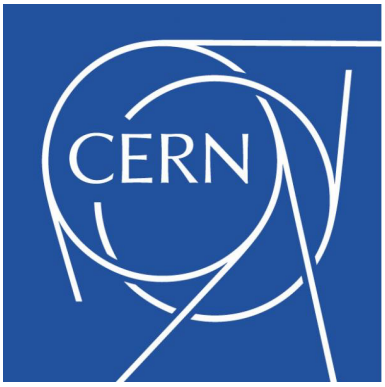


Deploying APEX Vulnerability Scanner

CERN Summer Student Report 2016

Author: Silvia Väli
Supervisor: Sebastian Lopienski
August 2016

Abstract

Most of the APEX applications have not been developed considering security in mind or were developed many years ago, as well as the old version of APEX used exposes those type of applications to a variety of potential security risks. CERN develops and uses many APEX applications, but none of the currently used tools provides a sufficient way of vulnerability scanning for such applications. The current version of APEX used in CERN is 4.2.6 whilst the latest version is 5.1.

This report provides the reader with the overview on APEX and the APEX-SERT vulnerability scanning tool as well as the summary of testing the APEX-SERT tool on existing APEX applications used in CERN and the samples, created during this project. The goal of this project was to research on existing tools for vulnerability scanning of APEX applications and to deploy the tool to be used APEX developers.

The project outline

The project began with a research on **APEX 4.2.6 applications** to know how these type of applications are created, exported and used, what functionalities they offer for developers and the potential vulnerabilities they hold. Following tutorials and gaining knowledge from APEX security books, the result was three different types of sample applications with purposely made vulnerabilities of different types, such as XSS (Cross-Site-Scripting), SQL-injection and missing item/page protection. The research on available tools resulted in finding an open-source tool APEX-SERT from github: https://github.com/OraOpenSource/apex-sert which later on was deployed and tested in various (test & development) environments, on sample applications and on existing CERN applications along with the developers. APEX-SERT is currently deployed in five different CERN databases and is visible for and ready to be used by the developers who have APEX applications in any of those workspaces mentioned above.

What is APEX?

APEX (**Ap**plication **Ex**press [1]) is a rapid application development tool which uses Oracle DB and PL/SQL. APEX enables to design, develop and deploy database-driven applications directly from the browser-based IDE and it is easily customisable. APEX Express is a no-cost feature which is fully supported if one already has Oracle database.

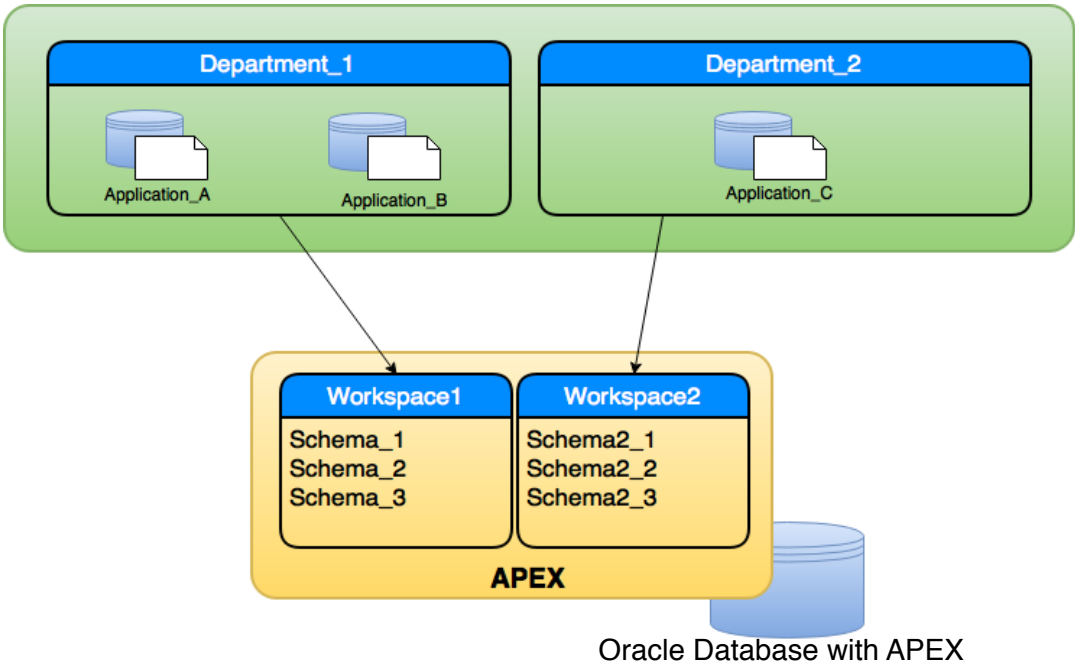


Image 1. APEX Structure

APEX is installed in the Oracle database where also all the application data is stored. Each "department" can have several separate APEX applications within a workspace which can have multiple schemas to store application information. Each of those applications consist of pages and page elements and applications that are used by multiple users.

What is APEX-SERT ?

*Security Evaluation and Recommendation Tool of Application Express

1. APEX-SERT is an open source APEX application, with the GNU Lesser General Public License, version 3.0 (LGPL-3.0) that is designed to evaluate APEX applications for security vulnerabilities;
2. APEX-SERT installs into your instance of APEX one time and is instantly available to any developer using their existing credentials;
3. APEX-SERT currently works with APEX 4.2.5 or later [in CERN the current version in use is APEX 4.2.6]; support for APEX 5 is coming (now in beta);
4. Once installed, any developer can run APEX-SERT on applications that reside in their respective workspace;
5. APEX-SERT is open source and 100% free to download and use;
6. It is actively being developed and supported by the author of "Oracle Application Expression Security" book, Scott Spendolini.

1. Spendolini, S. (2013). "**Expert Oracle Application Express Security**". New York: Apress

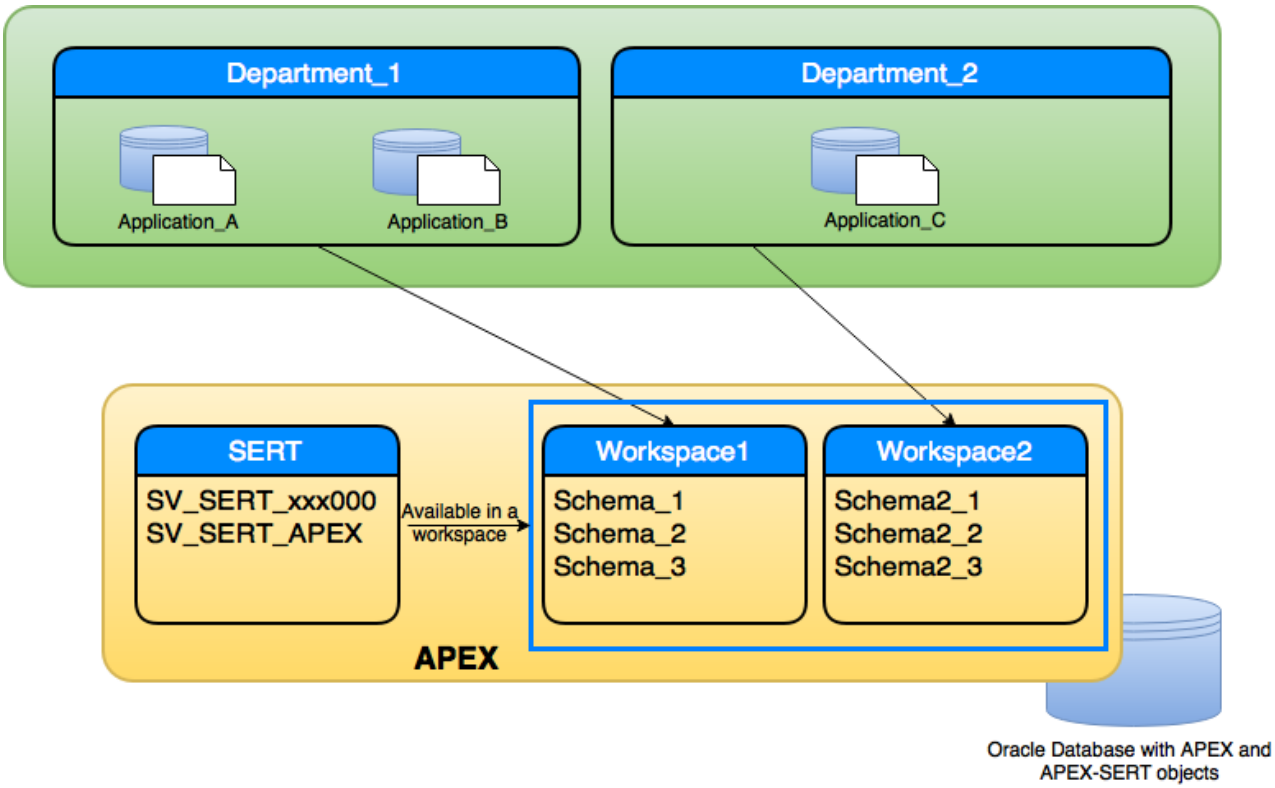


Image 2. APEX-SERT

APEX-SERT Installation is done via single SQL script, which installs required database objects, creates the APEX-SERT workspace called "SERT" and installs APEX-SERT applications within that workspace. Installation will create 2 schemas in the database "SV_SERT_xxx000" and "SV_SERT_APEX". SV_SERT_xxx000 holds all APEX-SERT database objects.

***Important note!** Schema SV_SERT_xxx000 - xxx depends on the version of APEX-SERT that is being installed

As a tool, APEX-SERT is easy to use and its workflow could be described as on the image below. A developer who is developing or owns an APEX application in a workspace should login to their APEX workspace and launch the APEX-SERT vulnerability scanner from that workspace, then choose an application to evaluate from the tools' interface, and after evaluation has started, a report with found vulnerabilities will be generated and displayed as a result.

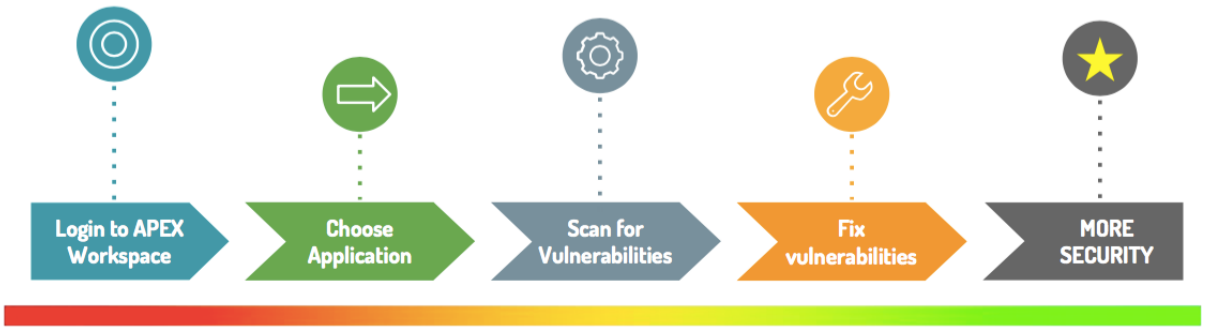
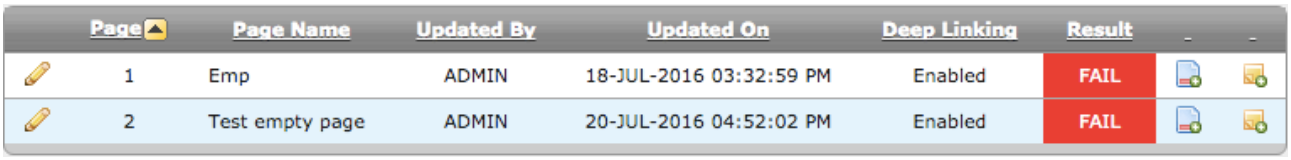


Image 3. APEX-SERT Tool 5 Steps

The report will provide the developer with a good overview of vulnerabilities found in the form of a chart, which when clicked, enables access to a more detailed view on each vulnerability category.Vulnerabilities can be described with fields such as the page number in the application, page name, which user gave the value to the item and when, item's current value, item's suggested value (not in all cases, depending on the category), result (FAIL/PASS) — whether it was detected as a vulnerability or not, exceptions, notes, and a direct link to the application to remedy the found vulnerability. It its also possible to create an exception to treat the vulnerability as a false-positive in which case the result will be marked as "PENDING" until a user has approved that exception.



Page	Page Name	Updated By	Updated On	Deep Linking	Result		
1	Emp	ADMIN	18-JUL-2016 03:32:59 PM	Enabled	FAIL		
2	Test empty page	ADMIN	20-JUL-2016 04:52:02 PM	Enabled	FAIL		

Image 4. Example of a Detailed View of Found Vulnerabilities

Important note! Users who make an exception cannot approve it or reject it. Therefore if an application has ONE user/developer working on it, the user needs two accounts, one as admin and one as a developer to use one for making the exceptions and one for approving/rejecting exceptions. For CERN, it would be more useful to find a solution where approving/rejecting would be combined under one account, since most APEX applications are developed by 1 developer.

APEX-SERT Admin Panel

APEX-SERT comes with an admin panel which is used to configure the instance of APEX-SERT, manage users, roles assigned to users and perform other administrative tasks such as scheduling job-runs (automatic weekly/monthly evaluations of APEX applications), following evaluation logs and managing e-mail notifications. Upon installation of APEX-SERT, the admin panel can be reached at the following URL:

URL: https://servername.com/dad/f?p=SERT_ADMIN
In CERN: https://apex-sso.cern.ch/pls/htmldb_some_database_name/f?p=SERT_ADMIN
SERVER NAME: apex-sso-cern.ch or webdev.cern.ch

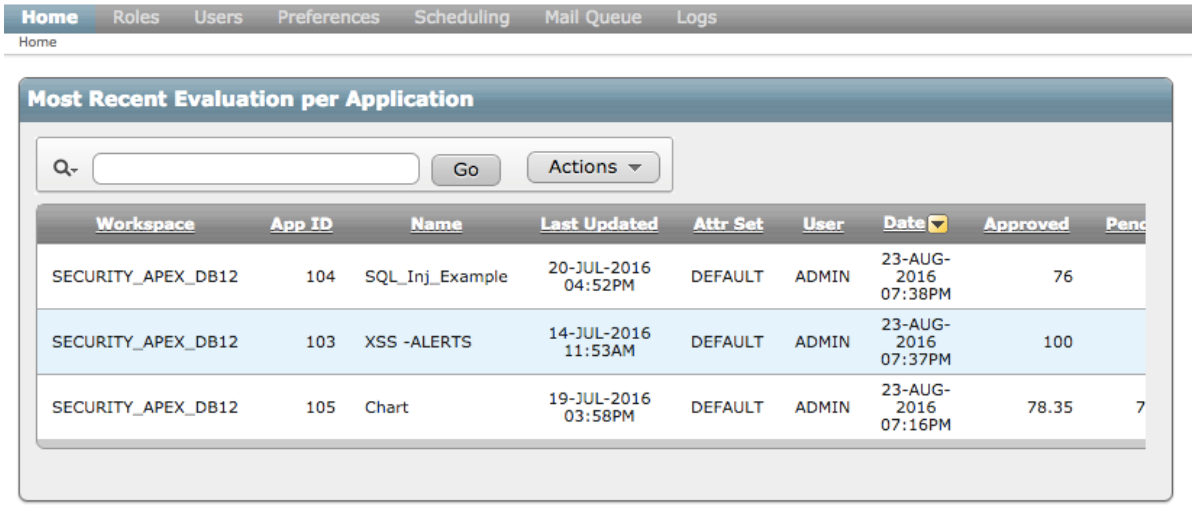


Image 5. APEX-SERT Admin Panel

Testing APEX-SERT

The tool has been tested on various databases with a number of APEX developers. Testing the tool showed that indeed it is rather easy to use and evaluation on available APEX applications in CERN does not take too much time (approximately 10 seconds). The tool was able to find vulnerabilities in each tested application from different categories: XSS (Cross-Site_scripting), SQL-injection, item protection, item encryption, no limitation on maximum row counts, deep linking, session duration, application settings and more. When testing the tool on sample applications with purposely made vulnerabilities, (SQL-Injection, XSS, missing item/page protection) the tool was able to identify all of them.

Another aspect that appeared from testing is that developers need training on APEX security and this tool could provide it to some extent, as it gives information on most discovered vulnerabilities and answers the question of why the found vulnerability was a vulnerability in the first place, gives a solution on how to fix it and a direct linkages to the correct application and a parameter to fix.

Evaluation example – XSS ALERTS

Application was 77, 14% approved.
Application was purposely made vulnerable for XSS in the application's report columns.

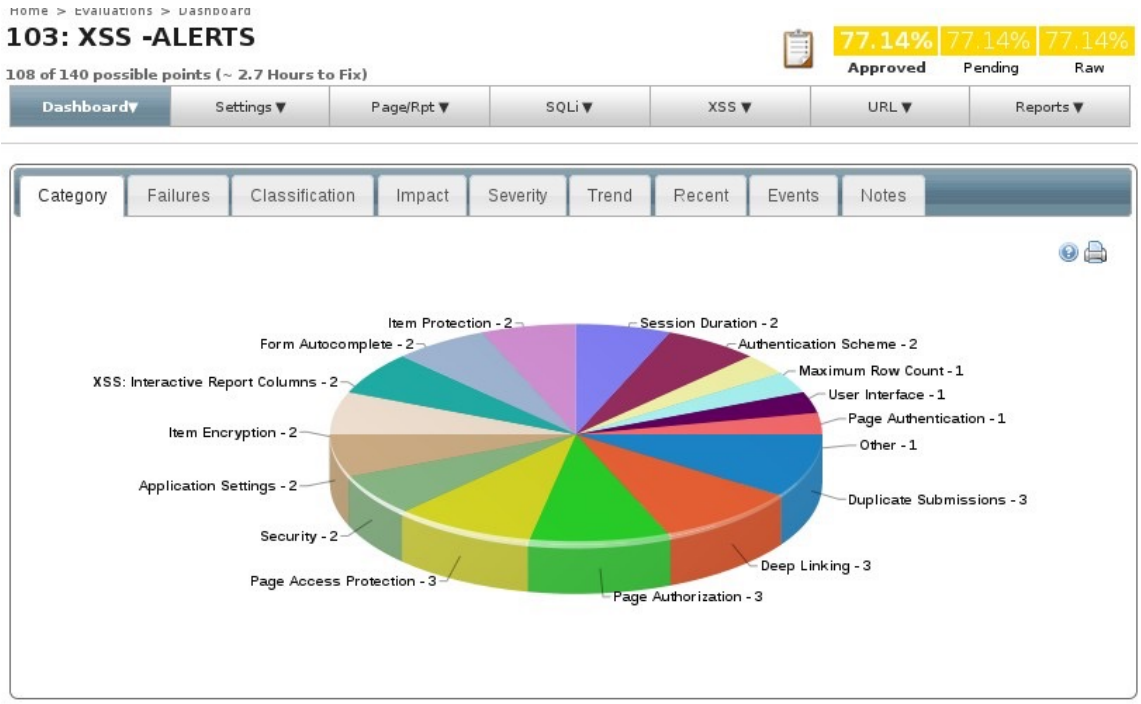
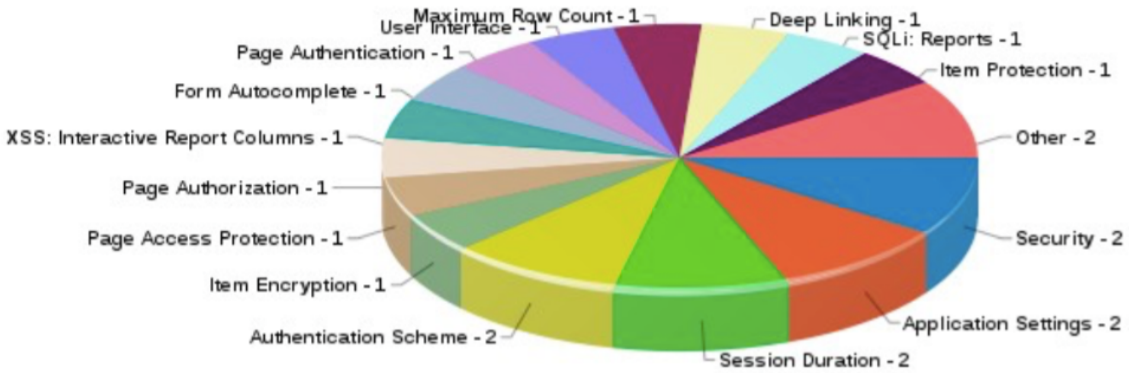


Image 6. Evaluation report of sample application with planted vulnerability - XSS Alert

The tool found the mistakes I did intentionally such as on interactive reports not escaping special characters, maximum row count over 1000 and item protection not enabled.

Evaluation example – SQL-injection

Application was 77, 01% approved.
Application was purposely made to be vulnerable for SQL-injection



The tool found the vulnerability and identified it as a SQL injection vulnerability
(SQL:Reports - 1)

Conclusions

APEX enables a quick development for web-based applications and finds usage by a variety of users from different departments within CERN, which makes it important to scan those web-applications for vulnerabilities, more over for vulnerabilities in APEX 4.2.6, since CERN is not using the latest version 5.1 yet. APEX-SERT tool provides a good overview on scanned applications and found vulnerabilities and an easy way to fix them. The tool needs more integration to the development phase of APEX applications, so it would be used throughout the developing process and vulnerabilities would be eliminated as soon as possible. For APEX applications where the development phase has already passed, the tool will provide feedback on their current condition and possible ways to remedy found vulnerabilities as well. The APEX-SERT tool has been deployed in multiple workspaces and available for the developers who are able to build those type of applications now being more aware of the potential vulnerabilities.

Further reading:

QUICK START Guide for Developers https://security.web.cern.ch/security/recommendations/en/APEX-security-QUICK-START.pdf

Securing APEX Applications – CERN Computer Security Web
https://security.web.cern.ch/security/recommendations/en/apex_applications.shtml

KB Articles about APEX
"How to Ensure The Security of My APEX Application"
https://cern.service-now.com/service-portal/article.do?n=KB0004190
"Comment assurer la sécurité de mes applications APEX"
https://cern.service-now.com/service-portal/article.do?n=KB0004191

More thorough materials on APEX-SERT, presentations, credentials to admin panel and workspaces
https://twiki.cern.ch/twiki/bin/viewauth/ComputerSecurity/ProjectsAPEXSecurity