
Welcome to the OWASP Toronto Meetup

Hello, and happy 2018!

Announcement: OWASP Top 10 2017

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Changes between 2013 and 2017



Hi, I am X. How do I get into AppSec/Security?

OWASP Toronto Chapter
January 17, 2018



Topics

- Overviews, Career Paths, Advice
- Secure SDLC frameworks
- Tools & Training
- Agile & DevSecOps
- Real Life Stories
- Training, Certifications and Career Fairs



Getting the Lay of the land

Find out what jobs/roles are commonly out there, figure out where your skills overlap, find out what skills you need, etc.

[NICE Cybersecurity Workforce Framework](#)

[SANS CISO Mind Map](#) (or, [Refeeq Rehman's](#))

Henry Jiang's [Map of Cyber Security Domains](#)

[Cyberseek Career Pathway](#)



Advice

Wisdom, editorials, and
on-point snark

Krebs on Security - [How to break into Security Series](#)

(Older, but still relevant advice)

Secure SDLC: Some frameworks

OWASP SAMM



BSIMM



DOE-C2M2



NIST CSF

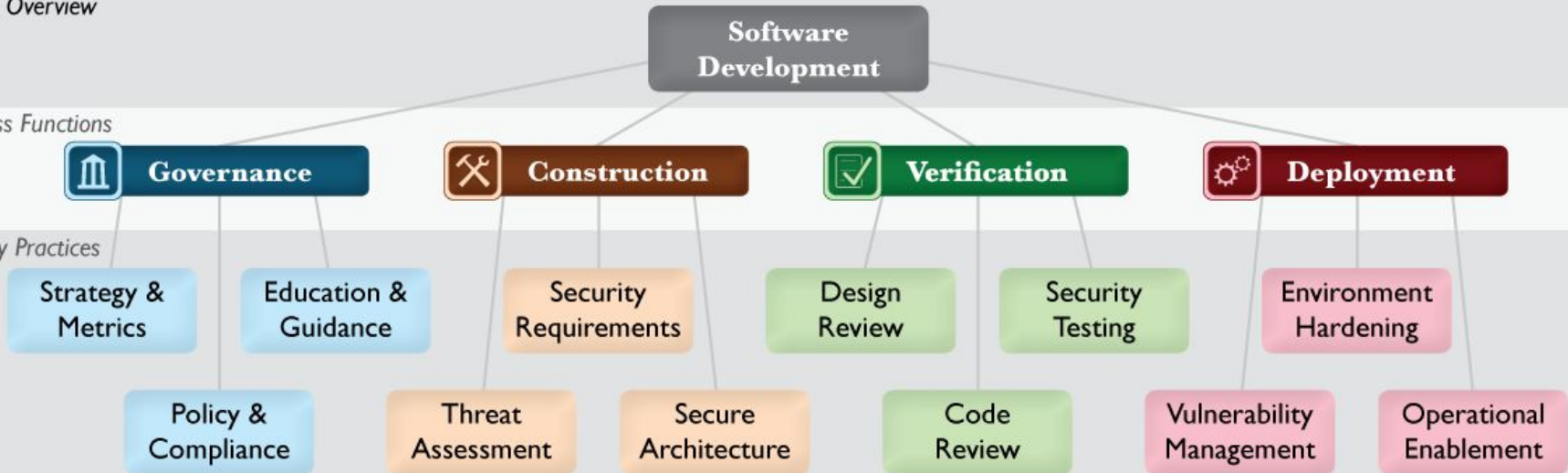


OWASP Software Assurance Maturity Model

SAMM Overview

Business Functions

Security Practices





BSIMM8

The Software Security Framework

The graphic below shows the software security framework (SSF) used to organize the 113 BSIMM activities. There are 12 practices organized into four domains.

The four domains are as follows:



Governance: Practices that help organize, manage, and measure a software security initiative. Staff development is also a central governance practice.



Intelligence: Practices that result in collections of corporate knowledge used in carrying out software security activities throughout the organization. Collections include both proactive security guidance and organizational threat modeling.



SSDL Touchpoints: Practices associated with analysis and assurance of particular software development artifacts and processes. All software security methodologies include these practices.



Deployment: Practices that interface with traditional network security and software maintenance organizations. Software configuration, maintenance, and other environment issues have direct impact on software security.

Here are the 12 practices:

Governance

1. Strategy & Metrics (SM)
2. Compliance & Policy (CP)
3. Training (T)

Intelligence

4. Attack Models (AM)
5. Security Features & Design (SFD)
6. Standards & Requirements (SR)

SSDL Touchpoints

7. Architecture Analysis (AA)
8. Code Review (CR)
9. Security Testing (ST)

Deployment

10. Penetration Testing (PT)
11. Software Environment (SE)
12. Configuration Management & Vulnerability Management (CMVM)

US Dept of Energy Capability Maturity Model

Level	Characteristics								
MIL0	<ul style="list-style-type: none"> Practices are not performed 	RISK	Risk Management	ASSET	Asset, Change, and Configuration Management	ACCESS	Identity and Access Management	THREAT	Threat and Vulnerability Management
MIL1	<ul style="list-style-type: none"> Initial practices are performed but may be ad hoc 								
MIL2	<p><i>Institutionalization characteristics:</i></p> <ul style="list-style-type: none"> Practices are documented Stakeholders are identified and involved Adequate resources are provided to support the process Standards or guidelines are used to guide practice implementation <p><i>Approach characteristic:</i></p> <ul style="list-style-type: none"> Practices are more complete or advanced than at MIL1 								
MIL3	<p><i>Institutionalization characteristics:</i></p> <ul style="list-style-type: none"> Activities are guided by policy (or other directives) and governance Policies include compliance requirements for specified standards or guidelines Activities are periodically reviewed for conformance to policy Responsibility and authority for practices are assigned to personnel Personnel performing the practice have adequate skills and knowledge <p><i>Approach characteristic:</i></p> <ul style="list-style-type: none"> Practices are more complete or advanced than at MIL2 	SITUATION	Situational Awareness	SHARING	Information Sharing and Communications	RESPONSE	Event and Incident Response, Continuity of Operations	DEPENDENCIES	Supply Chain and External Dependencies Management
		WORKFORCE	Workforce Management	CYBER	Cybersecurity Program Management	<ul style="list-style-type: none"> Domains are logical groupings of cybersecurity practices Each domain has a short name for easy reference 			



NIST Cyber Security Framework





General Sources of Info


Teach yourself, then keep up with the field.

[Infosec industry](#) site has some recommendations you can pick through.

[Blogs](#) like [SANS AppSec Blog](#) and [Google Project Zero](#)

Twitter #appsec and major players, including [Michael Geist](#) and [Office of the Privacy Commissioner of Canada](#)

[Security Podcasts](#) like [Defensive Security](#)



General Online Learning

Alternatives to Youtube, which actually has some pretty neat stuff on it too.

- [Coursera](#)
- [Cybrary](#)
- [edX](#)
- [Lynda](#) (free via Library!)
- [MIT Open Coursewear](#)
- [Udacity](#)
- [Udemy](#)



Audience ...

<http://money.cnn.com/2017/10/31/media/facebook-twitter-google-congress/index.html>

What is your job title, and what sources of information do you use regularly?

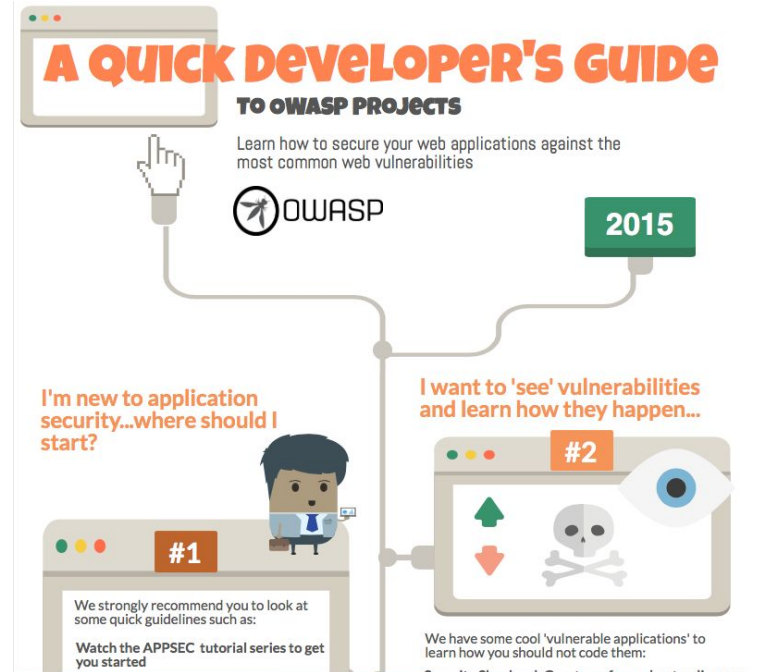


Point of View: Developers and Testers

OWASP resources

OWASP has a lot of projects that can be helpful for developers to start learning about security. Two good starting points:

- [A Quick Developer's Guide](#)
- [OWASP Security Knowledge Framework](#)



<https://create.piktochart.com/output/6400107-untitled-infographic>



Free Secure Coding Resources*

* The latter resources also can be mined for other security-related info.

OWASP Resources

- [OWASP Code Review Guide](#)
- [OWASP Developer/Builder Cheat Sheets](#)

Secure Coding Exercises

- [Hacksplaining](#)
- [Code Bashing](#)
- RIPSTECH [PHP Security Advent Calendar](#)

Other Publications

- [CERT Secure Coding](#)
- [Safecode training](#)



Security Testing Resources

Learn about the basic classes of application security vulnerabilities with hands-on, practical, guided lessons.

Deliberately Vulnerable Applications

- [OWASP Juice Shop](#)
- [OWASP WebGoat](#)
- [OWASP Security Shepherd](#)

HTTP Proxies (+ other awesomeness)

- [OWASP Zed Attack Proxy \(ZAP\)](#)
- [Burp Suite Community Edition](#)
- [Kali Linux \(+ forensics mode\)](#)



Capture the Flag!

Training Wheels are off.... Go hack stuff.

An [Intro to CTFs](#)

[CTF Time Calendar](#)

Vulnerable VMs to practice on in a lab, often abstracted from CTFs.

- <https://www.vulnhub.com/>
(they also suggest some resources)



Real Life Challenges

Legally try your skills against real targets.

Be sure to read the instructions, code of ethics, and bounty rules.

[Whitehat CERN hacking challenge](#)
(students only)

[Bug Bounty Programs](#)

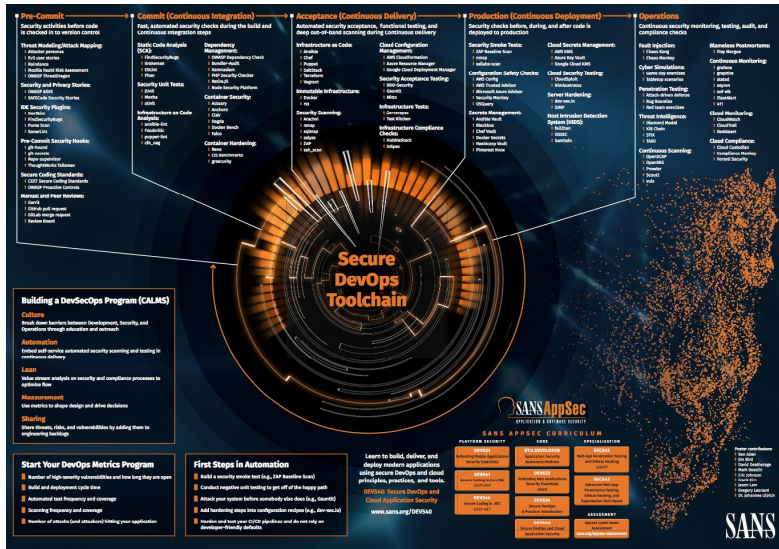


Agile?

- Secure SDLC vs CI (Continuous Integration) and CD (Continuous Development / Delivery / Deployment)
- [SDL-Agile Requirements?](#)
- Thoughts from the audience?

Point of View: Dev Ops

Secure DevOps Toolchain from SANS



Securing Web Application Technologies (SWAT) CHECKLIST

BY SANS AND SANS APPSEC

The best checklist practice is to use the reference as a best practice that one may use and then tailor based on their own secure applications. It's a baseline, not a checklist to be blindly followed and not a substitute for responsible vulnerability to your critical applications.

Category	Item	Priority
DATA PROTECTION	Encrypt sensitive data at rest and in transit	High
	Implement strong access controls for data	High
	Use secure protocols for data transfer	High
	Regularly update and patch data protection software	High
	Implement data backup and recovery procedures	High
	Use secure storage solutions	High
	Implement data retention and deletion policies	High
	Use secure APIs for data access	High
	Implement data encryption key management	High
	Use secure data processing pipelines	High
Implement data security monitoring and logging	High	
AUTHENTICATION	Implement strong authentication mechanisms	High
	Use secure protocols for authentication	High
	Implement multi-factor authentication	High
	Use secure session management	High
	Implement secure password storage	High
	Use secure authentication providers	High
	Implement secure API authentication	High
	Use secure authentication tokens	High
	Implement secure authentication flow	High
	Use secure authentication headers	High
ERROR HANDLING AND LOGGING	Implement secure error handling	High
	Use secure logging mechanisms	High
	Implement secure log storage	High
	Use secure log transport	High
	Implement secure log retention	High
	Use secure log access controls	High
	Implement secure log monitoring	High
	Use secure log alerting	High
	Implement secure log backup	High
	Use secure log recovery	High
SYSTEM HARDWARE	Implement secure hardware configurations	High
	Use secure hardware components	High
	Implement secure hardware updates	High
	Use secure hardware monitoring	High
	Implement secure hardware testing	High
	Use secure hardware validation	High
	Implement secure hardware configuration management	High
	Use secure hardware security monitoring	High
	Implement secure hardware security incident response	High
	Use secure hardware security recovery	High
CONSIDERATION AND OPERATIONS	Implement secure consideration and operations	High
	Use secure consideration and operations tools	High
	Implement secure consideration and operations updates	High
	Use secure consideration and operations monitoring	High
	Implement secure consideration and operations testing	High
	Use secure consideration and operations validation	High
	Implement secure consideration and operations configuration management	High
	Use secure consideration and operations security monitoring	High
	Implement secure consideration and operations security incident response	High
	Use secure consideration and operations security recovery	High
ACCESS CONTROL	Implement secure access control mechanisms	High
	Use secure access control protocols	High
	Implement secure access control updates	High
	Use secure access control monitoring	High
	Implement secure access control testing	High
	Use secure access control validation	High
	Implement secure access control configuration management	High
	Use secure access control security monitoring	High
	Implement secure access control security incident response	High
	Use secure access control security recovery	High

SANS APPSEC CURRICULUM

Platform Security | Cloud Security | Mobile Security | IoT Security | Hardware Security | Power Security | ES Security | Threat Modeling | Security Policy Review | Security and Privacy Stories | Security Scans | Cloud Security Monitoring | Configuration Management | Security Scans | Cloud Security Monitoring | Configuration Management

Securing Web Application Technologies (SWAT) CHECKLIST

BY SANS AND SANS APPSEC

Improving security into the mind of every developer.

software-security.sans.org

<https://www.sans.org/security-resources/posters/secure-devops-toolchain-swat-checklist/60/download>



Additional DevSecOps Resources

Whether you stay earthbound or
go to the cloud.

- [OWASP Appsec Pipeline](#)
- [DevSecOps Studio](#)
- [Awesome DevSecOps](#)
- [AWS codepipeline devsecops](#)

Point of View: Non-Devs



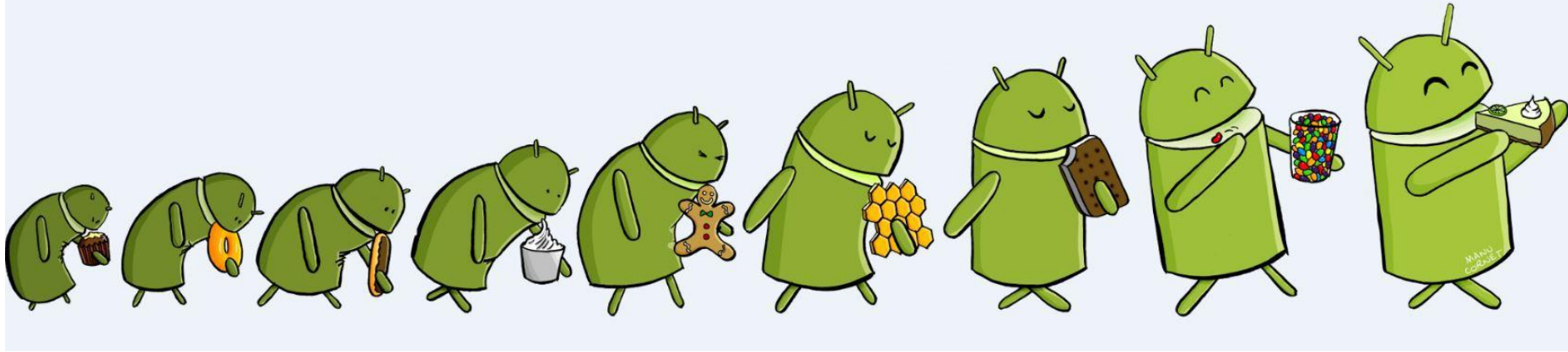
Learn to Program

Scripting experience and compiled language programming are both good to have.

Check out Laurence Bradford's [list](#) of resources..

- [Free Code Camp](#)
- [Code Wars](#)

Security Origin Stories



Certifications & Career Fairs



(ISC)²

- Not free!
- CISSP (Certified Information Systems Security Professional)
 - Concentrations:
 - ISSAP (Architecture)
 - ISSEP (Engineering)
 - ISSMP (Manager)
- Relevant to application security:
 - CSSLP (Certified Secure Software Lifecycle Professional)
- Others:
 - CCSP (Cloud)



SANS Courses / GIAC Certifications

- Not free!
- SANS training courses with associated GIAC certifications
- Relevant to application security:
 - GWAPT
 - GWEB
 - GSSP-JAVA, GSSP-NET



Pen Testing Certifications

- [Offensive Security Certified Professional](#) (heavy focus on network-based content, but still somewhat relevant)



Product Specific Certifications

- CCNA / CCNE
- Security+



Career Fairs

- [Sheridan College Biztech](#): February 14, 2018
- [SecTor Expo](#): October 1-3, 2018
- [TASK](#): TBD



Audience ...

- AppSec / Security professionals:

What training or certifications or skills have you found to be most useful to your career?



- Hiring managers:

What do you like to see in candidates?

Questions? Closing Comments?

