71%	-0.94% ↓ 51,138 vs 51,622	-47.29% ↓ 1.82 vs 3.46	-46.26% ↓ 00:01:58 vs 00:03:40	43.75% ↑ 70.67% vs 49.16%
4. Direct	-64.17% ↓ 104,822 vs 292,537	32.62% ↑ 71.96% vs 54.26%	-52.48% ↓ 75,431 vs 158,733	-38.58% ↓ 1.89 vs 3.08	-44.95% ↓ 00:01:58 vs 00:03:34	37.93% ↑ 70.92% vs 51.42%
5. (Other)	-98.96% ↓ 424 vs 40,672	-18.61% ↓ 32.08% vs 39.41%	-99.15% ↓ 136 vs 16,029	-19.02% ↓ 2.55 vs 3.15	14.62% ↑ 00:03:14 vs 00:02:49	22.13% ↑ 61.32% vs 50.21%
6. Email	-99.91% ↓ 24 vs 25,776	49.97% ↑ 79.17% vs 52.79%	-99.86% ↓ 19 vs 13,607	-67.23% ↓ 1.12 vs 3.43	-77.80% ↓ 00:00:44 vs 00:03:20	127.43% ↑ 87.50% vs 38.47%
7. Paid Search	-99.99% ↓ 12 vs 105,573	-84.02% ↓ 8.33% vs 52.14%	-100.00% ↓ 1 vs 55,046	-52.02% ↓ 1.75 vs 3.65	29.67% ↑ 00:03:29 vs 00:02:41	-30.41% ↓ 33.33% vs 47.90%
8. Display	-100.00% ↓ 0 vs 23,855	-100.00% ↓ 0.00% vs 47.44%	-100.00% ↓ 0 vs 11,318	-100.00% ↓ 0.00 vs 3.10	-100.00% ↓ 00:00:00 vs 00:02:15	-100.00% ↓ 0.00% vs 61.57%
9. Other Advertising	-100.00% ↓ 0 vs 35,937	-100.00% ↓ 0.00% vs 37.94%	-100.00% ↓ 0 vs 13,636	-100.00% ↓ 0.00 vs 2.86	-100.00% ↓ 00:00:00 vs 00:02:20	-100.00% ↓ 0.00% vs 39.63%



### Top 10 Pages

Page	Pageviews	Unique Pageviews	Avg. Time on Page	Entrances	Bounce Rate	% Exit
	1,859,127 <small>% of Total: 100.00% (1,859,127)</small>	1,570,740 <small>% of Total: 100.00% (1,570,740)</small>	00:02:44 <small>Avg for View: 00:02:44 (0.00%)</small>	952,253 <small>% of Total: 100.00% (952,253)</small>	68.11% <small>Avg for View: 68.11% (0.00%)</small>	51.22% <small>Avg for View: 51.22% (0.00%)</small>
1. /index.php/Main_Page	127,978 (6.88%)	100,035 (6.37%)	00:01:38	81,319 (8.54%)	50.96%	43.11%
2. /index.php/Category:OWASP_Top_Ten_Project	50,975 (2.74%)	40,747 (2.59%)	00:01:35	23,742 (2.49%)	46.10%	37.08%
3. /index.php/Top_10_2013-Top_10	38,550 (2.07%)	29,216 (1.86%)	00:02:16	19,041 (2.00%)	53.93%	43.33%
4. /index.php/Cross-site_Scripting_(XSS)	37,686 (2.03%)	33,312 (2.12%)	00:03:32	24,752 (2.60%)	60.46%	54.24%
5. /index.php/OWASP_Zed_Attack_Proxy_Project	36,776 (1.98%)	30,171 (1.92%)	00:04:32	23,273 (2.44%)	77.00%	70.17%
6. /index.php/XSS_(Cross_Site_Scripting)_Preventi on_Cheat_Sheet	36,653 (1.97%)	31,565 (2.01%)	00:04:36	19,621 (2.06%)	70.44%	60.44%
7. /index.php/XSS_Filter_Evasion_Cheat_Sheet	29,468 (1.59%)	25,735 (1.64%)	00:05:45	19,525 (2.05%)	75.58%	70.00%
8. /index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet	25,123 (1.35%)	22,387 (1.43%)	00:04:56	17,642 (1.85%)	76.01%	70.26%
9. /index.php/SQL_Injection_Prevention_Cheat_Sheet	23,531 (1.27%)	21,476 (1.37%)	00:04:49	16,026 (1.68%)	79.78%	70.09%
10. /index.php/Testing_for_SQL_Injection_(OTG-INP VAL-005)	21,651 (1.16%)	20,007 (1.27%)	00:05:34	15,522 (1.63%)	82.23%	76.06%

### One year - May 1st, 2015 - May 31st, 2016

#### New vs. Old Visitors



#### Desktop vs. Mobile Visitors

Device Category	Acquisition			Behavior		
	Sessions	% New Sessions	New Users	Bounce Rate	Pages / Session	Avg. Session Duration
<b>New Users</b>	6,100,792 <small>% of Total: 56.13% (10,868,920)</small>	100.00% <small>Avg for View: 56.13% (78.16%)</small>	6,100,792 <small>% of Total: 100.00% (6,100,792)</small>	70.40% <small>Avg for View: 66.75% (5.46%)</small>	1.77 <small>Avg for View: 1.99 (-11.06%)</small>	00:01:50 <small>Avg for View: 00:02:33 (-28.44%)</small>
<b>Returning Users</b>	4,768,128 <small>% of Total: 43.87% (10,868,920)</small>	0.00% <small>Avg for View: 56.13% (-100.00%)</small>	0 <small>% of Total: 0.00% (6,100,792)</small>	62.09% <small>Avg for View: 66.75% (-6.99%)</small>	2.27 <small>Avg for View: 1.99 (14.15%)</small>	00:03:29 <small>Avg for View: 00:02:33 (36.39%)</small>
1. desktop						
New Users	5,563,984 (91.20%)	100.00%	5,563,984 (91.20%)	69.99%	1.78	00:01:52
Returning Users	4,509,167 (94.57%)	0.00%	0 (0.00%)	61.39%	2.30	00:03:33
2. mobile						
New Users	445,251 (7.30%)	100.00%	445,251 (7.30%)	75.57%	1.64	00:01:18
Returning Users	195,211 (4.09%)	0.00%	0 (0.00%)	74.30%	1.75	00:02:01
3. tablet						
New Users	91,557 (1.50%)	100.00%	91,557 (1.50%)	70.39%	1.85	00:02:06
Returning Users	63,750 (1.34%)	0.00%	0 (0.00%)	74.20%	1.88	00:02:51

## Channels

Social Network	Sessions	% Sessions
1. <a href="#">Stack Overflow</a>	148,590	38.07%
2. <a href="#">Stack Exchange</a>	71,559	18.33%
3. <a href="#">Facebook</a>	40,565	10.39%
4. <a href="#">Twitter</a>	23,765	6.09%
5. <a href="#">Blogger</a>	19,467	4.99%
6. <a href="#">reddit</a>	17,312	4.44%
7. <a href="#">LinkedIn</a>	12,978	3.32%
8. <a href="#">YouTube</a>	7,649	1.96%
9. <a href="#">wikiHow</a>	7,008	1.80%
10. <a href="#">WordPress</a>	5,458	1.40%

Default Channel Grouping	Acquisition			Behavior		
	Sessions ?	% New Sessions ?	New Users ?	Pages / Session ?	Avg. Session Duration ?	Bounce Rate ?
	4.38%	1.04%	3.38%	35.50%	21.97%	25.81%
	10,868,920 vs 11,366,299	56.11% vs 55.53%	6,098,699 vs 6,312,219	1.99 vs 3.09	00:02:34 vs 00:03:17	67.00% vs 53.25%
1. Organic Search	52.38%	-11.65%	34.62%	-33.30%	-14.23%	22.98%
	7,948,378 vs 5,216,191	52.30% vs 59.20%	4,156,830 vs 3,087,802	2.02 vs 3.04	00:02:49 vs 00:03:17	66.69% vs 54.23%
2. Social	29.64%	25.43%	62.61%	-37.24%	-46.54%	26.49%
	390,347 vs 301,106	60.32% vs 48.09%	235,462 vs 144,802	1.60 vs 2.55	00:01:24 vs 00:02:37	75.65% vs 59.81%
3. Referral	-32.35%	26.41%	-14.49%	-43.28%	-42.97%	39.24%
	1,041,067 vs 1,538,979	57.43% vs 45.43%	597,916 vs 699,235	1.88 vs 3.32	00:01:58 vs 00:03:28	70.13% vs 50.37%
4. Direct	-58.87%	28.53%	-47.13%	-32.68%	-39.96%	16.72%
	1,412,634 vs 3,434,293	74.01% vs 57.58%	1,045,420 vs 1,977,346	2.03 vs 3.02	00:02:03 vs 00:03:25	62.67% vs 53.69%
5. Paid Search	-93.84%	68.09%	-89.64%	-68.61%	-94.86%	95.11%
	73,658 vs 1,194,817	91.13% vs 54.21%	67,122 vs 647,737	1.16 vs 3.69	00:00:09 vs 00:02:49	92.96% vs 47.65%
6. (Other)	-99.57%	-32.43%	-99.71%	-18.63%	3.85%	24.28%
	2,287 vs 526,338	28.86% vs 42.71%	660 vs 224,789	2.68 vs 3.29	00:03:02 vs 00:02:56	63.71% vs 51.26%
7. Email	-99.85%	76.37%	-99.73%	-51.34%	-58.18%	104.97%
	549 vs 360,884	59.56% vs 33.77%	327 vs 121,876	1.59 vs 3.26	00:01:24 vs 00:03:22	79.23% vs 38.66%
8. Display	-100.00%	-100.00%	-100.00%	-100.00%	-100.00%	-100.00%
	0 vs 380,440	0.00% vs 55.68%	0 vs 211,810	0.00 vs 2.54	00:00:00 vs 00:01:48	0.00% vs 64.19%
9. Other Advertising	-100.00%	-100.00%	-100.00%	-100.00%	-100.00%	-100.00%
	0 vs 392,710	0.00% vs 35.34%	0 vs 138,797	0.00 vs 2.55	00:00:00 vs 00:02:07	0.00% vs 55.42%

## Top 10 Pages

Page ?	Pageviews ? ↓	Unique Pageviews ?	Avg. Time on Page ?	Entrances ?	Bounce Rate ?	% Exit ?
	<b>21,639,824</b> % of Total: 100.00% (21,639,824)	<b>18,235,779</b> % of Total: 100.00% (18,235,779)	<b>00:02:35</b> Avg for View: 00:02:35 (0.00%)	<b>10,868,782</b> % of Total: 100.00% (10,868,782)	<b>67.00%</b> Avg for View: 67.00% (0.00%)	<b>50.23%</b> Avg for View: 50.23% (0.00%)
1. /index.php/Main_Page	<b>1,538,209</b> (7.11%)	<b>1,179,256</b> (6.47%)	00:01:40	<b>935,643</b> (8.61%)	50.39%	42.19%
2. /index.php/Category:OWASP_Top_Ten_Project	<b>585,067</b> (2.70%)	<b>470,707</b> (2.58%)	00:01:33	<b>273,447</b> (2.52%)	45.39%	36.62%
3. /index.php/XSS_Filter_Evasion_Cheat_Sheet	<b>501,445</b> (2.32%)	<b>458,805</b> (2.52%)	00:02:28	<b>388,196</b> (3.57%)	45.98%	48.51%
4. /index.php/Top_10_2013-Top_10	<b>444,057</b> (2.05%)	<b>337,890</b> (1.85%)	00:02:14	<b>225,683</b> (2.08%)	53.98%	43.54%
5. /index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet	<b>416,540</b> (1.92%)	<b>357,197</b> (1.96%)	00:04:35	<b>225,973</b> (2.08%)	69.65%	60.05%
6. /index.php/OWASP_Zed_Attack_Proxy_Project	<b>402,929</b> (1.86%)	<b>328,031</b> (1.80%)	00:04:19	<b>250,867</b> (2.31%)	76.22%	68.68%
7. /index.php/Cross-site_Scripting_(XSS)	<b>361,003</b> (1.67%)	<b>318,785</b> (1.75%)	00:03:22	<b>232,930</b> (2.14%)	60.46%	53.34%
8. /index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet	<b>277,918</b> (1.28%)	<b>250,430</b> (1.37%)	00:04:58	<b>197,558</b> (1.82%)	77.35%	71.38%
9. /index.php/SQL_Injection_Prevention_Cheat_Sheet	<b>238,172</b> (1.10%)	<b>217,101</b> (1.19%)	00:04:29	<b>153,101</b> (1.41%)	78.20%	67.58%
10. /index.php/Testing_for_SQL_Injection_(OTG-IN-PVAL-005)	<b>227,944</b> (1.05%)	<b>210,457</b> (1.15%)	00:05:21	<b>163,574</b> (1.50%)	81.77%	75.79%

## Logins (1 Year)

Page ?	Pageviews ? ↓	Unique Pageviews ?	Avg. Time on Page ?	Entrances ?	Bounce Rate ?	% Exit ?
<b>New Users</b>	<b>17,797</b> % of Total: 0.08% (21,653,028)	<b>13,932</b> % of Total: 0.08% (18,283,968)	<b>00:00:42</b> Avg for View: 00:02:34 (-72.88%)	<b>3,178</b> % of Total: 0.03% (10,868,789)	<b>44.48%</b> Avg for View: 66.75% (-33.37%)	<b>19.14%</b> Avg for View: 50.20% (-61.87%)
<b>Returning Users</b>	<b>12,886</b> % of Total: 0.06% (21,653,028)	<b>10,677</b> % of Total: 0.06% (18,283,968)	<b>00:00:46</b> Avg for View: 00:02:34 (-70.28%)	<b>963</b> % of Total: 0.01% (10,868,789)	<b>13.71%</b> Avg for View: 66.75% (-79.47%)	<b>9.87%</b> Avg for View: 50.20% (-80.33%)

## Signups (1 Year)

Page ?	Pageviews ? ↓	Unique Pageviews ?	Avg. Time on Page ?	Entrances ?	Bounce Rate ?	% Exit ?
<b>New Users</b>	<b>18,595</b> % of Total: 0.09% (21,653,028)	<b>11,418</b> % of Total: 0.06% (18,283,968)	<b>00:01:27</b> Avg for View: 00:02:34 (-43.96%)	<b>1,786</b> % of Total: 0.02% (10,868,789)	<b>80.46%</b> Avg for View: 66.75% (20.53%)	<b>36.07%</b> Avg for View: 50.20% (-28.14%)
<b>Returning Users</b>	<b>12,112</b> % of Total: 0.06% (21,653,028)	<b>6,372</b> % of Total: 0.03% (18,283,968)	<b>00:01:56</b> Avg for View: 00:02:34 (-24.88%)	<b>1,395</b> % of Total: 0.01% (10,868,789)	<b>46.88%</b> Avg for View: 66.75% (-29.77%)	<b>19.81%</b> Avg for View: 50.20% (-60.54%)

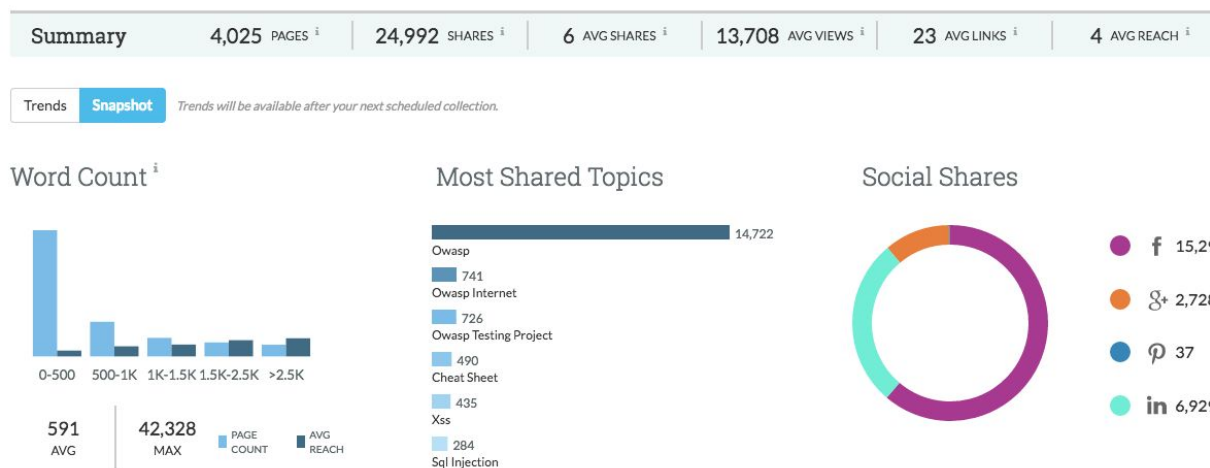
**Key Takeaway:** There is not a lot of difference for user behavior between new and returning visitors except for the duration of visits to the OWASP website and total number of pages viewed. This is expected as returning users are more familiar with the OWASP website and know where to look for certain pieces of information. There is also no tangible benefit in signing up for an account unless the user is intended on contributing to the OWASP Wiki.

## Moz Content Audit

In addition to Google Analytics, we conducted a content audit with using Moz Content<sup>9</sup> which crawled 4,025 pages overall - Moz Content is also connected to the OWASP Google Analytics account for more accurate results. The following is the dashboard showing the results of the crawl:

www.owasp.org

Discovery Complete!



Of the crawled pages, the average word count is 591; the maximum count of words is detected to be around 42,000 words. The page with the most word count is [OWASP Fuzzing Code Database](#) as this page includes a lot of links, file extensions, etc. under statements.

The most shared topic is the OWASP main page. In regards to social shares, Facebook appears to have the highest impact. The average page views per crawled topic are 13,708 views with an average share count of 6.

The following are the top 20 OWASP content based on the content audit via Moz Content:  
**Top 20 OWASP Content Overall** (based on most unique page views)

Overall OWASP Traffic						
Title	Bounce Rate	Unique Views	Page	Organic Bounce Rate	Organic Page Views	Unique
OWASP	50	2132804		45	1366582	
Category:OWASP Top Ten Project - OWASP	46	832663		39	597440	
Top 10 2013-Top 10 - OWASP	53	652392		48	486482	
Cross-site Scripting (XSS) - OWASP	59	585090		58	489546	

<sup>9</sup> Moz Content Audit - <https://moz.com/content/>

OWASP Zed Attack Proxy Project - OWASP	76	579202	75	401086
SQL Injection - OWASP	66	339958	65	257338
Category:OWASP Download - OWASP	50	296159	45	197503
About The Open Web Application Security Project - OWASP	54	259827	51	173856
Category:OWASP Top Ten Project - OWASP	60	239723	57	171846
Clickjacking Defense Cheat Sheet - OWASP	76	222251	74	172468
Top 10 2013-A1-Injection - OWASP	56	205976	44	134461
Category:OWASP WebGoat Project - OWASP	55	205784	48	134653
XML External Entity (XXE) Processing - OWASP	78	201045	76	148439
Category:Code Snippet - OWASP	35	198891	21	26327
Session Management Cheat Sheet - OWASP	78	198508	76	150976
Category:Attack - OWASP	50	193195	31	123547
Testing for Cross site scripting - OWASP	62	188265	61	178883
Web Application Firewall - OWASP	76	182138	76	162320
Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001) - OWASP	85	159065	85	150832
Certificate and Public Key Pinning - OWASP	82	158443	81	117612

### Top 20 OWASP Content Overall (based on social share)

Title	Url	Shares
OWASP	<a href="https://www.owasp.org/index.php/Main_Page">https://www.owasp.org/index.php/Main_Page</a>	2102
OWASP	<a href="https://www.owasp.org/">https://www.owasp.org/</a>	2096
OWASP	<a href="http://www.owasp.org">http://www.owasp.org</a>	2093
Category:OWASP Top Ten Project - OWASP	<a href="https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project">https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project</a>	1065
Category:OWASP Top Ten Project - OWASP	<a href="https://www.owasp.org/index.php/Top10">https://www.owasp.org/index.php/Top10</a>	1065

Category:OWASP Top Ten Project - OWASP	<a href="https://www.owasp.org/index.php/OWASP_Top_Ten_Project">https://www.owasp.org/index.php/OWASP_Top_Ten_Project</a>	885
Category:OWASP Top Ten Project - OWASP	<a href="https://www.owasp.org/index.php/OWASP_Top_10">https://www.owasp.org/index.php/OWASP_Top_10</a>	883
Category:OWASP Top Ten Project - OWASP	<a href="https://www.owasp.org/index.php/OWASP_Top_Ten">https://www.owasp.org/index.php/OWASP_Top_Ten</a>	729
Top 10 2013-Top 10 - OWASP	<a href="https://www.owasp.org/index.php/Top_10_2013-Top_10">https://www.owasp.org/index.php/Top_10_2013-Top_10</a>	695
OWASP Zed Attack Proxy Project - OWASP	<a href="https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project">https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project</a>	513
OWASP Internet of Things Project - OWASP	<a href="https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project">https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project</a>	384
OWASP Testing Project - OWASP	<a href="https://www.owasp.org/index.php/Category:OWASP_Testing_Project">https://www.owasp.org/index.php/Category:OWASP_Testing_Project</a>	362
OWASP Testing Project - OWASP	<a href="https://www.owasp.org/index.php/OWASP_Testing_Project">https://www.owasp.org/index.php/OWASP_Testing_Project</a>	362
OWASP Internet of Things Project - OWASP	<a href="https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project">https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project</a>	357
OWASP Mobile Security Project - OWASP	<a href="https://www.owasp.org/index.php/OWASP_Mobile_Security_Project">https://www.owasp.org/index.php/OWASP_Mobile_Security_Project</a>	273
OWASP Xenotix XSS Exploit Framework - OWASP	<a href="https://www.owasp.org/index.php/OWASP_Xenotix_XSS_Exploit_Framework">https://www.owasp.org/index.php/OWASP_Xenotix_XSS_Exploit_Framework</a>	271
Ireland-Dublin - OWASP	<a href="https://www.owasp.org/index.php/Ireland-Dublin">https://www.owasp.org/index.php/Ireland-Dublin</a>	252
OWASP Cheat Sheet Series - OWASP	<a href="https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series">https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series</a>	243
OWASP Cheat Sheet Series - OWASP	<a href="https://www.owasp.org/index.php/Cheat_Sheets">https://www.owasp.org/index.php/Cheat_Sheets</a>	243
Category:OWASP Application Security Verification Standard Project - OWASP	<a href="https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project">https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project</a>	240

**Key takeaway:** Though one of the initial intentions was to have Moz Content classify content type, it appears that there is still additional work that needs to be done to obtain more accurate results in content classification on the Moz platform. However, the content audit and crawl back up the data and conclusions we have drawn in Google Analytics.

## Information Architecture

For information architecture, we are examining how content on the OWASP website is being organized versus how users are attempting to access and find relevant content to them. In this, the top elements to examine are the current site map, content strategy, and navigation in relation to the industry's best practices. Information architecture appears to be one of the top issues of the OWASP website as users are having issues locating relevant information to them in a timely manner. Consequently, users are not as engaged with the OWASP website compared to that of other competitor sites, which is indicated by the website's high bounce rate. The following are 10 key Information Architecture best practices summarized - pitfalls to avoid based on the Nielsen Norman Group<sup>10</sup> that we kept in mind when conduct the IA evaluation.

### 10 Key Information Architecture Best Practices - Pitfalls to Avoid

1. **No structure** - When designers treat a site like “one big swamp” with no organizing principle for individual items. This creates no opportunities for the user to understand the site's offerings or help in locating related items
2. **Search and structure not integrated** - Search and navigation fail to support each other on many sites. Navigation designs need to indicate the user's current location within the site - after a user clicks a search results, they should be able to determine where they are in the site.
3. **Missing Category Landing Pages** - Categories should link to their own landing pages that gives users a section overview. When no page is clearly identified as a sub-topic page, users can misunderstand the site's scope and miss important details.
4. **Extreme Polyhierarchy** - Instead of spending time to develop intuitive top-level categories, teams may sometimes end up creating numerous weak categories which negatively impact usability as users agonize over top-level categories.
5. **Subsites/Microsites poorly integrated with main site** - Dedicated microsite may be a good idea for a product launch. However, it can undermine your online strategy and dilute your presence over time.
6. **Invisible Navigation Options** - The worst mistake is to have no navigation or one that users can not see. It is important to make the navigation permanently visible on all pages. Avoid “banner blindness bleed”, i.e. adding additional navigation into a banner.
7. **Uncontrollable Navigation Elements** - Navigation should remain static and fixed on a certain location on all pages and should not move around as this would cause user frustration.
8. **Made-up Menu Options** - Made up navigation terms hurt search, and users cannot find something if they don't know what it's called. Sites should not make up their own terminology for labels and other navigation choices.
9. **Inconsistent Navigation Elements** - Sites should not change their navigation features as users move through the site. This causes user confusion/frustration.

---

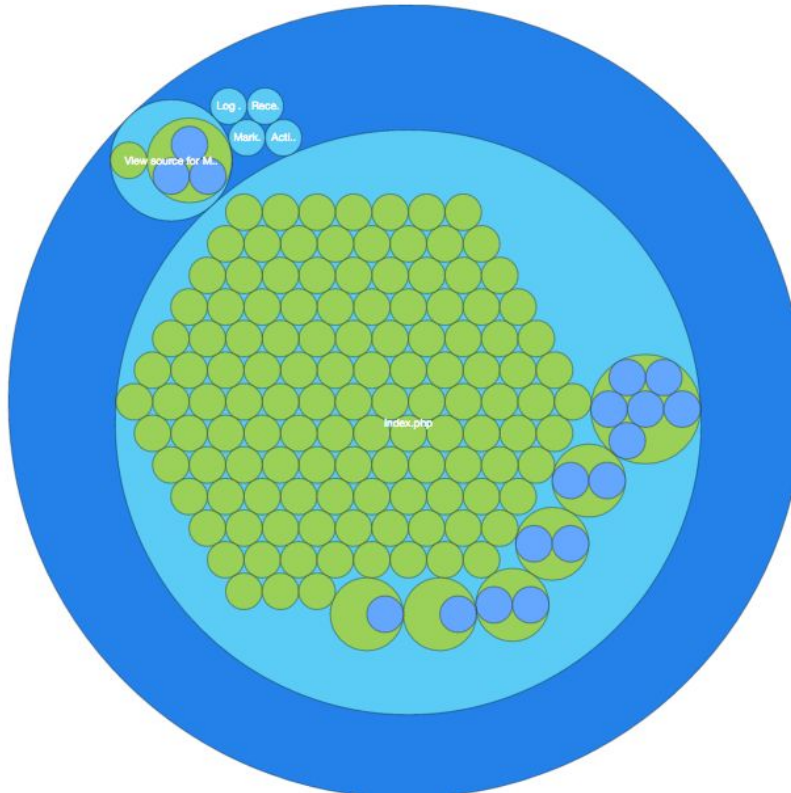
<sup>10</sup> Top 10 information architecture mistakes:

<https://www.nngroup.com/articles/top-10-ia-mistakes/>

10. **Too many navigation techniques** - There are numerous techniques to enhance website navigation, but using them all does not yield the sum of each technique's benefits.

### Generated Sitemap

The following is a generated sitemap of the OWASP website created via Dynamapper.



Instead of showing the site in a traditional sitemap diagram format, we opted to display it in Dynamapper's circle view for better readability. The above teal colored circle that encompasses `index.php` with a high number of accompany green circles demonstrates that the main site is a loose collection of links rather than clear hierarchical groupings of links and categories. This not only confuses the users, but also discourages users from exploring the site as they are confronted with too many choices to know where to start in exploring the OWASP website.

### Navigation

In terms of navigation, since there was no prior informed information architecture based on user behavior, the left-side panel navigation requires some consolidation. The navigation breaks the pattern of five to seven top level categories that are common across websites. A mega-menu is required here in order to further improve usability in helping users locate relevant information more quickly and encouraging them to explore the site further.



### **Content Strategy**

Although there appears to be some hierarchy and grouping in content, there needs to be a stronger content management strategy in place on the OWASP website. An example would be the current project inventory page<sup>11</sup>. There is no filtering mechanism for people to distinguish between code base versus documentation projects or sort through projects based on programming language. There is no content curation and appropriate groupings and cues to help users find what they are looking for.

Currently, there appears to be no strategy in place and the process is unregulated as signed up users can freely create and edit content. Although this can arguably be depicted as desirable and beneficial as it can help drive contribution, there needs to be some additional rules and curation policies in place to prevent the creation of redundant pages with potentially conflicting information.

---

<sup>11</sup> OWASP Project Inventory:  
[https://www.owasp.org/index.php/Category:OWASP\\_Project#tab=Project\\_Inventory](https://www.owasp.org/index.php/Category:OWASP_Project#tab=Project_Inventory)

## Design Evaluation

For the design evaluation, the following is the top 10 best practices we kept in mind when evaluating the OWASP website.

### 10 Key Web/UI Design Best Practices

- 1. Remembering UX (User Experience)** - User Interface design must keep in mind the user and their experience while using any website or app. How easy text is to read, the amount of clicks one must take to navigate the site, micro interactions that convey necessary feedback to the user, and more are key components to consider when designing the interface and structure of a website.
- 2. Know Your Audience/Market** - Additionally before designing, it is important to know your site's target audience as to maintain the correct purpose and "personality" of your site. Knowing *who* to design for will aid in determining *what* to design.
- 3. Responsive & Mobile-First** - A must in modern web/UI design is developing a site that responsive and mobile friendly. Design your site to be optimized in desktop, tablet, and mobile phone layouts, making sure type, images, icons, and more look and work optimally on all platforms.
- 4. Use a Grid System** - Using a grid system is vital tool to designing layouts with logical structure and positioning. Types of grids can involve the 12-column vertical grid system or the use of a font size and line height to measure spacing. With a grid in place, content can be positioned with purpose and consistency instead of seeming random and blindly-chosen.
- 5. Keep It Simple and Consistent** - "Less is More." Keep the design clean while purposeful. Show what *has* to be shown, not everything all at once. For example, create a main top navigation of no more than 7-8 links, and use drop down lists/compartments to house sublinks, maintaining a simple and clean main navigation throughout the site.
- 6. Develop a Visual Hierarchy** - A visual hierarchy conveys levels of importance with respect to type and visuals. For instance, a user who sees a line of large text and a body of smaller text can easily determine by hierarchy the larger line is the headline, with descriptive body copy underneath. Differences in color hue and contrast aid in conveying visual hierarchy as well, such as a solid bright button immediately grabbing the eyes attention over surround content, highlighting the button's importance.
- 7. Develop a Color Scheme** - Simplify colors around between 4-6 main colors, keeping in mind color theory, such as complimentary colors, hue and brightness, and contrast. Remember color psychology as well, such as red conveying alertness and action, while blue conveying trust and tranquility. Color contrast could be used to further convey visual hierarchy as well.
- 8. Keep Typography Simple** - Keep fonts under control. Use no more than 3 separate font families, while utilizing different font weights strategically. Simply using the same font with different font sizes can go a long way in conveying visual and information hierarchy. For example, an H1 headline could be Proxima Nova at 64px size, with the body copying being 32 px sizing. The change in size is enough to convey the difference between a header and body copy text while using one font family.
- 9. Create a Style Guide** - An easy way to maintain consistency and simplicity is referencing a site-wide style guide. This should include chosen fonts, colors, form styles, button styles, and even spacing measurements.
- 10. Keep an Eye on Design Trends** - When in doubt, look into contemporary UI/web design trends to find a reference point to anchor design choices. Seeing what other sites are using for design patterns is a useful comparison tool to see where your site stands. Trends should *not* be used as

the end-all to design, but merely a starting point to keeping a site design familiar enough to navigate and use with ease.

### **OWASP Site Design Assessment**

The following are the 3 areas that were assessed for the OWASP website.

1. Home / Landing Page
2. Navigation
3. Project / Content Page

### **Home Page Evaluation**

In assessing the OWASP's current website, the first aspect to examine is the home/landing page. For a new user to the OWASP website, a Wikipedia aesthetic and layout, as opposed to a traditional website home page layout, could mislead the user in questioning whether this page is a wiki for OWASP or in fact, the OWASP organization site. In the side by side comparison in Figure 1, looking at a competing site (ISC)<sup>2</sup>, a user finds a traditional home page layout with a clear header space, navigation bar and links, hero section and home body content. Compared with the OWASP website, the (ISC)<sup>2</sup> home/landing page is less cluttered and provides a friendlier user experience. We recommend redesigning the home/landing page to conform to a traditional and modern layout. The new page would include the following:

1. A clear header space with company logo and login and signup links and main global navigation space with top level links and a site search form. A well-defined global top navigation would help clarify which pages would be the site's main pages within the site structure.
2. A clear hero area with hero image and welcome message to OWASP. Opportunity for hero slider to display latest news and articles from OWASP.
3. Clearly defined home body content sections with condensed and concise information and text as to not overload the homepage with content. This could be achieved by blocking content into relevant sections, whether it be full width sections, or a mixture of large main blocks with secondary side panels on the left or right of the page.
4. A clearly defined footer with footer navigation links and a copyright message.

# Figure 1 - Home Page Comparison

## Current OWASP Homepage owasp.org

The screenshot shows the current OWASP homepage. It features a top navigation bar with a search box and a 'Log In / Request account' link. Below this is a large 'Welcome to OWASP' banner with a grid of links to various resources like ZAP, OWASP, and OWASP. The main content area is divided into several columns. On the left, there's a sidebar with a 'Home' button and a list of navigation links including 'About OWASP', 'Acknowledgments', 'Applicable Events', 'Books', 'Board Resources', 'Chapters', 'Donate to OWASP', 'Downloads', 'Events', 'Governance', 'Initiatives', 'Mailing Lists', 'Membership', 'Newsletters', 'Open Source', 'Partnerships', 'Press', 'Projects', 'Videos', 'Webinars', and 'Tools'. The main content area includes sections for 'Who Trusts OWASP', 'How OWASP help you?', 'Security 101', 'Security Conferences, Training', 'How to Start an OWASP Project', 'OWASP News', 'Social Media', 'OWASP Blog', 'Security Podcast', 'OWASP Chapters', 'OWASP Moderated Apple News Feed', and 'Global OWASP Events'. The footer contains a copyright notice and a list of sponsors including Cisco, IBM, and Rackspace.

## Competition Homepage - (ISC)<sup>2</sup> isc2.org

The screenshot shows the (ISC)<sup>2</sup> homepage. It has a clean, professional layout. At the top, there's a navigation bar with links for 'Home', 'Credentials', 'Associates of (ISC)<sup>2</sup>', 'Training', 'Events', 'Special Programs', 'Members Only', and 'About'. A prominent banner at the top right says 'REGISTER for Training & Exams'. Below the banner is a grid of featured articles and news items, including 'Women are a driving force in the evolution of security', 'First Ever SSCP Training Offered Using Cyber Range Format in Singapore', and 'Cybersecurity's Next Big Challenges: Mobile Devices and Wearables'. The main content area is organized into sections like '(ISC)<sup>2</sup> Blog', 'Latest Industry News', and 'Press Releases'. The footer includes a copyright notice and social media icons for Facebook, Twitter, LinkedIn, and YouTube.

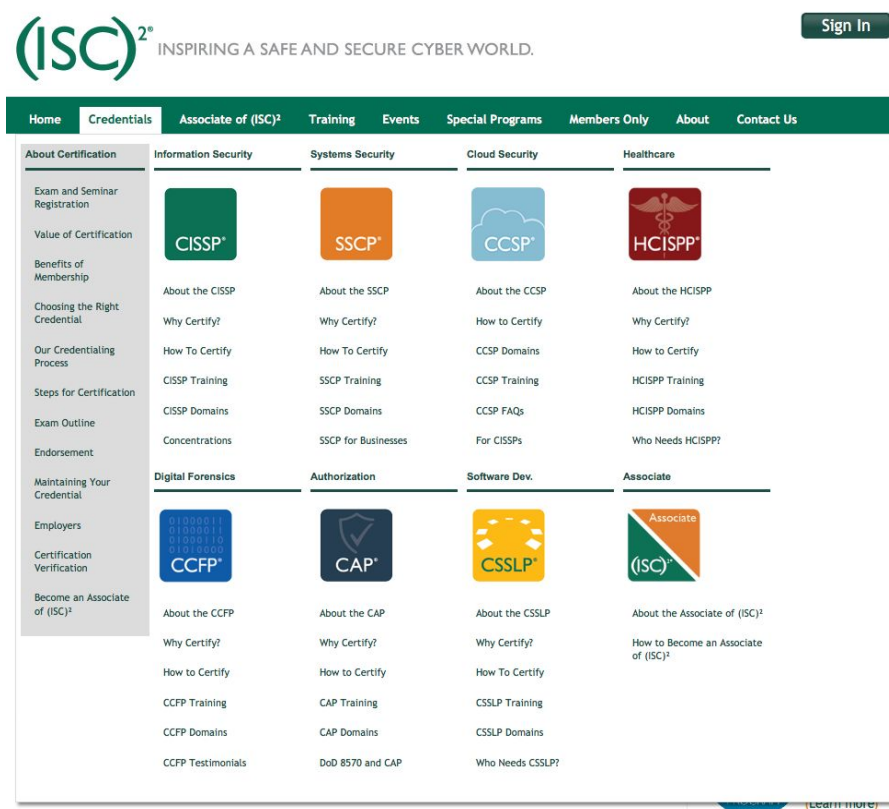
## Navigation

In comparison to the other site's navigation and link structures, OWASP's main site navigation requires further simplification and consolidation. OWASP has outgrown the traditional wikipedia navigation. Without any button and navigation bar design, too many links are created in differing arrangements. For example, we draw attention to the top banner, which currently emphasizes OWASP top projects.

Looking at another example in Figure 2 drawn from (ISC)<sup>2</sup>, a clear horizontal navigation bar with clear top level links helps avoid overloading the homepage with links. Additionally, the hover states reveal drop down boxes with pages appropriately categorized into their respective groups, which clearly convey a comprehensible and logical content hierarchy to guide users to content they are looking for.

Reviewing OWASP's navigation structure and overall site structure, a clear global top navigation would help clean up the design and the UX when navigating the site. Using drop downs and relevant categories hidden under hover states can further maintain a clean, easy-to-navigate design for a site that has a multitude of pages and subpages.

Figure 2 - Top Level Navigation



### Project / Content Pages

OWASP content and project pages should be redesigned for a better user experience as well. While the page content is divided into respective blocks, there should be further improvement and consistency in the arrangement and hierarchy of content. As seen in line with a content page from (ISC)<sup>2</sup>, the main content and headlines should take up the majority of the page, while the minor content and links should be arranged in a side panel section taking up less than

one-third of the width of the page. Furthermore, depending on the amount of content and related sub-content, tabbed sections and accordion blocks may be used to help declutter the page. See Figure 3 for comparison.

Figure 3 - Content / Project Page

Current OWASP Project Page  
owasp.org

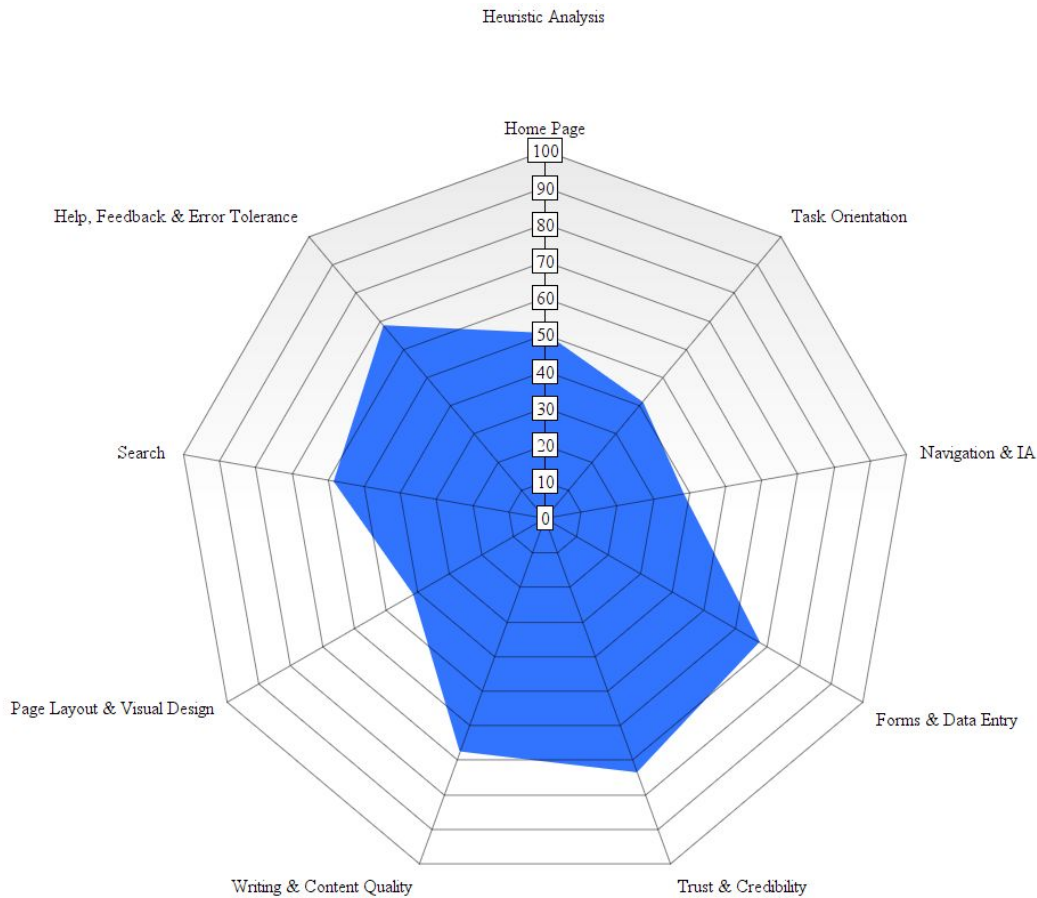
Competition Article Page - (ISC)<sup>2</sup>  
isc2.org

The screenshot shows the OWASP Project page. At the top, there's a navigation bar with 'Home', 'About OWASP', and 'Project Overview'. The main content area is titled 'Welcome to the OWASP Global Project Page' and includes a 'Who should start an OWASP Project?' section. Below this, there's a 'Subcategories' section listing various OWASP projects under letters A through S.

The screenshot shows the (ISC)² website. The main content area is titled 'CISSP® - Certified Information Systems Security Professional' and includes a 'Need More Information?' form with fields for 'First Name', 'Last Name', 'Email', and 'Phone'. The page also features a 'CISSP Exam Information' table and a 'Which CERT is right for you?' section.

### Heuristic Evaluation

In addition to the design evaluation, we conducted a heuristic evaluation to uncover additional usability problems in the UI. The following is the radar plot of the scores, overall scores and rationale behind the scoring.



Summary of Results				
	Raw score	# Questions	# Answers	Score
Home Page	0	20	20	50%
Task Orientation	-8	44	44	41%
Navigation & IA	-7	29	29	38%
Forms & Data Entry	8	23	23	67%
Trust & Credibility	6	13	13	73%
Writing & Content Quality	8	23	23	67%

Page Layout & Visual Design	-7	38	38	41%
Search	3	20	20	58%
Help, Feedback & Error Tolerance	13	37	37	68%
Overall score		247	247	56%

Results of Analysis	
Home Page	The OWASP homepage currently lacks a defined page structure or established design to match the brand and discourages user engagement. The page lacks distinctive features, such as a full width hero image/banner, call-to-action buttons, and introductory content, leading to a relevant content pages and/or user participation with the OWASP Foundation.
Task Orientation	The site's lack of design and structure leads to a confusing user experience - hampering the OWASP brand. Large blocks of text require the user to read through large paragraphs to learn information and direction across the site. Without a consistent top navigation or breadcrumb trail, navigating the confusing and requires backtracking to find one's place throughout the site.
Navigation & IA	Without a consistent top navigation or breadcrumb trail, navigating the confusing and requires backtracking to find one's place throughout the site.
Forms & Data Entry	A majority of forms appear to lead out of the OWASP website, there is some consistency in those forms however, this is bad for the user experience.
Trust & Credibility	The OWASP site needs a consistent site design to match the brand and clearly convey the organization's message.
Writing & Content Quality	The site is content heavy, with large blocks of text. However, the content quality in of itself is good.
Page Layout & Visual Design	The OWASP site lacks any defined and styled visual design, built currently on the WikiMedia platform. Pages lack any consistent layout pattern or grid system.



Search	Summary: Site search does not provide useful results in order of relevance and suggest appropriate results
Help, Feedback & Error Tolerance	Summary: Overall the website provides good help and feedback, however, it lacks a proper 404 page

### Peer Analysis

In the following section, we take a look at competitor and partner websites in the security space. The suggested sample set is the following:

1. Isc2.org
2. Sans.org
3. Issa.org
4. Isaca.org
5. Cloudsecurityalliance.org

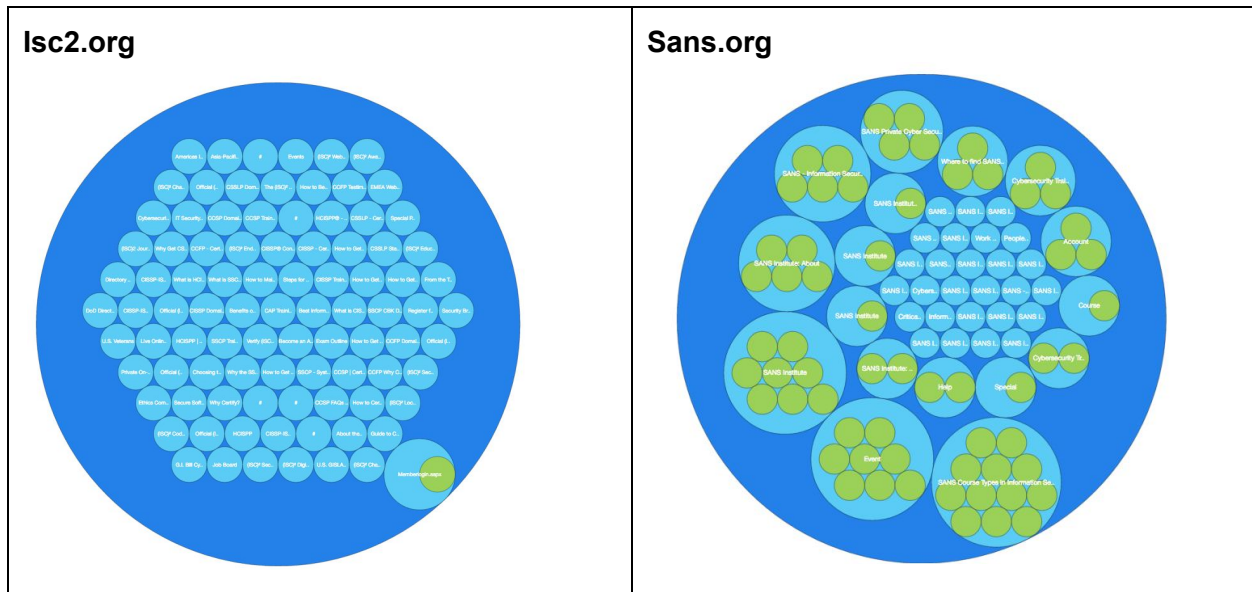
For the peer analysis, we examined each of the following areas:

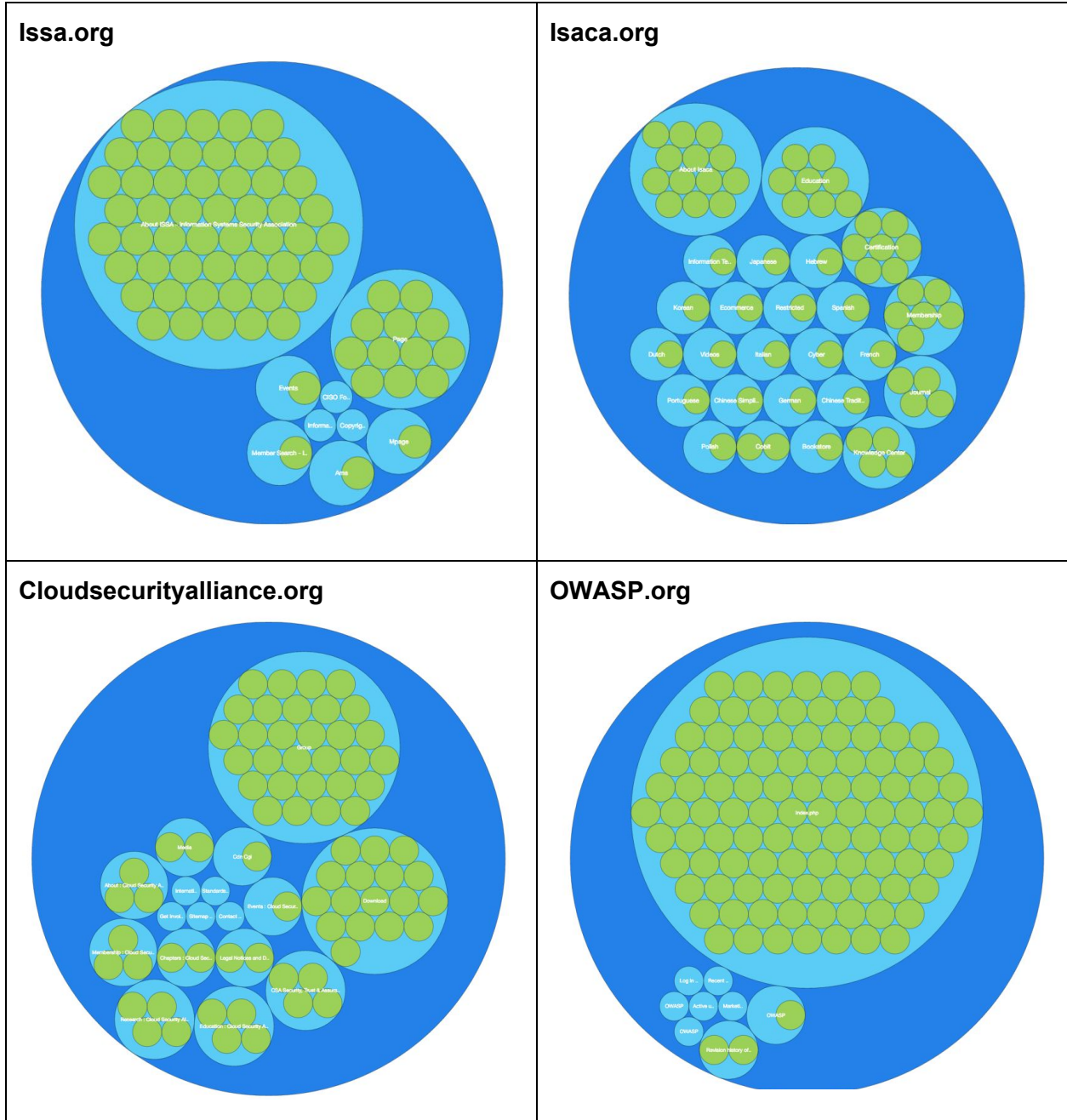
1. Design - Overall impression of the website in relation to best practices
2. Information Architecture - Organization of information and navigation
3. Platform - Underlying website infrastructure and application
4. Site Metrics - Traffic, engagement and demographics

### Information Architecture and Design

#### Generated Site Map Comparison

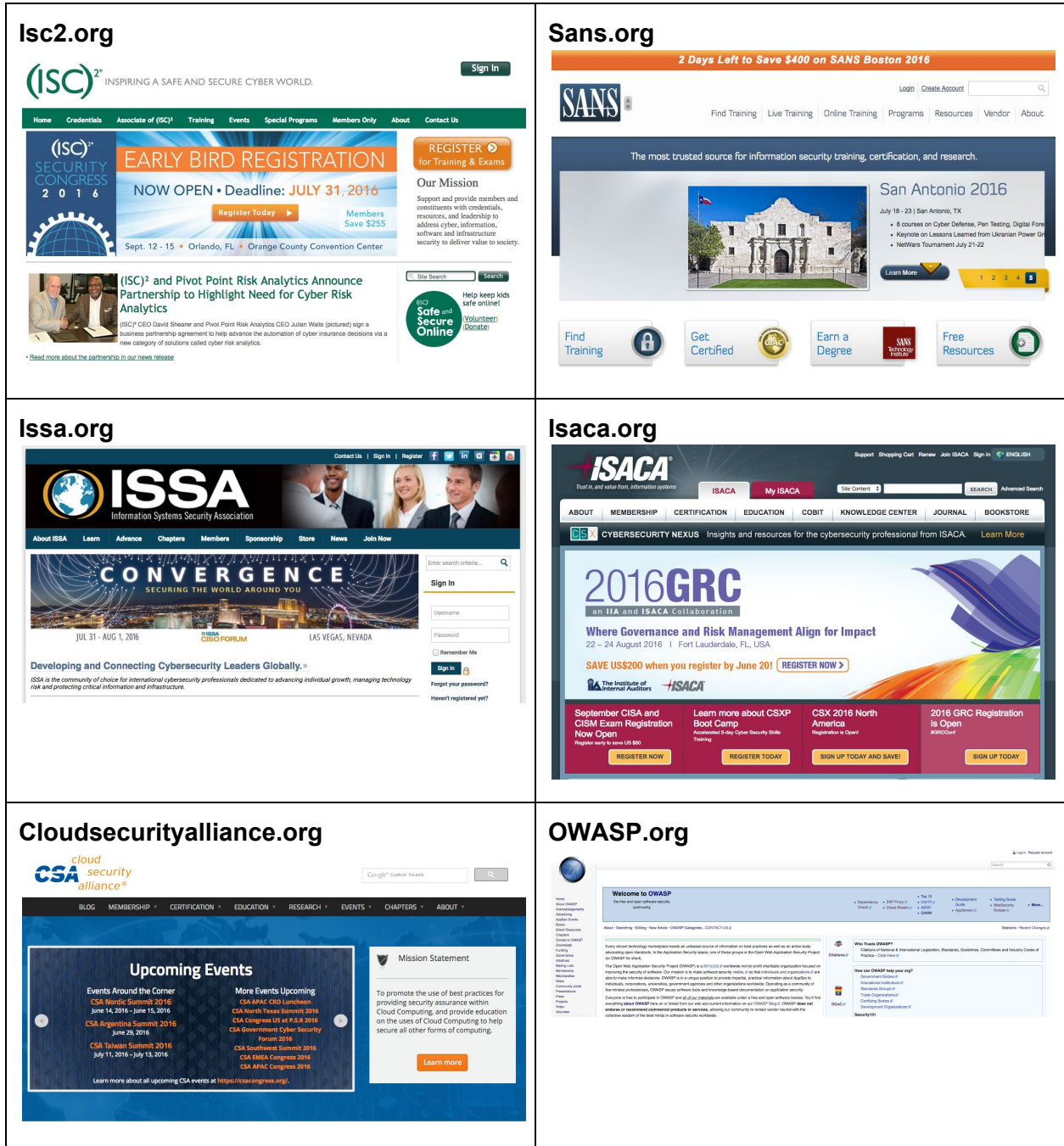
The following are site maps generated via Dynamapper per each site.





### Design and Navigation Comparison:

The following are screenshots of each competitor homepage and navigation.



### Key takeaway:

Based on the sitemaps generated by Dynamapper, OWASP is the only site where the navigation is cluttered and links are overloaded on the home page. A side-by-side comparison of the home pages and navigation also reveals that OWASP does not have a modern-looking site compared with its competitors/partners. OWASP may seem more like the go-to for security

information. However, this does not necessarily translate as an organization for first time visitors.

## Platform

The following are the platform comparison per each competitor.

	<a href="http://owasp.org">owasp.org</a>	<a href="http://sans.org">sans.org</a>	<a href="http://issa.org">issa.org</a>	<a href="http://isaca.org">isaca.org</a>	<a href="http://cloudsecurityalliance.org">cloudsecurityalliance.org</a>	<a href="http://isc2.org">isc2.org</a>
Web Server	Apache	Apache, Nginx	Apache	IIS	Nginx	IIS
CMS (if listed)	MediaWiki		Yourmembership	Sharepoint 2007	Wordpress	Ektron (Ecommerce)
Hosting Provider	Rackspace	Dedicated Hosting	Time Warner	Edgecast Networks Hosting	Cloudflare Hosting	CenturyLink

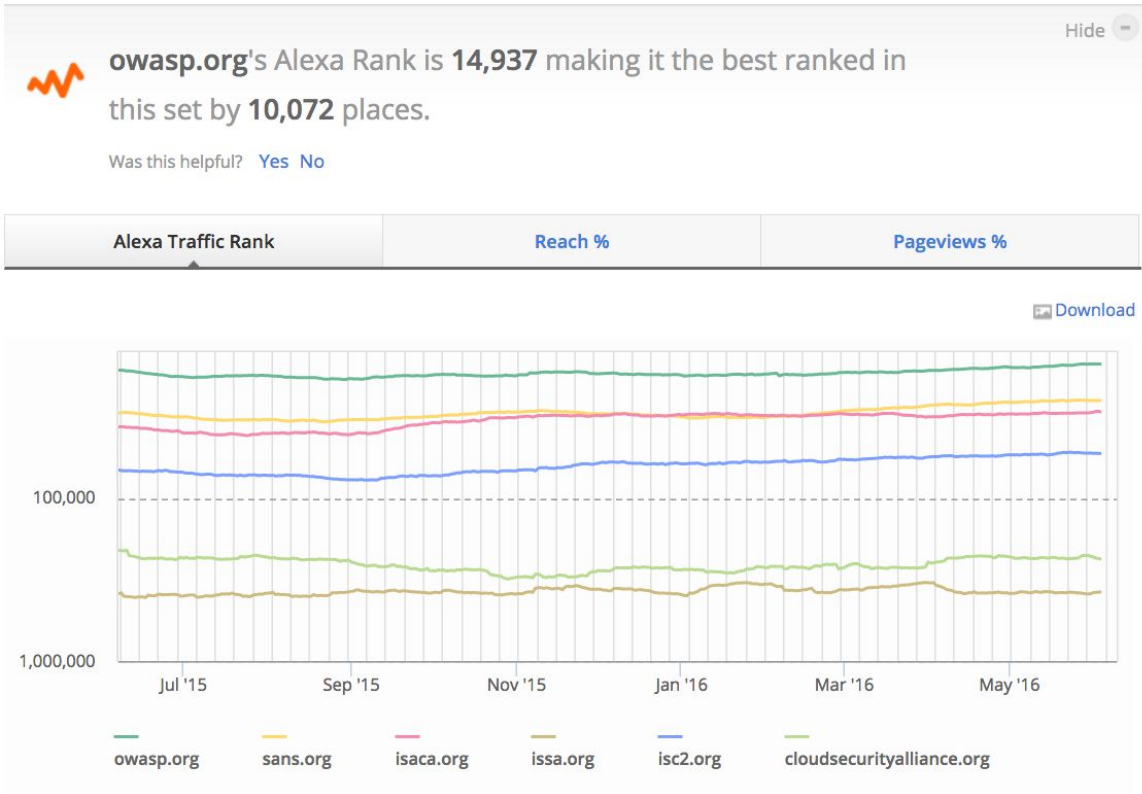
**Key takeaway:** With the exception of SANS, all competitors have some form of CMS. However, their use case differs from OWASP greatly in that all security documentation, projects and best practices of OWASP are open to the public in the form of a wiki.

## Site Metrics


For site metrics comparison, we used Alexa<sup>12</sup> to compare the historical traffic trends, traffic metrics, monthly unique visitors, engagement metrics, traffic sources, reputation metrics and demographics. Please note that the following metrics are estimates based on Alexa.

<sup>12</sup> Alexa Digital Marketing Tools- <http://www.alexa.com/>


### Historical Traffic Trends and Traffic Metrics



Traffic Metrics      Rank in Country:       [Export CSV](#)      ?

 **sans.org's** Alexa Rank in the United States is **9,710** making it the best ranked in this set by **5,039** places.

Was this helpful? [Yes](#) [No](#)

Hide 

Site	Global Rank	Rank in Country (US)	Global Reach %	Global Pageviews %
owasp.org	14,937 ▲1,910	14,749	0.00878% ▲4.00%	0.00024% ▲3.00%
sans.org	25,009 ▲3,692	9,710	0.0048% ▲2.00%	0.000163% ▲14.00%
isaca.org	29,473 ▲1,070	18,487	0.00355% ▼0.44%	0.000186% ▼15.97%
issa.org	376,836 ▼15,042	91,168	0.000207% ▼11.13%	0.0000082% ▼24.46%
isc2.org	52,741 ▲5,053	19,408	0.00188% ▲3.00%	0.0000991% ▼1.57%
cloudsecurityalliance.org	236,561 ▲16,853	90,169	0.0004% ▼5.54%	0.0000119% ▲4.00%
otalliance.org	708,605	295,589	0.000114%	0.0000026%

**Key takeaway:** Within the sample list of competitors and partners, OWASP has the highest Alexa ranking, reach percentage and pageview percentage, and global traffic ranking.

### Monthly Unique Visitors



**Key takeaway:** Within the sample list of competitors/partners, OWASP has the second highest estimated unique visitors.

## Engagement Metrics

Engagement Metrics

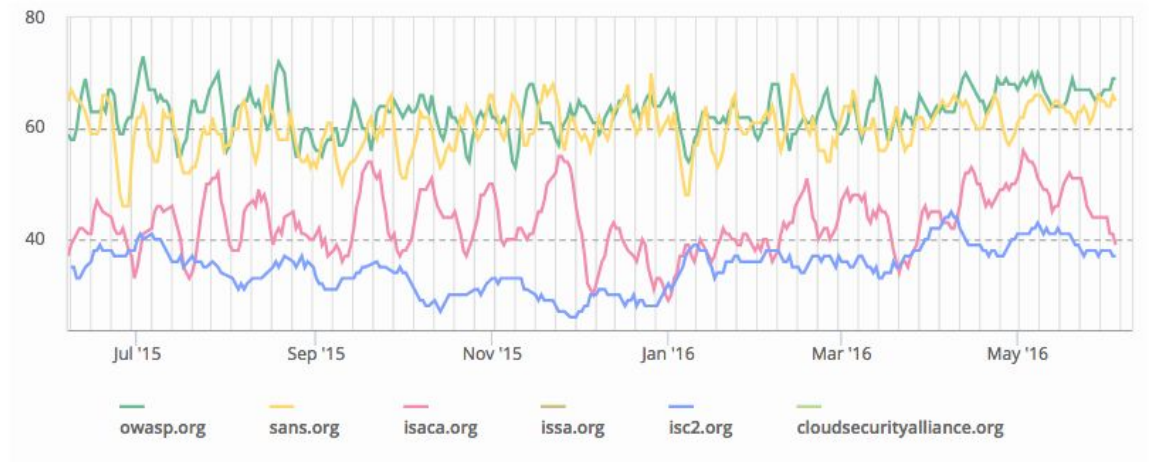
Date Range: 1 year

Export CSV



Pageviews/User
Bounce %
Time on Site

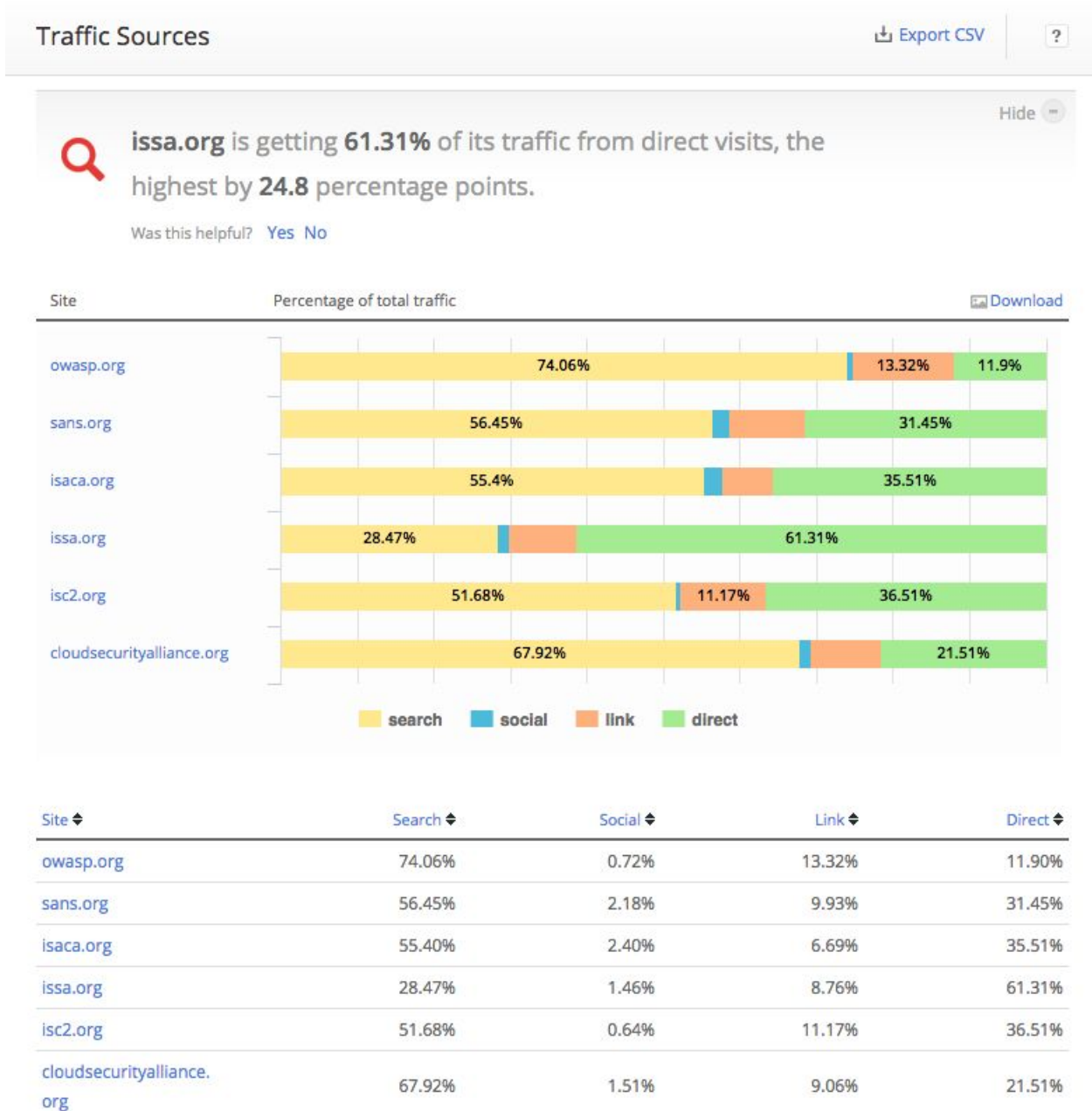
Download



Site	Pageviews/User	Bounce Rate	Time on Site (minutes)
owasp.org	1.87 ▼ 1.58%	65.80% ▲ 6.00%	2:21 ▼ 1.00%
sans.org	2.32 ▲ 12.00%	61.80% ▲ 5.00%	3:01 ▲ 3.00%
isaca.org	3.59 ▼ 15.13%	46.40% ▲ 21.00%	3:54 ▼ 19.00%
issa.org	2.70 ▼ 15.14%	51.50% ▲ 17.00%	2:47 ▼ 32.00%
isc2.org	3.61 ▼ 4.75%	38.60% ▲ 11.00%	4:19 ▼ 6.00%
cloudsecurityalliance.org	2.00 ▲ 11.00%	57.90% ▲ 4.00%	2:24 ▼ 10.00%

**Key takeaway:** Within the sample list of competitors and partners, although OWASP may be highly ranked on the Alexa and global traffic ranking, it also has the highest bounce rate.

### Traffic Sources



**Key takeaway:** Within the sample list of competitors and partners, OWASP has the highest percentage of search traffic.





## Reputation Metrics



**Key takeaway:** Within the sample list of competitors/partners, although OWASP has the highest number of Facebook shares, it ranks in the bottom half in terms of Google+1's.

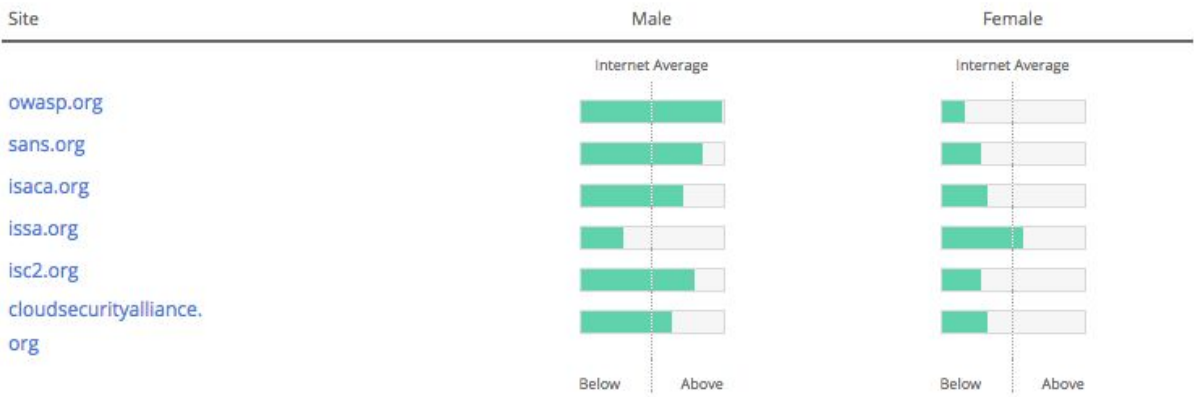
### Demographics

## Demographics ?

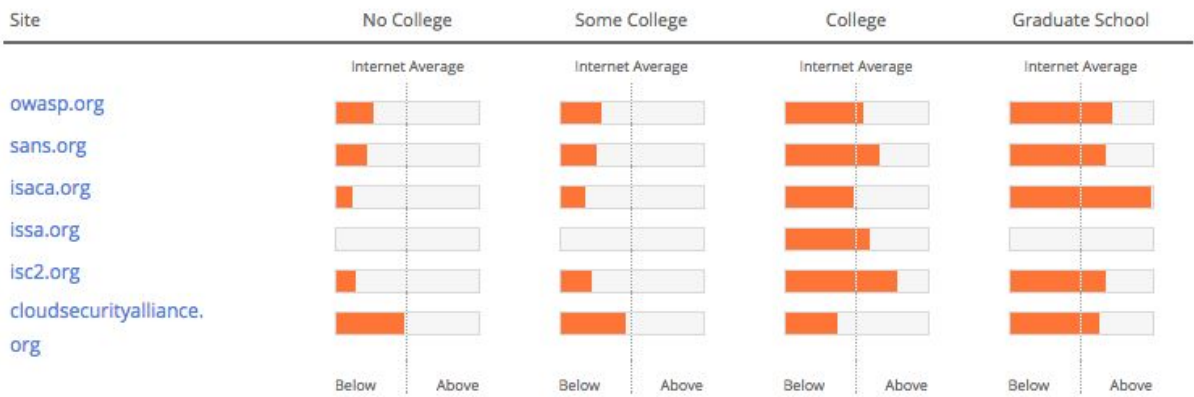
 **owasp.org's audience is the most disproportionately male.** Hide 

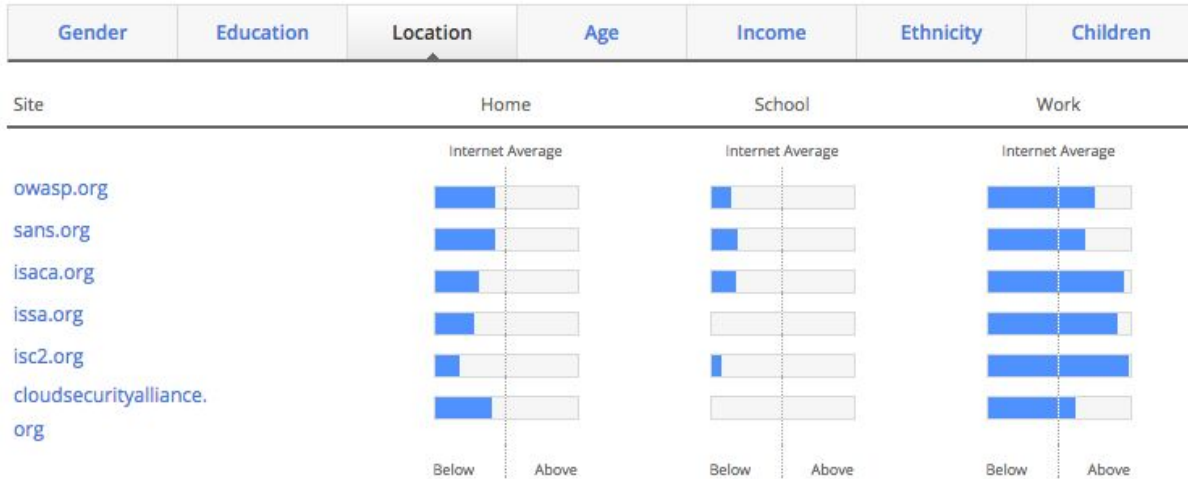
Was this helpful? [Yes](#) [No](#)

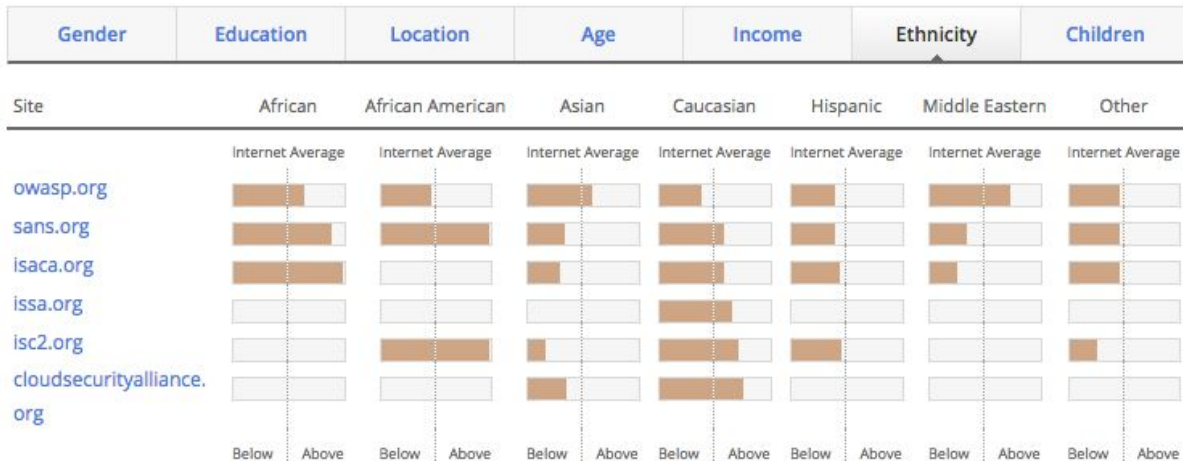
- Gender
- Education
- Location
- Age
- Income
- Ethnicity
- Children



- Gender
- Education
- Location
- Age
- Income
- Ethnicity
- Children







**Key takeaway:** The OWASP community is predominantly male; the majority of audience has a college degree; the majority access the site at work; the average age of users is between the range of 25 to 34 years old; and the average income of a typical user is between 30 to 60k.

### Summary of UX evaluation and site testing

The following are the strengths and weaknesses of the OWASP website based on the holistic evaluation of the site UI/UX and testing.

#### Strengths

1. High quality content and authority for application security.
2. Some site structure inherited from the MediaWiki format.
3. Active user base for content updates and generation.
4. High volume of users compared with competing sites.

#### Weaknesses

1. Outdated look inherited from MediaWiki
2. Lack of distinction between organization information and security content

3. Lack of information architecture, content strategy or content rules communicated to new users except on certain occasions like project page creation
4. Lack of strong top level categories for navigation, enhanced search and advanced filtering capabilities and call to action buttons
5. Lack of responsive design to accommodate for mobile use

## Back-office tools, project tools and infrastructure assessment

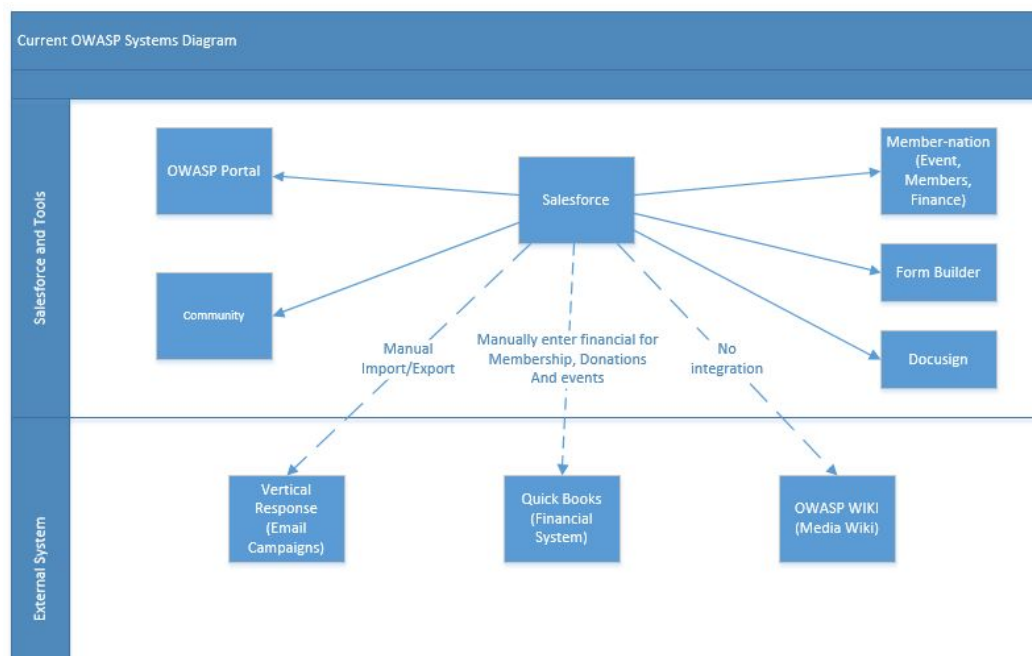
The following section is an evaluation of the OWASP back-office tools, project tools and infrastructure to determine if the current infrastructure fulfills the organization needs and growth plans.

### Salesforce CRM

OWASP has various systems and tools in place (Salesforce, Quickbooks, MediaWiki, Vertical Response, etc). However, there is a lack of integration between these tools which hampers efficiency, productivity and performance. In the interview with Kate Hartmann, who is the OWASP Operations Director, we identified several key challenges:

- 1) There is a permissions issue on what access level can be provided to chapter leaders to manage memberships, projects, demographics statistics, etc. This information does not flow into the current MediaWiki site as there are no integration in place to facilitate this.
- 2) Manual importing and exporting of data to/from Vertical Response.
- 3) Manual assignment of cases.
- 4) Lack of integration with Quickbooks.
- 5) Integration issues between event registration and portal.

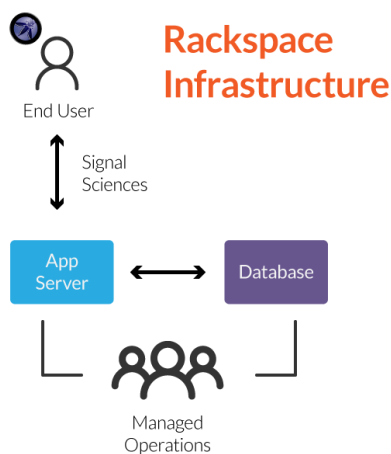
Below is the current OWASP system diagram from a Salesforce perspective:



There is a clear need to integrate all data source through one common platform for better management, productivity and efficiency.

## Rackspace Cloud Hosting and MediaWiki Application

The following section outlines the hosting solution and MediaWiki application currently in place for the OWASP website. The site is currently hosted on Rackspace as the company have donated \$2000 per month's worth of cloud infrastructure to the OWASP Foundation when



OWASP sought donations for cloud hosting for its projects previously. The current setup for the website infrastructure is outlined to the left and explained in detail below:

1) Signal Sciences is a recently added WAF to help filter out malicious traffic - this was added after our initial assessment interview with Matt Tesauro.

2) Application Server - The current MediaWiki currently resides in the application server with the following configurations:

- a) OS: Ubuntu 14.04
- b) Flavor: 8GB General Purpose
- c) Disk Space: 153.7 GB
- d) Region: Chicago
- e) Fail2ban Installed

- 3) Database Server - The MediaWiki database is on MariaDB in a separate server and has been tuned with mysql-tuner. The configurations are the same compared with the application server (Ubuntu 14.04, 8GB General Purpose, 153.7 GB Disk Space, Fail2ban, etc.).
- 4) The environment has a Rackspace managed operations sysops service subscription - meaning that Rackspace helps run the day-to-day operations (monitoring, OS maintenance and patching, application monitoring, etc.).
- 5) Files and database are backed up on a weekly and daily basis.
- 6) The following link contains the currently installed extensions:

<https://www.owasp.org/index.php/Special:Version>

The current issues with the following setup are the following:

- 1) There is no OWASP MediaWiki codebase. This means that upon server failure, a new snapshot and backup of the entire server need to be restored delaying recovery time. Additionally, extensions or any other add-ons are not kept track of and version upgrades can be a pain.
- 2) There is no load-balancer in place to create an elastic environment (i.e. scaling issues when needed for heavy traffic load).
- 3) Disaster recovery is dependent on Matt Tesauro's availability or Rackspace support (i.e. the application is not self healing or auto-scaling).

## Communication Tools

In the listed communication, social media, and discussion tools, the main issue revolves around access and visibility. Users require an account or OWASP email to access certain assets (ex.

Slack, shared documents, etc). Since communication is disproportionate across all communication mediums, some platforms may not have the same information as others and a standard platform should be selected.

Another concern is the Mailman tool - the current version is Mailman 2 and should be upgraded to Mailman 3 if mailing discussions are to be continued. However, this tool should be retired as it violates the OWASP transparency core value in that there may not be enough visibility around mailing lists for discussion; past discussions are not easily visible to newcomers; there is a lot of spam filtering needed to maintain the integrity of this service; and a lot of custom logic was written to facilitate the service, which leaves a lot of room for error. This can be resolved with a forum plugin on the MediaWiki platform.

### Project Tools and Workflow

There does not appear to be any major complaints in regard to project tooling during the conducted interviews. The major emphasize is on project visibility, status, maintenance, promotion, curation and defined workflow. A recent project that community members are working for is a dashboard with relevant project statistics for coding projects hosted on github. Similarly, Openhub presents this information as well.

A major concern identified from the interviews is a high segregation of project details and documentations. As the current process is ad hoc to an extent, users are not necessarily maintaining up to date information for their projects in the wiki which would result in user confusion and lower project visibility.

There is a clear need for project owners and the OWASP community to define a better workflow and centralized documentation process that is suitable for all and designate senior project leaders to guide new users and reach to the community and developers for volunteers and project visibility. In addition, standards for project promotion should be in place and a review board should be re-established.

### Summary of Results

The following is the summary of the strengths and weaknesses of the OWASP infrastructure:

#### Strengths

1. Functioning Salesforce platform that carries out key tasks to keep OWASP running smoothly.
2. Standardized practices and guidelines for project life cycle and tooling.

#### Weaknesses

1. No integration between all key tools into Salesforce for optimal efficiency.
2. No uniform distribution of content and communication across all platforms.
3. Lack of highly visible ticketing/bug tracking for all projects.
4. Need to remove all unused and unnecessary extensions from MediaWiki.



## Recommendations

Based on the results of the assessment, the key point of improvement that would yield the most benefit to the community is improving upon the OWASP MediaWiki site for better user experience; data centralization and transparency; increased member participation; and better organization, project, event and membership visibility. Other improvements to the back-office tools and processes will help the OWASP staff better serve the community in providing optimal efficiency and automation in their daily tasks.

### OWASP Website - Information Architecture, Platform Selection, Site Redesign and Functionality Enhancements

The OWASP website has the highest amount of traffic in comparison to other competitors and similar sites due to its wealth of security information, projects and tools. However, what hampers the experience is the information architecture and design and functionality of the site. As the site is a MediaWiki, it encourages users to use it as such - a Wikipedia for security. While this serves the purpose of knowledge sharing well, it does not help OWASP grow and encourage users to participate or join the organization.

To encourage more user interaction with the OWASP website and organization, there needs to be a new site information architecture, content management, design facelift and additional functionalities to better serve the community. This section details these recommendations for the OWASP website in providing guidance for each item listed. Please note that the mock ups and suggested navigation are not final as additional mockups, wireframes and adjustments are part of the phase two implementation stage along with additional recommended functionalities and integrations.

#### Platform Selection

An important consideration for site improvement is platform selection. As the current site is a MediaWiki and users are treating it as such, there has been some consideration for migrating to other platforms to improve user experience and the overall perception of the OWASP Foundation. The following outlines the 3 options available and considerations for each:

##### **1) Option A: Retain and enhance the MediaWiki platform**

Although the MediaWiki platform encourages users to use it as such, with proper improvements to the design, information architecture and added functionalities, the site can elicit desired user engagements. The OWASP website currently serves 2 main purposes:

- 1) Organization visibility and membership promotion/participation
- 2) Improve application security visibility through best practices, tools and projects (security material)

These 2 purposes are at odds with each other as they are contending for attention on the OWASP home page. An improved information architecture with proper segregation of the organization and security information would resolve this, encouraging members to return for the security information, participate, volunteer and join the organization. In skinning the MediaWiki site, this removes the stigma of the site as a wikipedia for security and retains some of the core features that allowed users to collaborate. Lastly, additional features would improve user workflow. Examples include but are not limited to the following:

- 1) Single sign-on - allowing users to sign up for an user account via LinkedIn, Facebook, Gmail, etc would remove the friction for signing up and participating on the site
- 2) Forums - retiring mailman and implementing an online forum would improve communication between new and existing members and removes the issue of transparency that mailman prose as new members have no visibility on past discussions or helpful tips
- 3) Meetup API - integrating with Meetup and other event management tools will help chapter leaders organize meetings and improve visibility for OWASP events worldwide
- 4) Openhub and Github - integrating with and pulling information via Openhub and Github would help further improve project visibility and help project reviewers determine the status and activities of code-base projects
- 5) Google Doc - integrating with Google Doc may create a new utility for live collaboration for documentation projects

### 2) Option B: Migrate the MediaWiki platform to a new CMS/Wiki-like platform

In migrating to a new platform such as Kuma<sup>13</sup>, used by the Mozilla Developer Network, this gives the organization a clean slate to start from scratch, remove out-dated content during the mass content migration and have similar features as those seen on MDN. However, this will be fairly expensive as this option requires the most effort in time for implementation and mass migration of content.

### 3) Option C: Hybrid approach

The hybrid approach entails segregating the organization and security content and hosting each on a separate platform. The organization content would reside on a new CMS such as Wordpress or Drupal and the security content would remain on MediaWiki with some of option A functionalities implemented. This approach would yield a similar effect as option B, but provide the least amount of friction as there is no need for a mass migration of content. However, one thing to take in caution is that users may be more likely to visit the wiki.owasp.org more frequently than they would for the organization page as it houses the security content they crave. The concern is in whether this segregation would ultimately increase organization visibility and whether wiki users would end up visiting the organization page.

In analyzing the 3 options, we recommend options A and C as these would be the most practical, cost effective and timely solutions.

---

<sup>13</sup> Kuma Github: <https://github.com/mozilla/kuma>

## Information Architecture and Site Redesign

Independent of platform selection, an improvement of the site information architecture (navigation, content layout and content strategy) and design would yield improved user experience and encourage user participation and membership. The site should cater to both new and existing users in providing a better information architecture to improve content discoverability and site usability and a design that would improve upon the OWASP Foundation's image as a professional non-profit cybersecurity organization.

The general consensus among groups interviewed, survey results and peer analysis reflect that there is a need to segregate the organization and security information, which can be accomplished through a better content strategy. The current site is unsuitable for the organization's business facing needs as there is a contention between organization and security information due to the overwhelming amount of detail on the home page which discourages new users from exploring the site and getting to know OWASP as an organization instead of a wikipedia of reliable security documentation and project.

The following is the suggested top level navigation and header that would reside on every page:

Top Level Navigation and Header						
OWASP Logo				Search Bar	Login	Request Account
Projects+	About OWASP	Membership	Events	Forum/Discussion	Volunteer (Same as pre-existing category)	Donate/Join
Flagship Projects	Global Board	Individual and student membership	Chapter meetings	(Extension to replace mailing list powered by mailman)		
Lab Projects	Governance	Chapters	Appsec Events			
Incubator Projects	Code of Conduct	Corporate and academic members (Originally Acknowledgement)	Training Sessions			
Project Archive	Initiatives	Outreach Funding				
Participate	Education Resources					

This content organization would promote a clear division between projects versus organization content.

The following are sample layouts of home and content pages:

Home Page - Content		
Home Page Banner - Show relevant events/announcements		
News/Blog Feed - Consider consolidating the blog into the main site	Appsec Feed - Live Post from Appsec	Global Events - chapter meetings, appsec, training, Global Board meeting, etc
Podcast/Media (Video/Presentation)	Training Sessions	Newsletter and Social Media

Project Home Page - Content		
About Projects - Start, Update and Fund Projects		Recent Project Activities
Project Filtering - Advance Search		
Flagship Projects	Incubator Projects - Contains more sub-categories and starter projects	Builder, Breaker, Defender Project View All
Lab Projects		View Project Archive - Inactive Projects

Project/Content Page Example	
Project Maturity Banner	
Project Sub-categories - Main, Acknowledgements, Roadmap and getting involved, etc	
Main Project Content - About, Introduction, Examples, Use cases, etc	Member Involvement - Founder, Leaders, Contributors, etc
	Quick Download - PDF documentation, files, etc
	Code Repository Link
	Project Health

We created mock ups to provide visuals on how the site can look with the proposed information architecture. Note that these are for directional guidance and not finalized as this would be done in phase 2 of the project where additional wireframes and designs would be created and voted on by the community prior to implementation.

## Homepage

The homepage is the first point of entry - making it the most crucial page to optimize to elicit user engagement in providing a high level overview regarding the organization and site navigation to other important assets. The design provides a new and contemporary aesthetic and content structure in place of the default MediaWiki layouts.

The home page is now sectioned into several major components - a global header and navigation, a top hero section with full width image including a call to action message per slide, a main feed section divided into 4 blocks to provide recent updates, a right side panel with an events ticker box and social links in the new global footer.

The restructured global header and navigation provides a cleaner and easy to follow site navigation for better usability and content discovery and remains consistent throughout the site. The original left side navigation has been reduced down to 7 key pages and directories such that users would not be overwhelmed on initial visit and the donate/join button provides a call to action for users to join the organization instead of interacting with the site as just a wiki.

Additionally, the home page content layout has been simplified to encourage users to browse through content. The user is met with a clear home hero banner with a CTA message and button for new promotions or events that OWASP may like to call out. Below, the user can easily navigate the four major feed sections of OWASP through the color-coded quadrants. An easy-to-read and scrollable events ticker displays important OWASP organization events such as chapter meetings, allowing users to quickly stay up to date and RSVP.

The global footer seen at the bottom is visible on all pages throughout the site, allowing for easy navigation and reference regardless of which page a user is viewing.

Home Page (Desktop)



[Login](#)
[Request Account](#)

[+Projects](#)
[About](#)
[Events](#)
[Membership](#)
[Forum](#)
[Volunteer](#)
[Donate](#)



OWASP AppSec Europe '16

27.06 - 01.07

REGISTER NOW

LATEST NEWS


News article entry title will be roughly two lines and it will be condensed if it exceeds...

News Source | 3 hours ago

---

This is another news article entry, and it is a bit shorter than top.

News Source | 7 hours ago

---

Alternatively, this one is a bit longer than the one right above this article.

News Source | 2 days ago

---

This is another news article entry, and it is as long as the very first entry, and it will go over...

News Source | 5 days ago

LATEST BLOG


OWASP needs your input!

The OWASP Foundation has begun the process to improve the critical infrastructure and system pla...

By Kelly Santalucia | May 18

---

OWASP SAMM Summit

OWASP SAMM (Software Assurance Maturity Model) is an open framework to help organizations...

By Kate Hartmann | May 12

---

2016 Global BoD Election Call for Candidates...

We are pleased to announce that the 2016 Global BoD Call for Candidates is now OPEN! You may...

By Kelly Santalucia | May 10

Global OWASP Events

**Wednesday, March 9**

All Day | OWASP NIGHT IN JAPAN

4:30am | Seminar on Architecting a Safer Internet

---

**Wednesday, March 16**

All Day | BeNeLux OWASP Day 2016

All Day | Global Board of Directors Call

All Day | OWASP Russia Meetup

---

**Thursday, March 17**

11:00pm | OWASP NEW JERSEY

---

**Friday, March 18**

2:00am | OWASP NEW JERSEY

---

**Saturday, March 19**

4:00am | OWASP Bangalore + null/G4H meet

5:30am | [OWASP+Null] Delhi/NCP Chapter meet

---

**Thursday, March 24**

4:00pm | Suncoast OWASP Chapter meeting

---

**Tuesday, March 29**

All Day | These Day Web Application Security...

Sign Up for OWASP Newsletter

PODCAST


2016 - What's in Store for the OWASP 24/7 Podcast Series

4:14 | 4 months ago

---

Communication Patterns in Open Source Component Supply Chains

12:16 | 1 month ago

---

Active Deception as a Methodology for Cybersecurity w/ Lawrence Pingree from...

18:35 | 2 months ago

APPSEC FEED


OWASP ASVS 2.0 (Application Security Verification Standard)

By Jim Manico | 2 days ago

---

Call for Speakers: OWASP Ghana Cybersecurity Conference

By Jim Manico | 4 days ago

---

This FRIDAY is the DEADLINE to SUBMIT your CANDIDACY for OWASP Board of Directors

Kelly Santalucia | 6 days ago

Brand Resources | Governance | OCoC | Acknowledgements  
References | Advertising | Books | Merchandise | Contact

Copyright | Privacy Policy | Disclaimers









## **Projects Directory**

Another important page that we mocked up was the projects directory. A new welcome block emphasizes the purpose of the page, welcoming new viewers and existing members to the OWASP project home page with three call to action buttons for starting, updating and getting funding for projects.

Directly under this welcome block is a 2 step advance filtering search to help users discover projects based on project type, programming languages and other filters. The search block expands to display top 10 results and a link to view all results on a separate page.

The content portion of the page features flagship, incubator, lab and low-activity projects separated into 4 distinct and easy to navigate blocks for improved project visibility. An additional right side panel, calls out recent activities on all projects (code commits, documentation edits, etc) and further options to discover projects based on their builder, breaker and defender categorization.

# Project Directory Home Page



[Login](#) [Request Account](#)

+Projects
About
Events
Membership
Initiatives
News
Donate

**Welcome to the OWASP Global Projects Page.**

An OWASP project is a collection of related tasks that have a defined roadmap and team members. OWASP project leaders are responsible for defining the vision, roadmap, and tasks for the project. The project leader also promotes the project and builds the team. OWASP currently has 'over '89' active projects', and new project applications are submitted every week. [Learn More](#)

START A PROJECT
UPDATE A PROJECT
GET FUNDED

Filter projects by:

Filter Type  
Program Language ▼

Language  
Javascript ▼

Filter

Showing top 10 filter results for Javascript projects: [View All Results](#)

- OWASP Javascript Project
- OWASP Javascript 2016
- OWASP Javascript 2015
- OWASP Javascript for Security
- OWASP Javascript for Security II

- Javascript Project Documentation
- OWASP Javascript Best Practices
- Javascript Project lorem ipsum 1
- Javascript Project lorem ipsum 2
- Javascript Project lorem ipsum 3

**FLAGSHIP** mature projects

**TOOLS**  
Reviewed: Sep. 2016 Health check: Feb. 2016

- OWASP Zed Attack Proxy
- OWASP Web Testing Environment Project
- OWASP OWTF
- OWASP Dependency Check

[View all](#)

**CODE**  
Reviewed: Nov. 2014 Health check: Feb. 2016

- OWASP ModSecurity Core Rule Set Project
- OWASP CSRFGuard Project
- OWASP AppSensor Project
- OWASP Flagship Project

[View all](#)

**DOCUMENTATION**  
Reviewed: Feb. 2015 Health check: Feb. 2016

- OWASP ASSV Project
- OWASP Software Assurance Maturity Model
- OWASP AppSensor Project
- OWASP Top Ten Project

[View all](#)

**LAB** medium level projects

**INCUBATOR** new projects

**TOOLS**  
Reviewed: May 2015 Health check: Feb. 2016

- OWASP Benchmark
- OWASP Wordpress Vulnerability Scanner
- OWASP Threat Dragon
- OWASP Security Knowledge Framework

[View all](#)

**CODE**  
Reviewed: Mar. 2016 Health check: Feb. 2016

- OWASP Zed Attack Proxy
- OWASP Java HTML Sanitizer Project
- OWASP Node.js Goat Project
- OWASP Security Logging Project

[View all](#)

**DOCUMENTATION**  
Reviewed: May 2015 Health check: Feb. 2016

- OWASP Snakes and Ladders Project
- OWASP Automated Threats to Web Applications
- OWASP.NET Project
- OWASP Incident Response Project

[View all](#)

**RESEARCH**  
Reviewed: Mar. 2016 Health check: Feb. 2016

VIEW ALL BUILDERS PROJECT

VIEW ALL BREAKERS PROJECT

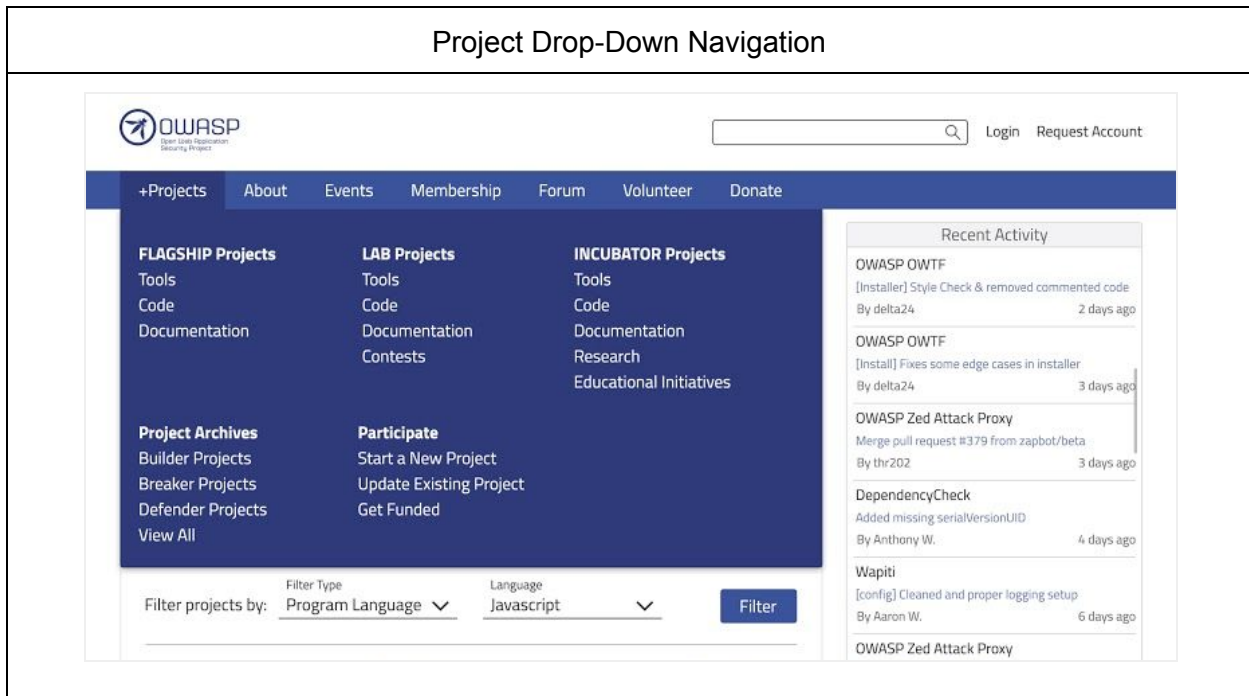
VIEW ALL DEFENDERS PROJECT

[View Full Archive](#)



### Projects Drop-down Navigation


To keep with the idea of simplicity and a clean design, navigational dropdown lists and menu blocks are implemented to maintain OWASP’s many page and subpage links, while keeping the site clear of clutter. Here, users can hover over Projects to find the many subdivisions within this dropdown menu block. By setting the links in the block, the user has access to the sub navigation elements without being overwhelmed by the amounts of navigation options at once.



## Project Wiki Article

An optimized layout for projects would help increase readability and appeal to new and exist users in helping them locate relevant information per project. A top banner is present to display the project category the current project falls under, in this example it is a flagship project. The content design has been simplified into 2 major blocks - a major article section for most relevant content pertaining to the project and a right side panel block for listing project leaders, links to downloads, code repositories, documentations and other quick helpful links.

### Project Page



[Login](#) [Request Account](#)

+Projects
About
Events
Membership
Forum
Volunteer
Donate

FLAGSHIP
mature projects

Main
Acknowledgements
Road Map & Getting Involved
Detection Points
Media

#### OWASP AppSensor

The AppSensor project defines a conceptual framework and methodology that offers prescriptive guidance to implement intrusion detection and automated response into applications.

The project offers a comprehensive guide and a reference implementation. These resources can be used by architects, developers, security analyst and system administrators to plan, implement and monitor an AppSensor system.

---

#### Introduction

If you walk into a bank and try opening random doors, you will be identified, led out of the building and possibly arrested. However, if you log into an online banking application and start looking for vulnerabilities no one will say anything. This needs to change! As critical applications continue to become more accessible and inter-connected, it is paramount that critical information is sufficiently protected. We must also realize that our defenses may not be perfect. Given enough time, attackers can identify security flaws in the design or implementation of an application.

In addition to implementing layers of defense within an application, we must identify malicious individuals before they are able to identify any gaps in our defenses. The best place to identify malicious activity against the application is within the application itself. Network based intrusion detection systems are not appropriate to handle the custom and intricate workings of an enterprise application and are ill-suited to detect attacks focusing on application logic such as authentication, access control, etc. This project delivers a framework which can be used to build a robust system of attack detection, analysis, and response within an enterprise application.

---

#### Detect & Respond to Attacks from Within the App

**Detection**  
AppSensor defines over 50 different detection points which can be used to identify a malicious attacker.

**Response**  
AppSensor provides guidance on how to respond once a malicious attacker has been identified. Possible actions include: logging out the user, locking the account or notifying an administrator. More than a dozen response actions are described.

**Defending the Application**  
An attacker often requires numerous probes and attack attempts in order to locate an exploitable vulnerability within the application. By using AppSensor it is possible to

#### Project Health

Maturity: Flagship  
Documentation: Under Review  
Rating: 3/5  
Contributors: 30  
Language: HTML, JavaScript, Java, Other

---

#### Project Founder

Michael Coates

#### Project Leaders

Michael Coates  
John Melton  
Colin Watson

---

#### Quick Download

OWASP AppSensor guide v2 EN  
[PDF](#)  
[DOC](#)  
[Hard Copy](#)

OWASP AppSensor Reference Implementation  
[v2 Code](#)

---

#### Code Repository

AppSensor v2  
<https://github.com/jtmelton/appsensor>  
(Current)

Note: LEGACY AppSensor v1  
<https://code.google.com/p/appsensor/>

---

#### Documents & Briefings


## Mobile

Modern sites require a mobile centric approach as users are accessing sites more frequently via their mobile devices. Based on google analytics, the bounce rate is 75.39%<sup>14</sup> for mobile device access - this is ~9% higher compared to desktop as the content does not resize appropriately, which renders the site unusable. The proposed design accounts for this with a mobile optimized layout. The global header is simplified and categories condensed under the hamburger menu icon. The text is further optimized for legibility and content is structured in single blocks to allow users to scroll through and focus on one item at a time for optimal mobile screen usage and better display.

### Mobile Home Page

<sup>14</sup> This is for the timeframe of May 1st, 2015 - May 31st, 2016

### Mobile Project Directory



Welcome to the OWASP  
Global Projects Page.

An OWASP project is a collection of related tasks that have a defined roadmap and team members. OWASP project leaders are responsible for defining the vision, roadmap, and tasks for the project. The project leader also promotes the project and builds the team. OWASP currently has 'over 100' active projects, and new project applications are submitted every week.

START A NEW PROJECT

UPDATE EXISTING PROJECT

GET FUNDED

**Filter projects by:**

Filter Type  
Program Language
Language  
Javascript

FILTER

Showing top 5 filter results for javascript projects

- + OWASP Javascript Project
- + OWASP Javascript 2016
- + OWASP Javascript 2015
- + OWASP Javascript for Security
- + OWASP Javascript for Security II

[View All Results](#)

FLAGSHIP mature projects

**TOOLS**  
Reviewed: Sep. 2016    Health check: Feb. 2016

- + OWASP ASST Project
- + OWASP Software Assurance Maturity Model
- + OWASP AppSensor Project
- + OWASP Top Ten Project

[View all](#)

**LAB** medium level projects

**TOOLS**  
Reviewed: Feb. 2016    Health check: Feb. 2016

- + O-Soft
- + OWASP Dependency Track Project
- + OWASP DnDc Project
- + OWASP Hackademic Challenges Project

[View all](#)

**CODE**  
Reviewed: Feb. 2016    Health check: Feb. 2016

- + OWASP Enterprise Security API
- + OWASP Python Security Project
- + OWASP Wsnam Project
- + OWASP Broken Web Applications Project

[View all](#)

**DOCUMENTATION**  
Reviewed: Feb/March 2015    Health check: Feb. 2015

- + OWASP Application Security Guide for CSOs
- + OWASP Cheat Sheet Project
- + OWASP CSD Survey
- + OWASP Code Review Guide Project

[View all](#)

INCUBATOR new projects

**TOOLS**  
Reviewed: May 2015    Health check: Feb. 2015

- + OWASP Benchmark
- + OWASP Wordpress Vulnerability Scanner
- + OWASP Threat Dragon
- + OWASP Security Knowledge Framework

[View all](#)

**CODE**  
Reviewed: Mar 2016    Health check: Feb. 2016

[View all](#)

**CODE**  
Reviewed: Mar 2016    Health check: Feb. 2016

- + OWASP Zed Attack Proxy
- + OWASP Java HTML Sanitizer Project
- + OWASP Nodejs Goat Project
- + OWASP Security Logging Project

[View all](#)

**DOCUMENTATION**  
Reviewed: May 2016    Health check: Feb. 2016

- + OWASP Snakes and Ladders Project
- + OWASP Automated Threats to Web Applications
- + OWASP .NET Project
- + OWASP Incident Response Project

[View all](#)

**RESEARCH**  
Reviewed: Mar 2015    Health check: Feb. 2016

- + OWASP WASC Distributed Web Honeypots Project

[View all](#)

**EDUCATION**  
Health check: Feb. 2016

- + OWASP Student Chapters Project
- + OWASP Education Project
- + OWASP Speakers Project
- + OWASP Media Project

[View all](#)

VIEW ALL BUILDERS PROJECT

VIEW ALL BREAKERS PROJECT

VIEW ALL DEFENDERS PROJECT

[Brand Resources](#) | [Governance](#) | [OCof](#)  
[Acknowledgements](#) | [References](#) | [Advertising](#)  
[Books](#) | [Merchandise](#) | [Contact](#)

[Copyright](#) | [Privacy Policy](#) | [Disclaimers](#)

## Back-office tools and Infrastructure architecture

The back-office tools and infrastructure is the backbone of OWASP in keeping the organization operational and thriving. With that in mind, we assessed all the key tasks that IT and staff team do on a daily basis for a comprehensive understanding of their pain points and identify inefficiencies that can be improved upon, which would enable the team to better serve the OWASP community.

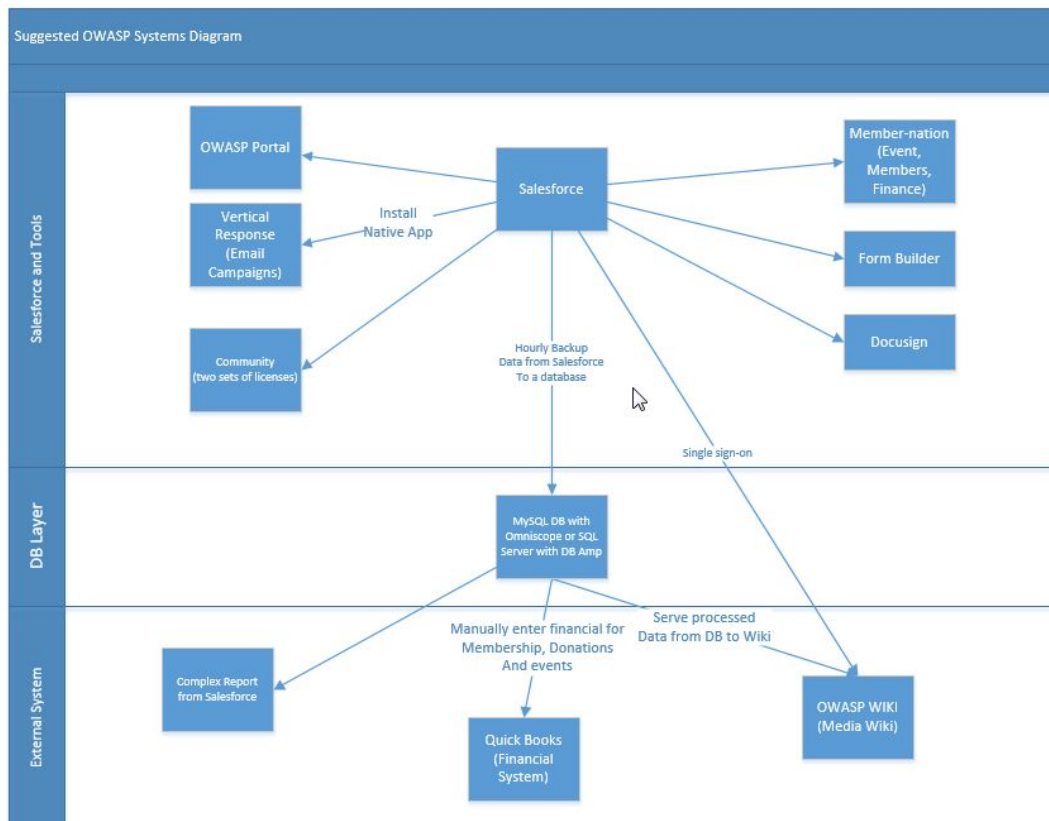
### Salesforce

There are many non-profit organizations using Salesforce and there are many apps available on App-Exchange to support their causes. Most popular apps are:

- NGO Connect from roundCorner which supports large organizations. Licensing fee applies.
- NPSP from Salesforce. This is a free application.
- Member-nation from Fonteva for small to medium size organization. Licensing fee applies.

The following is the suggested system map for Salesforce to address pain points identified during the initial interview session.

### Suggested System Map



**Database (MySQL or SQL Server)**

We suggest to have an instance of either MySQL or SQL Server which integrates with Salesforce. Using either Omnisciope/MySQL or DBamp/SQL Server combination data can be imported/exported from/to Salesforce. Most of the organization has this middle layer to integrate with other systems; for complex reporting and to have a backup of the data. This layer also helps with complex processes like calculating most recent donation amount, date, lifetime giving amount, generating ask string, usage stats matrix etc. Both system combinations have similar functionalities. But here are the pros and cons:

**SQL Server/DB Amp**

A non-profit organization can get standard version of SQL server license and DBamp application with minimal cost. DB amp is tool that connects Salesforce to SQL Server.

Pros: Very fast and efficient. Excellent reporting functionality. Integrates with office tools. Has capability of data warehousing, job scheduling and backup capabilities.

Cons: Maintenance cost and integration with MediaWiki.

**MySQL/Visokio Omnisciope**

MySQL is an open source database and Visokio Omnisciope is available for a cost. Omnisciope is used to import and export data from Salesforce.

Pros: Cost effective. Omnisciope reporting functionalities are excellent. Omnisciope has capability of running scheduled jobs, has ability to distribute reports and much more. MySQL can integrate with wiki.

Cons: Omnisciope is expensive, MySQL support.

**Integration with Finance system**

Most of the organizations use the middle layer to integrate with finance system. The integration process can be automated or could be a daily manual batch process depending upon finance system in place (i.e for Quickbooks there is an existing integration that can be implemented)

**Vertical Response and Campaigns**

OWASP has an account with VerticalResponse to manage their email campaigns. But, currently, Salesforce admin has to manually import and export data from/to VerticalResponse. This manual step can be avoided by using Salesforce Campaigns and with installation of vertical response app.

**Community+ Licenses for Chapter Coordinators**

OWASP can purchase Community plus licenses for Chapter coordinators, which will give them more features access in Salesforce like running report and dashboard. This will give Chapter coordinators the ability to run reports, and manage their chapter memberships.

**Integration with Wiki**

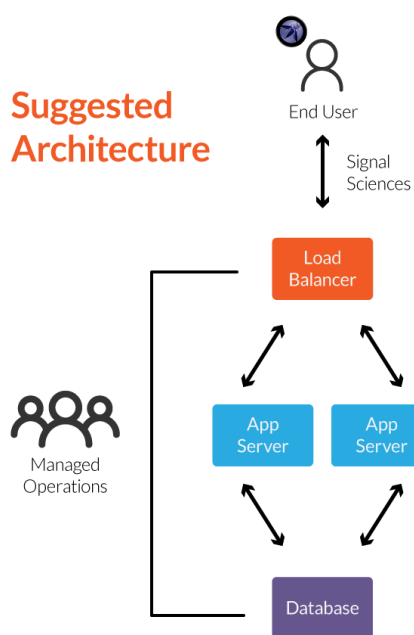
Salesforce has the ability to integrate with Wilki using single sign-on feature. This enables the organization to have one place of entry. Another option would be is to use the middle layer of database to integrate with Wiki to expose reports and dashboards on Wiki.

### Fundraising

Management of donors and donation is most critical part of any non-profit organization. Salesforce provides many different options to manage this critical feature. The best optimal option is to use Salesforce Accounts-Contacts-Opportunities to manage donors and donations. This provides native Salesforce functionality and reports and dashboards.

### Rackspace and OWASP website

The improvements needed for the Rackspace infrastructure is the code segregation for the MediaWiki component, a load balanced auto-scaling deployment process via chef scripts, retirement of Mailman for an open forum MediaWiki plugin that is clearly visible on the OWASP website, events promotion and visibility in integrating with Meetup via their API and advanced search and filtering with Elasticsearch.



### Project Workflow and Toolset

For better project visibility and promotion, we should be creating an API integration with Open Hub and/or create a custom crawl script/calls to the github api to draw in statistics, documentation updates and project updates back into the MediaWiki so it is more consumable for new users and projects are more visible for all users. In addition, an auto-generated project update summary should be generated weekly and distributed to all project leaders and contributors. Code projects that are currently not under the OWASP account should be required

to be if they are to be considered lab or flagship projects and documentation should be centralized and standardized.

### **Gamification and Engagement**

As suggested by some members of OWASP that we interviewed, we looked into badging and gamification for the current OWASP site. Currently, we don't believe gamification of the site should be a priority though it may be an interesting feature for future development. The benefit of this is to be able to award members almost automatically by this new badging system such as for the WASPY awards - a well defined scoring system needs to be in place for this to happen (example scoring activity: New code commit to project (1pt), Documentation Update (1pt), etc.). Similarly, this badging system can be used for training materials and accreditations that OWASP is creating to further engage with their community and new potential audiences.

We examined both Pearson Acclaim badges and Mozilla Open badges to help facilitate this and recommend the latter as it is open-source which encourage member adoption of the technology.



## Features and Release Roadmap

After reviewing the recommendations, the following are the features and release roadmap that we propose for OWASP to improve upon the current site and infrastructure and toolings. The roadmap is from most to least significant order and is suitable for all platform options outlined:

1. **Content Strategy** - there is a need for content curation and further organization beyond the proposed information architecture in this documentation. As there may be unknown content that may not have been highlighted by the site and volunteers and the content audit may not have identified in the crawl, it is to do a thorough content inventory sorting for improved content discovery. This process can be facilitated by a group of volunteers, by a hired content curation professional and programmatically archival of unused assets. MediaWiki older than 2 years and have not been accessed frequently should fall under the archive
2. **Design and frontend improvement of MediaWiki** - after content curation, OWASP can move forward with a new design and frontend improvements for the current MediaWiki with the new information architecture and mobile first approach
3. **DevOps for OWASP website** - in conjunction with the design and frontend improvements, OWASP can establish and create the code repository for the MediaWiki to segregate the current dependency of restoration of the website via an image of the server. In doing so, this allows for easier upgrades to the MediaWiki software, implementation of additional functionalities and front end customizations. Additional benefit of this would be implementation of chef scripts for quick consistent deployments, elasticity and fault tolerance as the current system is not self healing and disaster recovery is dependent on operations team intervention.
4. **Improved core MediaWiki functionalities** - additional features can be added in conjunction with features 1-3 these features include by are not limited to items mentioned in the platform section
  - a. Single Sign On
  - b. Forums
  - c. Project Dashboard via Openhub
  - d. Meet up API Integration
  - e. Google Docs
5. **Middle layer Integration with Salesforce** - for data transparency, a middle layer integration between Salesforce and the MediaWiki platform can automate information transfer and simplify permission issues for sharing data
6. **Automated scoring and badging** - training and course material can be supplemented with this scoring and badging system to further gamify the site and encourage users engagement

## Closing Remarks

We would like to acknowledge and thank the OWASP Board and staff and all volunteers who contributed their time for the interviews and gave us feedback to help make this needs assessment possible and help OWASP grow as an organization. We hope that this document was helpful in mapping out what OWASP can do to further their mission and engage more with their community. Lastly, we thank OWASP for this opportunity to contribute to their 2016 strategic objectives.

## Appendix

### List of Current Tools

Tools	Integrated Tools?	Summary	General use case	OWASP use case
Salesforce Enterprise		Customer Relationship Management	Customer Relationship Management	Customer Relationship Management
	Apsona	Filtering tool, different views of data, grid editing, importing and exporting data, allows for mass updating & deleting	Managing data	Import/export/data clean up tool
	Conga Composer	Create and deliver sophisticated documents, presentations and reports automatically populating templates with data from any standard or custom object Customize, streamline and scale their document generation and reporting for use cases	Quotes, proposals, account plans, invoices & receipts, contracts, reports & charts	Document output

	CRM Fusion (Demand Tools)	Modules for data deduplication, normalization, standardization, comparison, import, export, mass delete	Data quality & data cleansing toolset	Data clean up tool
	DocuSign	Electronic signatures	Electronic signatures	Electronic contract signature
	Form Assembly	Payment forms- Create order forms, service requests, or registration forms, and collect payments securely Online applications- Forms to help enroll students, process job applications, or qualify beneficiaries Surveys- Collect feedback from your customers, or design surveys for market or academic research Contact Forms- Let visitors and prospective customers reach out, and push those leads to your CRM	Building web forms and collecting the data	Creates forms that allow external input into SF Used primarily for the "Contact Us" form and the Project Applications
	Volunteers for Salesforce	Helps manage volunteer events and people Manages volunteers, jobs, shifts, and hours to track and report on all of the data as well as allow public signups via Sites pages on website		Organizes volunteer needs and allows for external posting
	MemberNation	Association Management System	Association Management System	Association Management System & vehicle for the OWASP Portal and the OWASP Community Includes modules for: Awards, Chapters,

				Committee, E-Business, Education, Events, Fundraising, Membership
Eventbrite and RegOnline		Self-service ticketing platform Event online event management and registration platform	Self-service ticketing platform Event online event management and registration platform	Event registration systems
Quickbooks		Accounting software package accept business payments, manage and pay bills, and payroll functions	Accounting software package accept business payments, manage and pay bills, and payroll functions	Accounting
PayPal		To send money, make an online payment, receive money or set up a merchant account	To send money, make an online payment, receive money or set up a merchant account	Payment processing
Vertical Response		Create, send, and track emails and social posts	Create, send, and track emails and social posts	Email marketing
Survey Monkey		Create and publish online surveys in minutes, and view results graphically and in real time	Create and publish online surveys in minutes, and view results graphically and in real time	Surveys
Vimeo and YouTube		Video posting/browsing	Video posting/browsing	Video posting
Citrix Systems (GoToMeeting and GoToWebinar)		Online meeting, desktop sharing, and video conferencing software that enables the user to meet with other computer users, customers, clients or colleagues via the Internet in real time Record webinars with additional features	Online meeting, desktop sharing, and video conferencing software that enables the user to meet with other computer users, customers, clients or colleagues via the Internet in	Not specified

			real time Record webinars with additional features	
Dropbox		File hosting service	File hosting service	Not specified
Trello		Visual organization tool	To visually track notes	Not specified
Twitter		Social Media	Social Media	Social Media
Slack		Social Media	Social Media	Social Media
Facebook		Social Media	Social Media	Social Media
Ning		Social Media	Social Media	Social Media
LinkedIn		Social Media	Social Media	Social Media
CrowdIn		Social Media	Social Media	Social Media
Blogspot		Social Media	Social Media	Social Media
Meetup		Social Media	Social Media	Social Media
Google Suite- email, docs, calendars, groups, etc		Social Media	Social Media	Social Media
MediaWiki		Free and open-source wiki application	Free and open-source wiki application	Web collaboration tool
Google for Nonprofits		Free access to Google tools like Gmail, Google Calendar, Google Drive, Google Ad Grants, YouTube for Nonprofits and more	Gmail, Google Calendar, Google Drive, Google Ad Grants, YouTube for Nonprofits and more	Email/collaboration tool
Rackspace Public Cloud		Managed cloud services for hosting needs (Projects, Websites, etc) - IaaS	Fully Managed Infrastructure hosting needs for projects, production and development environments, etc	Server hosting (web, mailing lists, experiments)
Github		Git Repository	Code Repository	Code repository tool
Mailman		Mailing List Management Tool		Discussion list tool

## Interview Questions

### Staff Meeting Questions

**Objective:** The purpose of the call was to review each of the tools listed in the RFP, who uses and manages it, and the pain points and advantages associated with the tools.

#### Agenda:

- 1) Introductions - Roll call
- 2) Please state your role and provide a list of the tools you use to facilitate this on a daily basis
- 3) Please identify your perceived strengths and weaknesses for the tools you use and/or inefficiencies/blockers you have encountered - identify the rationale behind why you picked the toolset
- 4) Is there difficulty switching between tools and would it be beneficial to centralize some of the tools you are using?

#### Interview Questions:

Project Manager/Funding- Claudia Casanovas

- 1) Since there are currently 200+ projects, what are the main challenges you perceive in tracking funding, progress and results? What are the inefficiencies/frustrations that may have come up with the current tool set used for this?
- 2) What are some common issues that project leaders/contributors have brought up, if any, such as logistical blockers/issues people have experienced with starting a project, obtaining funding, etc
- 3) What is the most time-consuming aspect in the process?
- 4) Are there any parts in the tracking process or project creation/initiation that you believe can be better organized? (Are there areas in the process that you feel are disorganized or needs better management?)

Contracts Manager (Membership/Business Liaison)- Kelly Santalucia

- 1) Has a standardized process been defined in initial engagements, contract generation and sign completion? If so, what are the steps taken from start to end and tools touched upon?
- 2) Is there a centralized repository for the contracts sent out and is there a backup process in place in case contract is lost digitally, etc.?
- 3) What is the typical turnaround time for each contract engagement and do you perceive any inefficiencies in the current process in place?
- 4) Are you satisfied with the toolsets in place to facilitate this or do you believe there are areas for improvement?
- 5) Is there a need for a tighter integration of tools or process to help increase productivity?
- 6) Are you happy with the tools in place?

### Global Events Coordinator- Laura Grau

- 1) Have you had any issues with collecting, tracking and/or processing ticketing for events?
- 2) What is the standard process involved coordinating a global event and what do you perceive is the most time consuming part that?
- 3) Are there any other tools that you have used or would like to incorporate into the process?

### IT Meeting Questions

**Objective:** The purpose of the call was to review the underlying infrastructure of the OWASP website and walkthrough Salesforce. Specific focus was on hosting, performance, scalability, security, integration and upgradability.

#### Agenda:

- 1) Go over current infrastructure footprint on Rackspace
- 2) Salesforce walkthrough with Kate

#### Interview Questions:

- 1) OWASP Website | Infrastructure Performance
  - a) Who manages the website and what are the internal processes and protocols in place?
  - b) In addition to Web admin, are there other roles involved in content management/administration?
  - c) Is there a content strategy/information architecture in place today? If not, do you have any suggestions on what you want this to be?
  - d) How is SEO managed for the website? Are there any problems that you currently face in this area e.g. duplicate content, missing META/Keywords, etc.?
  - e) What are the various page types and goals of each section of the website?
  - f) What information do you review on Google Analytics? Is it properly configured and is it useful for understanding audience engagement?
  - g) Are there any other logs/tools that you use to monitor the website?
  - h) What is your site availability metrics? Have you experienced involuntary downtime, slowness or outages? If yes, what are the reasons for that?

### Builders, Breakers, and Defenders Questions

**Objective:** Evaluate the current needs for the OWASP task forces who are primarily involved with project implementation, tracking and documentation. As these task forces (or categories) have the most integration with the MediaWiki and are the main contributors to the OWASP projects and future growth, it is crucial to identify any dissatisfactions with the current platform and infrastructure in place for collaboration.

#### Agenda:

- 1) Introduction and roll calls to ensure we have a representative group of users from the Builders/ Breakers/ Defenders community
- 2) Interview Questions
- 3) Additional Feedback
- 4) Meeting conclusion and summary (QA)

**Interview Questions:**

- 1) Project Logistics and Documentation
  - a) Have you had any issues with starting a project following the MediaWiki process?
  - b) Have you had any issues with creating the MediaWiki for the project, maintaining it and allowing others to help contribute to it?
  - c) Do you feel like there is a lack in process for funding, communication with other members and collaboration on the MediaWiki?
  - d) Do you feel the current templates in place for projects are sufficient for your needs? As adjustments can be made to these templates per project, is the layout for the information consistent enough?
  - e) Is there sufficient documentation for on-going projects such that new volunteers can go through the material and potentially contribute?
  - f) Do you believe there is enough visibility as to what projects the OWASP community is currently working on?
- 2) Project Code Repository and Collaboration
  - a) In your opinion, are the code repositories for existing projects well maintained?
  - b) Did you have trouble collaborating with others on projects?
  - c) What are some tools that you would suggest to help you streamline the process?
  - d) Was there a rationale behind choosing Github over Bitbucket? Is there a preference in the community for either or?
- 3) MediaWiki (OWASP Website)
  - a) In the last six months, have you visited the OWASP website?
  - b) Can you identify a representative group of resources that you as a builder/breaker/defender use?
  - c) How often has the main page for OWASP builders/breakers/defenders been maintained and are there other pieces of information that you would like to see there?
  - d) Is there something missing from the OWASP website that you were expecting?
  - e) Are the core MediaWiki functionalities (editing running documentations) intuitive and easy to use?
  - f) Have you had trouble finding information you are looking for? Is the information layout consistent such that you can easily locate relevant information to you?
  - g) On a scale of 1-10, please rate your overall impression of the OWASP website.
  - h) Can you name other websites that are doing something similar in a better manner?
- 4) What other improvements would you like to see with OWASP's frontend facelift?



- 5) Is there certain information that you believe should be more transparent for the community to evaluate such as membership demographics?
- 6) What is your thought on gamification or badging for users on the website?
- 7) What are other technology tools that would benefit your task force or the OWASP community in general in addition to this website or an extension to it?

## Chapter and Project Leader Questions

**Objective:** Evaluate the current needs for the OWASP chapter and project leaders who are primarily involved with initiating, managing and promoting the OWASP organization through their works. As these groups have the most direct contact with engaged volunteers, it is crucial to identify any dissatisfactions with the current platform, infrastructure, and measures in place to encourage collaboration and outreach.

### Agenda:

- 1) Introduction and roll calls to ensure we have a representative group of users from the chapter and project leader community
- 2) Interview Questions
- 3) Additional Feedback
- 4) Meeting conclusion and summary (QA)

### Interview Questions:

- 1) Chapter logistics
  - a) What are some tools that you are currently using for meeting setups? On average, how many members show per meeting? What other outreach efforts have you undertaken?
  - b) How are you managing member retention, engagements, identifying paying and non-paying members?
  - c) What are some data points that you would like to see on your chapter Mediawiki page (Such as demographics, paying/non-paying, project contributors, etc.)?
  - d) What are some changes you would like to see on the Mediawiki or chapter pages?
  - e) What would assist your efforts in outreach that is currently not being provided by OWASP?
- 2) Project Code Repository and Collaboration
  - a) In your opinion, how likely is centralizing project code repositories onto specific accounts (OWASP Account)? What are the main friction points you anticipate for this?
  - b) Have you had issues getting subject matter experts' opinions/volunteers for specific projects? What changes on the OWASP site do you believe would help facilitate this?

- c) Do you believe there is enough visibility as to what projects the OWASP community is currently working on? What should be the project promotion criteria on website?
  - d) What are some metrics for OWASP project health (code/documentation) and updates do you believe should be communicated on the Mediawiki for better visibility (ex. Code project details are noted on OpenHub)?
- 3) MediaWiki
- a) In the last six months, have you visited the OWASP website?
  - b) How often has the main page for your OWASP chapter or project been maintained?
  - c) Is there something missing from the OWASP website that you were expecting?
  - d) Are the core MediaWiki functionalities (editing running documentations - ongoing editing and creation of content) intuitive and easy to use?
  - e) On a scale of 1-10, please rate your overall impression of the OWASP website.
  - f) What other platforms do you suggest in place of mediawiki?
- 4) What other improvements would you like to see with OWASP's frontend facelift?
- 5) Do you think there should be a separation of the OWASP project documentations, chapter and organization information? Where would you draw the line?
- 6) What is your thought on gamification or badging for users on the website?
- a) Ex. What is your opinion on a stackoverflow-like implementation for the OWASP wiki to facilitate better communication and badging/gamification?
- 7) What are other technology tools that would benefit the OWASP community in general in addition to this website or an extension to it?
- 8) Have you had trouble finding information you are looking for? Is the information layout consistent such that you can easily locate relevant information to you?
- 9) Can you name other websites that are doing something similar in a better manner?
- 10) What do you believe would drive OWASP community engagement on the site?

### Global Board Questions

**Objective:** Evaluate the current needs for the OWASP community and website. As elected representatives of the OWASP community, the board members would have a better understanding of the needs of the community and help identify any dissatisfactions with the current platform, infrastructure, and measures in place to encourage collaboration and outreach.

#### Agenda:

- 1) Introduction and Roll Call
- 2) Interview Questions
- 3) Additional Feedback
- 4) Meeting conclusion and summary (QA)

#### Interview Questions:

- 1) Chapter logistics

- a) What are some tools that you are currently using for meeting setups? On average, how many members show per meeting? What other outreach efforts have you undertaken?
  - b) How are you managing member retention, engagements, identifying paying and non-paying members?
  - c) What are some data points that you would like to see on your chapter Mediawiki page (Such as demographics, paying/non-paying, project contributors, etc.)?
  - d) What are some changes you would like to see on the Mediawiki chapter pages?
  - e) What would assist your efforts in outreach that is currently not being provided by OWASP?
- 2) Project Logistics and Documentation
- a) Have you had any issues with starting a project following the MediaWiki process?
  - b) Have you had any issues with creating the MediaWiki for the project, maintaining it and allowing others to help contribute to it?
  - c) Do you feel like there is a lack in process for funding, communication with other members and collaboration on the MediaWiki?
  - d) Do you feel the current templates in place for projects are sufficient for your needs? As adjustments can be made to these templates per project, is the layout for the information consistent enough?
  - e) Is there sufficient documentation for on-going projects such that new volunteers can go through the material and potentially contribute?
  - f) Do you believe there is enough visibility as to what projects the OWASP community is currently working on?
- 3) Project Code Repository and Collaboration
- a) In your opinion, how likely is centralizing project code repositories onto specific accounts (OWASP Account)? What are the main friction points you anticipate for this?
  - b) Have you had issues getting subject matter experts' opinions/volunteers for specific projects? What changes on the OWASP site do you believe would help facilitate this?
  - c) What are some metrics for OWASP project health (code/documentation) and updates you believe should be communicated on the Mediawiki for better visibility (ex. Code project details are noted on OpenHub)?
  - d) What are some tools that you would suggest to help you streamline the process?
  - e) Was there a rationale behind choosing Github over Bitbucket? Is there a preference in the community for either or?
- 4) MediaWiki (OWASP Website)
- a) In the last six months, have you visited the OWASP website?
  - b) Can you identify a representative group of resources that you as a Global Board member uses?
  - c) How often has the main page for OWASP Global Board members been maintained and are there other pieces of information that you would like to see there?

- d) Is there something missing from the OWASP website that you were expecting?
  - e) Are the core MediaWiki functionalities (editing running documentations) intuitive and easy to use?
  - f) Have you had trouble finding information you are looking for? Is the information layout consistent such that you can easily locate relevant information to you?
  - g) On a scale of 1-10, please rate your overall impression of the OWASP website.
  - h) Can you name other websites that are doing something similar in a better manner?
- 5) What other improvements would you like to see with OWASP's frontend facelift?
  - 6) Is there certain information that you believe should be more transparent for the community to evaluate such as membership demographics?
  - 7) What is your thought on gamification or badging for users on the website?
    - a) Ex. What is your opinion on a stackoverflow-like implementation for the OWASP wiki to facilitate better communication and badging/gamification?
  - 8) What are other technology tools that would benefit the OWASP community in general outside of this website or an extension to it?
  - 9) What do you believe would drive OWASP community engagement on the site?

## Interview Summaries

<b>Date</b>	<b>April 28, 2016</b>
<b>Location</b>	<b>Conference call</b>
<b>Subject</b>	<b>OWASP Staff Meeting</b>
<b>Participants</b>	<p><b>OWASP</b></p> <p>Kelly Santalucia - Membership and Business liaison          Claudia Casanovas - Project Manager          Laura Grau - Events Manager          Kate Hartmann - Operations Director/Salesforce Administrator          Alison Shrader - Accounting</p> <p><b>Sooryen Technologies</b></p> <p>Gin Cheng- Tech Lead          Ahsun Kim- Project Manager          Ram Ganesan – CEO/ Co-Founder of Sooryen Technologies</p>
	<b>Items</b>
	<b>Objective and background:</b>

The purpose of the call was to review each of the tools listed in the RFP, who uses and manages it, and the pain points and advantages associated with the tools.

The Sooryen team shared an Excel spreadsheet that contained the following information:

- Tools and integrated tools listed on the RFP, corresponding summary, general use case, OWASP use case

#### **Key discussion items**

- **Project Manager/Funding- Claudia Casanovas**
  - Primary tools used: Salesforce, Wiki
    - Personal input: Wanting to incorporate Github and Openhub to coordinate activities and activity levels
    - Pain point:
      - Must manually add this information on Salesforce
      - Once project is added:
        - Excel form that needs to be edited manually with new project information from wiki page
        - Need to update Salesforce with Github
  - For tracking, get all data from wiki pages and Github
  - For funding, utilizes Salesforce and wiki pages for tracking
    - Alison uses Quickbooks for funding
  - Typical funding cycle: 1-2 days for answer and notice
    - Notice: Detailed proposal of what money is needed for, proposed invoice, and cost details
  - Centralized documentation used to track project funding: Salesforce
    - Submits a project funding request on Contact Us form and goes through Salesforce system
    - Makes a case and gets sent to Kate
    - If it's a case regarding projects, Claudia is assigned to it and gets in touch with requester or project leader
  - No common issues with starting a project, obtaining funding, etc.
  - Project administration
    - Main contributors to edit wiki: staff and project leaders
      - Discrepancies evident between projects
      - 3 templates available: Tools, codes, documentation
        - Main items that need to be available to be approved: Project leader, description, road map, project information, repository
    - Project leaders work on pages for typically 1-2 weeks, which is followed by review process
      - Followed by approval for project to be placed on inventory list; officially an incubator project
- **Contracts Manager (Membership/Business Liaison)- Kelly Santalucia**
  - Primary tools used: Salesforce, Wiki, Docusign
    - For corporate and individual memberships, sponsorships, contracts for events, co-marketing and partnership agreements
      - Personal input: Possibly not using Salesforce to the best of abilities; Would like to automate email or notification to let Alison know to send invoice

	<ul style="list-style-type: none"> <li>■ Standard process for contract for sponsorships and corporate memberships: <ul style="list-style-type: none"> <li>● Note: Individual members don't require contracts</li> <li>● Note: Sponsorship - event based; corporate membership- membership through foundation</li> <li>● Establishes contact with company or vice versa <ul style="list-style-type: none"> <li>○ Each has sponsorship document with cost for sponsorship/ corporate document with cost for corporate membership</li> </ul> </li> <li>● Create a contract in Salesforce and send through DocuSign <ul style="list-style-type: none"> <li>○ Goes to Kate first for review and signature</li> </ul> </li> <li>● Automatically sent to point of contact for sponsor/ corporation</li> <li>● Notified automatically electronically from DocuSign regarding signed contract</li> <li>● Kelly sends Alison an email to send an invoice <ul style="list-style-type: none"> <li>○ For sponsorship: for what event, level of sponsorship, cost, and company that invoice has to be sent to</li> <li>○ Would like to automate email or notification to let Alison know to send invoice</li> </ul> </li> <li>● Once marked paid in Salesforce, Kelly notified that contract has been paid</li> <li>● Contacts sponsor for deliverables that's related to sponsorship</li> </ul> </li> <li>■ Centralized repository for contracts: Salesforce and DocuSign</li> <li>■ Typical turnaround time for each contract engagement depends on how long it takes from the company respondent <ul style="list-style-type: none"> <li>● Along with Salesforce, keeps separate google document for own tracking</li> </ul> </li> <li>■ Wiki for: <ul style="list-style-type: none"> <li>● Keeping membership page up to date</li> <li>● Listing co-marketing and partnership agreement that have benefit for OWASP under partner and promotional event section</li> <li>● Entered in OCMS system; automatically creates event in Salesforce <ul style="list-style-type: none"> <li>○ Then added on wiki</li> </ul> </li> </ul> </li> <li>■ Can run reports regarding membership statistics through Salesforce</li> </ul> <ul style="list-style-type: none"> <li>● <b>Global Events Coordinator- Laura Grau</b> <ul style="list-style-type: none"> <li>○ Primary tools used: <ul style="list-style-type: none"> <li>■ Salesforce, Eventbrite, RegOnline, DocuSign <ul style="list-style-type: none"> <li>● Personal input: Possibly not using Salesforce to the best of abilities</li> <li>● Pain points: <ul style="list-style-type: none"> <li>○ Too many tools <ul style="list-style-type: none"> <li>■ Data is not all collected/ centralized on Salesforce</li> <li>■ I.e. Can't check last year events to send an invite out for this year's events</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>
--	---

	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>■ Standard process involved coordinating a global event           <ul style="list-style-type: none"> <li>● Gantt chart - Weekly meeting to track progress               <ul style="list-style-type: none"> <li>○ Note: Couple of years ago, used Trello, but only useful if people use it</li> <li>○ Initial venue plan, dates and prices</li> <li>○ Website setup for event</li> <li>○ Initial announcements</li> <li>○ Speakers/Activities Plan/Selections</li> <li>○ Review process</li> <li>○ Setup Program with information</li> <li>○ Marketing and promotion - sometimes PR company is used</li> <li>○ Social media/vertical responses/blog/mailling lists/events to promote own events</li> </ul> </li> <li>● Conference logistics - volunteers/coordinations</li> <li>■ Photographer/Video</li> <li>■ Survey, Signs, Program print on site</li> <li>■ Sponsorship handled by Kelly</li> </ul> </li> </ul> </li> </ul> </li> <li>● <b>Bookkeeping/ Accounting- Alison Shrader</b> <ul style="list-style-type: none"> <li>○ Primary tools used:           <ul style="list-style-type: none"> <li>■ Quickbooks, Salesforce, Registration tools               <ul style="list-style-type: none"> <li>● AR&amp;AP &amp; reconcile accounts</li> <li>● Personal input: Possibly not using Salesforce to best of abilities; wanting a centralized location for the registrations, bank deposits, event locations, donations, and transactions</li> <li>● Pain point:                   <ul style="list-style-type: none"> <li>○ Currently Quickbooks not linked up to Salesforce                       <ul style="list-style-type: none"> <li>■ Alison only has access</li> <li>■ Staff does not have access or view into this</li> <li>■ Needs to manually enter the information and keep track within Salesforce</li> <li>■ I.e. Local chapters with buckets of money and tracked via Quickbooks and Salesforce independently</li> <li>■ I.e. Event Registration:                           <ul style="list-style-type: none"> <li>● If paid with credit card online:                               <ul style="list-style-type: none"> <li>○ Payment gateway -&gt; processor -&gt; bank account -&gt; need to pull report from Gateway to show all transaction and pull report from Salesforce</li> </ul> </li> <li>● Synchronizing payment batch vs. transaction</li> <li>● Extremely time-consuming</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> <li>● <b>Operations Director/Salesforce Admin- Kate Hartmann</b> <ul style="list-style-type: none"> <li>○ Primary tools used:</li> </ul> </li> </ul> </li></ul>
--	---

	<ul style="list-style-type: none"><li>■ Salesforce, Wiki</li><li>■ Pain point: Connected few tools except Quickbooks</li></ul>
--	--

<b>Date</b>	<b>April 28, 2016</b>
<b>Location</b>	<b>Conference call</b>
<b>Subject</b>	<b>OWASP IT Interview Meeting</b>



<b>Participants</b>	<p><b>OWASP</b>  Kate Hartmann - Operations Director/Salesforce Administrator  Matt Tesauro - IT Administrator</p> <p><b>Sooryen Technologies</b>  Gin Cheng- Tech Lead  Ahsun Kim- Project Manager</p>
<b>Items</b>	
	<p><b>Objective and background:</b></p> <p>The purpose of the call was to review the underlying infrastructure of the OWASP website and walkthrough Salesforce. Specific focus was on hosting, performance, scalability, security, integration and upgradability.</p> <p><b><u>Key discussion items</u></b></p> <ul style="list-style-type: none"> <li>▪ <b>Walkthrough of Salesforce with Kate</b> <ul style="list-style-type: none"> <li>o Top 3 used Salesforce sections <ul style="list-style-type: none"> <li>▪ MemberNation</li> <li>▪ Salesforce Cases/Form Assembly</li> <li>▪ Events</li> </ul> </li> <li>o Pain points: <ul style="list-style-type: none"> <li>▪ Lack of visibility and communication to community, chapter leaders, project leaders despite open source and open community nature of OWASP <ul style="list-style-type: none"> <li>• Some specific pain points: <ul style="list-style-type: none"> <li>▪ Requires authentication to share information to certain parties</li> <li>▪ No communication between Salesforce and Wiki</li> <li>▪ Things in Salesforce have to be manually triggered <ul style="list-style-type: none"> <li>• I.e. Unspecific cases in FormAssembly have to be manually forwarded</li> </ul> </li> </ul> </li> <li>• Examples of what should automatically and securely be shared with community: <ul style="list-style-type: none"> <li>o Project visibility</li> <li>o Membership</li> <li>o Demographics statistics</li> <li>o Metrics on how many new chapters, projects were set up, etc.</li> <li>o Volunteers for Salesforce</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>▪ Opportunities to participate in the organization</li> </ul> </li> <li>○ <b>Note:</b> On hierarchy level- different amounts of information revealed to different positions</li> <li>○ Pain point:           <ul style="list-style-type: none"> <li>▪ Identifying how much information to divulge</li> </ul> </li> </ul> </li> <li>▪ Finding a suitable gamification systems/ platforms       <ul style="list-style-type: none"> <li>• Three alternatives considered           <ul style="list-style-type: none"> <li>○ ThinkSmartOne: Salesforce Gamification Tool</li> <li>○ Mozilla Badges</li> <li>○ Work.com</li> </ul> </li> <li>• Pain point: Needs to quantify/recognize volunteerism and be able to publish the information on/ integrate with Wiki without authentication</li> </ul> </li> <li>▪ Lack of identification method of an OWASP member such as owasp email, etc.</li> </ul> <ul style="list-style-type: none"> <li>▪ <b>Overview of IT with Matt:</b> <ul style="list-style-type: none"> <li>○ Management of owasp.org           <ul style="list-style-type: none"> <li>▪ Content-wise: Staff and project &amp; chapter leaders</li> <li>▪ Infrastructure: Matt</li> </ul> </li> <li>○ Count of extensions added to MediaWiki as of 2014: 44</li> <li>○ Version: <a href="https://www.owasp.org/index.php/Special:Version">https://www.owasp.org/index.php/Special:Version</a></li> <li>○ Media Temple for hosting Wordpress and AppSec2016 sites           <ul style="list-style-type: none"> <li>▪ Automatically patch MediaWiki</li> <li>▪ Pain point: Bad support time</li> </ul> </li> <li>○ Pain points:           <ul style="list-style-type: none"> <li>▪ No content strategy or architecture in place               <ul style="list-style-type: none"> <li>• No enforcement group of such</li> </ul> </li> <li>▪ No SEO done for OWASP</li> <li>▪ Little interaction with Google Analytics               <ul style="list-style-type: none"> <li>• To identify geographic location, what pages are being accessed, bounce rates, etc.</li> </ul> </li> </ul> </li> <li>○ Rackspace Overview:           <ul style="list-style-type: none"> <li>▪ Two cloud-based servers provided by Rackspace               <ul style="list-style-type: none"> <li>• [\$2000/month donation]</li> <li>• WikiWeb                   <ul style="list-style-type: none"> <li>○ Apache, MediaWiki software</li> </ul> </li> <li>• WikiDB                   <ul style="list-style-type: none"> <li>○ MariaDB- Database that holds all information from Wiki</li> </ul> </li> <li>• Used to be same server; split because high CPU load</li> </ul> </li> <li>▪ Monitoring by Cloud Monitoring by Rackspace               <ul style="list-style-type: none"> <li>• SSL certificate expiration &amp; HTTP Response Time                   <ul style="list-style-type: none"> <li>○ Originating requests come from London, Hong Kong, Dallas, Chicago</li> </ul> </li> <li>• Diskspace</li> <li>• CPU</li> <li>• Overall load on system</li> </ul> </li> <li>▪ Back up procedures for server/database failure               <ul style="list-style-type: none"> <li>• Server</li> </ul> </li> </ul> </li> </ul> </li> </ul>
--	--

	<ul style="list-style-type: none"><li><ul style="list-style-type: none"><li>o Weekly images of server</li><li>o Daily file backups/differentials</li></ul></li><li>• Database<ul style="list-style-type: none"><li>o Holland- Sequel dump of database</li></ul></li><li>▪ OWASP recovery time in case server is nuked: 1 hour<ul style="list-style-type: none"><li>• Pain point: Dependent on Matt's availability</li><li>• Rackspace has ability for autoscaling or DevOps (higher level of support)</li></ul></li><li>▪ No staging or dev servers<ul style="list-style-type: none"><li>• Due to lack of cost-effectiveness</li></ul></li><li>▪ No code repository in place for the mediawiki (core/extensions/customizations)</li><li>▪ Pain points:<ul style="list-style-type: none"><li>• Web Client Connection Refusal Errors<ul style="list-style-type: none"><li>o Banning those that rapidly click through the site to prevent site from going down<ul style="list-style-type: none"><li>▪ End up banning actual users</li></ul></li></ul></li><li>• Limitations of Matt being unable to update server due to 10-hour work weeks</li><li>• No formalized way of testing and automated testing if MediaWiki is working</li></ul></li></ul>
--	---

<b>Date</b>	<b>May 3, 2016</b>
<b>Location</b>	<b>Conference call</b>
<b>Subject</b>	<b>OWASP Builders Meeting</b>
<b>Participants</b>	<p><b>OWASP</b></p> <p>Kate Hartmann - Operations Director/Salesforce Administrator  Tom Brennan- Global Board Member  Aaron Weaver- Project Leader for AppSec Pipeline Project  Kevin W. Wall- Project Contributor for ESAPI Project</p> <p><b>Sooryen Technologies</b></p> <p>Gin Cheng- Tech Lead  Ahsun Kim- Project Manager  Ram Ganesan – CEO/ Co-Founder of Sooryen Technologies</p>
<b>Items</b>	
	<p><b>Objective and background:</b></p> <p>The purpose of the call was to evaluate the current needs for the OWASP task forces who are primarily involved with project implementation, tracking and documentation. As these task forces (or categories) have the most integration with the MediaWiki and are the main contributors to the OWASP projects and future growth, it is crucial to identify any dissatisfactions with the current platform and infrastructure in place for collaboration.</p> <p>The Sooryen team shared a Google document that contained the following information:</p> <ul style="list-style-type: none"> <li>● Objective, agenda and interview questions</li> </ul> <p><b>Key discussion items</b></p> <ul style="list-style-type: none"> <li>● Overview of task forces <ul style="list-style-type: none"> <li>○ Loose group of contributors who classify themselves as either builder, breaker, or defender</li> </ul> </li> <li>● Aaron Weaver <ul style="list-style-type: none"> <li>○ Created AppSec Pipeline project with Matt Tesauro <ul style="list-style-type: none"> <li>■ Creating tools that developers and defenders to use</li> <li>■ In early stages of project</li> </ul> </li> <li>○ Using MediaWiki for project course <ul style="list-style-type: none"> <li>■ Typically doesn't use other technology <ul style="list-style-type: none"> <li>● Trello, Slack, email</li> </ul> </li> </ul> </li> <li>○ Pain points with Builder Task Force being decentralized <ul style="list-style-type: none"> <li>■ Matt Konda's Pipeline Project- named similarly to AppSec Pipeline Project in similar time frame <ul style="list-style-type: none"> <li>● Merged together</li> </ul> </li> <li>■ Can easily create duplicate projects or be unaware of another project</li> </ul> </li> </ul> </li> <li>● Kevin Wall</li> </ul>

	<ul style="list-style-type: none"> <li>○ ESAPI project (started in 2008, joined in 2009)- Project leaders with Chris Schmidt <ul style="list-style-type: none"> <li>■ Joined when project was already set up on MediaWiki</li> <li>■ Used to be on Google code, moved to Github</li> <li>■ Initially envisioned as common interfaces across a variety of programming languages <ul style="list-style-type: none"> <li>● Provide a common set of APIs across different programming languages for various security controls (data validation, authorization, etc.)</li> <li>● Dozen implementation in different languages <ul style="list-style-type: none"> <li>○ Java, PHP, C-Programming, C++, Ruby, ColdFusion</li> <li>○ Many died out, what remains active is ESAPI for Java</li> </ul> </li> </ul> </li> <li>■ Difficult to obtain/retain volunteers for keeping updated with ESAPI for Java</li> <li>■ Discussions of how to revive project again (ESAPI 3.0) <ul style="list-style-type: none"> <li>● Micro-services driven</li> <li>● Not much momentum</li> </ul> </li> </ul> </li> <li>○ Primarily uses emailing list for communication <ul style="list-style-type: none"> <li>■ Less responsive group of volunteers compared to AppSec Pipeline project</li> </ul> </li> <li>○ Notices for new releases spread through Twitter, Google+, and updated on MediaWiki page <ul style="list-style-type: none"> <li>■ Pain point: Not effective enough, OWASP does not have same visibility that Apache does</li> <li>■ I.e. Feedback from Oracle that there were vulnerabilities when they had been fixed</li> <li>■ Even those with CVEs had not been updated</li> </ul> </li> <li>● Have you had any issues with starting a project following the MediaWiki process? <ul style="list-style-type: none"> <li>○ Aaron- not any particular issues <ul style="list-style-type: none"> <li>■ Templates not the easiest to edit</li> <li>■ Overall, for MediaWiki, difficult to find what you're looking for <ul style="list-style-type: none"> <li>● Reference to older documents that aren't valid</li> </ul> </li> </ul> </li> <li>○ Tom <ul style="list-style-type: none"> <li>■ Wiki's very difficult to navigate to start a project, information overload <ul style="list-style-type: none"> <li>● Provided link: <a href="https://docs.google.com/document/u/1/d/1ncNTj6C7Qllmxn_4LwgePt8eMRU7ZVLcbWFBZGfwmek/edit?usp=sharing">https://docs.google.com/document/u/1/d/1ncNTj6C7Qllmxn_4LwgePt8eMRU7ZVLcbWFBZGfwmek/edit?usp=sharing</a></li> </ul> </li> <li>■ Navigation is not intuitive</li> </ul> </li> </ul> </li> <li>● Have you had any issues with creating the MediaWiki for the project, maintaining it and allowing others to help contribute to it? <ul style="list-style-type: none"> <li>○ Aaron- Usability issues <ul style="list-style-type: none"> <li>■ Put information in Google Docs, mark it up, edit it, place it back in MediaWiki because MediaWiki isn't conducive to editing in real time</li> <li>■ In process of creating another site because of inflexibility of MediaWiki <ul style="list-style-type: none"> <li>● Basing it on Github</li> <li>● When putting in changes, put PR requests to track changes <ul style="list-style-type: none"> <li>○ Would get pushed out to site that's been created</li> </ul> </li> <li>● Driving traffic away from OWASP to new site</li> </ul> </li> </ul> </li> <li>○ Kevin <ul style="list-style-type: none"> <li>■ Multiple links from different tabs that link to the same thing; difficult to update</li> <li>■ Suggestion: To create template particularly for builders <ul style="list-style-type: none"> <li>● Where the source code is, where the binaries are deployed at, continuous build status, patches that have been done, where the Java dock is, if you have test cases, etc.</li> </ul> </li> <li>■ End up typically referring to Github main page <ul style="list-style-type: none"> <li>● Driving traffic away <ul style="list-style-type: none"> <li>○ Sometimes sees some wiki pieces hosted on Github wiki</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>
--	---

	<ul style="list-style-type: none"> <li>● Do you feel like there is a lack in process for funding, communication with other members and collaboration on the MediaWiki?       <ul style="list-style-type: none"> <li>○ Kevin           <ul style="list-style-type: none"> <li>■ Difficulty in sustaining volunteers rather than problems regarding the Wiki</li> </ul> </li> </ul> </li> <li>● As adjustments can be made to these templates per project, is the layout for the information consistent enough?       <ul style="list-style-type: none"> <li>○ Aaron           <ul style="list-style-type: none"> <li>■ Table format can easily be messed up</li> </ul> </li> </ul> </li> <li>● Is there sufficient documentation for on-going projects such that new volunteers can go through the material and potentially contribute?       <ul style="list-style-type: none"> <li>○ Kevin           <ul style="list-style-type: none"> <li>■ Yes, but not necessarily the fault of Wiki</li> <li>■ Certain expectation: Volunteers have to look at information provided on Github if they'd like to contribute</li> <li>■ Pain point:               <ul style="list-style-type: none"> <li>● Some pages that link back to Wiki that are kept out of date or were updated by people outside of project</li> <li>● First result for ESAPI on OWASP.org for a period of time was that ESAPI wasn't being maintained                   <ul style="list-style-type: none"> <li>○ ESAPI link was on 5th link</li> </ul> </li> <li>● Not realized that this is an issue until brought up by other people</li> </ul> </li> </ul> </li> </ul> </li> <li>● Do you believe there is enough visibility as to what projects the OWASP community is currently working on?       <ul style="list-style-type: none"> <li>○ Kevin           <ul style="list-style-type: none"> <li>■ Not enough visibility               <ul style="list-style-type: none"> <li>● Pain point: ESAPI was listed as flagship project for two years when there was virtually no activity on it (now a lab status)</li> </ul> </li> </ul> </li> <li>○ Tom           <ul style="list-style-type: none"> <li>■ Obscure- metrics that are being measured are not well-defined               <ul style="list-style-type: none"> <li>● I.e. Code commits, edits to a page, people who have self-assigned themselves to a project                   <ul style="list-style-type: none"> <li>○ At scale is a problem- how to manage globally; need to look at projects</li> </ul> </li> </ul> </li> <li>■ Default is to call everything a project</li> </ul> </li> </ul> </li> <li>● Recommendations for how to pair down the main project page (<a href="https://www.owasp.org/index.php/OWASP_Project_Inventory">https://www.owasp.org/index.php/OWASP_Project_Inventory</a>)       <ul style="list-style-type: none"> <li>○ Aaron           <ul style="list-style-type: none"> <li>■ Simplification needed               <ul style="list-style-type: none"> <li>● I.e. what exactly is the purpose of the icons</li> </ul> </li> <li>■ Purpose of page unclear               <ul style="list-style-type: none"> <li>● I.e. Is this page for people who are trying to start a project/ is this a project inventory</li> </ul> </li> <li>■ For starting a project, there should be a clearly defined set of instructions</li> <li>■ For project inventory, seems static- would like to be dynamic</li> </ul> </li> <li>○ Tom           <ul style="list-style-type: none"> <li>■ Adding visuals to help with this message</li> <li>■ Suggestion: Setting up a fake project to figure out where to go from here</li> </ul> </li> <li>○ Kevin</li> </ul> </li> </ul>
--	---

	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>■ Looking at list of archived projects, shows OWASP having difficulty maintaining projects</li> </ul> </li> <li>● Regarding Builders giving to foundation           <ul style="list-style-type: none"> <li>○ Notes need to be made regarding license assignment process that's meaningful</li> <li>○ Giving funding to projects               <ul style="list-style-type: none"> <li>■ More than one project leader needed to give cross-validation for approval of expenses</li> <li>■ Insight for where workflow is going: <a href="https://docs.google.com/document/u/1/d/1ncNTj6C7Qllmxn_4LwgePt8eMRU7ZVLcbWFBZGfwmek/edit?usp=sharing">https://docs.google.com/document/u/1/d/1ncNTj6C7Qllmxn_4LwgePt8eMRU7ZVLcbWFBZGfwmek/edit?usp=sharing</a></li> </ul> </li> </ul> </li> <li>● In your opinion, are the code repositories for existing projects well maintained (well-known, well-publicized, standardized)?           <ul style="list-style-type: none"> <li>○ Tom               <ul style="list-style-type: none"> <li>■ Standard has changed from:                   <ul style="list-style-type: none"> <li>● Google Code -&gt; SourceForge -&gt; GitHub</li> <li>● Many repositories</li> <li>● No agreed up process for standardization</li> <li>● Recommendation from community for standardization for flagship projects to require a certain repository:                       <ul style="list-style-type: none"> <li>○ Currently is GitHub</li> </ul> </li> </ul> </li> </ul> </li> <li>○ Kevin               <ul style="list-style-type: none"> <li>■ No standard practice maintaining repositories, branches, etc.                   <ul style="list-style-type: none"> <li>● Some smaller projects have default branch as master branch</li> <li>● Should allow flexibility to an extent, but for flagship projects, should be standardized</li> </ul> </li> <li>■ Releases can be held up by lack of tool-specific expertise                   <ul style="list-style-type: none"> <li>● Suggestion: Having subject matter expert in their expertise available to help people out</li> <li>● Tom's suggestion- Senior project coordinator; filming relevant videos</li> </ul> </li> </ul> </li> <li>○ Suggestion: Videos for certain content to be more engaging               <ul style="list-style-type: none"> <li>■ Have to be conscientious of global audience</li> </ul> </li> <li>○ Aaron               <ul style="list-style-type: none"> <li>■ Pain point: Not really seeing enforcement or standards                   <ul style="list-style-type: none"> <li>● Suggestion: Having someone reach out for project updates, etc.                       <ul style="list-style-type: none"> <li>○ Potentially fulfilled by senior project coordinator</li> </ul> </li> <li>● Used to have project assessment</li> </ul> </li> </ul> </li> </ul> </li> <li>● Can you name other websites that are doing something similar in a better manner? What websites should OWASP mirror?           <ul style="list-style-type: none"> <li>○ Taking as action item</li> <li>○ <b>Asking as micro-surveys (~3 questions)</b> <ul style="list-style-type: none"> <li>■ Asking task forces</li> <li>■ Asking sponsors</li> </ul> </li> </ul> </li> <li>● Suggestion of main page as face for OWASP           <ul style="list-style-type: none"> <li>○ May present as hindrance to technical users</li> <li>○ To be conscious of mobile access</li> </ul> </li> <li>● Google works better than search engine on MediaWiki           <ul style="list-style-type: none"> <li>○ MediaWiki search relies on keywords, Google works better with help of cross-referencing</li> </ul> </li> <li>● Any suggested tools, website extensions from a community or builder's perspective?</li> </ul> </li></ul>
--	--

	<ul style="list-style-type: none"> <li>○ Currently for tickets- Salesforce, JIRA           <ul style="list-style-type: none"> <li>■ Kevin- Suggesting standardization for tickets               <ul style="list-style-type: none"> <li>● Partly a branding perspective- Seen for Apache</li> <li>● Synchronizing closing bugs</li> </ul> </li> <li>■ Atlassian toolset licensed for entire suite               <ul style="list-style-type: none"> <li>● Not yet rolled out, experimented with by project reviewers</li> <li>● Have to ensure that staff can utilize/manage it</li> </ul> </li> <li>■ Although flexibility could be allowed, more standardization for flagship projects</li> </ul> </li> </ul>
--	---

<b>Date</b>	<b>May 10, 2016</b>
<b>Location</b>	<b>Conference call</b>
<b>Subject</b>	<b>OWASP Defenders Meeting</b>
<b>Participants</b>	<p><b>OWASP</b>          Kate Hartmann - Operations Director/Salesforce Administrator          Nikola Milosevic - Project Leader for SeraphimDroid project/OWASP Manchester Chapter Leader          Gabriel Gumbs - Project Leader for OWASP Application Security Program Quick Start Guide          Haral Tsitsivas - Chapter Leader for OWASP Orange County, CA</p> <p><b>Sooryen Technologies</b>          Gin Cheng - Tech Lead          Ahsun Kim - Project Manager          Ram Ganesan - CEO/ Co-Founder of Sooryen Technologies</p>
	<b>Items</b>
	<p><b>Objective and background:</b></p> <p>The purpose of the call was to evaluate the current needs for the OWASP task forces who are primarily involved with project implementation, tracking and documentation. As these task forces (or categories) have the most integration with the MediaWiki and are the main contributors to the OWASP projects and future growth, it is crucial to identify any dissatisfactions with the current platform and infrastructure in place for collaboration.</p> <p>The Sooryen team shared a Google document that contained the following information:</p> <ul style="list-style-type: none"> <li>● Objective, agenda and interview questions</li> </ul>



**Key discussion items**

- Have you had any issues with starting a project following the MediaWiki process?
  - Nikola
    - Didn't have much trouble except with mark ups, getting right template
  - Gabriel
    - Didn't have problems
- Have you had any issues with creating the MediaWiki for the project, maintaining it and allowing others to help contribute to it?
  - Nikola
    - Modifying directly on MediaWiki
      - Most of other members' contribution goes through GitHub
      - Nikola modifies MediaWiki once that is done
  - Gabriel
    - Didn't have problems
- Do you feel like there is a lack in process for funding, communication with other members and collaboration on the MediaWiki?
  - Gabriel
    - Process for funding not clear
  - Nikola
    - Content is outdated, difficult to know what's happening
    - Main source of information regarding the community: mailing list
- Do you feel the current templates in place for projects are sufficient for your needs? As adjustments can be made to these templates per project, is the layout for the information consistent enough?
  - Nikola
    - Templates look old in terms of design
    - Content seems sufficient
  - Gabriel
    - Didn't know existence of templates in beginning
      - Did mostly from scratch; borrowed elements from other projects
    - Templates seem outdated; don't lend themselves to consuming information
- Would it be helpful to have a template specifically for defenders? What would be on it?
  - Gabriel
    - Too broad of a distinction
      - Defender projects can be broken down in documentation and code-based
        - Recommendation to split template this way
        - Code
          - Application is involved
        - Documentation
          - No actual code, maybe code snippets
          - Documenting a process or procedure for application security
        - Code and documentation- Can be split
  - Nikola
    - More content for documentation than code-based projects
- Haral- Not involved in current OWASP project

- As adjustments can be made to these templates per project, is the layout for the information consistent enough?
  - Nikola
    - Certain information/ paragraphs needed to be added that were important to
    - Added new tabs that weren't in template
    - Incubator-project
    - Tried to develop some of best-shaped template/page to suit project
      - Required some work
- Is there sufficient documentation for on-going projects such that new volunteers can go through the material and potentially contribute?
  - Nikola
    - Depends on the project
  - Gabriel
    - Documentation- Not necessarily what's necessary
    - Layout of information in general doesn't lend itself well to someone new to explore all OWASP projects
      - I.e. On front page, flagship projects are highlighted
      - Beyond that, locating another project based on need or interest is more difficult
- Do you believe there is enough visibility as to what projects the OWASP community is currently working on?
  - Nikola
    - Huge problem with graduation of project
    - Used to be a task force that reviewed and ran through projects, but the task force no longer exists
      - Cannot get to lab stage because that task force doesn't exist; remains in incubator stage
    - Less visibility as a result, because not at that level
  - Gabriel
    - Outside of flagship projects, not enough visibility
    - When looking at flagship projects, typically geared towards technology
      - Less regarding business side of application security
      - Self-segregating from overall mission of promotion of application security
      - May be because the task force no longer exists
        - However, task force mostly was comprised of technophiles
- In your opinion, are the code repositories for existing projects well maintained?
  - Gabriel and Nikola
    - Depends on the project
  - Thoughts on standardizing code repositories for flagship projects
    - Nikola
      - Might be difficult to require older projects to maintain one main code repository
      - Should have same methodology to follow from beginning of projects
    - Gabriel
      - Standardization for all types of projects
- Did you have trouble collaborating with others on projects?

- Gabriel
  - OWASP lacks platform to put out request for people with certain skill sets
  - People not organically joining to work on the project
- Nikola
  - Some collaborators come through programs
  - Those who initially were motivated by money and remained on the project as volunteers
- What are some tools that you would suggest to help you streamline the process?
  - Nikola
    - Not currently using anything for testing
  - Gabriel
    - A mechanism/ board to initially introduce people into projects to find volunteers
- Was there a rationale behind choosing Github over Bitbucket? Is there a preference in the community for either or?
  - Gabriel
    - Traction, been around longer, familiarity
- In the last six months, how often have you visited the OWASP website?
  - Haral
    - As chapter leader, often for resources
  - Nikola
    - Weekly
    - Updating chapter page, personal page
    - Accessing funding, etc.
    - Doesn't access the front page
  - Gabriel
    - Not often
    - People involved heavily in chapters or new visitors to the website
    - Front page's information should be more organized, more visually appealing
- Thoughts on separating OWASP wiki with home page itself?
  - Gabriel
    - Mandatory
- What information belongs on the home page?
  - Gabriel
    - Things about organizational information: mission, members, finding local members
    - Should have back linking
    - Should lend itself to members and projects
- Some examples of well laid-out websites that
  - Gabriel
    - <https://www.isaca.org/Pages/default.aspx>
    - <http://www1.nyc.gov/>
  - Nikola
    - <https://www.mozilla.org/en-US/>
  - Haral
    - <https://www.issa.org/>
- Can you identify a representative group of resources that you as a defender use?
  - Nikola

- Couple of related projects
        - OWASP mobile projects, top 10 projects
      - OWASP project handbook, funding, presentation templates
    - Gabriel
      - Top 10 privacy, more so documentation projects
  - How often has the main page for OWASP defenders been maintained and are there other pieces of information that you would like to see there?
    - Nikola
      - No
      - Short description, name of projects, mission statements, links to actual project page, download links
    - Gabriel & Haral
      - Didn't know of its existence
      - Gabriel:
        - Seems too technically geared
        - More inclusiveness on overall life cycle of application security
  - Is there something missing from the OWASP website that you were expecting?
    - Gabriel
      - Better organization and presentation
    - Nikola
      - Organization is main issue
      - Not enough linking to projects on pages like the OWASP defenders website
  - Are the core MediaWiki functionalities (editing running documentations) intuitive and easy to use?
    - Gabriel
      - Was easy to use because familiar with it
      - Maybe something more CMS style
    - Nikola
      - Was easy to use because familiar with it
  - Have you had trouble finding information you are looking for? Is the information layout consistent such that you can easily locate relevant information to you?
    - Gabriel
      - No trouble finding information
      - Issue discovering new information
    - Nikola
      - Some trouble finding information- especially specific information
        - How to submit funding requests- multiple different pages with conflicting information due to being written by different groups
  - On a scale of 1-10, please rate your overall impression of the OWASP website.
    - Gabriel
      - 3.5
    - Nikola
      - 5
    - Haral
      - 4 or 5- Not the easiest to find information
  - Is there certain information that you believe should be more transparent for the community to evaluate such as membership demographics?
    - Gabriel

	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>■ Information that should be easily accessible, but not necessarily emphasized</li> </ul> </li> <li>○ Nikola           <ul style="list-style-type: none"> <li>■ How active are certain chapters, how many members attend the events</li> <li>■ How active projects are, how many contributors do they have</li> </ul> </li> </ul> </li> <li>● What is your thought on gamification or badging for users on the website?       <ul style="list-style-type: none"> <li>○ Gabriel           <ul style="list-style-type: none"> <li>■ Focus on website redesign is important</li> <li>■ Bad gamification will turn away certain users</li> <li>■ Salesforce gamification</li> </ul> </li> <li>○ Nikola           <ul style="list-style-type: none"> <li>■ Not in favor, because gamification</li> <li>■ Used to have badges, but didn't correlate with status of project</li> <li>■ Shouldn't be for short-term tasks</li> </ul> </li> </ul> </li> <li>● What are other technology tools that would benefit your task force or the OWASP community in general in addition to this website or an extension to it?       <ul style="list-style-type: none"> <li>○ Gabriel           <ul style="list-style-type: none"> <li>■ Not necessarily in need of new tools, just mostly improvements to the website itself</li> <li>■ Possibly going from Wiki to CMS</li> </ul> </li> </ul> </li> </ul>
--	--

<b>Date</b>	<b>May 17, 2016</b>
<b>Location</b>	<b>Conference call</b>
<b>Subject</b>	<b>OWASP Chapter and Project Leaders Interview Meeting</b>

<b>Participants</b>	<p><b>OWASP</b></p> <p>Kate Hartmann - Operations Director/Salesforce Administrator  Aaron Weaver - Project Leader for AppSec Pipeline Project, Chapter Leader for OWASP Philadelphia, PA  Oana Cornea - Chapter Leader for OWASP Bucharest, Romania  Haral Tsitsivas - Chapter Leader for OWASP Orange County, CA  Edgar David Salazar - Chapter Leader for OWASP Venezuela</p> <p><b>Sooryen Technologies</b></p> <p>Gin Cheng - Tech Lead  Ahsun Kim - Project Manager  Ram Ganesan - CEO/ Co-Founder of Sooryen Technologies</p>
<b>Items</b>	
	<p><b>Objective and background:</b></p> <p>The purpose of the call was to evaluate the current needs for the OWASP chapter and project leaders who are primarily involved with initiating, managing and promoting the OWASP organization through their works. As these groups have the most direct contact with engaged volunteers, it is crucial to identify any dissatisfactions with the current platform, infrastructure, and measures in place to encourage collaboration and outreach.</p> <p>The Sooryen team shared a Google document that contained the following information:</p> <ul style="list-style-type: none"> <li>• Objective, agenda and interview questions</li> </ul> <p><b>Key discussion items</b></p> <ul style="list-style-type: none"> <li>• What are some tools that you are currently using for meeting setups? On average, how many members show per meeting? What other outreach efforts have you undertaken? <ul style="list-style-type: none"> <li>○ Aaron <ul style="list-style-type: none"> <li>■ Registration <ul style="list-style-type: none"> <li>• Eventbrite</li> <li>• Talked about switching over Meetup</li> </ul> </li> <li>■ For social updating and status: Buffer- Schedule tweets on OWASP Philadelphia handle</li> <li>■ Posting on LinkedIn group</li> <li>■ 15-30 members</li> <li>■ Outreach efforts: Cross meetups with local security chapters <ul style="list-style-type: none"> <li>• Startup Security Group, ISSA, Secure World, etc.</li> </ul> </li> </ul> </li> <li>○ Haral <ul style="list-style-type: none"> <li>■ Meetup</li> <li>■ LinkedIn</li> <li>■ Local ISSA page, bringing up OWASP at local ISSA meeting</li> <li>■ 40-60 people</li> </ul> </li> <li>○ Oana <ul style="list-style-type: none"> <li>■ 20 people</li> <li>■ EventBrite or mailing list, Facebook</li> <li>■ Partnership with DevTalks, Agile Talks</li> </ul> </li> </ul> </li> <li>• How are you managing member retention, engagements, identifying paying and non-paying members? <ul style="list-style-type: none"> <li>○ Oana <ul style="list-style-type: none"> <li>■ Hard to identify paying and nonpaying member</li> </ul> </li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>■ Advertises membership whenever has a chance           <ul style="list-style-type: none"> <li>● Only one paying member</li> </ul> </li> <li>■ People come for content</li> </ul> </li> <li>○ Aaron           <ul style="list-style-type: none"> <li>■ Don't track paying vs nonpaying members           <ul style="list-style-type: none"> <li>● Would be nice to track it</li> </ul> </li> <li>■ Doesn't particularly push OWASP membership due to lack of tangible benefit for membership</li> <li>■ Member retention: Core group           <ul style="list-style-type: none"> <li>● Will show up for topic</li> </ul> </li> </ul> </li> <li>○ Haral           <ul style="list-style-type: none"> <li>■ Don't track paying vs nonpaying members</li> <li>■ Promotes membership time to time</li> <li>■ Local chapters put together yearly conference</li> </ul> </li> </ul> </li> <li>● What are some data points that you would like to see on your chapter Mediawiki page (Such as demographics, paying/non-paying, project contributors, etc.)?       <ul style="list-style-type: none"> <li>○ Aaron           <ul style="list-style-type: none"> <li>■ Uses Mediawiki out of requirement</li> <li>■ Links next chapter notice</li> <li>■ Pain point: Would prefer for it to be automated</li> <li>■ Data points: Integration with Social Media           <ul style="list-style-type: none"> <li>● When promoting event, people coming through EventBrite, LinkedIn, Twitter</li> <li>● Not only scheduling, but if certain topics brought in more people</li> </ul> </li> <li>■ Pain point: Using multiple tools to get what you're looking for           <ul style="list-style-type: none"> <li>● Have to pay more for more advanced features on Buffer</li> <li>● Would be beneficial to identify a series of tools to make this process more streamlined</li> </ul> </li> </ul> </li> <li>○ Haral           <ul style="list-style-type: none"> <li>■ Doesn't use page- everything done via Meetup           <ul style="list-style-type: none"> <li>● Meeting notices, discussions, presentations</li> </ul> </li> <li>■ Meetup used to send emails to people who signed up, people who attended a specific meeting, cross-promotion of security groups in area</li> </ul> </li> <li>○ Oana           <ul style="list-style-type: none"> <li>■ Uses Wiki to post meetings</li> <li>■ Data points: Project contributors, chapter supporters</li> </ul> </li> </ul> </li> <li>● What would assist your efforts in outreach that is currently not being provided by OWASP?       <ul style="list-style-type: none"> <li>○ Aaron           <ul style="list-style-type: none"> <li>■ Upgraded tooling</li> <li>■ Would be nice to have it centralized</li> </ul> </li> <li>○ Oana           <ul style="list-style-type: none"> <li>■ To have an example of a press release</li> <li>■ Upgraded tooling</li> </ul> </li> <li>○ Haral           <ul style="list-style-type: none"> <li>■ Potentially a twitter channel about all the meetings/Meetups with blurbs about presentation to raise visibility</li> </ul> </li> </ul> </li> <li>● In your opinion, are the code repositories for existing projects well maintained?       <ul style="list-style-type: none"> <li>○ Oana           <ul style="list-style-type: none"> <li>■ Not really</li> </ul> </li> </ul> </li> </ul>
--	---

	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>■ May have multiple places for where project code repositories are maintained where some are out of date</li> </ul> </li> </ul> </li> <li>● In your opinion, how likely is centralizing project code repositories onto specific accounts (OWASP Account)?       <ul style="list-style-type: none"> <li>○ Aaron           <ul style="list-style-type: none"> <li>■ Need to have definite upside for bringing it to OWASP project code repositories</li> </ul> </li> </ul> </li> <li>● Have you had issues getting subject matter experts' opinions/volunteers for specific projects? What changes on the OWASP site do you believe would help facilitate this?       <ul style="list-style-type: none"> <li>○ Aaron           <ul style="list-style-type: none"> <li>■ No, relies on connections to people within community</li> <li>■ Would be good to spotlight certain projects               <ul style="list-style-type: none"> <li>● Connector tries to do some of this</li> </ul> </li> <li>■ Volunteer board to have people be able to pick on a task and work on it</li> </ul> </li> <li>○ Oana           <ul style="list-style-type: none"> <li>■ Advertises projects</li> <li>■ People question benefits of volunteering for specific projects</li> <li>■ Asks people to subscribe to mailing list, but would potentially be beneficial for people to see discussions regarding this</li> </ul> </li> </ul> </li> <li>● Do you believe there is enough visibility as to what projects the OWASP community is currently working on? What should be the project promotion criteria on website?       <ul style="list-style-type: none"> <li>○ Aaron           <ul style="list-style-type: none"> <li>■ Wiki is static</li> <li>■ Unaware of OWASP OpenHub- could highlight the metrics on there on the OWASP MediaWiki</li> </ul> </li> <li>○ Oana &amp; Haral           <ul style="list-style-type: none"> <li>■ Unaware of OWASP OpenHub</li> </ul> </li> </ul> </li> <li>● In the last six months, how often have you visited the OWASP website?       <ul style="list-style-type: none"> <li>○ Oana           <ul style="list-style-type: none"> <li>■ Daily basis for references for work, to update chapter meetings, et.c</li> </ul> </li> <li>○ Haral           <ul style="list-style-type: none"> <li>■ Couple times a month to look for information on vendor sponsorships, current budget information for chapter, etc.</li> </ul> </li> </ul> </li> <li>● Is there something missing from the OWASP website that you were expecting?       <ul style="list-style-type: none"> <li>○ Haral           <ul style="list-style-type: none"> <li>■ Chapter sponsors- What is difference between 3 vendor levels?</li> </ul> </li> </ul> </li> <li>● Are the core MediaWiki functionalities (editing running documentations - ongoing editing and creation of content) intuitive and easy to use?       <ul style="list-style-type: none"> <li>○ Oana           <ul style="list-style-type: none"> <li>■ Not initially; would likely to be difficult to use for someone new</li> </ul> </li> <li>○ Haral           <ul style="list-style-type: none"> <li>■ May be better to have non-Wiki portal for general public to find and look for things               <ul style="list-style-type: none"> <li>● Note: Disadvantage of potentially looking messy</li> </ul> </li> </ul> </li> </ul> </li> <li>● On a scale of 1-10, please rate your overall impression of the OWASP website.       <ul style="list-style-type: none"> <li>○ Haral           <ul style="list-style-type: none"> <li>■ 5</li> </ul> </li> <li>○ Oana           <ul style="list-style-type: none"> <li>■ 7</li> </ul> </li> <li>○ Aaron</li> </ul> </li> </ul>
--	--



	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>■ 4-5                             <ul style="list-style-type: none"> <li>● Issues with content and searchability</li> </ul> </li> </ul> </li> </ul> </li> <li>● What other platforms do you suggest in place of Mediawiki?             <ul style="list-style-type: none"> <li>○ Aaron                 <ul style="list-style-type: none"> <li>■ Something easy to publish</li> <li>■ More social aspects</li> </ul> </li> </ul> </li> <li>● What other improvements would you like to see with OWASP's frontend facelift?             <ul style="list-style-type: none"> <li>○ Aaron                 <ul style="list-style-type: none"> <li>■ Needs to be more aesthetically pleasing</li> <li>■ Improvements for usability</li> </ul> </li> <li>○ Haral                 <ul style="list-style-type: none"> <li>■ Having the portal be more attractive, better public facing home page</li> </ul> </li> <li>○ Oana                 <ul style="list-style-type: none"> <li>■ Issues with searchability/ ease of accessing information</li> <li>■ Derives from MediaWiki</li> </ul> </li> </ul> </li> <li>● What is your thought on gamification or badging for users on the website? What is your opinion on a stackoverflow-like implementation for the OWASP wiki to facilitate better communication and badging/gamification?             <ul style="list-style-type: none"> <li>○ Oana                 <ul style="list-style-type: none"> <li>■ Good idea- Would be more dynamic</li> </ul> </li> <li>○ Aaron                 <ul style="list-style-type: none"> <li>■ Good idea- May increase volunteer participation</li> <li>■ Top contributors may potentially be get a free ticket to regional OWASP event</li> </ul> </li> <li>○ Haral                 <ul style="list-style-type: none"> <li>■ Should have different portal for general community vs. those participating in projects</li> </ul> </li> </ul> </li> <li>● Aaron             <ul style="list-style-type: none"> <li>○ Would potentially encourage volunteers if you could link accounts together so that there was one less sign up to go through</li> </ul> </li> <li>● What do you believe would drive OWASP community engagement on the site?             <ul style="list-style-type: none"> <li>○ Aaron                 <ul style="list-style-type: none"> <li>■ Unification on tools</li> <li>■ Not necessarily mandating tools, but still encouraging project leaders/ chapter leaders to use it by setting up/integrating a tool so that things would automatically get updated on community site</li> <li>■ When joining different projects, people would be less likely to have to pick up a new set of tools for each project</li> </ul> </li> </ul> </li> <li>● Note: Edgar David Salazar sat in on the call, but could not verbally participate.</li> </ul>
--	---

<b>Date</b>	<b>May 19, 2016</b>
<b>Location</b>	<b>Conference call</b>

<b>Subject</b>	<b>OWASP Chapter and Project Leaders Interview Meeting</b>
<b>Participants</b>	<p><b>OWASP</b>  Kate Hartmann - Operations Director/Salesforce Administrator  Tom Brennan - Chapter Leader for OWASP New York/New Jersey  Colin Watson - Project Leader for AppSensor, Cornucopia, Project Threats, Snakes &amp; Ladders</p> <p><b>Sooryen Technologies</b>  Gin Cheng - Tech Lead  Ahsun Kim - Project Manager  Ram Ganesan - CEO/ Co-Founder of Sooryen Technologies</p>
<b>Items</b>	
	<p><b>Objective and background:</b></p> <p>The purpose of the call was to evaluate the current needs for the OWASP chapter and project leaders who are primarily involved with initiating, managing and promoting the OWASP organization through their works. As these groups have the most direct contact with engaged volunteers, it is crucial to identify any dissatisfactions with the current platform, infrastructure, and measures in place to encourage collaboration and outreach.</p> <p>The Sooryen team shared a Google document that contained the following information:</p> <ul style="list-style-type: none"> <li>● Objective, agenda and interview questions</li> </ul> <p><b>Key discussion items</b></p> <ul style="list-style-type: none"> <li>● What are some tools that you are currently using for meeting setups? On average, how many members show per meeting? What other outreach efforts have you undertaken? - <ul style="list-style-type: none"> <li>○ Colin <ul style="list-style-type: none"> <li>■ Don't use any tools for meeting setups: not chapter leader.</li> </ul> </li> <li>○ Tom <ul style="list-style-type: none"> <li>■ Using the OS Foundation Google Work account that incorporates email, forums, Google groups, surveys, hangouts.</li> <li>■ Use Meetup for meeting management</li> <li>■ Also use GoToWebinar or GoToMeeting</li> </ul> </li> </ul> </li> <li>● On average, how many members show up per meeting? <ul style="list-style-type: none"> <li>○ Tom <ul style="list-style-type: none"> <li>■ Difficult to say due to variation (online meeting, vs in-person meeting, varying time zones), but New York meetings regularly exceed fire code (178 people one night)</li> </ul> </li> </ul> </li> <li>● What other outreach efforts have you undertaken? <ul style="list-style-type: none"> <li>○ Tom <ul style="list-style-type: none"> <li>■ Empower local members to speak at local events, conferences, provide free education about OSF materials, in addition to having chapter meetings.</li> </ul> </li> </ul> </li> <li>● How are you managing member retention, engagements, identifying paying and non-paying members? <ul style="list-style-type: none"> <li>○ List of members is available on the website. Quarterly, we check how many people join/leave. In person, check to see who has bags (indicating member), and see if people who don't hold bags are willing to join</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>● What are some data points that you would like to see on your chapter Mediawiki page (Such as demographics, paying/non-paying, project contributors, etc.)?       <ul style="list-style-type: none"> <li>○ Tom           <ul style="list-style-type: none"> <li>■ Every individual who is a member of the organization               <ul style="list-style-type: none"> <li>● Having their demographics is important</li> </ul> </li> <li>■ If they are a chapter leader or project leader, need to know leader of what</li> <li>■ Important to have this information public facing such that the people who are contributing are recognized, and can be celebrated on an annual basis</li> </ul> </li> </ul> </li> <li>● What are some changes you would like to see on the Mediawiki or chapter pages?       <ul style="list-style-type: none"> <li>○ Tom           <ul style="list-style-type: none"> <li>■ Mediawiki- a total failure for the purposes of chapters</li> <li>■ Something as simple as the "what you see is what you get" (WYSIWYG) editor in the Mediawiki not been done               <ul style="list-style-type: none"> <li>● Been asked for, for 3 years</li> <li>● Makes it difficult for users to edit the wiki, as users who are managing chapters are not technical</li> <li>● People trying to organize community efforts may have difficulties with using the Wiki editor                   <ul style="list-style-type: none"> <li>○ Makes the barrier to entry high.</li> </ul> </li> </ul> </li> <li>■ Need to recognize that we are targeting non-technical people for chapter pages               <ul style="list-style-type: none"> <li>● Chapters should be manage by a managed database system where information is inputted once, such as Excel spreadsheets</li> <li>● Data would be much easier to check if in a database for each chapter, which could be checked and updated easily</li> <li>● Too many chapters are moving towards Meetup because of their frustration with the Wiki, and this change is important to the success of the project</li> </ul> </li> </ul> </li> </ul> </li> <li>● What would assist your efforts in outreach that is currently not being provided by OWASP?       <ul style="list-style-type: none"> <li>○ Tom           <ul style="list-style-type: none"> <li>■ OWASP has a poor approach to the purposes of public relations</li> <li>■ Do not have skilled public relations who are communicating to the global community in a global way</li> <li>■ i.e., was asked, "Did you read the global announcement regarding the global elections that are coming up?"               <ul style="list-style-type: none"> <li>● Read like it was written by someone who was from the big city, and didn't have a sense of driving the community globally                   <ul style="list-style-type: none"> <li>○ Need to be aware of how we're talking to people.</li> </ul> </li> </ul> </li> <li>■ OWASP needs a public relations group to communicate better to the audience               <ul style="list-style-type: none"> <li>● Not every organization of individual comes from a metropolitan area, and we need to do better at speaking to people from all different areas (3rd world country, small town, etc.)</li> <li>● OWASP does not have any marketing professionals, and it is a severe deficiency.</li> </ul> </li> </ul> </li> </ul> </li> <li>● In your opinion, how likely is centralizing project code repositories onto specific accounts (OWASP Account)? What are the main friction points you anticipate for this?</li> </ul>
--	--

	<ul style="list-style-type: none"> <li>○ Colin <ul style="list-style-type: none"> <li>■ Only project involved with is using Github</li> <li>■ Using coleader John Melton's account</li> <li>■ Not very involved in code repositories, so would be better to ask other people <ul style="list-style-type: none"> <li>● Involved primarily in documentation</li> <li>● Uploads everything (source files, etc.) onto the wiki.</li> </ul> </li> </ul> </li> <li>○ Tom <ul style="list-style-type: none"> <li>■ If going to dictate to a global community on how to unlock features, money, public relations, then OWASP can define terms of that relationship</li> <li>■ If people want to work with the foundation, must meet certain criteria</li> <li>■ Can be done by communicating the value of the best practice and suggesting that the current practice is to assist <ul style="list-style-type: none"> <li>● Cannot be very Draconian and say "You must do this"</li> <li>● Would make the community try to work around the rules.</li> </ul> </li> <li>■ Define the process and then sell it internally in order to build momentum <ul style="list-style-type: none"> <li>● Previously used Google Code for repositories</li> <li>● Due to changes, should say "OWASP prefers these standards" but cannot dictate to audience that they must do a certain thing without making it easy for them.</li> </ul> </li> </ul> </li> <li>● Have you had issues getting subject matter experts' opinions/volunteers for specific projects? <ul style="list-style-type: none"> <li>○ Colin <ul style="list-style-type: none"> <li>■ Always a need to get more people involved, so yes</li> </ul> </li> <li>○ Tom <ul style="list-style-type: none"> <li>■ Yes, global aspect of the community means a lack of a centralized hub</li> <li>■ Can incentivize users from joining when they don't feel that they know what the exact goals are and are no longer talking face to face.</li> </ul> </li> </ul> </li> <li>● What changes on the OWASP site do you believe would help facilitate this? <ul style="list-style-type: none"> <li>○ Colin <ul style="list-style-type: none"> <li>■ Perhaps who visit the website believe they are not experts or that they could not contribute adequately <ul style="list-style-type: none"> <li>● However, most people generally able to contribute in at least some area</li> </ul> </li> </ul> </li> <li>○ Tom <ul style="list-style-type: none"> <li>■ Website can be streamlined by taking the user into account</li> <li>■ Must take a list of the different kinds of users, and then prioritize the features for each of the users</li> <li>■ Better idea would be to have a project newsletter go out monthly like OWASP connector but just on projects</li> <li>■ Better organization on the wiki divided into categories like: <ul style="list-style-type: none"> <li>● Project Admin, Projects Promotions, Projects needing help, Project of the month, OWASP projects statics.</li> </ul> </li> </ul> </li> </ul> </li> <li>● Do you believe there is enough visibility as to what projects the OWASP community is currently working on? What should be the project promotion criteria on website? <ul style="list-style-type: none"> <li>○ Colin <ul style="list-style-type: none"> <li>■ Project that is being worked on now is not being highlighted very well <ul style="list-style-type: none"> <li>● While some projects are being highlighted, everything is in a big bucket</li> </ul> </li> </ul> </li> </ul> </li> </ul>
--	--

	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>• Can be difficult to highlight significant projects.</li> </ul> </li> <li>■ Not necessarily best to highlight the most active projects, as different people will gravitate towards to different projects           <ul style="list-style-type: none"> <li>• Would want to encourage people to look at active projects rather than ones that haven't been looked at in a while.</li> </ul> </li> <li>■ However, it can also be good to look at projects that need some initiative or a project leader. So there is not much need to change the current criteria.</li> </ul> </li> <li>○ Tom       <ul style="list-style-type: none"> <li>■ Poor marketing and poor communication</li> <li>■ Should:           <ul style="list-style-type: none"> <li>• Highlight project of the month/quarter</li> <li>• Celebrate things at our conferences to celebrate projects that hit a milestone or just graduated/started.</li> </ul> </li> <li>■ Natural stages of evolution are:           <ul style="list-style-type: none"> <li>• Idea (incubator)</li> <li>• Lab (roadmap, getting things off the ground)</li> <li>• Release (natural progression that can be measured/celebrated/understood)</li> </ul> </li> <li>■ Current project requirements are popularity contest as to what is a flagship project, which is not a good measurement of what is a good project</li> </ul> </li> <li>• What are some metrics for OWASP project health (code/documentation) and updates do you believe should be communicated on the Mediawiki for better visibility (ex. Code project details are noted on OpenHub)?       <ul style="list-style-type: none"> <li>○ Tom           <ul style="list-style-type: none"> <li>■ Mediawiki not the end all-be all               <ul style="list-style-type: none"> <li>• If that's what the final project is, then OWASP has failed</li> </ul> </li> <li>■ Two components of metrics:               <ul style="list-style-type: none"> <li>• 1 - Management - Tied to operations team to help them do their job</li> <li>• 2 - Project - Tied to the project itself</li> </ul> </li> <li>■ If I can see activities of leaders, people communicating on mailing lists, and graduation made, that needs to be done as people log in, then a project is healthy</li> <li>■ For code-based projects, check the API or we can just scrape the pages to see metrics, and then put it into a displayable format               <ul style="list-style-type: none"> <li>• See how many updates have been sent, etc.</li> </ul> </li> </ul> </li> <li>○ Colin           <ul style="list-style-type: none"> <li>■ Only thing that is currently highlighted is "last updated", the roadmap, and "page impressions"</li> <li>■ Things like "activity" or mailing lists or forums could be helpful</li> <li>■ Agree with Tom               <ul style="list-style-type: none"> <li>• Not the entire thing, but important we don't throw anything out</li> <li>• <a href="https://www.owasp.org/index.php/Talk:Summit_2011_Working_Sessions/Session023#On_Designs.2C_Layout_and_Standards">https://www.owasp.org/index.php/Talk:Summit_2011_Working_Sessions/Session023#On_Designs.2C_Layout_and_Standards</a></li> </ul> </li> </ul> </li> </ul> </li> <li>• How likely is it that we migrate project documents away from Mediawiki and more towards something like Confluence?       <ul style="list-style-type: none"> <li>○ Tom</li> </ul> </li> </ul>
--	--

	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>■ If we enable WYSIWYG, they are the similar</li> <li>■ Regarding the aging, the requests, other metrics that come out of Confluence and Mediawiki are extremely similar</li> <li>■ Community would probably not be totally open to adopting commercial software for an open source project           <ul style="list-style-type: none"> <li>● Goes against the idea of open source.</li> </ul> </li> </ul> </li> <li>○ Colin           <ul style="list-style-type: none"> <li>■ Agree with Tom</li> </ul> </li> </ul> </li> <li>● In the last six months, have you visited the OWASP website?       <ul style="list-style-type: none"> <li>○ Colin           <ul style="list-style-type: none"> <li>■ Yes, visited a few times a week</li> </ul> </li> </ul> </li> <li>● How often has the main page for your OWASP chapter or project been maintained?       <ul style="list-style-type: none"> <li>○ Colin           <ul style="list-style-type: none"> <li>■ Every month or 2</li> </ul> </li> </ul> </li> <li>● Is there something missing from the OWASP website that you were expecting?       <ul style="list-style-type: none"> <li>○ Colin           <ul style="list-style-type: none"> <li>■ Not really</li> </ul> </li> </ul> </li> <li>● Are the core MediaWiki functionalities (editing running documentations - ongoing editing and creation of content) intuitive and easy to use?       <ul style="list-style-type: none"> <li>○ Colin           <ul style="list-style-type: none"> <li>■ If you've used a wiki before, then yes</li> <li>■ Some constraints that come with using a wiki but is overall good</li> </ul> </li> </ul> </li> <li>● On a scale of 1-10, please rate your overall impression of the OWASP website.       <ul style="list-style-type: none"> <li>○ Colin           <ul style="list-style-type: none"> <li>■ 7; lot of great content</li> <li>■ Difficult to tell what is current content, what is old content</li> <li>■ Little old-fashioned in terms of design, navigation can be difficult for newcomers.</li> </ul> </li> </ul> </li> <li>● What other platforms do you suggest in place of mediawiki?       <ul style="list-style-type: none"> <li>○ Colin           <ul style="list-style-type: none"> <li>■ No- Wiki's are a useful component               <ul style="list-style-type: none"> <li>● Maybe not necessarily the main page or homepage</li> <li>● But a good place to keep all of the existing information</li> <li>● Been discussed previously at summit</li> </ul> </li> </ul> </li> </ul> </li> <li>● What other improvements would you like to see with OWASP's frontend facelift?       <ul style="list-style-type: none"> <li>○ Colin           <ul style="list-style-type: none"> <li>■ <a href="https://www.owasp.org/index.php/Talk:Summit_2011_Working_Sessions/Session023#On_Designs.2C_Layout_and_Standards">https://www.owasp.org/index.php/Talk:Summit_2011_Working_Sessions/Session023#On_Designs.2C_Layout_and_Standards</a></li> </ul> </li> <li>○ Tom           <ul style="list-style-type: none"> <li>■ Static pages maintained by operations for official information to communicate information</li> <li>■ Use the database on the backend for each chapter giving them a global and single database to work with</li> </ul> </li> </ul> </li> <li>● Do you think there should be a separation of the OWASP project documentations, chapter and organization information? Where would you draw the line?       <ul style="list-style-type: none"> <li>○ Colin           <ul style="list-style-type: none"> <li>■ Should be a separate site that is more external-facing. Nothing should be removed from the wiki.</li> </ul> </li> </ul> </li> <li>● What is your thought on gamification or badging for users on the website?       <ul style="list-style-type: none"> <li>○ Colin</li> </ul> </li> </ul>
--	--

	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>■ Not keen on it</li> <li>■ Website is not the whole organization</li> <li>■ Organization is much more than the website and it's not needed to get people involved</li> </ul> </li> <li>○ Tom           <ul style="list-style-type: none"> <li>■ Think in terms of <a href="https://www.owasp.org/index.php/WASPY_Awards_2015">https://www.owasp.org/index.php/WASPY_Awards_2015</a> and how would the tool aka website for the community help measure and report on this</li> </ul> </li> <li>● Ex. What is your opinion on a stackoverflow-like implementation for the OWASP wiki to facilitate better communication and badging/gamification?           <ul style="list-style-type: none"> <li>○ Colin               <ul style="list-style-type: none"> <li>■ Not necessary</li> <li>■ Would take a lot of effort to create something that doesn't contribute very much</li> <li>■ More important is the contribution community, not the actual architecture</li> </ul> </li> </ul> </li> <li>● What are other technology tools that would benefit the OWASP community in general in addition to this website or an extension to it?           <ul style="list-style-type: none"> <li>○ Colin               <ul style="list-style-type: none"> <li>■ A lot of people use Google docs or Google groups, for their own reasons</li> <li>■ Sometimes, things like conference calls could make things easier</li> <li>■ Video recordings for sessions and summits</li> <li>■ OWASP hasn't been able to maintain a list of upcoming events across the world. Chapter meetings occur and there is no evidence of it.</li> </ul> </li> <li>○ Tom               <ul style="list-style-type: none"> <li>■ WYSIWYG editor enabled on the current wiki, embedding scripts on pages that are static for inclusion/display of content</li> <li>■ Incorporate the Google collobration tools already using and managed via @owasp.org accounts</li> <li>■ <a href="https://www.google.com/work/">https://www.google.com/work/</a> use all the features when possible</li> </ul> </li> </ul> </li> <li>● Have you had trouble finding information you are looking for? Is the information layout consistent such that you can easily locate relevant information to you?           <ul style="list-style-type: none"> <li>○ Colin               <ul style="list-style-type: none"> <li>■ Yes, nature of a Wiki</li> <li>■ Sometimes will use internal search and Google search, but can normally find needed information using a combination of the two                   <ul style="list-style-type: none"> <li>● Have different benefits</li> <li>● If looking for a broader topic or content, google search is better</li> <li>● For specific file or page title, internal search is better</li> </ul> </li> </ul> </li> <li>○ Tom               <ul style="list-style-type: none"> <li>■ Mediawiki search is ok but the search engine search is more useful</li> <li>■ Problem is NOT search- is layout and design of the site                   <ul style="list-style-type: none"> <li>● People use search due to poor layout</li> </ul> </li> </ul> </li> </ul> </li> <li>● Did you find that the layout was consistent such that you could find information that is relevant to you?           <ul style="list-style-type: none"> <li>○ Colin               <ul style="list-style-type: none"> <li>■ Not always consistent, but that's nature of a large community contributing</li> <li>■ Better to have slightly inconsistent layouts for the freedom of contribution.</li> </ul> </li> </ul> </li> </ul>
--	--

	<ul style="list-style-type: none"><li>● Could you name other websites that are doing the same thing but in a better manner?<ul style="list-style-type: none"><li>○ Colin<ul style="list-style-type: none"><li>■ No</li></ul></li><li>○ Tom<ul style="list-style-type: none"><li>■ <a href="https://otalliance.org/">https://otalliance.org/</a></li><li>■ <a href="https://cloudsecurityalliance.org/">https://cloudsecurityalliance.org/</a></li></ul></li></ul></li><li>● What do you believe would drive OWASP community engagement on the site?<ul style="list-style-type: none"><li>○ Colin<ul style="list-style-type: none"><li>■ Don't care about the metric that there are sites that are only visited once<ul style="list-style-type: none"><li>● Expected that most of the visitations are by bots</li><li>● Single page visits are not necessarily a good metric of "community engagement".</li></ul></li><li>■ Another example, people visit the site from a Google search and then find the page they need and don't go to other sites on the same domain</li><li>■ If the question is "How do we decrease the number of single-page visits", the answer is incorrect</li></ul></li><li>○ Tom<ul style="list-style-type: none"><li>■ Expose the use of mailing lists and forums</li></ul></li></ul></li><li>● Some people, instead of engaging with OWASP, will engage with other sites, so how can we get people to engage with the OWASP website more?<ul style="list-style-type: none"><li>○ Colin<ul style="list-style-type: none"><li>■ Should not be measuring the number of visitors to the site, but rather, the wider access to information security</li><li>■ If OWASP helps people to put content on their own website, better for everyone</li><li>■ Don't think that the number of visitors matters.</li></ul></li></ul></li><li>● Further questions/logistics<ul style="list-style-type: none"><li>○ Colin<ul style="list-style-type: none"><li>■ Some content has been translated to Spanish, and multilingual content is fantastic</li><li>■ Wiki system is great</li><li>■ If anything does change, make sure URLs don't change</li></ul></li><li>○ Tom<ul style="list-style-type: none"><li>■ Need to look at building integrations between the open source space as well as our commercial spaces</li><li>■ Needs to be integrations and conversion points from a scraper or data feed and then push it into other codes, such as from Mediawiki to Sales force or Confluence</li><li>■ Can't just slap together a bunch of commercial projects.</li></ul></li></ul></li></ul>
--	--



<b>Date</b>	<b>May 24, 2016</b>
<b>Location</b>	<b>Conference call</b>
<b>Subject</b>	<b>OWASP Global Board Interview Meeting- Josh Sokol</b>
<b>Participants</b>	<p><b>OWASP</b> Josh Sokol - Global Board Member, Local Board of Chapter of OWASP Austin, TX</p> <p><b>Sooryen Technologies</b> Gin Cheng - Tech Lead Ahsun Kim - Project Manager Ram Ganesan - CEO/ Co-Founder of Sooryen Technologies</p>
	<b>Items</b>
	<p><b>Objective and background:</b></p> <p>The purpose of the call was to evaluate the current needs for the OWASP community and website. As elected representatives of the OWASP community, the board members would have a better understanding of the needs of the community and help identify any dissatisfactions with the current platform, infrastructure, and measures in place to encourage collaboration and outreach.</p> <p>The Sooryen team shared a Google document that contained the following information:</p> <ul style="list-style-type: none"> <li>Objective, agenda and interview questions</li> </ul> <p><b>Key discussion items</b></p> <ul style="list-style-type: none"> <li>What are some tools that you are currently using for meeting setups? On average, how many members show per meeting? What other outreach efforts have you undertaken?</li> </ul>

	<ul style="list-style-type: none"> <li>○ OWASP Austin operates differently from a lot of other chapters- stemming from Josh's early leadership of chapter</li> <li>○ Meetings on monthly basis- Last Tuesday of every month (~60-70)</li> <li>○ Used budget to buy audio-visual equipment       <ul style="list-style-type: none"> <li>■ Developed large catalogue of recorded meeting content</li> <li>■ Once created documentation on what you should buy as a chapter, how you assemble it</li> </ul> </li> <li>○ Group used to use GoToMeeting       <ul style="list-style-type: none"> <li>■ Due to limitation of people, moved to GoToWebinar</li> <li>■ Live broadcast of chapter meetings, record content for future playback</li> </ul> </li> <li>○ Weekly study group (10-20 people)       <ul style="list-style-type: none"> <li>■ Pick a book</li> </ul> </li> <li>○ Annual conference</li> <li>○ Monthly happy hours</li> <li>○ Outreach efforts that could be undertaken:       <ul style="list-style-type: none"> <li>■ Reaching out to local ISSA chapter, local security groups, local meetups for PHP users/other developmental groups</li> </ul> </li> <li>● How are you managing member retention, engagements, identifying paying and non-paying members?       <ul style="list-style-type: none"> <li>○ In general, OWASP has problem with membership</li> <li>○ Very hard to justify the value of paying \$50 when everything OWASP does is free           <ul style="list-style-type: none"> <li>■ Maybe incentivize people with discounts for other events, organizations</li> </ul> </li> <li>○ Don't really use a lot of tools           <ul style="list-style-type: none"> <li>■ Use Evernote to track how many people attend meetings</li> <li>■ Track people from National Instruments who attend the meetings, overall attendants, online attendants</li> <li>■ EventBrite- Sending out meeting invitations/reservations</li> </ul> </li> <li>○ OWASP mailing list           <ul style="list-style-type: none"> <li>■ For marketing, about upcoming meetings, happy hours</li> </ul> </li> <li>○ GoToWebinar</li> </ul> </li> <li>● What are some data points that you would like to see on your chapter Mediawiki page (Such as demographics, paying/non-paying, project contributors, etc.)?       <ul style="list-style-type: none"> <li>○ Formatting of Austin page done by Josh</li> <li>○ Serves rough purpose</li> <li>○ Template staff injects into page           <ul style="list-style-type: none"> <li>■ About OWASP Austin</li> </ul> </li> <li>○ Upcoming events, history of events, archive of some presentations, information about chapter leadership, roles, sponsorship opportunities           <ul style="list-style-type: none"> <li>■ Organization and historical perspective to show activity- not necessarily seeing across other chapters</li> <li>■ A lot of chapters using Google or Meetup</li> </ul> </li> <li>○ Tried starting chapter project           <ul style="list-style-type: none"> <li>■ One of German chapter did PHP project</li> <li>■ Not enough people with necessary skill sets; project didn't take off</li> </ul> </li> <li>○ Displaying project contributors on chapter Mediawiki page - Would potentially add to problem of disorganization of data           <ul style="list-style-type: none"> <li>■ Maybe a single page that acknowledges project contributors</li> <li>■ Becomes a way for vendors to utilize it to get their name out/ buying visibility</li> </ul> </li> </ul> </li> </ul>
--	---

	<ul style="list-style-type: none"> <li>○ Displaying demographics on chapter Mediawiki page - Would potentially add to problem of vendors utilizing this to buy visibility</li> <li>○ Displaying paying/non-paying members - Not as much value as displaying the length of time they've participated in</li> <li>● What are some changes you would like to see on the Mediawiki chapter pages?       <ul style="list-style-type: none"> <li>○ Mediawiki- extremely difficult to search           <ul style="list-style-type: none"> <li>■ End up with irrelevant results</li> </ul> </li> <li>○ Links on left hand navigation- disorganized</li> <li>○ Slimmed down front end seems necessary           <ul style="list-style-type: none"> <li>■ Wiki should be end result, not necessarily starting point</li> </ul> </li> </ul> </li> <li>● Have you had any issues with starting a project following the MediaWiki process?       <ul style="list-style-type: none"> <li>○ No, more so on finding volunteers for project</li> </ul> </li> <li>● Is there sufficient documentation for on-going projects such that new volunteers can go through the material and potentially contribute?       <ul style="list-style-type: none"> <li>○ Finding a project is a pain point</li> <li>○ No method to recruit volunteers</li> <li>○ I.e., If in particular need of volunteers for PHP project           <ul style="list-style-type: none"> <li>■ No current method of finding volunteer with specific PHP skill set</li> </ul> </li> <li>○ Volunteer funnel</li> </ul> </li> <li>● Do you feel the current templates in place for projects are sufficient for your needs? As adjustments can be made to these templates per project, is the layout for the information consistent enough?       <ul style="list-style-type: none"> <li>○ Templates were sufficient</li> <li>○ Layout for information did not seem consistent</li> <li>○ Creation of multiple sources of information for projects that conflict- problematic</li> </ul> </li> <li>● In your opinion, how likely is centralizing project code repositories onto specific accounts (OWASP Account)? What are the main friction points you anticipate for this?       <ul style="list-style-type: none"> <li>○ Currently, more or less standardized around Github           <ul style="list-style-type: none"> <li>■ Free for open source projects</li> </ul> </li> <li>○ Is currently a recommendation, but not a requirement</li> </ul> </li> <li>● What are some metrics for OWASP project health (code/documentation) and updates you believe should be communicated on the Mediawiki for better visibility (ex. Code project details are noted on Open Hub)?       <ul style="list-style-type: none"> <li>○ OWASP has wrong take on projects- Currently an emphasis of quantity over quality</li> <li>○ A lot of projects on website, little consistency among projects</li> <li>○ Metrics for OWASP project health:           <ul style="list-style-type: none"> <li>■ Project with multiple contributors, large code base, secure code base, diligence around security (scanning, code reviews, etc.), needs to be trusted by community, need to fulfill actual need               <ul style="list-style-type: none"> <li>● Volunteer management system might help with this</li> </ul> </li> </ul> </li> <li>○ OpenHub- More in line with depicting relevant information; community rating feature, how active project is           <ul style="list-style-type: none"> <li>■ Once you enter main page, should see certain information:               <ul style="list-style-type: none"> <li>● A wiki page about why you should start a project</li> <li>● Funding for projects</li> <li>● Link for flagship, lab, and incubators</li> <li>● When searching OWASP projects, would expect to see a page that lists OWASP projects</li> </ul> </li> </ul> </li> </ul> </li> </ul>
--	--

	<ul style="list-style-type: none"><li><ul style="list-style-type: none"><li>○ Should be able to filter based on flagship, lab, incubator, programming language</li></ul></li><li>● What are some tools that you would suggest to help you streamline the process?<ul style="list-style-type: none"><li>○ Github as repository</li><li>○ Static analysis tools to be run across repositories</li><li>○ Driving some automation pieces<ul style="list-style-type: none"><li>■ Grabbing how many lines in code, how many things changed, release notes on new functionality has been developed into this</li></ul></li></ul></li><li>● What other improvements would you like to see with OWASP's frontend facelift?<ul style="list-style-type: none"><li>○ Wiki's good for documentation<ul style="list-style-type: none"><li>■ Currently both marketing tool and knowledge base- should not be</li></ul></li><li>○ my.owasp.org<ul style="list-style-type: none"><li>■ Ning site that is a rough sketch of what Josh considers important</li><li>■ Currently being used by OWASP Austin study group and OWASP Austin chapter</li></ul></li></ul></li><li>● What is your opinion on the portal?<ul style="list-style-type: none"><li>○ What is problematic is that you need a login to get there- inhibitor for anyone in community</li></ul></li><li>● What is your thought on gamification or badging for users on the website?<ul style="list-style-type: none"><li>○ Cool idea- framing gamification so that it highlights/recognizes people who are contributing the most</li><li>○ Tangible rewards: Possibly awarding these members with gift cards to OWASP store</li><li>○ Should treat OWASP more like a business (not for profit corporation) rather than social club</li></ul></li><li>● Ex. What is your opinion on a stackoverflow-like implementation for the OWASP wiki to facilitate better communication and badging/gamification?<ul style="list-style-type: none"><li>○ Good idea- frame more like how to asking security questions, finding a project</li></ul></li><li>● What are other technology tools that would benefit the OWASP community in general outside of this website or an extension to it?<ul style="list-style-type: none"><li>○ OWASP volunteer community- makes heavy use of mailing list formats<ul style="list-style-type: none"><li>■ Interaction with it is outdated</li><li>■ Having it be more like a forum</li><li>■ A live-chat feature (more so like Slack)</li><li>■ Most people don't find the communications</li><li>■ Still could email on backend</li><li>■ Potentially having:<ul style="list-style-type: none"><li>● Posting on news group and email would cause it to post to the forum</li><li>● Have users choose to work out how they use the site instead of forcing them to interact with it a certain way</li></ul></li></ul></li></ul></li><li>● Barrier of entry is very high<ul style="list-style-type: none"><li>○ Becoming part of chapter leadership team, OWASP governance stuff isn't highlighted</li></ul></li></ul>
--	--

<b>Date</b>	<b>May 26, 2016</b>
<b>Location</b>	<b>Conference call</b>
<b>Subject</b>	<b>OWASP Global Board Interview Meeting- Andrew van der Stock</b>
<b>Participants</b>	<b>OWASP</b> Andrew van der Stock - Global Board Member; Key contributor of OWASP Developer Guide; OWASP Top 10 2007; Application Security Verifications Standard  <b>Sooryen Technologies</b> Gin Cheng - Tech Lead Ahsun Kim - Project Manager Ram Ganesan - CEO/ Co-Founder of Sooryen Technologies
	<b>Items</b>
	<b>Objective and background:</b>

The purpose of the call was to evaluate the current needs for the OWASP community and website. As elected representatives of the OWASP community, the board members would have a better understanding of the needs of the community and help identify any dissatisfactions with the current platform, infrastructure, and measures in place to encourage collaboration and outreach.

The Sooryen team shared a Google document that contained the following information:

- Objective, agenda and interview questions

**Key discussion items**

- Have you had any issues with starting a project following the MediaWiki process?
  - Most projects before Mediawiki of OWASP was formalized and before project review process was formalized
- Have you had any issues with creating the MediaWiki for the project, maintaining it and allowing others to help contribute to it?
  - Yes as a project manager
  - OWASP Developer Guide
    - Word document- no obvious way of how to place pages of word document go into Mediawiki
  - With word documents, previously worked with Google Documents
  - Workflow is a Github
    - Integrating Github into Mediawiki is difficult
  - Documentation on Wiki is particularly difficult
    - If there aren't many links, Mediawiki is straightforward
    - However, if heavily interlinked, you run into problems
  - No good editing tools, doesn't have real flows
  - If could have something that would allow project managers to republish the information that they've got
    - To have it discoverable by search
      - A lot of dead pages in Mediawiki
- Do you feel like there is a lack in process for funding, communication with other members and collaboration on the MediaWiki?
  - Serves the people who aren't doing creation of projects
  - Group of five to six people who edit pages to keep in check
    - No real process except identifying pages that are broken
  - Project reviews
    - Separate from Wiki itself
    - Identifies whether you're a flagship, lab, incubator
    - Determines what headers and templates you use
    - Not sure if this has value
    - Refining process so it's transparent and making it automated based on metrics
      - By bringing status of project up, get increasing community feedback that project is valuable
- Do you feel the current templates in place for projects are sufficient for your needs? As adjustments can be made to these templates per project, is the layout for the information consistent enough?
  - Three communities: Builders, breakers, defenders
    - Primarily, material is for breakers
    - OWASP is about providing defenses and helping developers build secure software
  - Need a way for results and searches to be effectively able to sort through this
  - Currently on templates, just listed as a category

- In 2012, had many distinct styles
  - Because Wiki is so big, especially in earlier stages of OWASP, no consistency in feel, no easy navigation path
  - Would be good to unify this:
    - Those with project on Github to look one way
    - Those with documentation project to appear another way
    - Chapter and outreach to appear a certain way
    - To be consistent amongst them all
  - Targeting having templates that are designed in fewer styles and better branding and allow for better search results
- Is there sufficient documentation for on-going projects such that new volunteers can go through the material and potentially contribute?
  - No- even successful projects have difficult time recruiting volunteers
    - Example: Simon Bennetts- OWASP Zed Attack Proxy (ZAP) project lead; one of two full time staff members on a project
      - Can really only recognize 10 active volunteers
- Do you believe there is enough visibility as to what projects the OWASP community is currently working on?
  - Yes if you go searching for it: OWASP Connector, podcast
  - Many projects that are similar; should combine forces
    - May be prevented if they raised more awareness on the types of projects that exist to prevent the creation of multiple similar projects
- In your opinion, how likely is centralizing project code repositories onto specific accounts (OWASP Account)? What are the main friction points you anticipate for this?
  - No formal requirement for this, yet has been very successful due to closure of [code.google.com/](http://code.google.com/) SourceForge puts malicious installers
  - Makes the project easier to find
    - 70-80 projects on Github
    - Separately, one of 150,000 code repositories; less easy to discover
- Have you had issues getting subject matter experts' opinions/volunteers for specific projects? What changes on the OWASP site do you believe would help facilitate this?
  - Problems with retention
    - Observable through leaders mailing list going down
  - To make it easier to discover projects and materials
  - Difficult to find training materials; discoverability is terrible
- What are some metrics for OWASP project health (code/documentation) and updates you believe should be communicated on the Mediawiki for better visibility (ex. Code project details are noted on OpenHub)?
  - Metrics need to serve community of builders that build the project
  - Things like how active the project not really important if it takes a while for project leaders to collect and doesn't contribute to their project
    - Need to be automated as much as possible based on flows that are available
    - Even though ZAP and Application Security Verification Standard (ASVS) are both flagship projects that are in good health, ASVS looks to be in bad health from punch card based on current metrics
  - Useful, not heavy friction for project leaders, not time consuming for project managers
  - Hiring senior project coordinator shortly
    - Shouldn't be time consuming to come up with these metrics

- Had 5-6 project coordinators since 2012
  - Due to being done through process that isn't particularly valuable
- OpenHub- provides discoverability, not sure how many users are on there
  - Claudia and Johanna used it as part of project reviews
  - Not sure how many project managers used it other than project coordinators
- What are some tools that you would suggest to help you streamline the process?
  - Integration between Github and Wiki
    - Particularly if you can find some way for documentation projects, to allow building of documentation projects on Wiki
    - When you build release on Github
      - All the APIs on Github
      - If there's a way to update current release download on Wiki- so it operates as effectively read only repository rather than something you'd have to go and edit
- Was there a rationale behind choosing Github over Bitbucket? Is there a preference in the community for either or?
  - At the time, didn't have Atlassian sponsorship and Github was essentially free
  - Github has more openness; many people think Atlassian products are close-sourced alternative
  - Relative straightforward to fork things for Github
  - JIRA- Need to clone it and create your own
  - Atlassian works well when you have closed, private repositories; not as good of a fit for OWASP
- In the last six months, how often have you visited the OWASP website?
  - Typically daily, weekly basis, especially for board meetings
- How often has the main page for OWASP Global Board members been maintained and are there other pieces of information that you would like to see there?
  - Not revealing what OWASP Global Board members do; should be more transparent and shows that the Board is more active
  - Currently only showing when meetings are
- Is there something missing from the OWASP website that you were expecting?
  - Something more professional
  - Bio sections are lacking; meet up twice a year- could take a board portrait photo that looks cohesive
  - How people can raise issues and concerns to OWASP board
  - Very little about how Board tries to meet strategic goals, future initiatives and how the community can help
- Are the core MediaWiki functionalities (editing running documentations) intuitive and easy to use?
  - Not really a MediaWiki person- would be great if something can take word documents and turn them into MediaWiki documents that don't look horrible
    - Importer from Google Documents for same purpose
  - Something that takes Github content (release of a project or markdown document) and put it up on MediaWiki and reads all the way
  - OWASP MediaWiki is behind in terms of versions (about 3)
  - Inline editor is primitive; puts a lot of people off and prevents people from contributing
  - Difficulties: How to do translations/ as many languages as you can



- Currently not aware of examples of such on OWASP website
  - Important to cross-link like-sided materials
    - If you know how to do MediaWiki and you know how to do URLs, is relatively straightforward
- Would you be open to an option where we move to a Content Management System (CMS) as opposed to Wiki paradigm? Do you think it's time for some sort of professional content editor to review and sanitize the content?
  - Realistically, looking at Sharepoint, one of major CMS, without active curation, not going to have great result
  - No one feels like they own the front page and that it was designed by a committee, but it isn't
  - Having succinct branding within a tool that is designed to get information out is ideal
  - None of projects are using MediaWiki in the way it was intended- anonymous editing
  - Spam problem- People are actively using known problems with MediaWiki
    - Causes IT support person grief, because spends all his time clearing out spam
    - Linkages between tools used (such as Github) provide translations and make sure project leaders can look after space, wouldn't necessarily need curator
  - Lot of unmanaged Sharepoint, Magento, MediaWiki
    - Unless people have opinion on what content should be, ends up with a lot of abandoned pages, etc.

Feedback regarding mock ups made for New Jersey OWASP Chapter meeting

- Home page
  - Top menu items-
    - Chapters, projects, membership
  - Boxes-
    - Mock up missing start of membership process
      - Hovering around 2000-2200 member mark
      - 45,000 participants
      - Not high conversion rate
  - Strategic areas: Chapters, projects, outreach, education
    - Events is important, initiatives
  - Main reason for going to OWASP website is to find chapter meetings
    - Able to search events by chapter or potentially through geocoding
    - To encourage engagement
- Project page
  - Likes overall list of all projects
  - Good to have filters for builders, breakers, defenders
  - May be good to have buttons that says:
    - I'm a developer
    - I'm a CISO
    - I'm a risk manager
  - Difficult to have discovery
    - Biggest users for documentation are risk managers and CISO's
- Mobile pages
  - Responsive web apps are important
  - Curious to see how engagement improves

	<ul style="list-style-type: none"> <li>● Should highlight how many layers of information is too much</li> <li>● Is there certain information that you believe should be more transparent for the community to evaluate such as membership demographics? <ul style="list-style-type: none"> <li>○ Need to fix membership classes, which is currently too expensive for developing nations and students to join OWASP at the moment</li> <li>○ Additional class to integrate with Salesforce</li> </ul> </li> <li>● Integrate CMS to Salesforce- make as transparent as possible so people don't have to re-enter password</li> <li>● MediaWiki to Salesforce- different look and feel <ul style="list-style-type: none"> <li>○ Would be ideal to have the transition be less jarring</li> <li>○ Salesforce has some customization possibilities</li> </ul> </li> <li>● Getting people to come to events, paying for events, paying for membership- Income streams <ul style="list-style-type: none"> <li>○ Should be front and center and easy to do</li> </ul> </li> <li>● Should talk to Kelly regarding if advertisements have been sold to sponsors</li> <li>● What is your thought on gamification or badging for users on the website? <ul style="list-style-type: none"> <li>○ For projects, chapters members- might have value, but might have missed timeframe for it</li> </ul> </li> <li>● What is your opinion on a stackoverflow-like implementation for the OWASP wiki to facilitate better communication and badging/gamification? <ul style="list-style-type: none"> <li>○ Supportive of it <ul style="list-style-type: none"> <li>■ Shows good contributors, helps understand who are big players of organization</li> </ul> </li> </ul> </li> </ul>
--	--

<b>Date</b>	<b>May 26, 2016</b>
<b>Location</b>	<b>Conference call</b>
<b>Subject</b>	<b>OWASP Global Board Interview Meeting- Michael Coates</b>

<b>Participant</b> <b>s</b>	<p><b>OWASP</b> Michael Coates - Global Board Member, Chapter leader of OWASP San Francisco Bay Area</p> <p><b>Sooryen Technologies</b> Gin Cheng - Tech Lead Ahsun Kim - Project Manager Ram Ganesan - CEO/ Co-Founder of Sooryen Technologies</p>
<b>Items</b>	
	<p><b>Objective and background:</b></p> <p>The purpose of the call was to evaluate the current needs for the OWASP community and website. As elected representatives of the OWASP community, the board members would have a better understanding of the needs of the community and help identify any dissatisfactions with the current platform, infrastructure, and measures in place to encourage collaboration and outreach.</p> <p>The Sooryen team shared a Google document that contained the following information:</p> <ul style="list-style-type: none"> <li>● Objective, agenda and interview questions</li> </ul> <p><b>Key discussion items</b></p> <ul style="list-style-type: none"> <li>● What are some tools that you are currently using for meeting setups? On average, how many members show per meeting? What other outreach efforts have you undertaken?       <ul style="list-style-type: none"> <li>○ Meeting setup tools:           <ul style="list-style-type: none"> <li>■ Biggest tool used is Meetup</li> <li>■ Used Google Surveys a little bit</li> <li>■ Used OWASP wiki for the chapter page</li> <li>■ Twitter to broadcast awareness</li> <li>■ OWASP mailing list</li> </ul> </li> <li>○ About 100 members show up per meeting</li> <li>○ Outreach:           <ul style="list-style-type: none"> <li>■ Held a National Conference in there in the Bay Area</li> <li>■ Rotate chapter locations to different spaces that want to host for new exposure</li> </ul> </li> </ul> </li> <li>● How are you managing member retention, engagements, identifying paying and non-paying members?       <ul style="list-style-type: none"> <li>○ Normally, achieve maximum capacity at any event very easily and have over 1000 people in their Meetup group</li> <li>○ As a result, the goal has not been member retention but rather having good quality events and attracting people</li> <li>○ Not much of an incentive to identifying paying and non-paying members           <ul style="list-style-type: none"> <li>■ Promote everything as free, and every meeting, reminds people that it is non-profit and funded by volunteers and that their support is valuable; no other reason to distinguish members.</li> </ul> </li> </ul> </li> <li>● What are some data points that you would like to see on your chapter Mediawiki page (Such as demographics, paying/non-paying, project contributors, etc.)?       <ul style="list-style-type: none"> <li>○ Projects on which individuals from chapter are participating</li> </ul> </li> </ul>

- Average number of attendees at their meeting
- What are some changes you would like to see on the Mediawiki chapter pages?
  - Integration via some sort of plugin to Meetup because Meetup is fantastic way to get people to attend events
- What would assist your efforts in outreach that is currently not being provided by OWASP?
  - Larger focus on building a national or regional list of quality speakers that are willing to travel
- Have you had any issues with starting a project following the MediaWiki process?
  - Have not started a project following the MediaWiki process in about seven years, so no issue to recall
- Have you had any issues with creating the MediaWiki for the project, maintaining it and allowing others to help contribute to it?
  - No, when handed off the project, transition was smooth and were no difficulties
- Do you feel like there is a lack in process for funding, communication with other members and collaboration on the MediaWiki?
  - Not much to say since so far removed from the MediaWiki and lacked much involvement for a long time
- Is there sufficient documentation for on-going projects such that new volunteers can go through the material and potentially contribute?
  - Can be organized better
  - Segmented off from the groups of people they want to engage
  - Live on an island of the OWASP wiki while everyone else lives on GitHub
  - If single repository containing all projects on a popular site like GitHub, then there would be a lot more engagement
  - Also, integration between GitHub and the OWASP wiki
- Do you believe there is enough visibility as to what projects the OWASP community is currently working on?
  - Nope
  - OWASP newsletter is great
  - Would love for someone that is shepherding projects to have frequent communication with the OWASP community with weekly discussions on a project that is fun and interesting to excite more people
- In your opinion, how likely is centralizing project code repositories onto specific accounts (OWASP Account)? What are the main friction points you anticipate for this?
  - If they agree, centralization is the way to go and can become a reality
  - Donated projects can become tricky because it may be set up elsewhere
  - Even so, this can be done easily
- Have you had issues getting subject matter experts' opinions/volunteers for specific projects? What changes on the OWASP site do you believe would help facilitate this?
  - Certain projects do suffer from this problem
  - More developer engagement can help because the developers are the experts on those projects
  - However, many of those developers live on GitHub and not on the OWASP wiki page
  - One great fix will be to have better flows for different types of visitors (developers, security professional, CISO, etc.) to get them to navigate the site more easily
- What are some metrics for OWASP project health (code/documentation) and updates you believe should be communicated on the Mediawiki for better visibility (ex. Code project details are noted on OpenHub)?

- Number of code commits, number of developers involved, number of unique companies represented in the volunteer base, number of downloads of code, number of views of documentation
  - OWASP wiki should have integration with other sources like OpenHub, GitHub, etc. as well as interesting data points
- What are some tools that you would suggest to help you streamline the process?
  - Plugins that pull that relevant data mentioned previously
  - Interesting data sets on the MediaWiki page regarding languages, lines of code, etc.
  - Adding relevant code data as well
  - Less clutter and easier navigation with a consistent look and feel
- Was there a rationale behind choosing Github over Bitbucket? Is there a preference in the community for either or?
  - No known rationale
- In the last six months, have you visited the OWASP website?
  - Monthly visits
- Can you identify a representative group of resources that you as a Global Board member uses?
  - Mainly the material under the Global Board member page
  - Governance section
  - Home page, projects page, chapters page
- How often has the main page for OWASP Global Board members been maintained and are there other pieces of information that you would like to see there?
  - Updated appropriately with monthly agendas, so the assumption is monthly
  - Would not like to see additional pieces of information on the page since it has everything it needs
- Is there something missing from the OWASP website that you were expecting?
  - Flow based on type of visitor
  - Would like more information on CISO Michael Coates (himself)
- Are the core MediaWiki functionalities (editing running documentations) intuitive and easy to use?
  - Not very intuitive; just okay
  - Prefers Confluence over MediaWiki in terms of ease of use because there is a barrier for new users who want to contribute
    - MediaWiki can be confusing
    - Confluence is much more intuitive since it behaves like a familiar word processor and is easy to use for any user.
- Have you had trouble finding information you are looking for? Is the information layout consistent such that you can easily locate relevant information to you?
  - Have trouble all the time
  - Generally when looking for technical details in applications security that he knows is on the OWASP website
  - Usually has to use Google in order to find those details
  - Browsing through the OWASP site is not a successful endeavor (bad search and lack of organization and structure and flow)
  - Information layout is not consistent
  - Duplicate and abandoned content
- On a scale of 1-10, please rate your overall impression of the OWASP website.
  - 7 because there are a lot challenges with the usability but the content is great
- Can you name other websites that are doing something similar in a better manner?

	<ul style="list-style-type: none"><li>○ Apache has done a better job, because their projects are better organized</li><li>○ SANS does a good job of organizing their content (sans.org)</li><li>● What other improvements would you like to see with OWASP's frontend facelift?<ul style="list-style-type: none"><li>○ The flows for developers, security experts, CISO, etc.</li><li>○ The blogs don't have enough content generated regularly</li><li>○ Events calendar is great</li><li>○ Metrics from all OWASP projects would be cool</li><li>○ Look on mobile should focus on what the user sees on any given page, but the mockup looks good</li></ul></li></ul>
--	---

<b>Date</b>	<b>May 27, 2016</b>
<b>Location</b>	<b>Conference call</b>
<b>Subject</b>	<b>OWASP Global Board Interview Meeting- Matt Konda</b>
<b>Participants</b>	<p><b>OWASP</b> Matt Konda - Global Board Member, Project Leader for Pipeline project</p> <p><b>Sooryen Technologies</b> Gin Cheng - Tech Lead Ahsun Kim - Project Manager</p>
<b>Items</b>	
	<p><b>Objective and background:</b></p> <p>The purpose of the call was to evaluate the current needs for the OWASP community and website. As elected representatives of the OWASP community, the board members would have a better understanding of the needs of the community and help identify any dissatisfactions with the current platform, infrastructure, and measures in place to encourage collaboration and outreach.</p> <p>The Sooryen team shared a Google document that contained the following information:</p> <ul style="list-style-type: none"> <li>• Objective, agenda and interview questions</li> </ul> <p><b>Key discussion items</b></p> <ul style="list-style-type: none"> <li>• What are some tools that you are currently using for meeting setups? On average, how many members show per meeting? What other outreach efforts have you undertaken?       <ul style="list-style-type: none"> <li>○ As previous chapter leader for Chicago, used EventBrite and moved to using MeetUp           <ul style="list-style-type: none"> <li>■ Have had better success with MeetUp because allows for Chicago Tech community can find OWASP</li> <li>■ EventBrite- fine for managing attendance and getting names for list (for security guards to utilize during check-in)</li> <li>■ MeetUp- better because people who are looking to engage with technologists use MeetUp more heavily in Chicago               <ul style="list-style-type: none"> <li>• People occasionally have complained about MeetUp due to privacy concerns</li> </ul> </li> </ul> </li> <li>○ About 50 members per meeting           <ul style="list-style-type: none"> <li>■ Previously had meetings quarterly or biannually               <ul style="list-style-type: none"> <li>• More people would attend/ great talks but was rarer and less community building</li> </ul> </li> <li>■ To make community more regular, lost the size, but not has meetings every other month</li> </ul> </li> <li>○ Use Slack           <ul style="list-style-type: none"> <li>■ OWASP Slack channel</li> <li>■ Chicago Tech Slack               <ul style="list-style-type: none"> <li>• 600-800 developers on Slack</li> </ul> </li> </ul> </li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>● Remaining active on security channel</li> </ul> </li> <li>○ Partner with Chicago-based conference call: Chicago Coder Conference           <ul style="list-style-type: none"> <li>■ Run a security track at the conference</li> </ul> </li> </ul> </li> <li>● How are you managing member retention, engagements, identifying paying and non-paying members?       <ul style="list-style-type: none"> <li>○ Will encourage people to be members at meetings via short statements</li> <li>○ Frequently encountered question: Why would I be a member of OWASP if everything's open?</li> <li>○ Talked to Kelly if could give members something more tangible</li> <li>○ Possibly communicating more clearly what membership money goes to- funding tool, education, outreach session, etc.</li> </ul> </li> <li>● What are some data points that you would like to see on your chapter Mediawiki page (Such as demographics, paying/non-paying, project contributors, etc.)?       <ul style="list-style-type: none"> <li>○ MediaWiki only used to put up next meeting</li> <li>○ Unsure, but possibly: Being able to say "We as a chapter are trying to help fund one of the projects" or highlighting members in chapters who are project contributors</li> </ul> </li> <li>● What would assist your efforts in outreach that is currently not being provided by OWASP?       <ul style="list-style-type: none"> <li>○ Interviewing candidate for community manager- not Matt Konda's ideas           <ul style="list-style-type: none"> <li>■ As chapter leader, get name on spreadsheet, chapter handbook, and OWASP email</li> <li>■ Not tremendous amount of support</li> <li>■ Although building mini communities locally, doesn't know if chapter leaders have much ability to learn from each other and share resources</li> <li>■ Not sure if OWASP has umbrella MeetUp account that OWASP Chicago is under</li> <li>■ Fair amount of tangible support that can be given to chapter leaders- Two way conversations               <ul style="list-style-type: none"> <li>● Would be great if on a monthly basis, an email sent out to each chapter leader asking if there's anything needed/ asking how things are going/ do you need help finding speakers, etc.</li> <li>● Would be helpful to have someone to bounce ideas off of regarding best methods to finding locations and speakers about                   <ul style="list-style-type: none"> <li>○ Currently for Chicago chapter, certain groups assigned to finding location or speakers</li> </ul> </li> </ul> </li> <li>■ Encouraging chapters to hold regional events               <ul style="list-style-type: none"> <li>● Currently, Austin and Southern California each hold large regional events by working with local chapters</li> </ul> </li> </ul> </li> <li>○ Something that hasn't been done- effectively paying for certain parts of chapter work to get done to not burden volunteers           <ul style="list-style-type: none"> <li>■ Having someone map out where this would be useful- i.e. for chapters with the budgets to do so</li> </ul> </li> </ul> </li> <li>● Have you had any issues with starting a project following the MediaWiki process? Have you had any issues with creating the MediaWiki for the project, maintaining it and allowing others to help contribute to it? Have you had issues getting subject matter experts' opinions/volunteers for specific projects? What changes on the OWASP site do you believe would help facilitate this?       <ul style="list-style-type: none"> <li>○ Started it, created and edited the Wiki page</li> <li>○ Hasn't really updated it since- not a good indication for state of project</li> </ul> </li> </ul>
--	---



	<ul style="list-style-type: none"> <li>○ Keeps it in OWASP Github <ul style="list-style-type: none"> <li>■ Better place to look to know what's going on with the project</li> </ul> </li> <li>○ Didn't find Wiki particularly useful as a project leader; done more so because it's mandatory</li> <li>○ Doesn't find much value with status of project <ul style="list-style-type: none"> <li>■ More so concerned with having people to look at code and contribute and to use it</li> <li>■ Would like to be able to find people who are interested in writing code in language comfort zone or topically interesting to them</li> </ul> </li> <li>● Do you feel like there is a lack in process for funding, communication with other members and collaboration on the MediaWiki? <ul style="list-style-type: none"> <li>○ Yes, unclear when there's funding, what it's supposed to be used for, and what constraints are <ul style="list-style-type: none"> <li>■ From own project perspective, not necessarily have use for funding</li> </ul> </li> <li>○ Would be possible for OWASP to help projects receive funding when necessary and beneficial and to raise visibility for OWASP</li> <li>○ Not a good platform for communication <ul style="list-style-type: none"> <li>■ Having Wiki and OWASP email as cornerstone for OWASP communication seems unfavorable</li> </ul> </li> </ul> </li> <li>● Do you feel the current templates in place for projects are sufficient for your needs? <ul style="list-style-type: none"> <li>○ Used the templates out of requirement</li> </ul> </li> <li>● Is there sufficient documentation for on-going projects such that new volunteers can go through the material and potentially contribute? <ul style="list-style-type: none"> <li>○ Varies project to project</li> <li>○ Most projects struggle with documentation</li> <li>○ Wiki doesn't seem like platform geared to drawing in new volunteers</li> </ul> </li> <li>● How can OWASP raise more visibility as to what projects the OWASP community is currently working on? <ul style="list-style-type: none"> <li>○ ZAP got attention in media and tools list (being voted as good open tool)</li> <li>○ To consistently raise software quality, could potentially recruit and engage skilled software developers</li> <li>○ Would be great to be able to find out number of developers contributing to projects and seeing if there's a growth</li> <li>○ Being able to identify people who are not security experts, but are development experts</li> </ul> </li> <li>● In your opinion, how likely is centralizing project code repositories onto specific accounts (OWASP Account)? What are the main friction points you anticipate for this? <ul style="list-style-type: none"> <li>○ Right thing to do and everyone will get there eventually</li> <li>○ Github provides the collaboration tools that are industry's standards for managing and updating code- makes sense for why it should be mandatory</li> <li>○ Some people create a personal Github account <ul style="list-style-type: none"> <li>■ Personally, wasn't immediately clear how to create Git repository within OWASP Foundation's account <ul style="list-style-type: none"> <li>● Want to make this easier; help people understand how to do this</li> </ul> </li> </ul> </li> <li>○ To standardize and make it easy to deploy with OWASP Github and OWASP Docker- would be easier for people to follow the rules</li> <li>○ Friction point: People don't want to have a lot of work to move the code</li> <li>○ In necessary cases, necessary to mandate processes and licenses</li> </ul> </li> </ul>
--	---

- OWASP has to have the ability to mark something as old/ not active- hard to do if OWASP doesn't own where the code comes from
- What are some metrics for OWASP project health (code/documentation) and updates you believe should be communicated on the Mediawiki for better visibility (ex. Code project details are noted on OpenHub)?
  - Github is very useful for:
    - When last commits were (Want to see active commits over time)
    - How many committers there are
    - How many branches there are
    - How many issues there are
  - How to know which project you care about/ why you would care about them
    - On Github, shows most active, but not necessarily being able to navigate to a tool
      - Based on contributors versus users
      - If contributing, what languages
      - If users, what are you using it for?
- Can you identify a representative group of resources that you as a Global Board member uses?
  - Pages for Global Board meetings
    - Have times + agenda
  - Voting history
  - Governance
  - Accessible content but not easiest to find
- Have you had trouble finding information you are looking for? Is the information layout consistent such that you can easily locate relevant information to you?
  - Searches with Google, never uses OWASP search engine
- Can you name other websites that are doing something similar in a better manner?
  - Not necessarily a specific site but site that has industry standard bars of navigation
- What other improvements would you like to see with OWASP's frontend facelift?
  - Wiki should be subpart of what OWASP has in terms of web presence
    - The people who come in for different reasons should have different experiences
      - Based on if sponsor, member, etc.
    - Polished front-end: Marketing oriented page that conveys what mission is, projects positive image
- What is your thought on gamification or badging for users on the website?
  - Interested and very open
    - Would be more interested to see how a frontend facelift and process flows where volunteers interact with staff
- What are other technology tools that would benefit the OWASP community in general outside of this website or an extension to it?
  - Potentially having it so that you can get curated information via email/other platform based on your interests (interested in projects, chapters) to encourage membership
    - Tricky because low engagement with email
    - Move to different platform- Slack, Google+, a platform that lets other people tell OWASP how they want to engage with OWASP
- What do you believe would drive OWASP community engagement on the site?

	<ul style="list-style-type: none"><li>○ Wiki doesn't need to be only/main website that OWASP has/ for people to engage in<ul style="list-style-type: none"><li>■ Not surprising that there's a high bounce rate for OWASP<ul style="list-style-type: none"><li>● When looking for one page to access information in read mode, wouldn't really need to go to another page of Wiki</li><li>● Personally not case for contributing- would expect better engagement</li></ul></li><li>■ For main site, public-focused front web page, would like more engagement in that<ul style="list-style-type: none"><li>● Aids people trying to learn more about OWASP and people trying to become a member</li></ul></li></ul></li><li>○ Workflows that are consumer driven, as opposed for staff to be able to keep track of members</li><li>● Is there something missing from the OWASP website that you were expecting?<ul style="list-style-type: none"><li>○ Developer outreach project with Kelly<ul style="list-style-type: none"><li>■ Want to be able to find a volunteer, assign a task in a non-management manner</li><li>■ Have been doing so with Trello and Slack</li></ul></li></ul></li></ul> <p>Feedback regarding mock ups made for New Jersey OWASP Chapter meeting</p> <ul style="list-style-type: none"><li>● Home page<ul style="list-style-type: none"><li>○ Navigation bar<ul style="list-style-type: none"><li>■ May want to find as organization a better way to reach out to sponsors besides donate</li><li>■ Events, initiatives and news might be semi-related- may be tricky to call those out</li><li>■ Membership as top level<ul style="list-style-type: none"><li>● Might want to highlight certain information for members</li></ul></li></ul></li></ul></li><li>● Filters:<ul style="list-style-type: none"><li>○ Legislature</li><li>○ Training</li></ul></li></ul>
--	---

<b>Date</b>	<b>May 27, 2016</b>
<b>Location</b>	<b>Conference call</b>
<b>Subject</b>	<b>OWASP IT Follow up Meeting- Matt Tesauro</b>
<b>Participants</b>	<p><b>OWASP</b> Matt Tesauro - IT Administrator</p> <p><b>Sooryen Technologies</b> Gin Cheng - Tech Lead Ahsun Kim - Project Manager</p>
	<b>Items</b>
	<p><b>Objective and background:</b></p> <p>The purpose of the call was a follow-up discussion regarding the OWASP website infrastructure. Specific focus was on hosting, performance, scalability, security, integration and upgradability.</p> <p><b>Key discussion items</b></p> <ul style="list-style-type: none"> <li>● Preface <ul style="list-style-type: none"> <li>○ Requesting read permission in order to look into cloud infrastructure and server specifications</li> </ul> </li> <li>● Do you have a load balancer in place? <ul style="list-style-type: none"> <li>○ No</li> </ul> </li> </ul>

- Previously, if drifted away from an A rating from SSL Labs community does not favor change
- Used Akamai CDN and drifted below an A. So we unhooked it due to the community response
- Currently, Rackspace cloud load balancer does not support forward secrecy and does not get an A rating on SSL Labs
  - Non-starter with the community
  - Recently, working around this by running a two-node MediaWiki install and using an Nginx on just a very small cloud server to do HTTP proxying
  - Have full control of the Nginx and can get us an A rating with forward secrecy
- In terms of the application layer, what alterations did you do on the server-side itself, such as Apache optimization, MariaDB, Linux downsizing, or DDOS protection?
  - Some of that changed since first IT interview; some is in the process of changing
  - Current state:
    - ApacheBuddy, a script you can run as you run Apache and gives you feedback on how to optimize your settings
    - Due to traffic spikes in March and April, Rackspace did some Apache changes by mostly changing the number of workers and changing a few of the internals
      - Under a managed service level with Rackspace so OS patching and those kinds of things are done automatically via the Rackspace people
        - Handles service outages or other problems
    - During the traffic spikes in March and April, Rackspace went in and set up Varnish as an HTTP cache on the current production Wiki server
      - Apache hands off the initial connection to Varnish which then hands it back to Apache because Varnish can't do SSL
      - Current setup but will probably unhook that and go back to two-node MediaWiki setup
      - For extra complexity, didn't do much
      - Will be better to have more nodes than bigger cached nodes-easier to scale up since just firing up an extra node.
    - Regarding DDOS protection, currently using a product from Signal Sciences that is a small Apache module that intercepts and reviews traffic prior to going off to Apache
      - Is now installed and in "blocking" mode
      - Anybody actively and aggressively cURL-ing us or running scanners against the website will get blocked for 24 hours by default
      - Can watch people sending SQL injection and set thresholds for attack attempts
      - Installed this Tuesday May 17th
  - Do you remember mid-April last year (2015) where I see a very severe spike on April 12 until April 14 on Google Analytics? After about April 27, the amount of traffic normalized.
    - During that period, Rackspace was doing the Varnish install
    - Doing some stuff with Fail2Ban but that's kind of a sledgehammer of a tool and is not very fine-grained
      - Set up a rule, some staff got caught by the rule and got banned for five minutes

- Product from Signal Sciences is much better since is native to HTTP
- Fail2Ban- not a good tool
  - In the moment, decided is better to ban a few legitimate users and keep the site up rather than let the site fall apart
  - Had to go through Rackspace's control panel and restart the VMs
- Did you install ModSecurity or mod\_evasive by any chance?
  - Have not installed ModSecurity
  - mod\_evasive isn't in the Debian repo and wasn't a Debian package last time
- Mod\_evasive is available for Ubuntu at least. There might even be a binary for it already.
  - Want to keep packages within the Debian repo because supported by Rackspace
  - Want to minimize maintenance done by OWASP by minimizing the number of outside resources
- Since you guys signed up for managed services, one additional recommendation that we were thinking of is to separate out your code base as well, because even though it is a managed service, it may not make sense to spin up an AMI Connected on to it. But that's assuming you don't do any additional changes in the near future. We were thinking of having a Git repo of the code and extensions minus the configuration and have a Chef script do the deployment and do the auto-scaling for you. Is this still necessary? Unless you have someone there to do work 24/7, then it is not necessary; but if you want completely hands-free, then segregation is necessary.
  - In favor, automation is good
  - Wanted to do this but didn't have the bandwidth
- Current Fail2Ban rules that are in place
  - Have them pretty much all turned off except for the SSH brute force
  - As for web stuff, they are all turned off since Signal Sciences does a much better job.
- Do you do any database optimization for MariaDB?
  - Yes
    - Cloud server team at Rackspace wrote a MySQL tuner that will run against your MySQL and provide optimizations
    - Can also turn on additional logging and run it a week apart and compare performance
      - Will provide recommendations
      - Have done that on the MariaDB and that's running on Rackspace
- What about the snapshots? Are the snapshots automated right now?
  - Yes, depends on how you mean snapshots
  - Two different ways natively on how Rackspace has to do backups
    - Backup the full image- a copy of the VM in essence
    - File-level backups
      - Have a cloud backup agent that runs on the box and say "these directories are the ones I care about so back them up on this schedule"
  - Doing VM-based backups once a week
    - Doing daily file-based backups for bits of the file system that make sense
      - Web root and Apache configs
    - To handle DB backups, a tool Rackspace created called Holland
      - Will make a tar.gz or bzip SQL dump of MySQL

- Write that to the file system and that gets backed up to cloud backup
        - Personally backs up the SQL dump of the databases but can do a restore in just minutes- are functionally equivalent
    - Rackspace recently added MariaDB to their cloud database products
      - When doing the two-node upgrade, going to look at the MariaDB using cloud database as a service or what they call DBaaS
        - Have automatic master slave and fail over
        - Can dynamically change the RAM and hardware allocations for the DB
        - So can significantly scale down the server with our DB
          - Doing maybe 5 or 7 percent load all the time
          - Can get a cheaper install with automatic failover and dynamically scale up if needed to the DBaaS that Rackspace has and taking it off of VM
- Yes, that was one of the recommendations. While you're grabbing the configurations, do you also have the search logs and Apache logs for the server?
  - Yes, but are huge (Gigabytes-big)
  - Do not currently enable logging for the MediaWiki search
    - Don't think it's in var/log/ don't believe is currently turned on
    - Potentially logged in the database itself- there are extensions that do log this
      - Will look for it and even give a database dump if somewhere in there out of the MariaDB and the backups
- Are you just using the default search for MediaWiki?
  - Yes- Has been several things over the time that it has been running
  - Was Sphinx search engine -> switched to an embedded Google search
  - Switched to MediaWiki search because of privacy concerns of the Europeans and primarily German community members
    - Not in favor of searches going to Google
- Do you also manage the Google Suites for OWASP?
  - One of the admins, but I do that on an ad hoc basis
    - Once to check the email logs in order to confirm delivery
    - Another instance, removing a community member from Google Apps and MediaWiki
      - Went in and deactivated his account
    - Only go in to solve particular requests or when Kate can't figure something out
- Is there anything in particular be aware of? For example, are there any Google Sites?
  - Don't think anyone has used Google Sites
  - People have used the shortener service from Google Apps
  - Couple chapters or projects that are using Google Groups
  - Have been issues with Google Groups and Mailman
    - China cannot access Google Groups
    - Europeans have privacy concerns with Google Groups
    - Have been a few small experiments outside the main Google Drive and Apps
  - All big projects are on Docs and the other Apps
- Speaking of Mailman, is there anything you prefer over it or recommend?

- Three very public attempts to do something other than Mailman that got turned down by certain members of community
  - Desire to install Mailman 3
    - Mailman- Many bad practices built into that software
    - Mailman 3- Complete rewrite and is significantly better; finally just came out of beta
    - Feel okay with installing
  - Discuss, written with Ruby on Rail
    - Better forum software
    - Mobile friendly
    - Can upvote things
  - Hard to get either community consensus or the board to bless radical change
  - In regards to the SaaS, a lot of the solutions we have been looking at, for example going from GitHub to BitBucket (because Atlassian donated a license to OWASP), have Confluence where you can do the documentation and is more intuitive than that of MediaWiki and the data from GitHub is not flowing into MediaWiki to begin with.
    - Would be interesting- have worked with Confluence at companies; have no major gripes about it
  - There is a lot of great content on MediaWiki, but there needs to be clear segregation between OWASP foundation, business, marketing side versus the projects themselves. It should not be nested into one single location and there should be better navigation and layout to reduce confusion.
    - Should have a brochure-like site that can be static that does not have to be editable by the community as well as wiki.owasp.org where the wiki stuff lives
- Feedback regarding mock ups made for New Jersey OWASP Chapter meeting
- In favor of
  - Navigation
    - As long as chapters is a category- would be fine to have under Membership as chapters are the main way to get members involved
  - Project page
    - Agreement that start/update an existing project is important
    - Agreement that adding a button to get project funding
      - Many users are not aware that they can get funding for their projects.
    - Would switch Incubators and Labs positions
      - Would also be nice to somehow highlight the higher level projects even though there are a lot of lower end projects
  - We were also thinking about similar projects, but that would require a project curator who has in-depth knowledge on every single project.
    - Would be a good idea
  - Navigation for projects
    - Looks good
  - Regarding a sample project page mockup that is being discussed and designed.
    - Likes the idea of skinning MediaWiki and add additional functions similar to what is in mockups with some functionality integrated with Meetup and Salesforce
    - Likes the idea of allowing users to create a Meetup on the MediaWiki site itself
      - Chapter leaders who rarely touch their chapter pages can engage members through Meetup instead
      - One of the biggest complaint about MediaWiki because markup is its own thing
      - Editing should be easier so the barrier to entry can be lowered



- Would be nice to do a clean MediaWiki install, get databases into it and select the extensions that we really need
  - Wants to turn off some of the 50+ extensions that currently are on the Wiki without breaking functionality
  - Extensions are a headache.
- Because there's no flow from GitHub to MediaWiki, the wiki pages are outdated compared to the GitHub repo contents. That's why we were thinking BitBucket and Confluence, but there may be a problem with the SaaS model.
  - Privacy concerns with SaaS are always there
  - Some people especially like that it's Wiki- a level of trust due to not being some faceless U.S. corporation
- The mailing list is mainly used for facilitating discussion. Do you think a Stack Overflow-like implementation will be helpful and will that also help retire Mailman to some extent?
  - Would be useful
  - Looked at other packages like Discuss that are like Stack Exchange
    - This kind of model is best for these kinds of discussions
  - Mailman is for people to make announcements within the subscribed group; not in favor of Mailman
    - Implemented a spam filter that essentially kept Mailman alive, but a maintenance headache
  - Having it more open like Stack Exchange is a better and more useful and more transparent model
  - Visibility aspect is a good hook
- In terms of other technology tools, what other suggestions do you have that will benefit the OWASP community that are not currently being fulfilled right now?
  - Let's Encrypt that finally came out of its beta
  - Have to do that across the board for SSL certs but that doesn't affect the community per se
  - Would like to see some sort of badges thing
    - Mozilla has their Mozilla's Open Badges
    - Linux foundation has the core infrastructure of badges application
    - Project leaders and chapter leaders that tick so many boxes can get a badge
      - Opened the OWASP supporters badge thing and got some negative feedback.
- Are there any improvements you would like to see on the OWASP frontend?
  - No- In favor of mockups
- Are there certain pieces of information that you feel like is missing from the OWASP website?
  - Metadata on GitHub
  - Meetup being integrated into the OWASP site
  - Integrations will be huge boons to community
- What else do you believe will help drive community engagement on the site?
  - Segregating content by users
  - Stale versus not-stale content on the wiki
  - Brochure-like website or a better skin on MediaWiki that looks more modern
  - Mobile-friendly designs are also important.
- Have you had any issues with starting a project following the MediaWiki process?
  - No, but because has worked with MediaWiki for many years

- Rackspace open source project that Matt encouraged into becoming an OWASP project instead of sitting in GitHub
  - Sent the creator a link to the form and was able to get an OWASP project
    - Didn't complain
- Likely finding that link is the key part of the problem
- Is there sufficient documentation for on-going projects such that new volunteers can go through the material and potentially contribute?
  - Project Handbook needs help
    - Very useful document to handle point questions- not many will read through all of it
    - Making sure bits are discoverable inside that handbook is really important
  - For developers that want to ask remediation advice, at Pearson, have a bot that sits in an AppSec group chatroom
    - Can ask the bot advice on cross-site scripting
    - Will give a little blurb on cross-site scripting and link to our OWASP page
    - Some sort of chat bot on how to start a project will be good
- Do you believe there is enough visibility as to what projects the OWASP community is currently working on?
  - Hardly any visibility
  - Even project leaders don't have a scope on the other projects out there
  - Even when looking for something on OWASP, have to Google it
- Have you had any issues getting subject matter experts or volunteers for specific projects?
  - Haven't tried to do that for own projects
  - Had cases before where people approach me to help and then disappear for life reasons
  - Had people come and go particularly with OWASP WTE
  - Last time with a technical question, reached out on a PM on Twitter to someone from the community
- Are there some tools you would retire in the list: Twitter, Slack, Meetup, etc.?
  - Don't think any of those are in the near-term retireable
  - Should make Meetup and CrowdIn work really well with OWASP and work with chapters leaders
  - Heard about Taiga.io which is open source and has a lot of cool features
- What are some metrics for OWASP project health (code/documentation) and updates you believe should be communicated on the Mediawiki for better visibility (ex. Code project details are noted on OpenHub)?
  - How recently a project was released, the latest commit, "velocity" on commits in order to measure "staleness"
  - Number of bugs, license, language, any assumed infrastructure (like Tomcat, Python, etc.)
  - A rating system where community members can say "I like this" or "I don't like this"
  - Categorization of breaker, builder, defender, dev, etc.
  - Demos of projects and Docker images and Vagrant scripts and other ways to try the code out quickly and easily