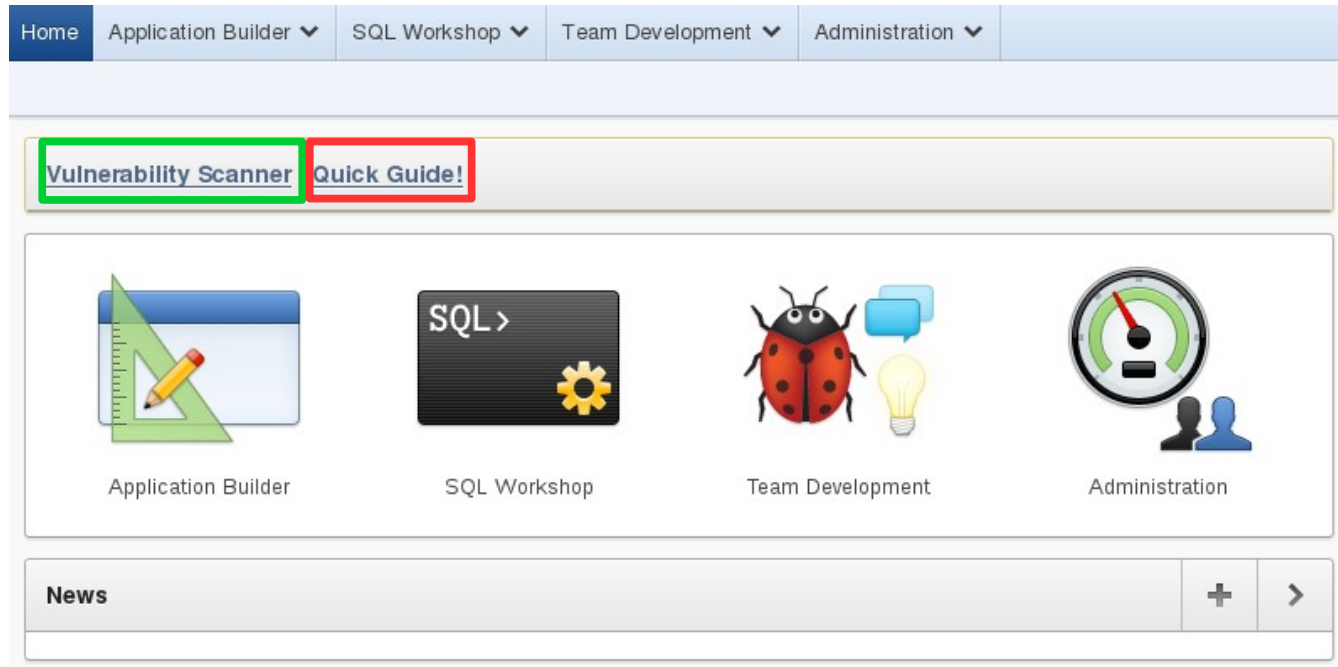


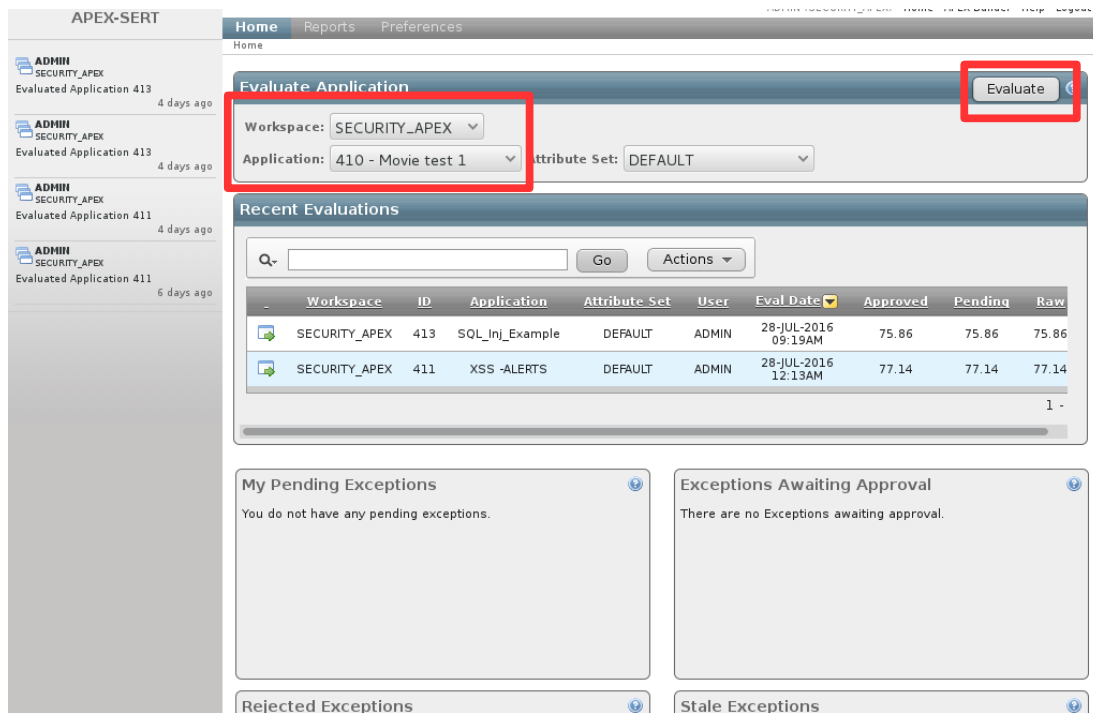
# QUICK START

## Vulnerability scanner for APEX Applications

**1. Launch vulnerability scanner by clicking on the button “Vulnerability Scanner” shown below in your APEX workspace (Quick Guide - for information on the tool):**



**2. Choose a “Workspace” and “Application” you want to evaluate and click “Evaluate”**



### 3. Evaluation report – chart displays different categories of possible vulnerabilities found

**APEX-SERT**

Attribute Set:  
DEFAULT

Recalculate Entire Score

ADMIN (SECURITY\_APEX) Home APEX Builder Help Logout

Home > Reports > Preferences

Home > Evaluations > Dashboard

**413: SQL\_Inj\_Example**

66 of 87 possible points (~ 1.8 Hours to Fix)

75.86% Approved 75.86% Pending 75.86% Raw

Dashboard Settings Page/Rpt SQLi XSS URL Reports

Category	Count
Settings	7
Page/Rpt	1
SQLi	1
XSS	1
URL	3

Category
Failures
Classification
Impact
Severity
Trend
Recent
Events
Notes

Category	Count
Maximum Row Count	1
User Interface	1
Deep Linking	1
SQLi: Reports	1
Item Protection	1
Other	2
Security	2
Application Settings	2
Session Duration	2
Authentication Scheme	2
Page Access Protection	1
Page Authorization	1
XSS: Interactive Report Columns	1
Form Autocomplete	1
Page Authentication	1

**ADMIN SECURITY\_APEX**  
Evaluated Application 413  
26 seconds ago

**ADMIN SECURITY\_APEX**  
Evaluated Application 413  
4 days ago

**ADMIN SECURITY\_APEX**  
Evaluated Application 413  
4 days ago

**4.1 To see vulnerabilities more detailed, click on any of the chart fields or text descriptions shown above and a more detailed list will appear (shown below)**

The screenshot displays the APEX-SERT interface for a security evaluation. The main report is titled '413: SQL\_Inj\_Example' with a score of 75.86%. The interface includes a sidebar with a bar chart showing scores for various categories: Settings (7), Page/Rpt (1), SQLi (1), XSS (1), and URL (3). The main content area shows a table of findings for 'Region Name : EMP'.

Alias	Label	Format	Result	Exception	Notes
COMM	Comm	Escape Sc	PASS	-	-
DEPTNO	Deptno	Escape Sc	PASS	-	-
EMPNO	Empno	Escape Sc	PASS	-	-
ENAME	Ename	Without Modification	FAIL	<input type="checkbox"/>	<input type="text"/>
HIREDATE	Hiredate	Escape Sc	PASS	-	-
JOB	Job	Escape Sc	PASS	-	-
MGR	Mgr	Escape Sc	PASS	-	-
SAL	Sal	Escape Sc	PASS	-	-

- A) Fix – description of how to fix a found vulnerability
- B) More information on the vulnerability
- C) Pencil sign – direct link to the application to fix the vulnerability
- D) Result field (PASS – no vulnerability detected, FAIL – vulnerability detected)
- E) Exceptions – in case of false positive or acceptable risk, user can mark found vulnerability as an exception.
- F) Notes – to write notes manually (will appear in Dashboard – menu)

**4.2 ... or click from the Menu on “Reports” > “Issues per page” which gives a quick overview as a list of vulnerability categories per page.**

Reports > Issues by Page

### 410: Movie test 1

92 of 123 possible points (~ 2.6 Hours to Fix)

74.8% Approved 74.8% Pending 74.8% Raw

Dashboard Settings Page/Rpt SQLi XSS URL Reports

#### Issues by Page

Q- [ ] Go [ ] [ ] Actions

1 2

Page : -1			
Category Name	Attribute	Component Name	Result
<a href="#">Settings: Application Settings</a>	Availability Status	-	FAIL
<a href="#">Settings: Application Settings</a>	Build Status	-	FAIL
<a href="#">Settings: Authentication Scheme</a>	Logout URL	-	FAIL
<a href="#">Settings: Authentication Scheme</a>	Secure Cookie	-	FAIL
<a href="#">Settings: Security</a>	Deep Linking	-	FAIL
<a href="#">Settings: Security</a>	Authorization Scheme	-	FAIL
<a href="#">Settings: Session Duration</a>	Maximum Session Length	-	FAIL
<a href="#">Settings: Session Duration</a>	Maximum Session Idle	-	FAIL
<a href="#">Settings: User Interface</a>	Include Legacy Javascript	-	FAIL
Page : 1			
Category Name	Attribute	Component Name	Result
<a href="#">Page Settings: Deep Linking</a>	Deep Linking	-	FAIL
<a href="#">Page Settings: Duplicate Submissions</a>	Allow Duplicate Submissions	-	FAIL
<a href="#">Page Settings: Form Autocomplete</a>	Form Autocomplete	-	FAIL
<a href="#">Page Settings: Page Authorization</a>	Authorization Scheme	-	FAIL
<a href="#">URL Tampering: Page Access Protection</a>	Page Access Protection	-	FAIL
Page : 2			
Category Name	Attribute	Component Name	Result
<a href="#">Page Settings: Deep Linking</a>	Deep Linking	-	FAIL

1 - 15

- A) **Category name** – if clicked, it allows to see the vulnerabilities under this category more detailed
- B) **Example:** Page “-1”, Category name: “Settings: Application Settings”. (more detailed view below):

## Application Settings

Q-

Go



Actions ▾

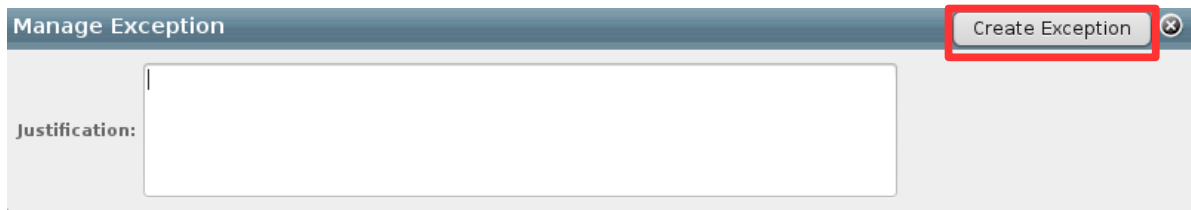
3

Setting Name ▲	Severity	Setting Value	Recommended	Result
Alias	1	F_410	-	PASS
Application E-Mail From Address	1	-	-	PASS
Application Name	1	Movie test 1	-	PASS
Availability Status	1	Available with Edit Links	Available	FAIL
Build Status	1	Run and Develop	Run Only	FAIL
Compatibility Mode	1	4.2	<ul style="list-style-type: none"> <li>4.1</li> <li>4.2</li> </ul>	PASS
Debugging	1	Not Allowed	Not Allowed	PASS
Exact Substitutions	1	Yes	Yes	PASS
Image Prefix	1	-	-	PASS
Logging	1	Yes	Yes	PASS
Proxy Server	1	-	-	PASS
Restricted User List	1	-	-	PASS
Schema Name	1	SECURITY_APEX	-	PASS
Unavailable Message	1	This application is currently unavailable at this time.	-	PASS
Version	1	release 1.0	-	PASS

## 5. Creating exceptions

**RULE:** User who makes an exception cannot approve it or reject it. Therefore if an application has ONE user/developer working on it, the user needs 2 accounts, one as an admin and one as a developer to use one for making the exceptions and one for approving/rejecting the exceptions.

1. Enter text for the exception and click “Create Exception”

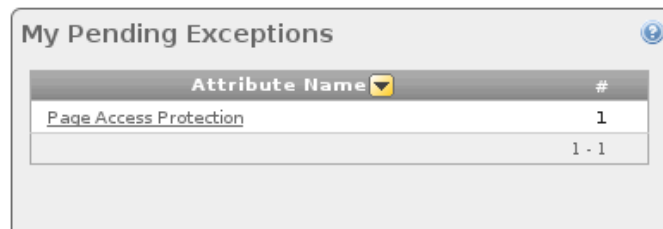


Manage Exception

Justification:

Create Exception

2. Exceptions will appear on the Dashboard under My Pending Exceptions:



My Pending Exceptions

Attribute Name	#
Page Access Protection	1

1 - 1

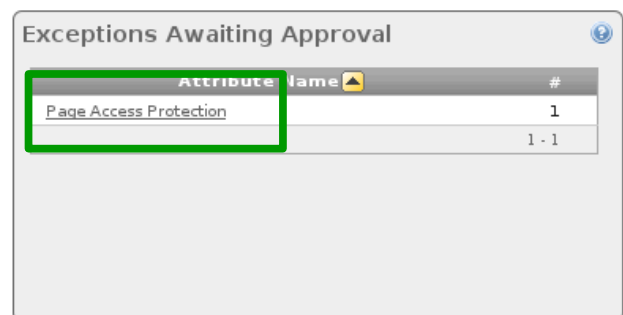
3. In order to approve or reject the exception, another user must login into the same workspace, click on “VULNERABILITY SCANNER” button to enter to the tool display, and the exception waiting to be approved/rejected appears under “Exceptions awaiting approval” on the dashboard. Click on button (shown in red), which will take the user to the evaluation report, from where to get to the exception, click on Attribute name waiting to be approved (green)



Exceptions Awaiting Approval

ID	Name	Attribute Set	#
411	XSS -ALERTS	DEFAULT	1

1 - 1



Exceptions Awaiting Approval

Attribute Name	#
Page Access Protection	1

1 - 1

4. **PENDING** marks the pending exception waiting to be approved or rejected. Click on the exception button and a manually written exception will appear.



	Page	Page Access Protection	Updated By	Updated On	Result	
	1	Unrestricted	SVALI	04-JUL-2016 10:45AM	PENDING	
	2	Unrestricted	SVALI	08-JUL-2016 11:00AM	FAIL	
	101	Unrestricted	-	04-JUL-2016 10:38AM	FAIL	

1 - 3

5. Manage Exceptions:

- **If rejected**, user can choose “Reject” and submit the reason for rejection, then click on “Submit Approval/Rejection”.
- **If approved**, just click on “Submit Approval/Rejection”



**Manage Exception** Submit Approval/Rejection

Justification: I need this to be an exception  
Created By: ADMIN (SECURITY\_APEX\_DB12) Created On: 21-JUL-2016 12:56PM

Result:  Approve  Reject

Rejection: