APEX-SERT

Version 4.2 Users Guide

Table of Contents

1. Preface

1.1. Audience

The *APEX-SERT Installation Guide* is provided as a reference to install and configure APEX-SERT. It is intended for system administrators and/or DBAs. You will require access to a database account with SYSDBA privileges to install APEX-SERT.

1.2. Conventions

The following typeset conventions are used throughout this document:

Plain Text

Plain text is nothing more than standard, narrative text. No special actions are required.

`Fixed Width`

`Fixed width` is used to denote input required from the user. When something is in the **`fixed width`** font, that text should be entered into the corresponding field or region.

Bold

Bold is used to indicate that you should perform an action, such as clicking a link or pressing a button, which corresponds to the value of the **Bold** text.

Bold Underline

Bold Underline is used to refer to a label or section of a page. **Bold Underline** labels will typically denote where an action should occur, not the action itself.

2. Introduction

2.1. Security - Why You Should Care

Security is hard. If it's not, then you're probably not doing it right. And unfortunately, more and more companies of all sizes and demographics are failing to get security right. Whether it be a major game manufacturer or credit card issuer being hacked, or a federal employee with privileges to too much data handing documents over to WikiLeaks, the news is filled with examples of companies that should have, and you would expect ***would have***, known better having their security compromised in a very public way.

This guide, along with APEX-SERT, will help you understand the potential security risks that may occur within an APEX application, how to identify then, and how to do your best to mitigate them.

NOTE: APEX-SERT focuses specifically on application level security. There are many other areas of security that should be addressed, including but not limited to: the application server, firewalls, database security, APEX instance level settings, etc.

2.2. Security Terminology

When talking about web security, there are many common terms of which you should have at least a basic understanding. Outlined in this section are the areas which web-based systems are potentially vulnerable.

2.2.1. Authentication

Authentication is the act of "logging in" to an application. Within APEX you can dictate which pages require a user to be logged-in to be able to view them. While this is a very basic level of security, the wrong setting on a page could potentially allow un-authenticated user to access data that they should not see.

2.2.2. Authorization

Authorization is a layer below Authentication. Even though the user may be logged into the application, are they authorized to see the certain aspects of the application. Authorization schemes can be applied at various levels within APEX from the Page all the way down to individual items on a form or columns within a report, allowing you to restrict specific data on a page to only those who are authorized to see it.

2.2.3. SQL Injection

SQL Injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.

Within APEX, SQL injection attacks can be introduced in one of 3 general ways:

- Use of **`&ITEM`**. notation within a SQL statement
- Calls to **`DBMS_SQL`** that could potentially make use of user input
- Calls to **`EXECUTE IMMEDIATE`** that could potentially make use of user input

In each of these circumstances, the possibility that user entered data might be used as part of the SQL Statement being executed is what introduces the risk. For example, suppose there is a a form online that allows a user to sign on with a username and password which ultimately executes this query:

```
SELECT COUNT(*) FROM users
 WHERE username = '&USERNAME.'
   AND password = '&PASSWORD.'
```

If the user were to enter this as their password:

```
i_dont_know' OR 'x' = 'x
```

The resulting SQL would be:

```
SELECT COUNT(*) FROM users
 WHERE username = 'SCOTT'
   AND password = 'i_dont_know' OR 'x' = 'x'
```

This will erroneously return **1** rather than **No Data Found** and allow the user to log in.

By using bind variables, this can be avoided:

```
SELECT COUNT(*) FROM users
 WHERE username = :USERNAME
   AND password = :PASSWORD
```

Now, if you enter this as your password:

```
i_dont_know' OR 'x' = 'x
```

Unless that is specifically your password, the database will return **No Data Found.**

Because of the potential risk, great care should be taken when using any of these methods inside of any SQL or PL/SQL executed by APEX.

2.2.4. Cross Site Scripting (XSS)

Cross Site Scripting (XSS) is a type of computer security vulnerability typically found in web applications that enables attackers to inject client-side script (such as JavaScript) into web pages viewed buy others. XSS attacks may be used to bypass access control, expose cookie information, capture and send data to other sites, etc.

An example of XSS within APEX would be a form where a user is allowed to enter free-form text and later that text is rendered back to the screen without being properly escaped. For instance if the user were to enter the following value in a COMMENT field:

```
<script type=”text/javascript”>
 alert('Hello world');
</script>
```

If the data were emitted unescaped into an APEX page, the javascript would actually be run. Therefore great care should be taken when displaying user input back to an APEX page.

2.2.5. URL Tampering

URL Tampering is potentially the most dangerous and most likely form of security breach as it does not take any programming skills to initiate and it is not an attack that most developers are trained to protect against. Any curious or malicious user can access and manipulate the URL and, if proper security measures are not in place, may be able to access data that was not meant for them.

Historically, APEX links have been coded to pass arguments un-checked on the URL as shown :

```
http://server/apex/f?p=134:10:24612647691::NO::P10_ATTRIBUTE_ID:83
```

It would be very easy for a user to simply change the value being passed to **`P10_ATTRIBUTE_ID`** and potentially see something they may not be authorized to see.

3. Overview

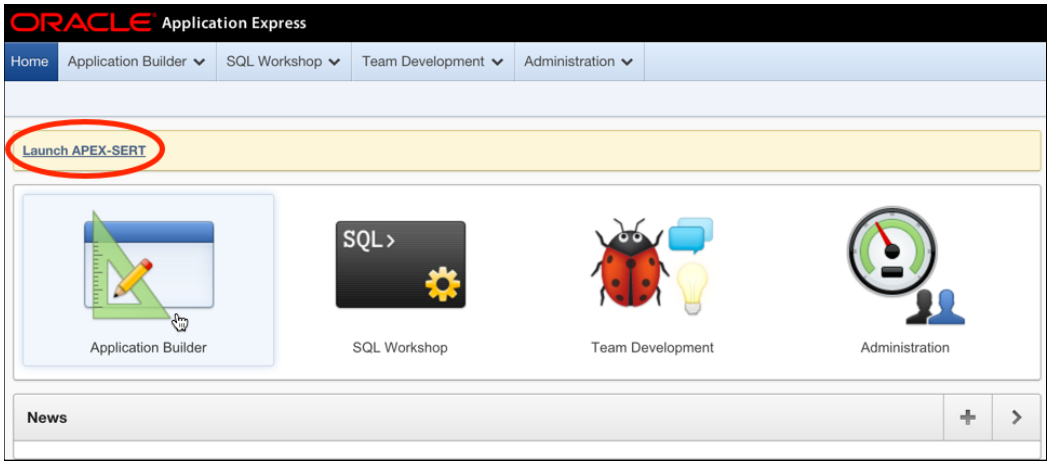
3.1. Users & Roles

APEX-SERT is designed to use your APEX workspace credentials. It does so in a way that once you are authenticated to your APEX workspace, all you will have to do is click a link to start APEX-SERT. Once APEX-SERT is installed, all users with at least developer privileges will automatically have access to run APEX-SERT for applications in their workspaces.

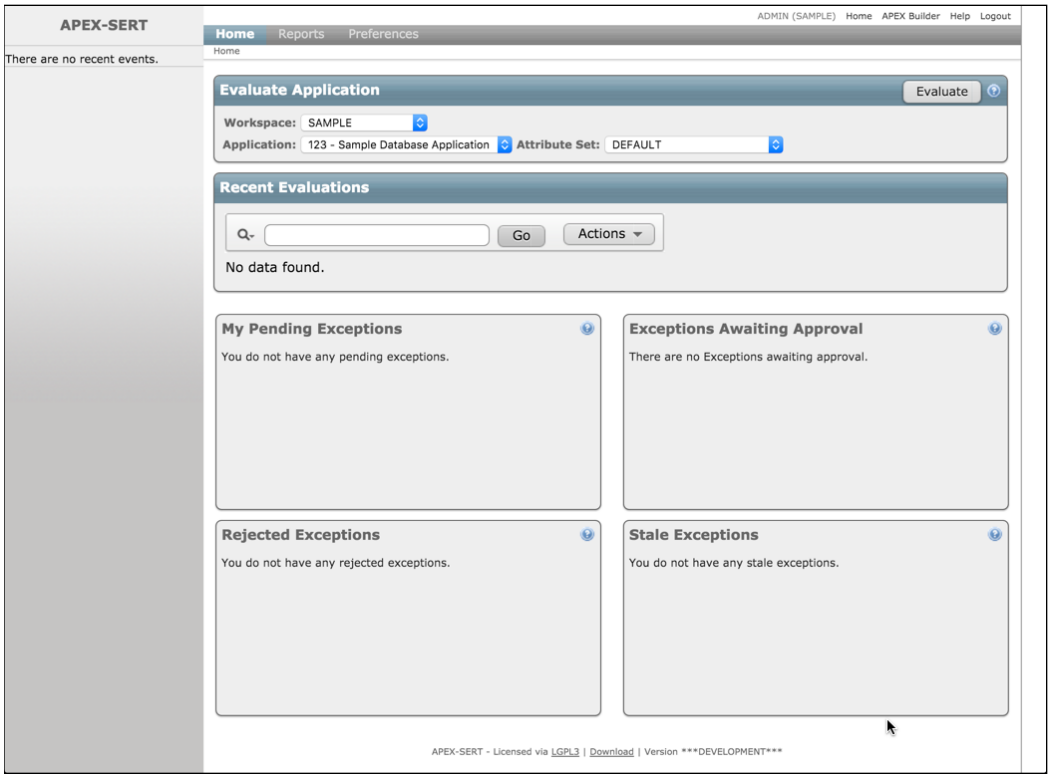
An APEX-SERT administrator can assign additional roles to your user - such as the ability to schedule evaluations or to evaluate applications from different workspaces. Please refer to the *APEX-SERT Administration Guide* for details on how this is done.

3.2. Running APEX-SERT

To run APEX-SERT, simply click the “Launch APEX-SERT” link, which can be found in the System Messages window throughout the APEX development environment.



There is no need to re-enter your credentials; APEX-SERT will securely verify that you are authenticated as a workspace developer or administrator when you click on the Launch APEX-SERT link. Upon clicking the link, APEX-SERT will open in a new browser tab:



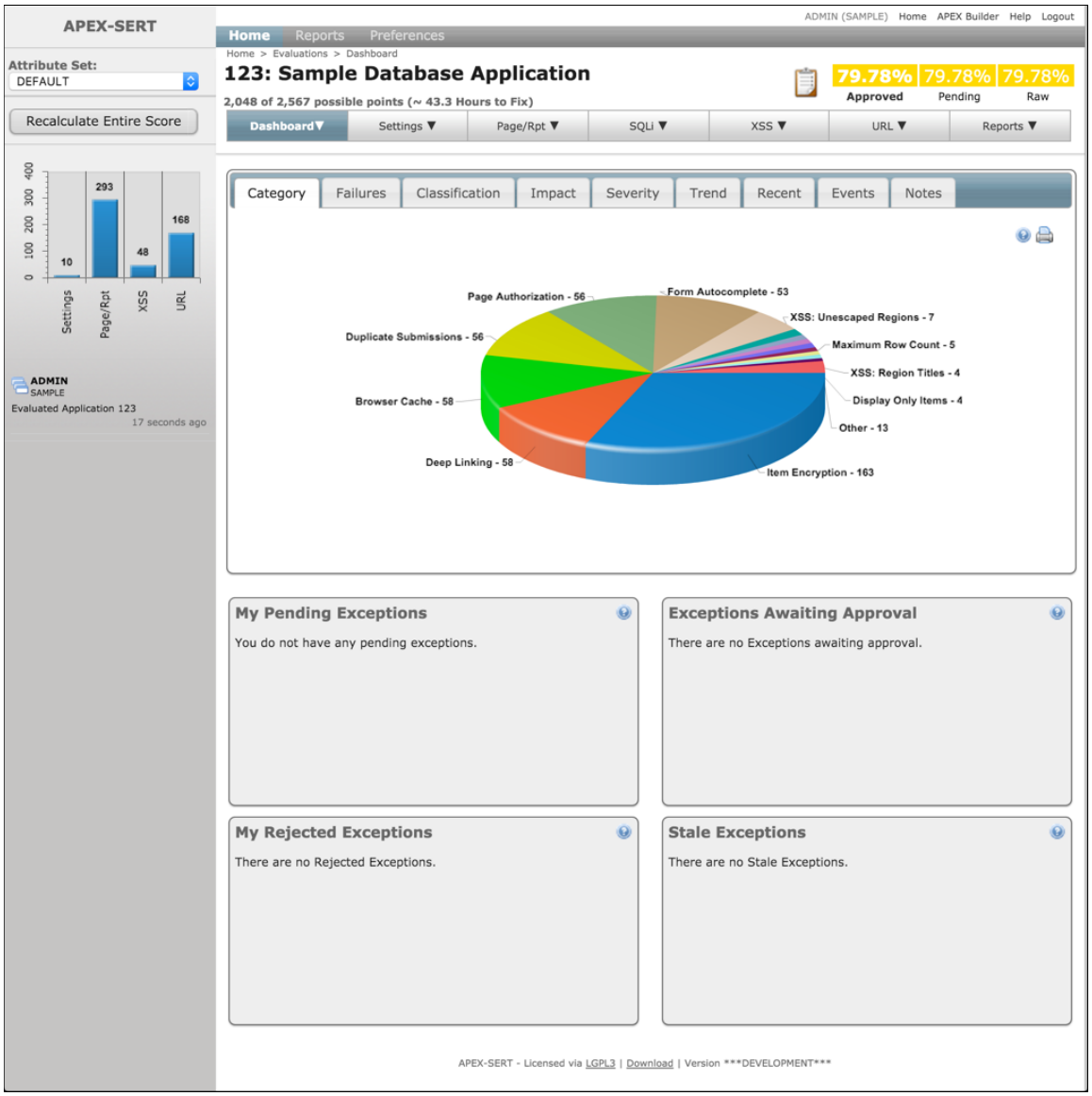
On the first launch, the home page will be quite sparse, as there have not been any evaluations run yet. As APEX-SERT is used, this page will display the high-level metrics about evaluations and exceptions.

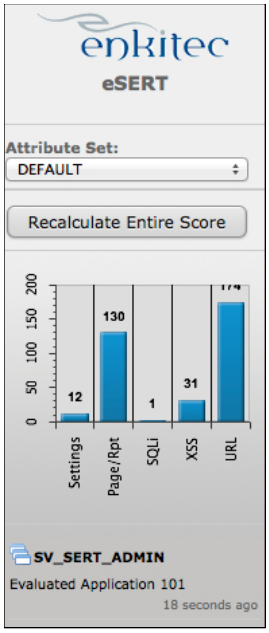
3.3. Navigation Basics

Most pages in APEX-SERT share a common set of components for consistency and ease of use. Each page can be divided up into three different regions: the sidebar, the navigation controls, and the page contents. Each of these components are used on every single page of APEX-SERT. Only the content which appears in each will differ, often just slightly in the case of the sidebar & navigation controls.

First, the left sidebar contains a number of different components, depending on which section of the tool that you're viewing. When not running an evaluation, the sidebar region may not contain anything at all. However, when running an evaluation, there are a number of components displayed there.

Within an evaluation, at the top of the sidebar is a select list with all available **Attribute Sets**, with the current one selected. To re-run the evaluation with a different **Attribute Set**, simply select it from the list. APEX-SERT will automatically re-run the evaluation with the selected **Attribute Set**.





Underneath the **Attribute Set** select list is a button to manually re-calculate the entire evaluation score. This button will be available on all pages within the evaluation, and can be clicked after identified issues are fixed in the APEX application. On most pages, there will also be a button entitled **Recalculate Page Score**. This button will only re-evaluate the score of a specific attribute, and takes a fraction of the time that a full evaluation does. In most cases, using **Recalculate Page Score** is preferred over using **Recalculate Entire Score**, especially when fixing issues outlined on the current page in APEX-SERT.

Next, a small bar chart highlights the number of deficiencies for each major classification: **Settings**, **Page/Report**, **XSS**, **SQLi** and **URL Tampering**. Clicking on any of the bars in the chart will redirect you to the dashboard for that classification.

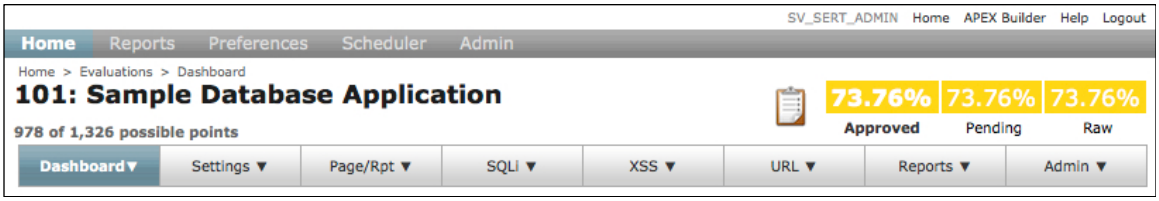
Lastly, a list of events relating to the **Application** and **Attribute Set** are displayed. These events highlight when an evaluation was run and exceptions or notations that were entered, rejected and/or approved. Only the last few events are displayed. A full list is available by clicking on the Events tab on the **Dashboard** page.

In the top-right corner of the page are the navigation bar entries. These are available from any page with APEX-SERT. The currently logged in user is first displayed. Next is the **Home** link. Clicking this will bring you to the main page of APEX-SERT.

If the application that you are running is in the same workspace that you launched APEX-SERT from, there will be an entry for **APEX Builder**. When clicked, this link will take you back to the main APEX development environment home page.

Each page also has its own context sensitive **Help**. Simply click the **Help** link in the navigation bar to reveal help for that specific page. Last is the **Logout** link. Clicking this will log out the user close the APEX-SERT tab or window.

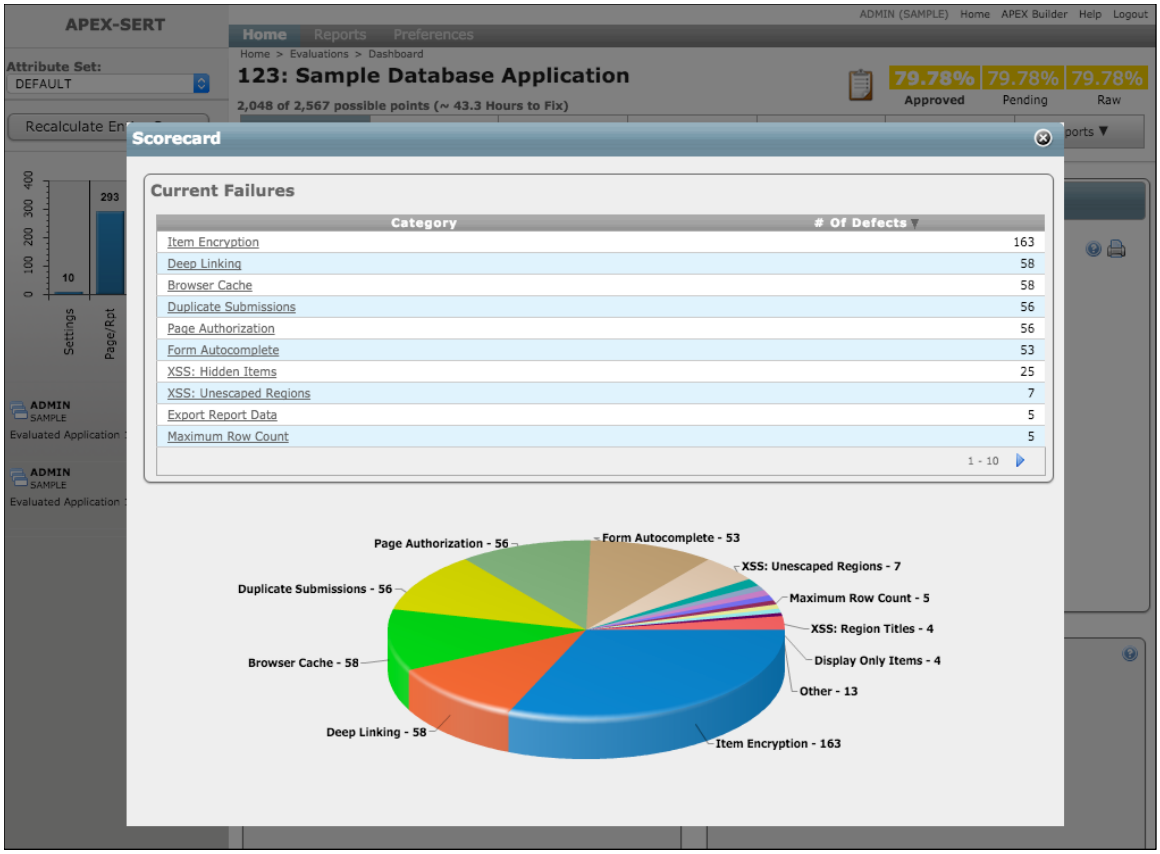
The next components are the top level tabs. These tabs - **Home**, **Reports**, **Preferences**, **Scheduler** and **Admin** - will also be available on every page of APEX-SERT. Depending on which group your user is a member of will determine which tabs are displayed.



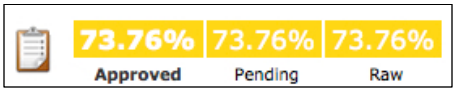
When running an evaluation, the ID and name of the application being evaluated is displayed in bold type, just under the top level tabs. This will only change when a different application is evaluated. Just below the application ID and name is the score summary. This will list the number of points that the application received as compared to the total number of possible points.

To the right of the Application ID & name is a small icon that resembles a clipboard. When clicked, the **Scorecard** will be displayed in a pop-up region. The **Scorecard** contains both a report and

chart detailing all currently outstanding deficiencies in the application. Clicking on the **Category** in the report will redirect the user to that specific section of APEX-SERT.

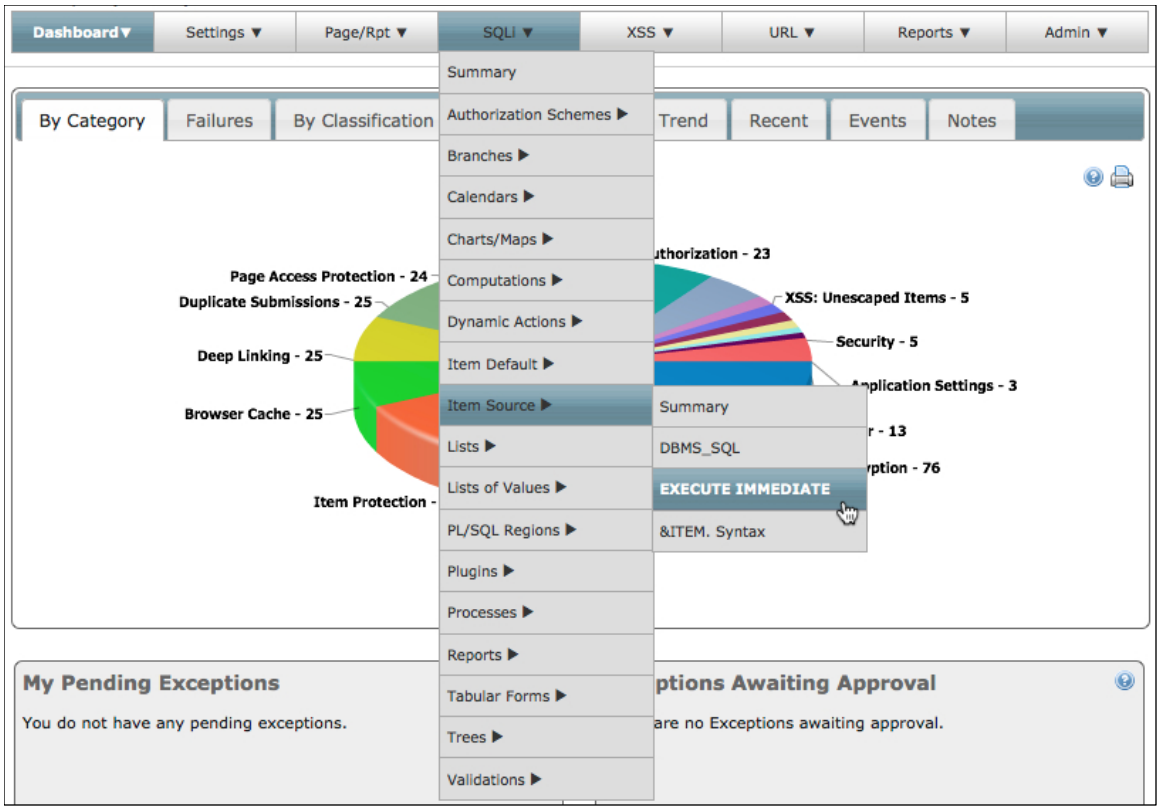


To the right of the scorecard are three color-coded scores: **Approved**, **Pending** & **Raw**. Clicking on any of the three scores will change the mode of the evaluation to the corresponding score. The currently selected mode is denoted by bold text for the score and the mode name. In the illustration below, the **Approved** mode is the current mode.



By default, a score less than 60 will be displayed in red; from 60 through 99, yellow, and 100, green. These levels can be altered on a user-by-user basis in the **Preferences** section of APEX-SERT.

Lastly are the evaluation sub-tabs. This set of tabs, available only when browsing an evaluation, serves as a way to quickly navigate the results of an evaluation. When hovered over, each of these tabs will expand to at least one additional level, revealing more options that the user can choose from. Some tabs - specifically those under the **SQLi**, **XSS** & **URL**, will contain additional sub-tabs, as shown below. The **Admin** tab will only be available to users who have been granted the **Administrator** role.

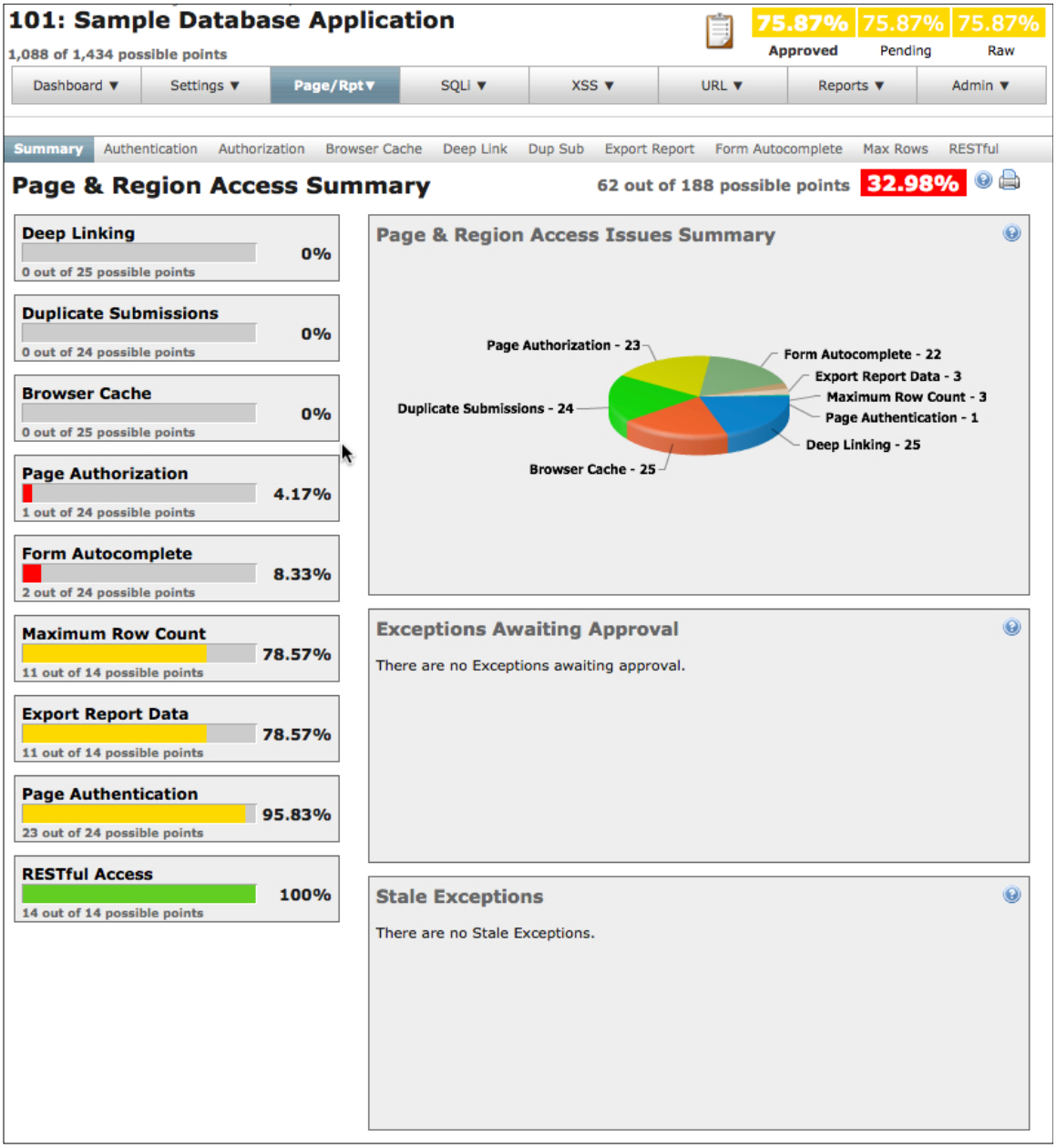


APEX-SERT makes extensive use of APEX interactive reports, something that most developers will be very familiar with. These reports allow each user of APEX-SERT to select which columns are available, apply filters and perform other functions on a report, all without the need to get a developer involved. Users can then save their changes so that each time they use a specific report in APEX-SERT, the options that they have selected will be available.

3.4. Classifications

APEX-SERT evaluates attributes that can be divided into five major classifications: Settings, Page & Reports, SQL Injection, Cross Site Scripting and URL Tampering. Each of these classifications is listed as part of the tabs displayed from within an evaluation. Hovering the mouse over any of these tabs will produce a list of all of the associated categories or attributes for that classification.

Clicking on either the top-level item in the tab or on the **Summary** item within any of the five classifications will display the classification summary page.



This page displays all associated attributes or categories of attributes and their respective scores. Clicking on either the bar chart in the left column of a slice of the pie chart will bring you to that specific attribute's page, where the discrete details of that attribute will be displayed.

The score displayed at the top of the page here represents the score only for this classification. In the above example, the score of 32.98% is derived from achieving only 62 out of a possible 188 points. Additionally, the values displayed on this page are based on which “mode” APEX-SERT is running in. In this example, APEX-SERT is running in **Approved** mode, denoted by the label of the approved score being rendered in bold text. Clicking either **Pending** or **Raw** may alter the values displayed on the summary page.

Exceptions that are ready to be approved as well as Stale Exceptions for attributes in this classification will also be displayed here.

4. Evaluating Applications

The vast majority of time spent in APEX-SERT will be spent browsing the results of an evaluation. Evaluating an application is easy: simply select the corresponding **Application** and **Attribute Set**, and click on the **Evaluate** button. APEX-SERT will immediately start the evaluation process, which can take as little as a few seconds to as long as a couple of minutes, depending on the underlying hardware and complexity of the application being evaluated.

4.1. Attributes & Attribute Sets

The rules that APEX-SERT uses when evaluating an application are called attributes. Each attribute is configured to search for and report on potential security vulnerabilities in an application. Some attributes are simple, in that they inspect a single component and look for a specific value, while others are more sophisticated and require a SQL query and function to determine if a threat exists. As an end user of APEX-SERT, is is not important to understand how the attributes are computed as much as it is to understand how to interpret the results of the evaluation and take any corrective action, if needed.

Each time an evaluation is run in APEX-SERT, it is done in conjunction with an attribute set. An attribute set is simply a list of attributes that are grouped together. Out of the box, APEX-SERT contains a single attribute set called **DEFAULT**. The **DEFAULT** attribute set includes all of APEX-SERT's almost 150 attributes, and cannot be modified in any way. Additional attribute sets can be created by a user with the **Administrator** role, and any number of attributes can be included.

4.2. Scoring & Exceptions

When an evaluation is run, three separate scores are generated. Each score is a percentage and represents the number of vulnerabilities detected, divided by the number of components evaluated. The more complex the application, the more components that will have to be evaluated.

Each of the scores are computed slightly differently, as described below:

Score	Description
Raw	The raw score represents the actual results of the evaluation. Any attribute that returned a FAIL deducts one point from the total possible raw score.
Pending	The pending score is made up of a combination of the raw score plus any exceptions that have been added but not yet approved.
Approved	The approved score is made up of a combination of the raw score plus any exceptions that have been both added and approved.

When an application is first evaluated, all three scores will be the same, since no exceptions have been created. As a first step, developers should examine the results and attempt to fix as many vulnerabilities as possible. When a group of vulnerabilities are fixed, the developer can re-evaluate the page or the entire application to update the scores.

At some point, all vulnerabilities that can be fixed will have been addressed. When this occurs, the score will still not be 100%. To achieve a score of 100%, it will be necessary to create exceptions. An exception is simply a reason as to why the developer feels that even though a component failed, the risk is mitigated elsewhere.

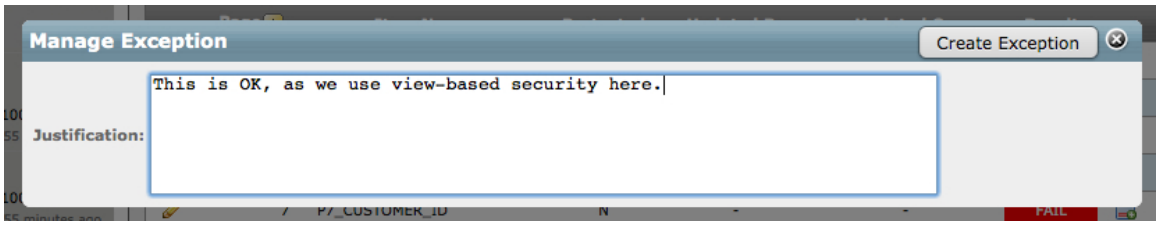
For example, one of the attributes in APEX-SERT checks to ensure that all pages require authentication. However, if by design, there are several pages that are set to public, APEX-SERT will still fail those pages. Setting those pages to require authentication is not an option, as it would break the intended functionality of the application. In this case, the developer can create an exception and justify why it is OK that these pages failed the evaluation.

An exception is simply a justification that the developer creates for a component that otherwise fails the evaluation. It can be as brief as a couple of words or as long as a few sentences. Essentially, it should state why it is OK for a component to be configured the way that it is, despite it failing the evaluation.

When in pending mode, a pending exception will be scored the same as if the component passed the evaluation. This allows the developer to keep track of which failures truly need to be addressed versus which have been mitigated by an exception.

4.2.1. Creating an Exception

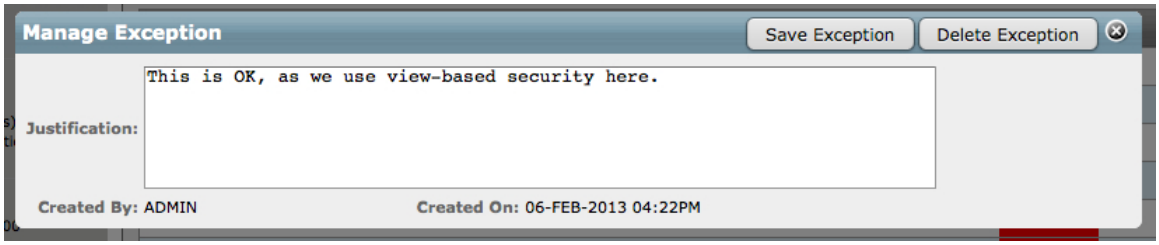
To create an exception, simply click on the  icon next to a failed component in a report. A popup region will appear. Simply enter the exception in the **Justification** region and click **Create Exception**.



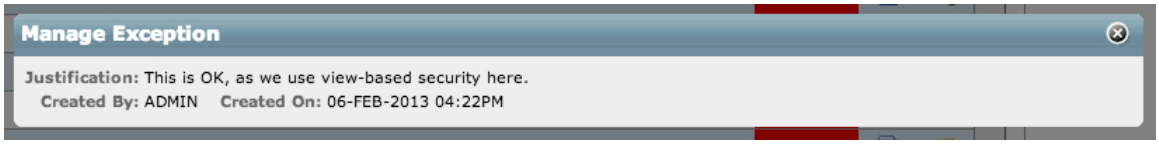
After the exception is created, the status of that component will change from **FAIL** to **PENDING**, indicating that there is a pending exception in place.

	6	P6_PRODUCT_ID	Y	ADMIN	06-FEB-2013 03:34PM	PASS	-	
	6	P6_BRANCH	Y	-	-	PASS	-	
	7	P7_BRANCH	N	-	-	PENDING		
	7	P7_CUSTOMER_ID	N	-	-	FAIL		
	10	P10_CALENDAR_DATE	N	-	-	FAIL		

Any pending exception created by the developer can be edited by clicking on the icon.



Here, the **Justification** can be altered, if need be. Alternatively, a developer can also delete the exception by clicking **Delete Exception**. Developers can only make changes to or delete their own exceptions. Exceptions logged by other users can still be viewed, but cannot be modified. Simply click on the icon to view another developer's exception.



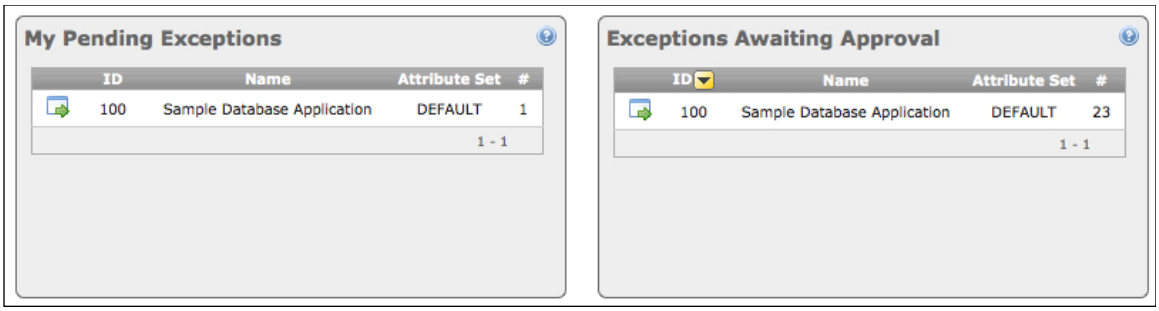
4.2.2. Creating Multiple Exceptions

Exceptions can also be created en masse for all instances of a specific attribute that have failed. Simply click the **Submit All** button to submit a single exception for all failures. Each exception will be created as if it were entered as an individual exception, and can be individually edited or deleted later.

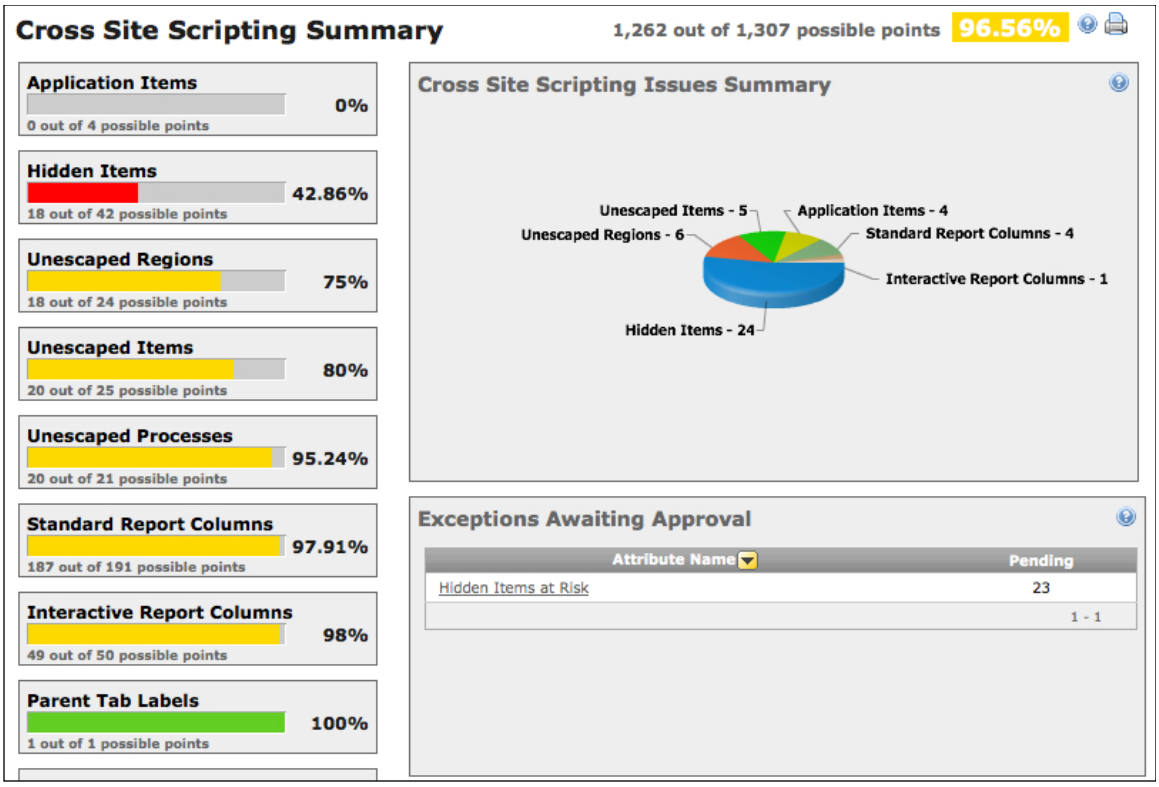
4.2.3. Approving & Rejecting Exceptions

One of the main goals of APEX-SERT is to allow developers to quickly and efficiently secure their APEX applications. A great deal of time was spent ensuring that the tool provided clear guidance as to what needed attention and what didn't. This is evident on the home page, where once

exceptions have been submitted and/or are awaiting approval, the corresponding summary regions start to display data.



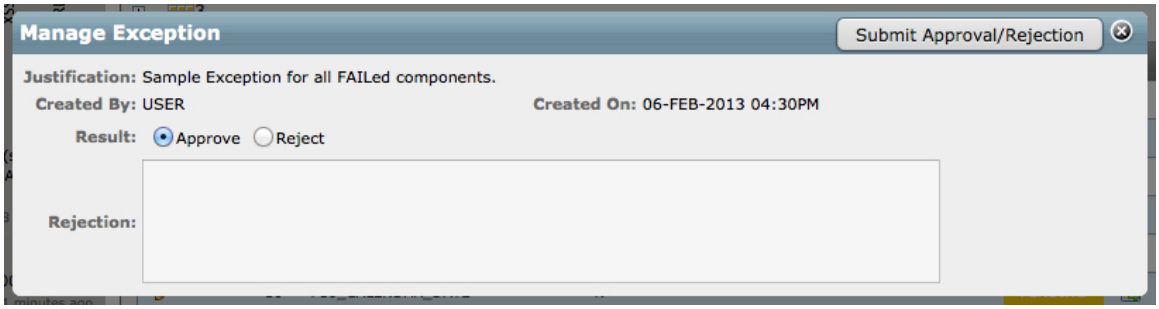
Additionally, on the application evaluation dashboard and classification pages, similar reports are now displaying data.



Simply click on either of the links, and you will be taken to the specific page where the exceptions have been created. If your user has the **Approver** role, then you will be able to approve exceptions, so long as they were created by someone else. It is not possible to self-approve exceptions in APEX-SERT. At least two different APEX users are required, with the approver having the **Approver** role.

	6	P6_BRANCH	Y	-	-	PASS	-	
	7	P7_BRANCH	N	-	-	PENDING		
	7	P7_CUSTOMER_ID	N	-	-	PENDING		
	10	P10_CALENDAR_DATE	N	-	-	PENDING		
	10	P10_CALENDAR_TYPE	N	-	-	PENDING		
	10	P10_CALENDAR_END_DATE	N	-	-	PENDING		
	11	P11_CUSTOMER_ID_NEW	N	-	-	PENDING		
	11	P11_BRANCH	N	-	-	PENDING		
	12	P12_CUSTOMER_NAME	N	-	-	PENDING		
	12	P12_PRODUCT_ID	N	-	-	PENDING		
	12	P12_BRANCH	Y	-	-	PASS	-	

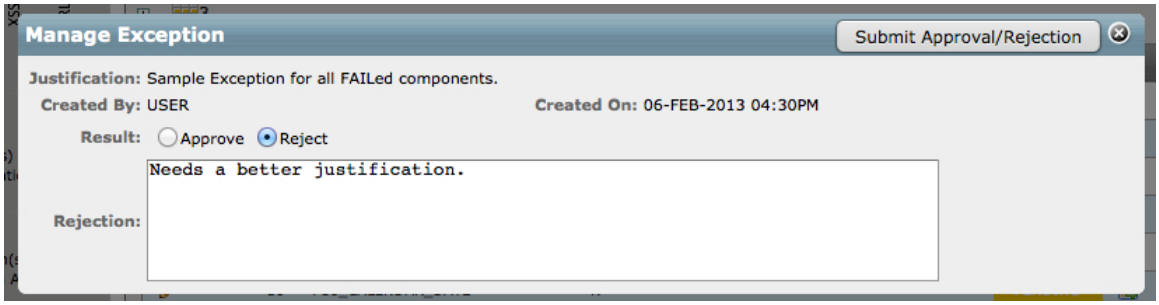
To approve or reject an individual exception, click on the icon. A popup window will appear, offering two options: **Approve** or **Reject**.



If approving the exception, simply ensure that the **Result** it set to **Approve** and click **Submit Approval/Rejection**. When the popup disappears, the corresponding **PENDING** exception should now display as **APPROVED**, and the approved score should increase slightly.

	6	P6_BRANCH	Y	-	-	PASS	-	
	7	P7_BRANCH	N	-	-	PENDING		
	7	P7_CUSTOMER_ID	N	-	-	APPROVED		
	10	P10_CALENDAR_DATE	N	-	-	PENDING		

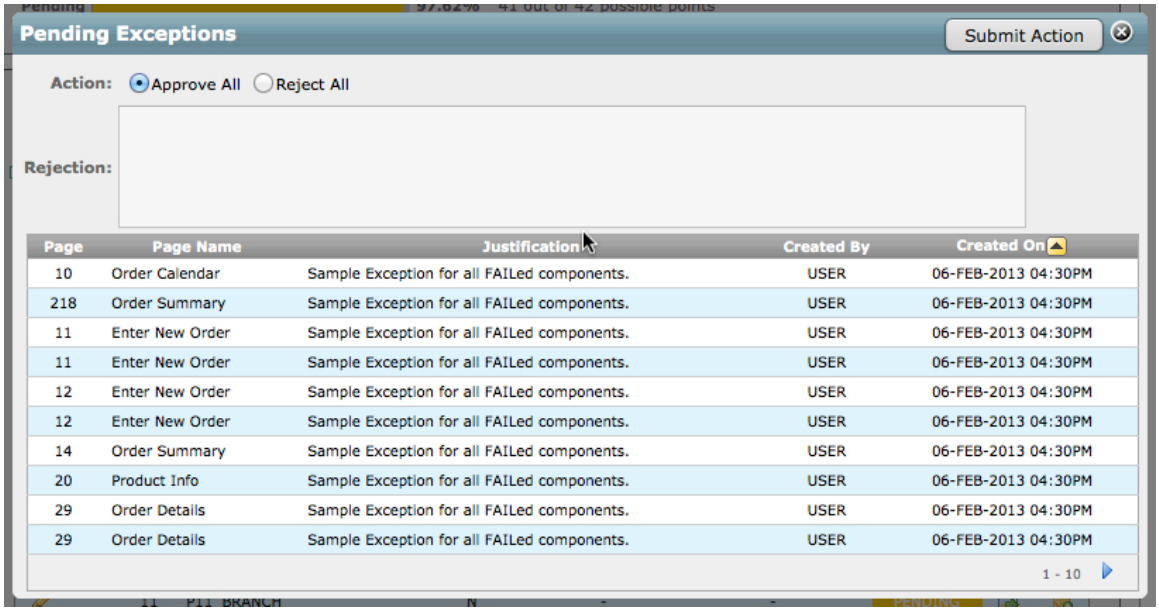
Alternatively, any exception can also be rejected, if the reason provided is not sufficient. When rejecting an exception, a **Rejection** reason is required. Simply set the **Result** to **Reject**, enter a reason and click **Submit Approval/Rejection**.



Now, when the popup disappears and the page reloads, the corresponding component's status will change from **PENDING** to **REJECTED**.

	6	P6_BRANCH	Y	-	-	PASS	-	
	7	P7_BRANCH	N	-	-	PENDING		
	7	P7_CUSTOMER_ID	N	-	-	APPROVED		
	10	P10_CALENDAR_DATE	N	-	-	REJECTED		

If there are multiple pending exceptions that need to be either approved or rejected, they can be done in batch as well. Simply click on **Approve/Reject All**, and a popup window will appear, detailing all components that have been submitted.



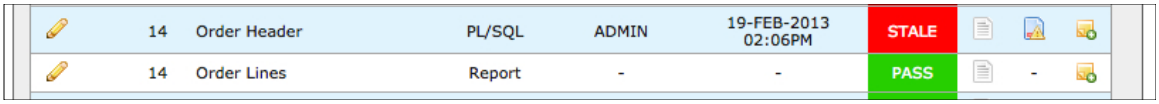
Simply choose whether to **Approve** or **Reject** all, enter a reason if rejecting, and click **Submit Action**. When the page reloads, all previously pending exceptions that were submitted by others will now be either **APPROVED** or **REJECTED**, depending on which action was selected.

	10	P10_CALENDAR_TYPE	N	-	-	APPROVED		
	10	P10_CALENDAR_END_DATE	N	-	-	APPROVED		
	11	P11_CUSTOMER_ID_NEW	N	-	-	APPROVED		
	11	P11_BRANCH	N	-	-	APPROVED		

4.2.4. Stale Exceptions

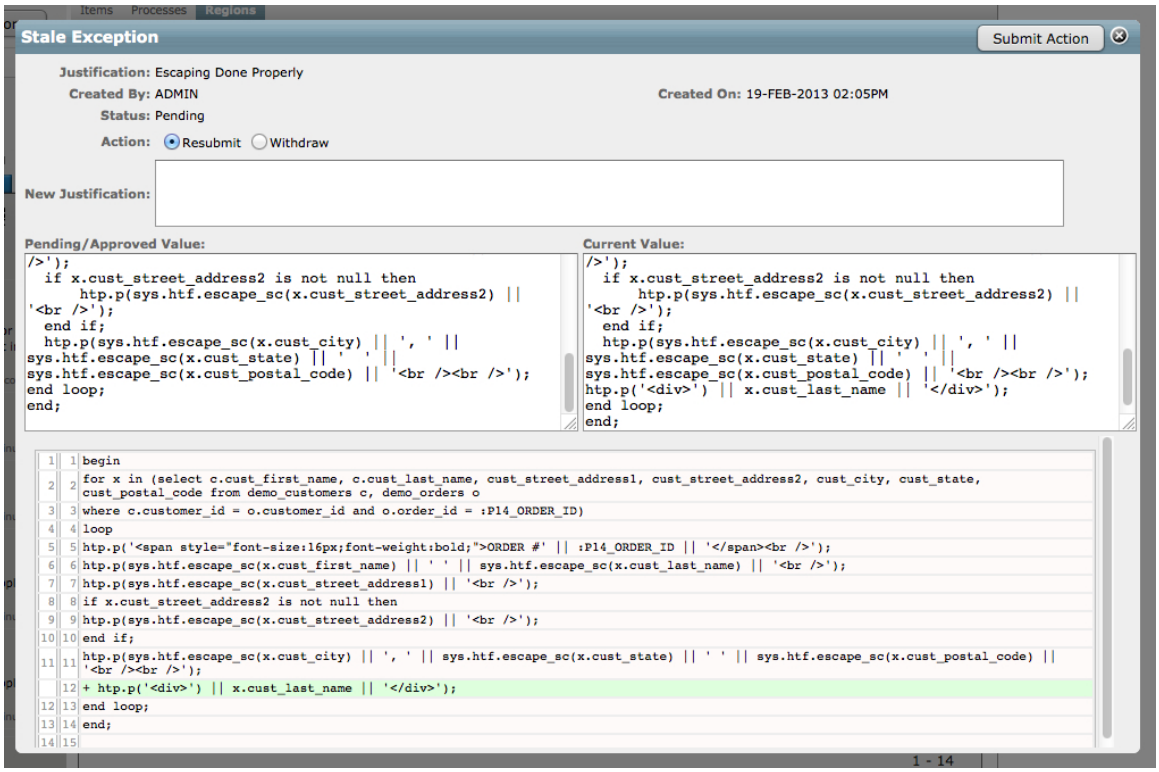
Security is not an event, but rather a process. If an exception is put in place and then approved, and then the underlying value of that attribute is changed, is the exception still valid? Perhaps not. Therefore, APEX-SERT exceptions can go "stale" if the data for which they were approved changes. This process occurs automatically each time that an APEX-SERT evaluation is run.

When an attribute goes **Stale**, it will be noted in its status column.



	14	Order Header	PL/SQL	ADMIN	19-FEB-2013 02:06PM	STALE			
	14	Order Lines	Report	-	-	PASS		-	

The user can click on the icon to display details about why the exception went stale.

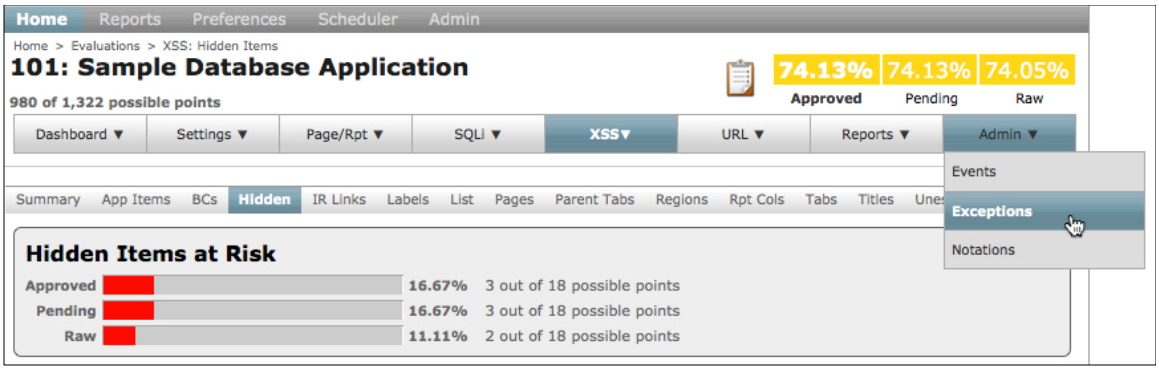


Both the value at the time the exception was submitted and the current value are displayed. Additionally, a second region will display a "diff" between the two regions, highlighting code that was added in green and code that was removed in red.

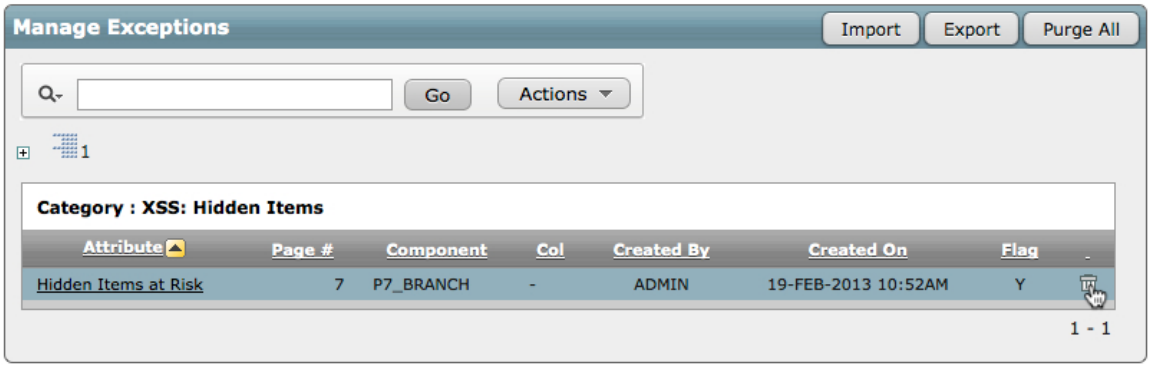
If the code change did not alter the exception, the developer can provide another justification and simply re-submit it. If the code change did, in fact, introduce a vulnerability, the developer can withdraw the exception and properly address the defect.

4.2.5. Deleting an Approved Exception

Once an exception is approved, it cannot be modified. Only a user who has the **Administrator** role can remove the approved exception. To remove an exception, select the **Exceptions** item from the **Admin** tab.



Next, using the interactive report, locate the exception that it to be removed and click on the trash can icon.



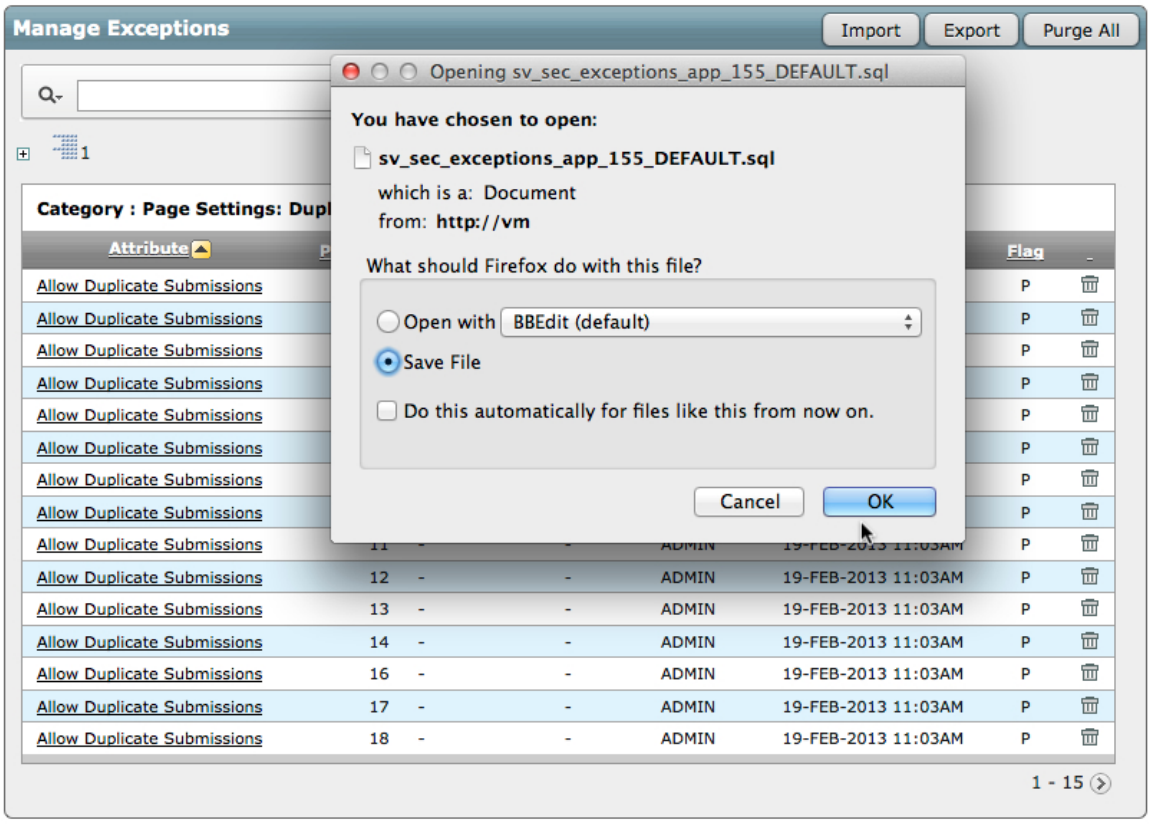
Confirm the deletion by clicking OK. In order to see the changes, the evaluation will have to be re-run for either the entire application or the specific attribute that has exception(s) removed.

4.2.6. Importing & Exporting Exceptions

A lot of work will go into developers entering, approving and/or rejecting exceptions. As applications move from the development server to the QA server, it is important to be able to move the exceptions in tandem with the applications. Thus, APEX-SERT provides the ability for an administrator to import and export exceptions, similar to how APEX applications are imported and exported.

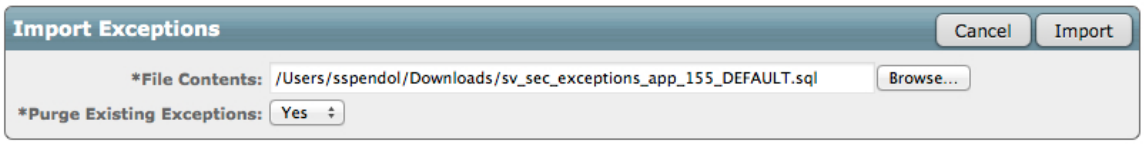
However, there are a couple of restrictions when importing and exporting exceptions: first of all, the source and target applications should be as similar as possible. If there are any differences between them and the exception from the source cannot be mapped to the target, it will be displayed in the exception report after the import completes. Second, the Attribute Set used must be the same in both applications. Currently it is not possible to export & import a group of exceptions from one attribute set to another.

To export exceptions, select the **Exceptions** item from the **Admin** menu. Next, click on the **Export** button. You should be prompted to either open or save the resulting file. Elect to save the file to your local disk.



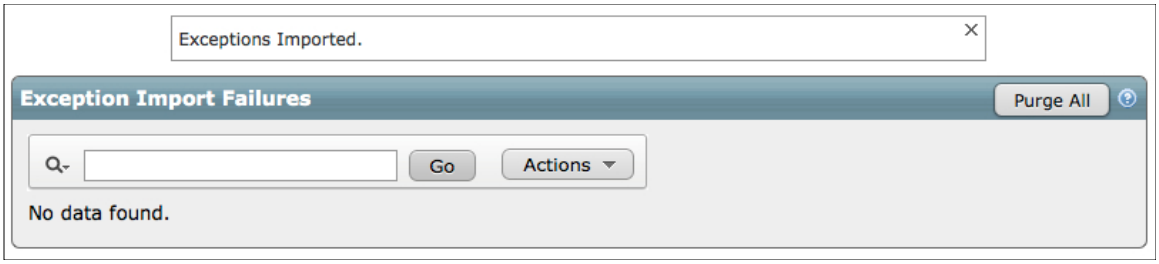
Next, switch to the target application. This can be a copy of the source application in the same workspace, a different workspace, or on a completely different server. Evaluate the target application, and once that is complete, click on the **Exceptions** item in the **Admin** tab. This time, click the **Import** button.

Click on **Browse** and locate the file that was just created. Also, decide if you want to purge any existing exceptions that exists for this application & attribute set. Setting this option to **No** may result in some exceptions not being successfully imported.



When you are ready, click **Import** to begin importing the exceptions. It will take from a few seconds to a couple of minutes to complete the import, as APEX-SERT will also perform a full evaluation of the application as part of the import process.

Upon completion of the exception import, a report will display any exceptions that could not be imported, if any did.



At this point, all exceptions should be imported and visible from APEX-SERT just like those entered into the application natively.

4.2.7. Purging Exceptions

If all exceptions for an application & attribute set need to be deleted, this can also be done by an administrator. Simply click on the **Exceptions** item in the **Admin** tab. This time, click the **Purge All** button. You will be prompted to confirm the action. Do so, and all exceptions associated with the application & attribute set will be deleted.

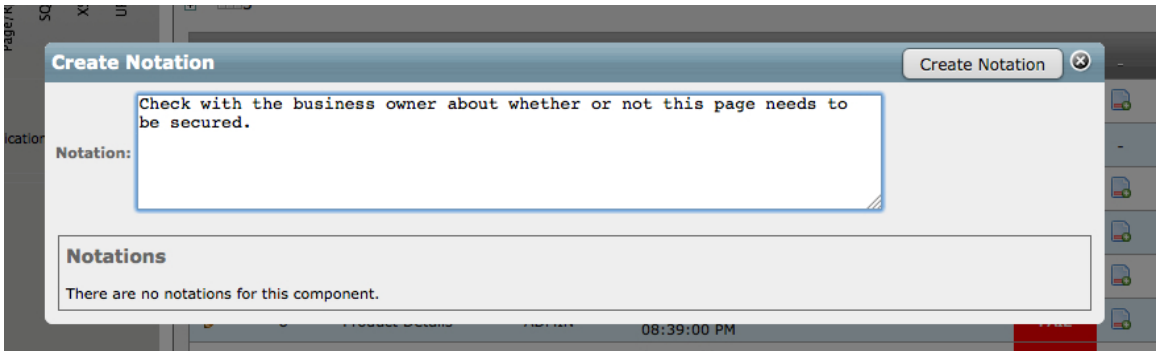
Upon completion of a purge, a new evaluation is not run. To see the changes, simply re-run the application evaluation by clicking on the **Recalculate Entire Score** button in the sidebar.

4.3. Notations

APEX-SERT allows a developer to add notations to any discrete instance of an attribute. These notations have no bearing on the score of the application, but are rather for informational purposes only. For example, as a developer uses APEX-SERT to secure an application, notations can be made for items that he is unsure of, and has to do more research for later.

4.3.1. Creating Notations

To create a notation, simply click on the  icon within any report in APEX-SERT. Once the popup window appears, simply enter the text for the **Notation** and click on **Create Notation**.

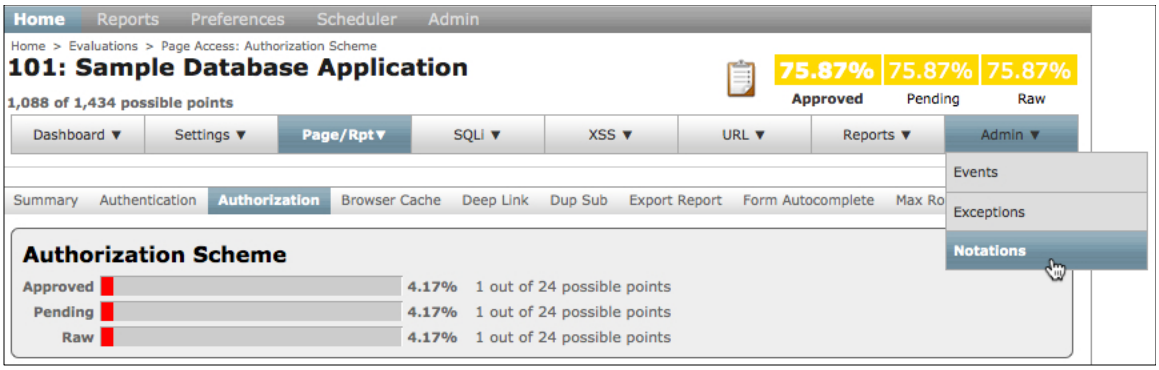


When an element has a notation, the number of notations associated with that element will be displayed above the icon itself.

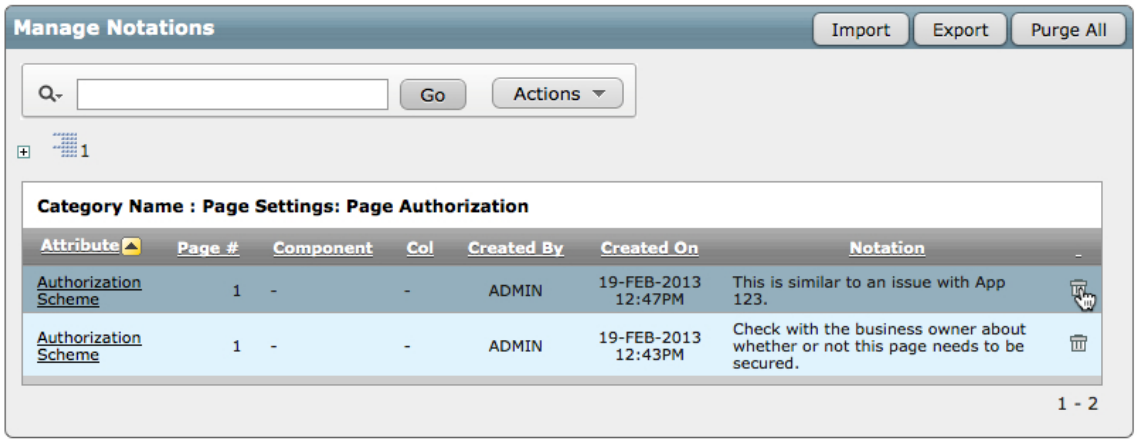
	Page	Page Name	Updated By	Updated On	Auth Scheme	Result		
	1	Sample Database Application	ADMIN	01-NOV-2012 04:20:43 PM	-	FAIL		2
	2	Customers	ADMIN	25-JUN-2012 10:44:46 AM	MUST_NOT_BE_PUBLIC_USER	PASS	-	

4.3.2. Deleting a Notation

Once a notation is created, it cannot be modified or removed. Only a user who is a member of the **SV_SERT_ADMIN** group can remove the notation. To remove a notation, select the **Notations** item from the **Admin** tab.



Next, using the interactive report, locate the notation that it to be removed and click on the trash can icon.



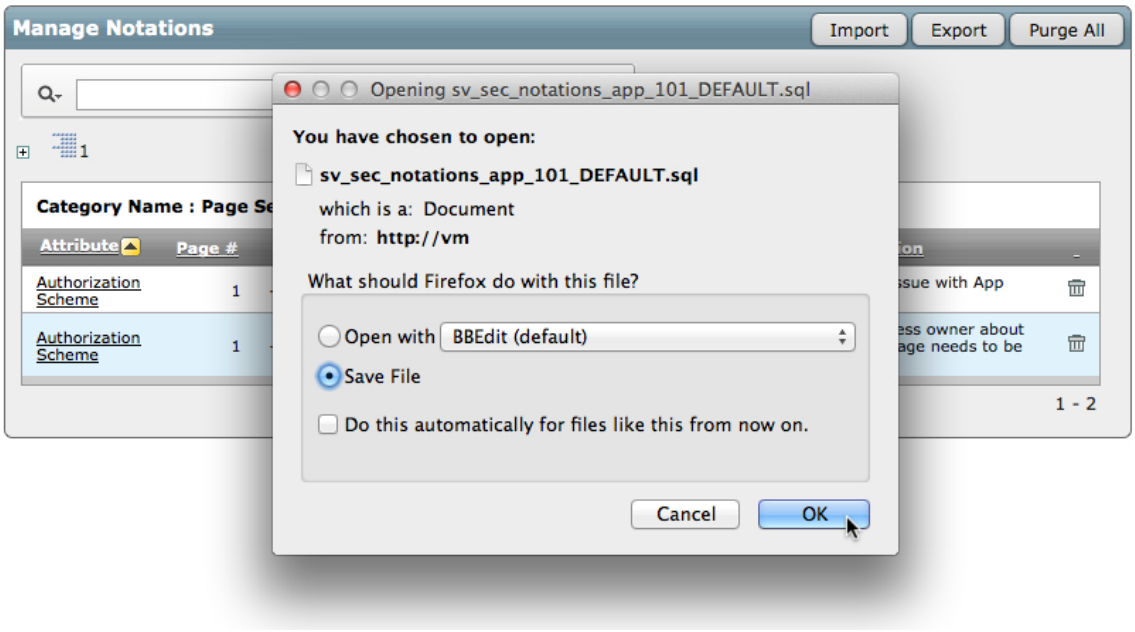
Confirm the deletion by clicking **OK**. In order to see the changes, the evaluation will have to be re-run for either the entire application or the specific attribute that has notation(s) removed.

4.3.3. Importing & Exporting Notations

A lot of work will go into developers entering notations. As applications move from the development server to the QA server, it may be necessary to be able to move the notations in tandem with the applications. Thus, APEX-SERT provides the ability for an administrator to import and export notations, similar to how APEX applications are imported and exported.

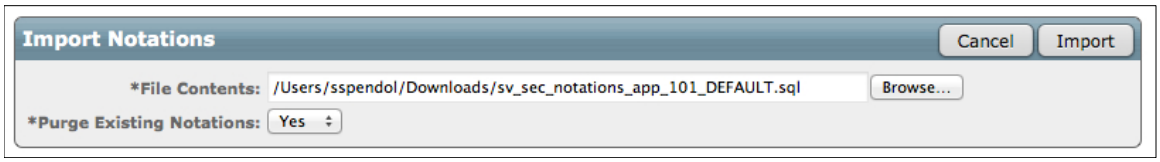
Like exceptions, there are a couple of restrictions when importing and exporting notations: first of all, the source and target applications should be as similar as possible. If there are any differences between them and the notation from the source cannot be mapped to the target, it will be displayed in the exception report after the import completes. Second, the Attribute Set used must be the same in both applications. Currently it is not possible to export & import a group of notations from one attribute set to another.

To export notations, select the **Notations** item from the **Admin** menu. Next, click on the **Export** button. You should be prompted to either open or save the resulting file. Elect to save the file to your local disk.



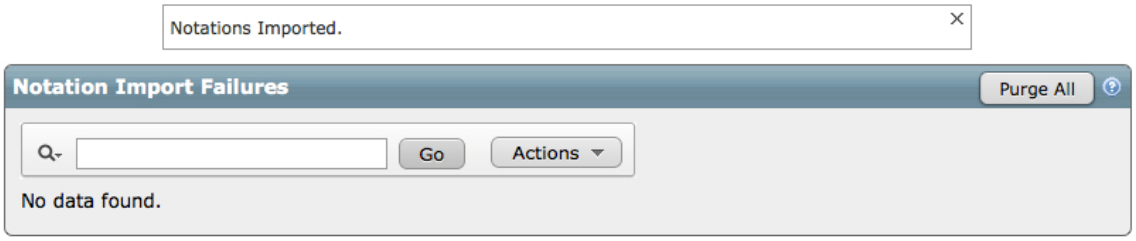
Next, switch to the target application. This can be a copy of the source application in the same workspace, a different workspace, on on a completely different server. Evaluate the target application, and once that is complete, click on the **Notations** item in the **Admin** tab. This time, click the **Import** button.

Click on **Browse** and locate the file that was just created. Also, decide if you want to purge any existing notations for this application & attribute set. Setting this option to **No** may result in some notations not being successfully imported.



When you are ready, click **Import** to begin importing the notations. It will take from a few seconds to a couple of minutes to complete the import, as APEX-SERT will also perform a full evaluation of the application as part of the import process.

Upon completion of the notation import, a report will display any notations that could not be imported.



At this point, all notations should be imported and visible from APEX-SERT just like those entered into the application natively.

4.3.4. Purging Notations

If all notations for an application & attribute set need to be deleted, this can also be done by an administrator. Simply click on the **Notations** item in the **Admin** tab. This time, click the **Purge All** button. You will be prompted to confirm the action. Do so, and all notations associated with the application & attribute set will be deleted.

Upon completion of a purge, a new evaluation is not run. To see the changes, simply re-run the application evaluation by clicking on the **Recalculate Entire Score** button in the sidebar.

5. Reports

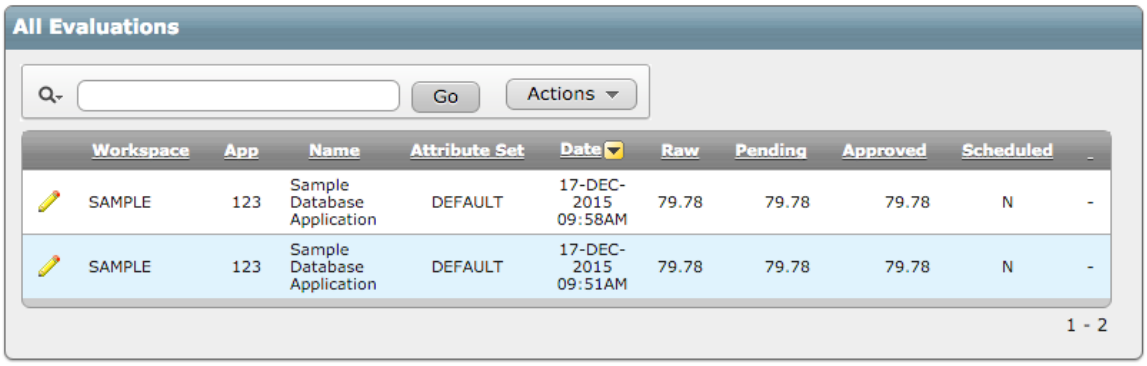
Report in APEX-SERT can be found in one of two places: at the specific application level and at the workspace level. Each type of report focuses on the specifics of the evaluation of the application or evaluations across multiple applications, respectively.

5.1. Workspace Reports

Workspace reports include information from all applications within a workspace. They can be accessed by clicking the **Reports** tab in the upper-most set of tabs.

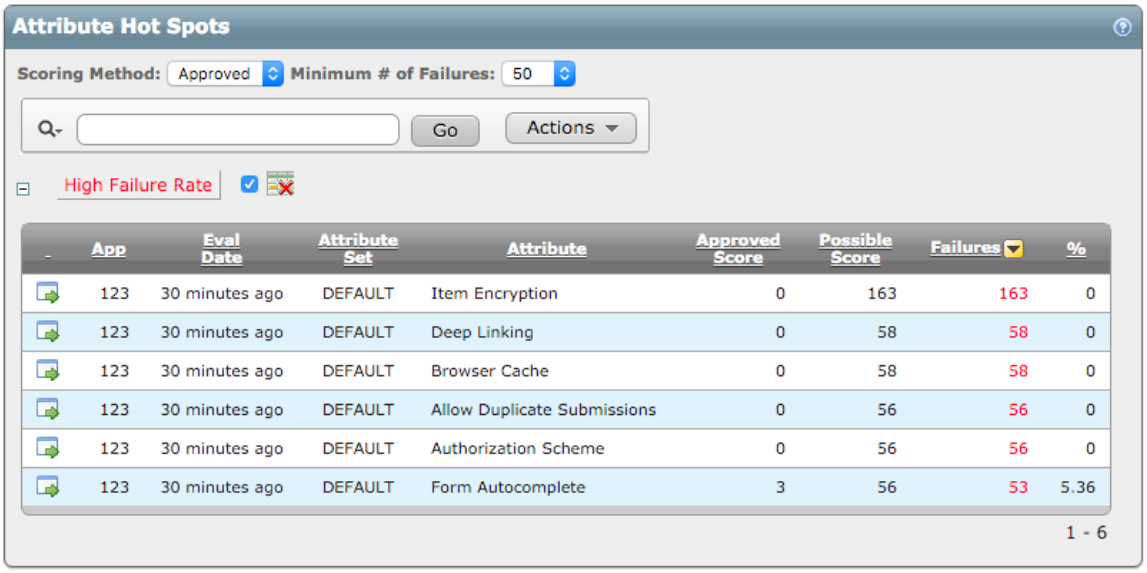
5.1.1. All Evaluations

The **All Evaluations** report summarizes all applications that have ever been evaluated by APEX-SERT. Only the top level scores are available in this report.



5.1.2. Attribute Hot Spots

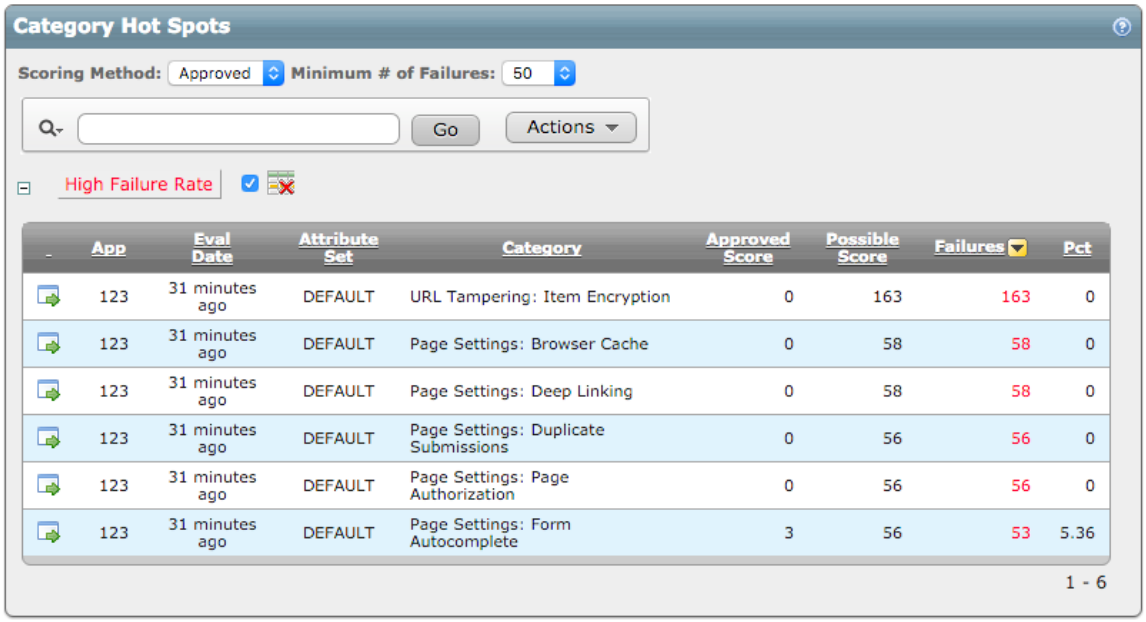
The **Attribute Hot Spots** report is designed to call attention to Attributes that have an unusually high number of potential vulnerabilities. The Scoring Method for this report can be adjusted, as can the minimum number of vulnerabilities discovered.



App	Eval Date	Attribute Set	Attribute	Approved Score	Possible Score	Failures	%
123	30 minutes ago	DEFAULT	Item Encryption	0	163	163	0
123	30 minutes ago	DEFAULT	Deep Linking	0	58	58	0
123	30 minutes ago	DEFAULT	Browser Cache	0	58	58	0
123	30 minutes ago	DEFAULT	Allow Duplicate Submissions	0	56	56	0
123	30 minutes ago	DEFAULT	Authorization Scheme	0	56	56	0
123	30 minutes ago	DEFAULT	Form Autocomplete	3	56	53	5.36

5.1.3. Category Hot Spots

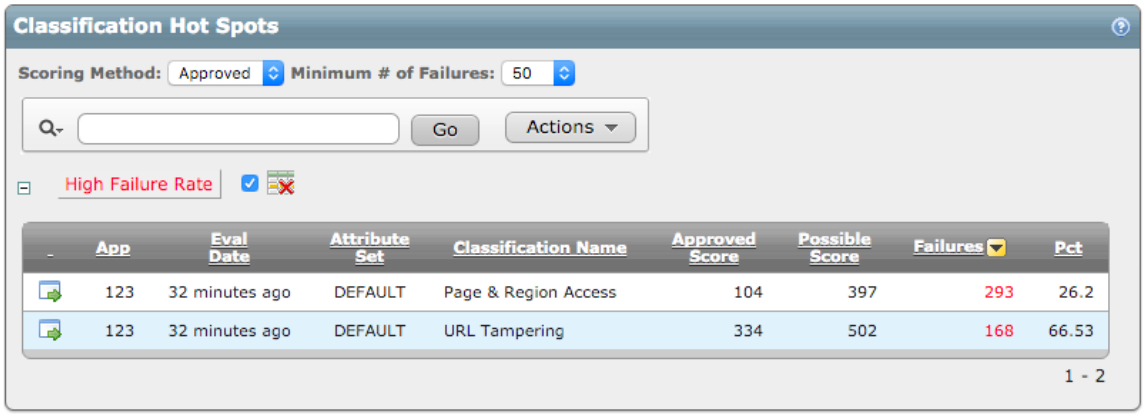
The **Category Hot Spots** report is designed to call attention to Categories that have an unusually high number of potential vulnerabilities. The Scoring Method for this report can be adjusted, as can the minimum number of vulnerabilities discovered.



App	Eval Date	Attribute Set	Category	Approved Score	Possible Score	Failures	Pct
123	31 minutes ago	DEFAULT	URL Tampering: Item Encryption	0	163	163	0
123	31 minutes ago	DEFAULT	Page Settings: Browser Cache	0	58	58	0
123	31 minutes ago	DEFAULT	Page Settings: Deep Linking	0	58	58	0
123	31 minutes ago	DEFAULT	Page Settings: Duplicate Submissions	0	56	56	0
123	31 minutes ago	DEFAULT	Page Settings: Page Authorization	0	56	56	0
123	31 minutes ago	DEFAULT	Page Settings: Form Autocomplete	3	56	53	5.36

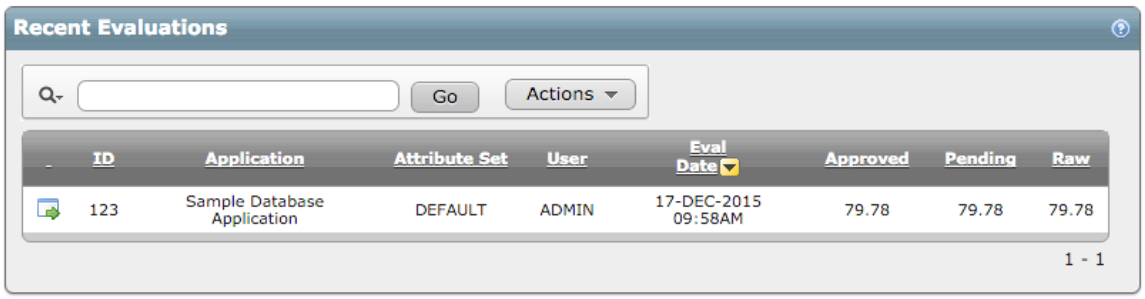
5.1.4. Classification Hot Spots

The **Classification Hot Spots** report is designed to call attention to Classifications that have an unusually high number of potential vulnerabilities. The Scoring Method for this report can be adjusted, as can the minimum number of vulnerabilities discovered.



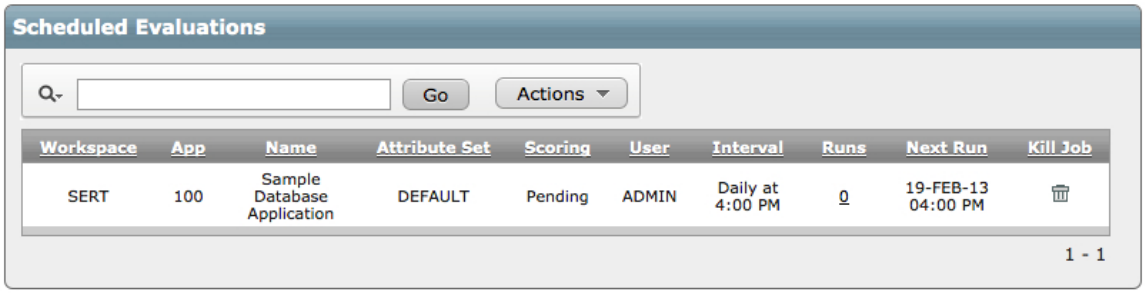
5.1.5. Recent Evaluations

The **Recent Evaluations** report shows the summary info from the most recent evaluation for each application in the workspace that has been evaluated.



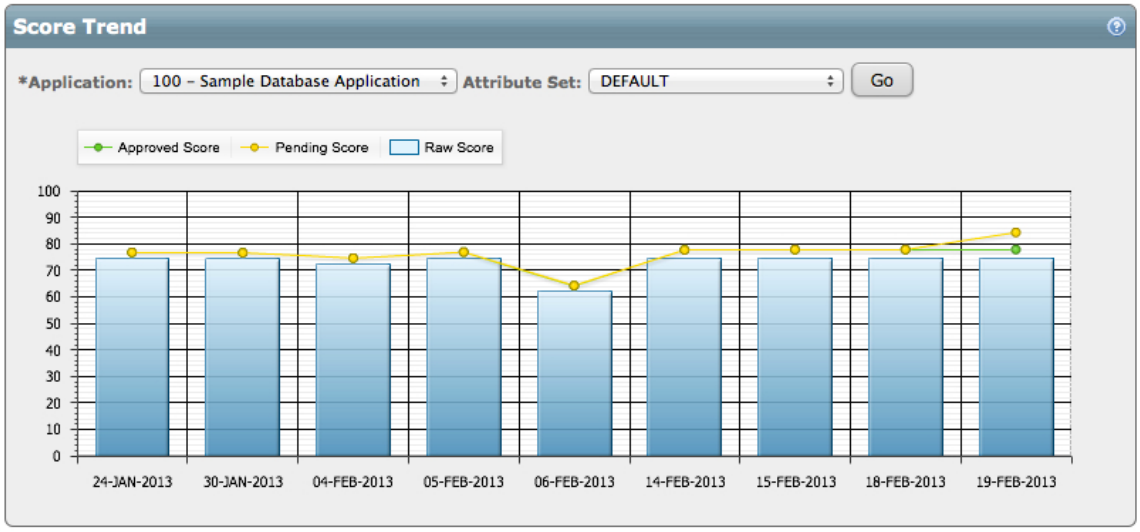
5.1.6. Completed Scheduled Evaluations

The Scheduled Evaluations report displays all reports that are scheduled to run. Clicking on the number in the **Runs** column will displays each individual run of the report.



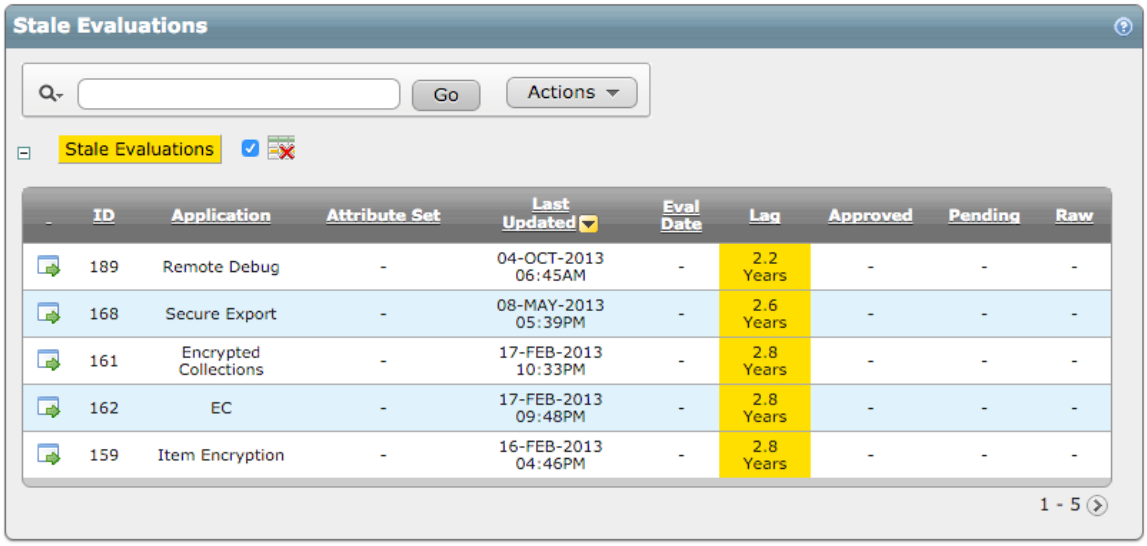
5.1.7. Score Trends

The **Score Trends** chart displays the scoring trend of a specific application and attribute set.



5.1.8. Stale Evaluations

The **Stale Evaluations** report displays all applications within a workspace and highlights those that have either never been evaluated by APEX-SERT or have been updated more recently than their last evaluation.

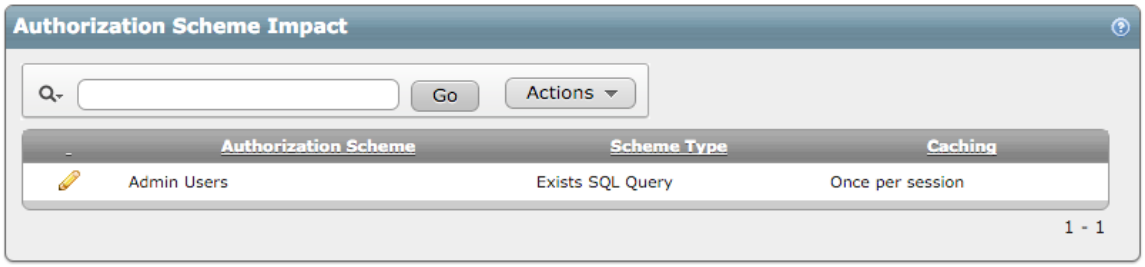


5.2. Application Reports

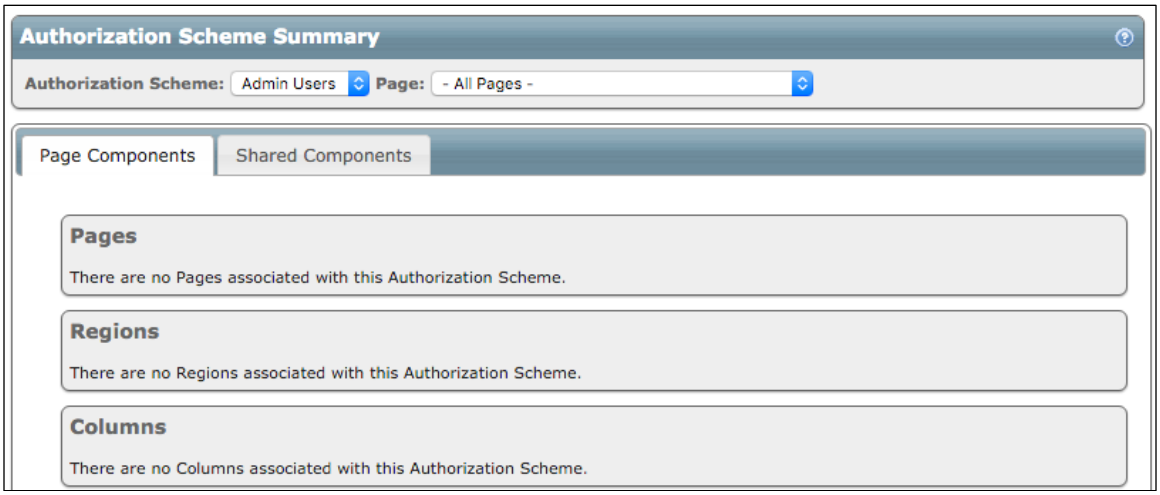
Application reports focus on a specific application. They are only available when an evaluation has been run, and can be accessed from the **Reports** tab in the lower-most set of tabs.

5.2.1. Authorization Scheme Impact

The **Authorization Scheme Impact** report displays a list of which component is associated with which authorization scheme.

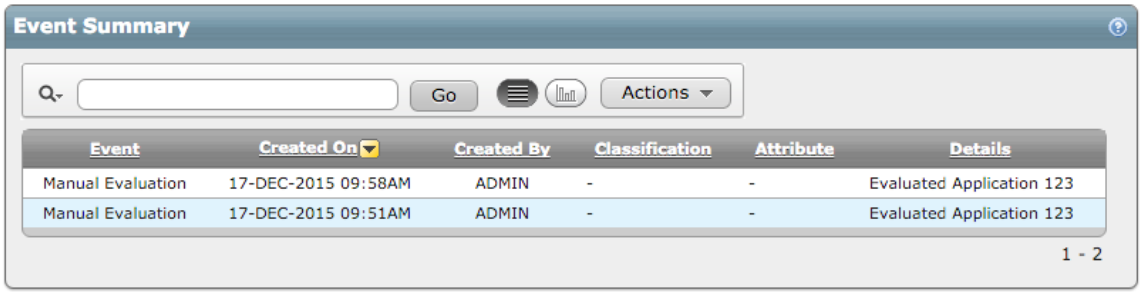


Clicking on the edit icon will display the results of the report. From this screen, the report can be filtered based on either the **Authorization Scheme** and **Page**. Additionally, there are two sub-tabs that can be toggled: **Page Components** and **Shared Components**.



5.2.2. Events Summary

The **Events Summary** report outlines all events that have occurred for a specific application. Events include things such as evaluations, creation, approval and rejection of exceptions.



5.2.3. Exceptions Detail

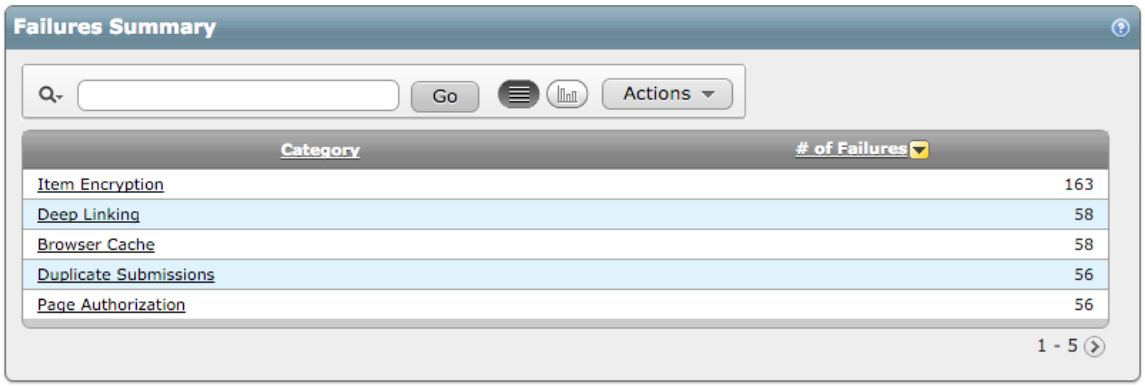
The **Exceptions Detail** report provides a detailed list of all exceptions that have been created for an application.

5.2.4. Exceptions Summary

The **Exceptions Summary** report provides a summary of all exceptions that have been created for an application.

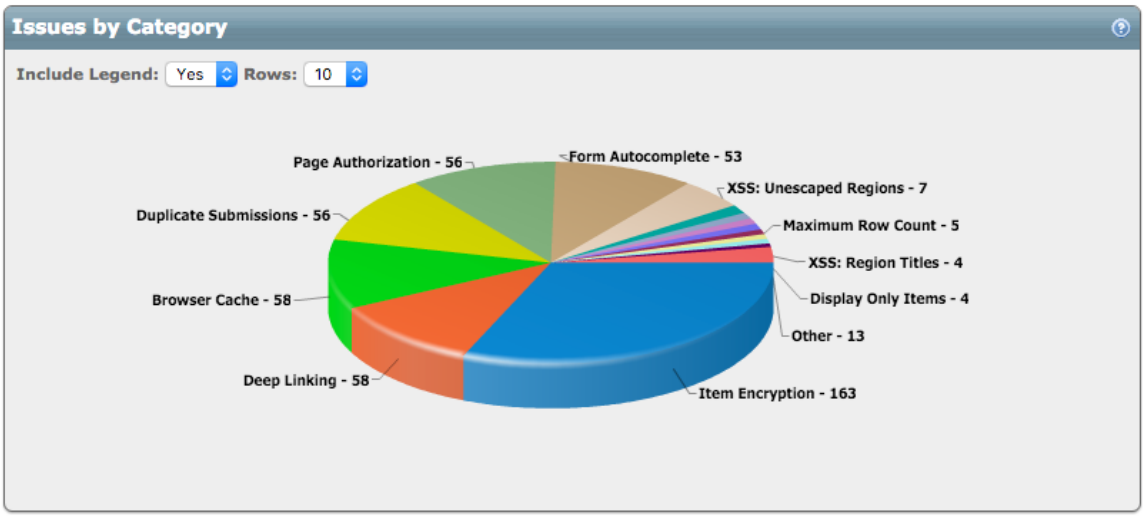
5.2.5. Failures Summary

The **Failures Summary** report displays a summary of how many failures are associated with each attribute. Clicking the value in the **Category** column will redirect to the corresponding page in APEX-SERT for that category.



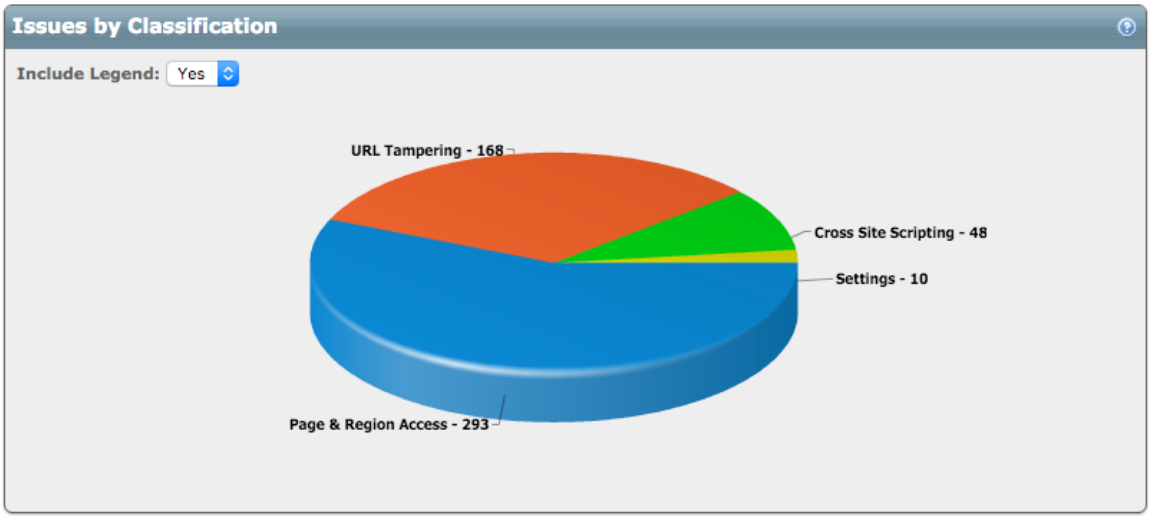
5.2.6. Issues by Category

The **Issues by Category** chart displays a summary of issues based on their category.



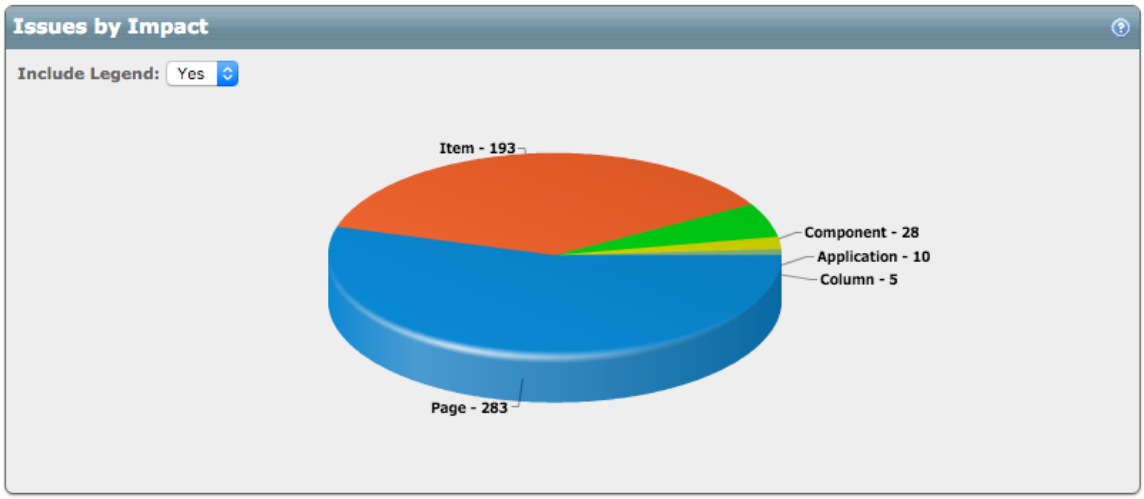
5.2.7. Issues by Classification

The **Issues by Classification** chart displays a summary of issues based on their classification.



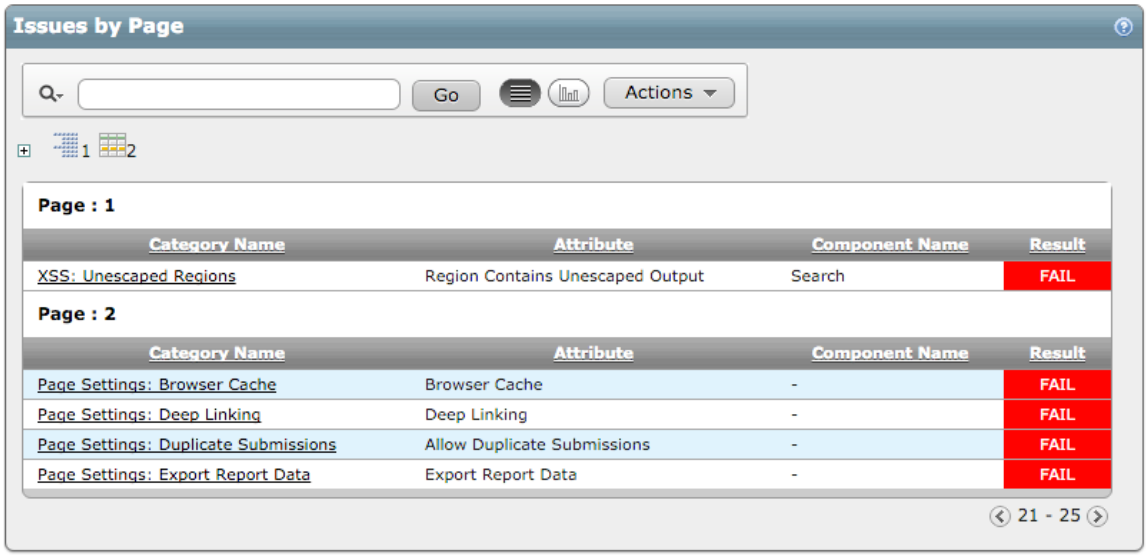
5.2.8. Issues by Impact

The **Issues by Impact** chart displays a summary of issues based on their impact.



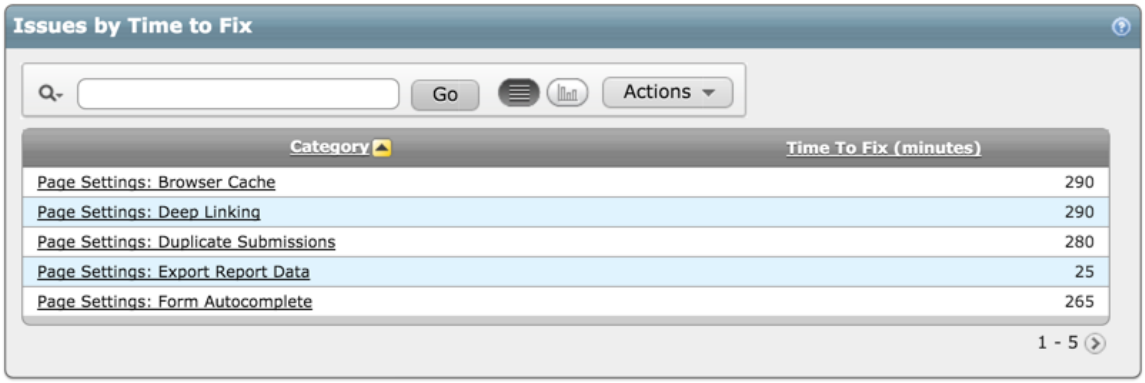
5.2.9. Issues by Page

The **Issues by Page** report displays a summary of issues based segmented by page.



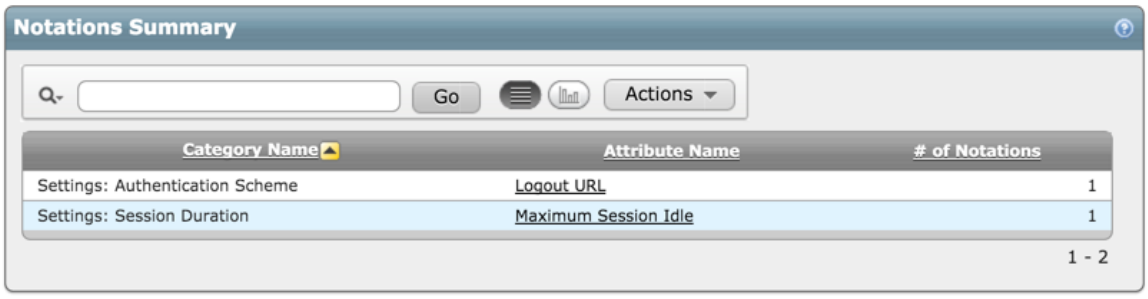
5.2.10. Issues by Time to Fix

The **Issues by Time to Fix** report displays a summary of estimated times to fix issues broken down by category.



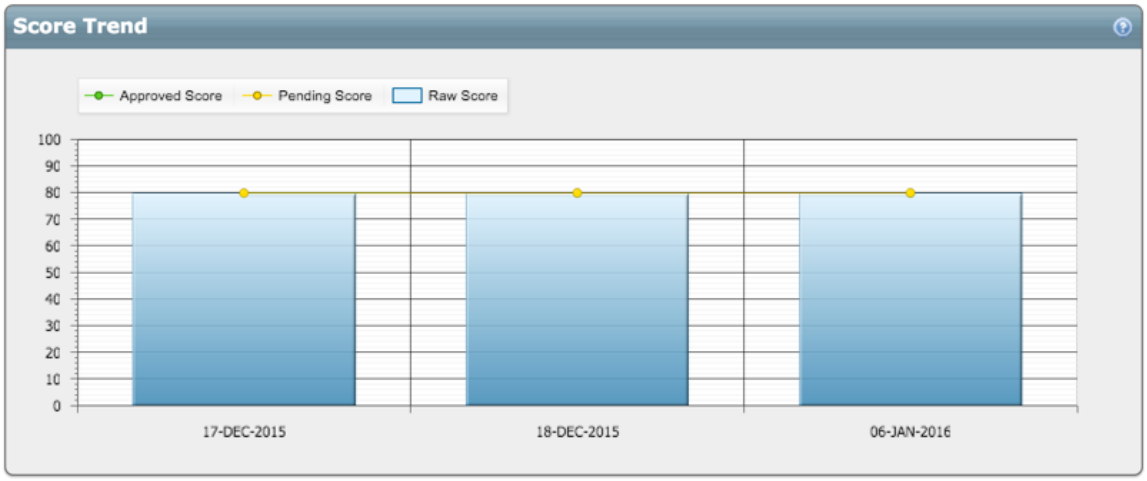
5.2.11. Notations Summary

The **Notations Summary** report summarizes the number of notations for each attribute. Clicking on the **Attribute Name** will bring you to that attribute's page in APEX-SERT.



5.2.12. Score Trend

The **Score Trend** chart displays the approved, pending and raw score in a line/bar chart format.



6. Preferences

Each user can set a number of preferences that will impact scoring tolerances & precision and help file locations. All preferences are located in the main **Preferences** tab.

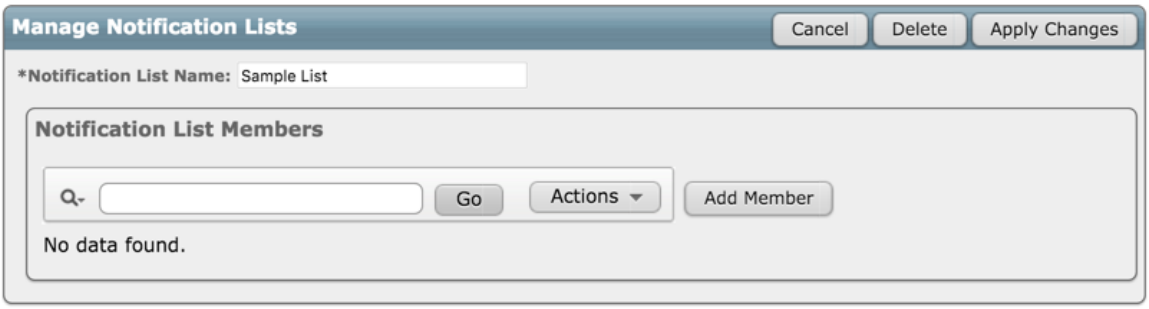
7. Scheduling Evaluations

APEX-SERT allows granted either the **Evaluate & Schedule in All Workspaces** or **Schedule in a Specific Workspace** role to schedule an evaluation to be run on either a weekly or daily basis. Evaluations can only be run for one of the three scoring methods: Approved, Pending or Raw. Results of scheduled evaluations can be e-mailed out to a group of users - even if they do not have an APEX workspace account.

7.1. Notification Lists

Notification Lists contain the e-mail addresses of users who wish to be notified when a scheduled evaluation runs. Users on a notification list do not need an APEX workspace account.

To create a **Notification List**, click on the **Scheduler** tab. Next, click on the **Notification Lists** sub-tab. Click **Create** and enter a value for the **Notification List Name** and click **Create** again.

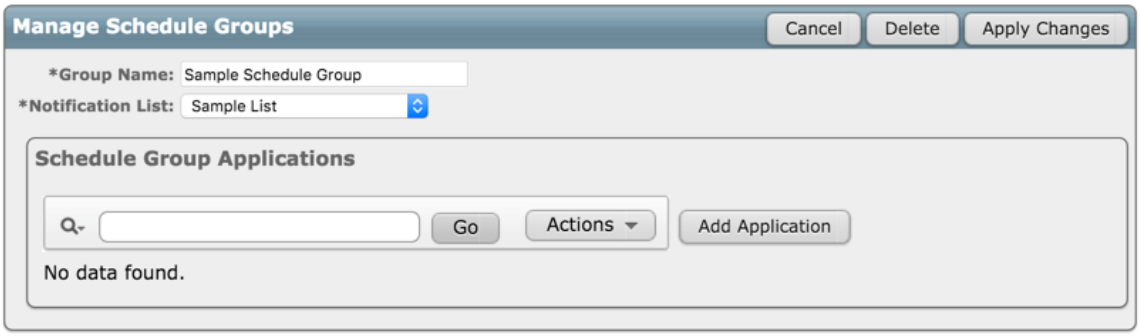


Now that the list is created, click **Add Member** to add a recipient. Enter the user's first and last name and e-mail address that they wish to receive notifications and click **Create**. Repeat this process for each user.

7.2. Scheduling Groups

Scheduling Groups associate a group of applications to be evaluated with a **Notification List**. This allows several APEX applications to be evaluated at once and the consolidated results to be sent to users on a specific **Notification List**. Any number or **Scheduling Groups** can be added to cover a wide range of purposes or needs. For example, one **Scheduling Group** may evaluate a specific application and sent the results to a **Notification List** that contains upper management personnel, whereas another **Scheduling Group** may evaluate a large number of applications and send the results to only developers.

To create a **Scheduling Group**, click on the **Scheduler** tab. Next, click on the **Schedule Groups** sub-tab. Click **Create** and enter a value for the **Group Name**, select a **Notification List** and click **Create** again.



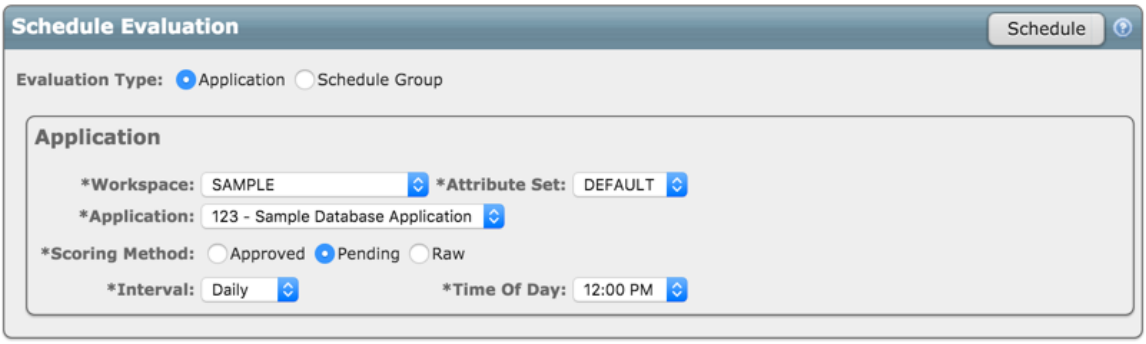
Next, click **Add Application** to add an Application to the **Schedule Group**. Select the **Workspace**, **Application** and **Attribute Set** to add and click **Create**. Repeat this process for each application you wish to add to the **Scheduling Group**.

7.3. Scheduling an Evaluation

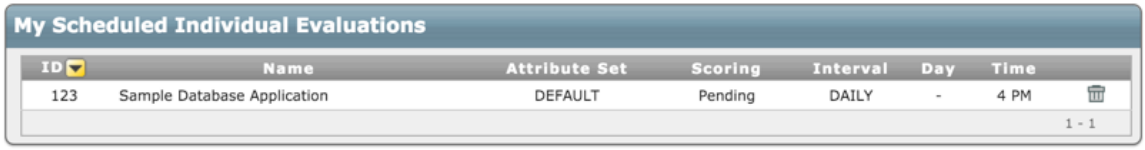
Applications can be scheduled to evaluate at a regular interval - either daily or weekly. This will keep the evaluation scores of the applications fresh while at the same time producing historical data that can be mined for trends.

There are two types of scheduled evaluation: an individual application or a **Schedule Group**. **Schedule Groups** are a set of any number of applications and are discussed in the previous section in more detail.

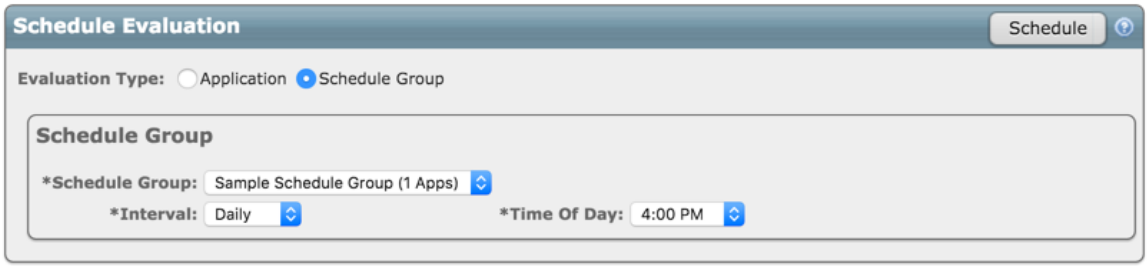
To schedule an evaluation, navigate to the main **Scheduler** tab by clicking on it. If you're scheduling a single application, leave the **Evaluation Type** set to **Application** and simply fill out the details of the form and click **Schedule**.



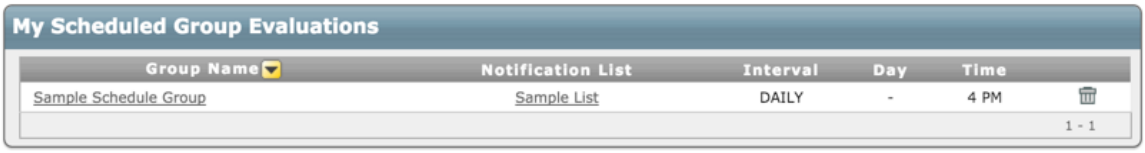
Your application should then show up under the **My Scheduled Individual Evaluations** report with the details of when it will run.



To schedule a Schedule Group, set the **Evaluation Type** to **Schedule Group**, and then fill out the details of the form and click **Schedule**.



Your application should then show up under the **My Scheduled Group Evaluations** report with the details of when it will run.



To removed a scheduled evaluation - either an individual or group - simply click the trash can icon next to the corresponding application. No further evaluations for that application or group will occur.

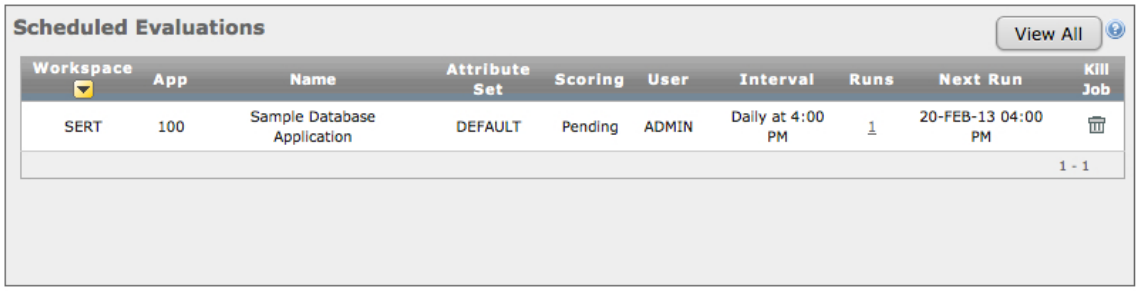
7.4. Scheduled Evaluation Results

To view scheduled evaluation results, navigate to Reports > Completed Scheduled Evaluations. Any user can see this report, though it will be limited to the application in their corresponding workspace.

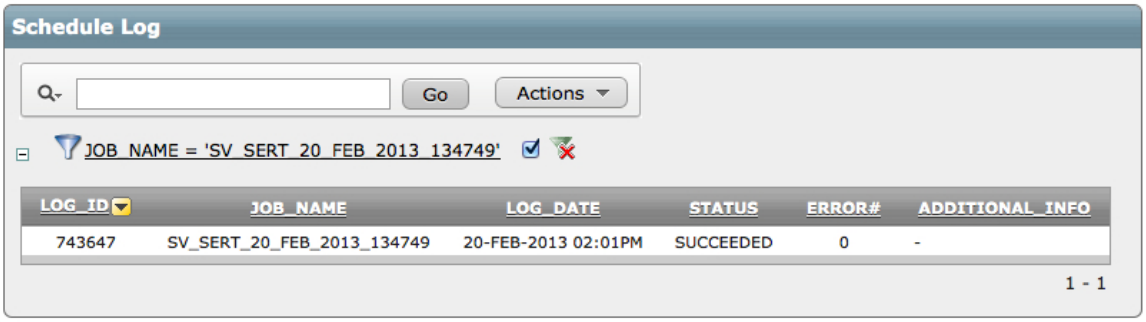
7.5. Scheduled Evaluations

The **Scheduled Evaluations** region highlights all currently scheduled evaluations and their properties. To remove a scheduled evaluation, click on the corresponding icon in the **Kill Job** column.

Clicking **View All** will display an interactive report which contains all scheduled evaluations.



Clicking on the number in the **Runs** column will display a log of all runs for a specific scheduled evaluation. If an error had occurred while running the evaluation, it would be displayed here.

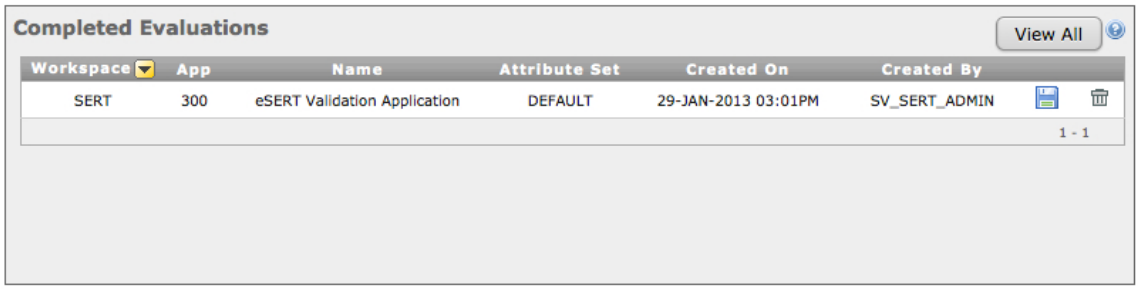


7.6. Completed Evaluations

The Completed Evaluations region will show all scheduled evaluations that have successfully completed. If a PDF report was selected when the evaluation was scheduled, it can be downloaded from here by clicking on the icon.

Click on the to delete the evaluation results. This will not delete the scheduled evaluation.

Clicking **View All** will display an interactive report which contains all completed evaluations.

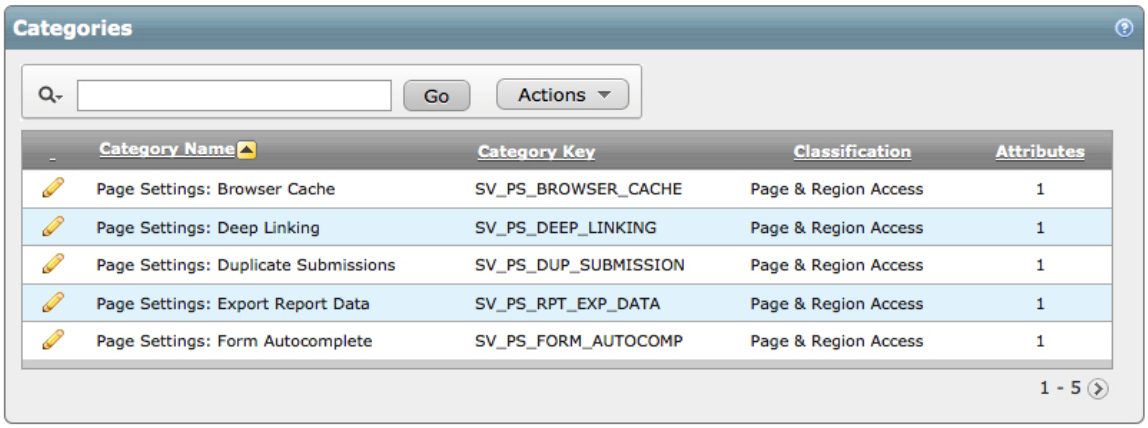


8. Administration

Accessible to only with the **Administration** role, the Administration components of APEX-SERT are used to manage some of the core components of the tool. Most developers will not need access to the Administration pages. Even those with access will not spend a lot of time here, once APEX-SERT is configured.

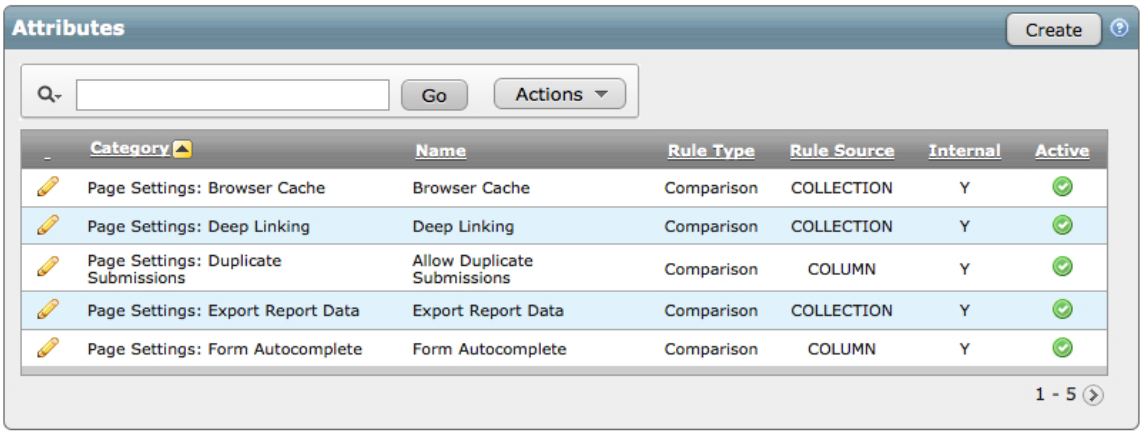
8.1. Categories

Attributes in APEX-SERT are grouped into **Categories**. Some categories have as few as 1 associated attribute, while others have upwards of 15 or more. Categories cannot be modified nor created in APEX-SERT.



8.2. Attributes

Attributes are what APEX-SERT uses when evaluating APEX applications. An attribute tells APEX-SERT where to look for a security vulnerability, the associated valid values, and the info and help text.



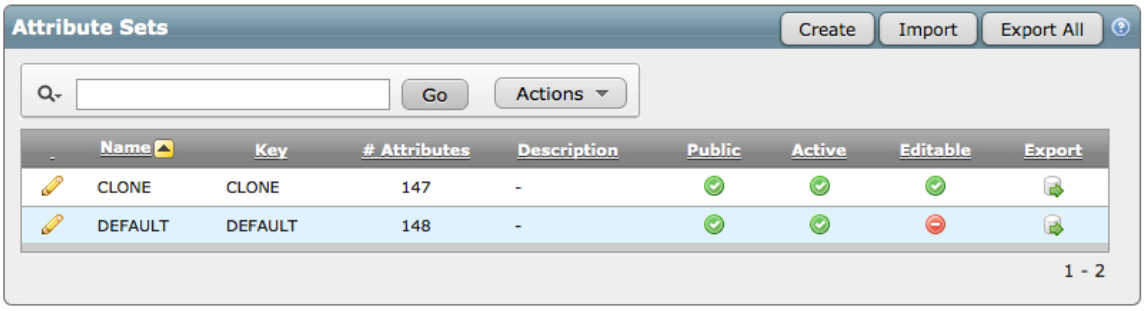
8.3. Attribute Sets

Attribute Sets are grouping of attributes that an application is evaluated against. APEX-SERT included a single attribute set called DEFAULT. The DEFAULT attribute set contains almost 150 attributes. Each time an application is evaluated in APEX-SERT, an attribute set must be selected. When the evaluation runs, it will only use the attributes in the specified attribute set.

Additional attribute sets can be created and customized by a developer. However, the DEFAULT attribute set cannot be modified in any way.

8.3.1. Overview

The main **Attribute Set** page displays all attribute sets and their associated properties. Options include creating a new attribute set, importing an existing one or exporting all attribute sets. Additionally, a specific attribute set may be exported by clicking on the icon in the corresponding row.

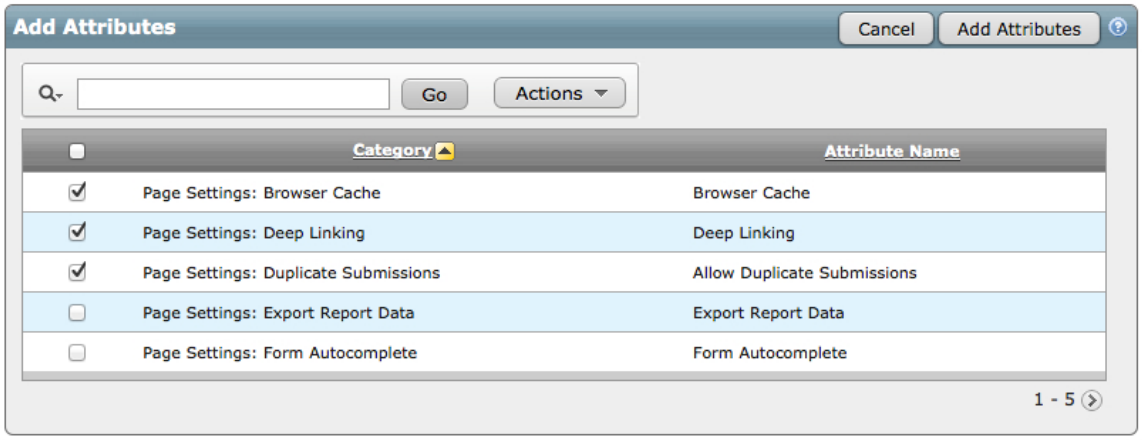


8.3.2. Creating an Attribute Set

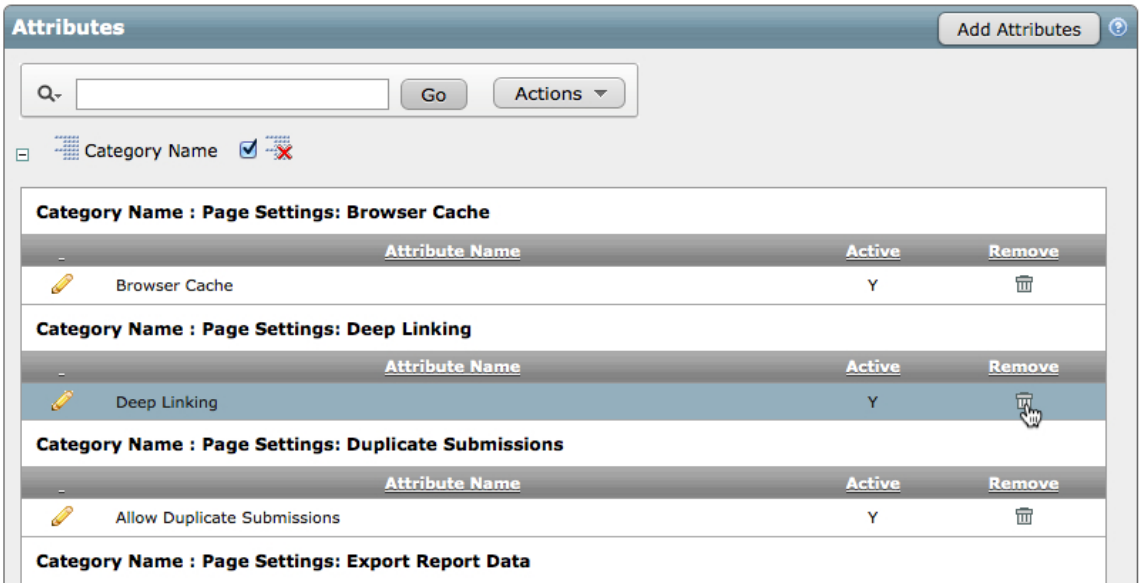
To create an attribute set, simply click on the **Create** button. Next, specify the new attribute set **Name** and **Key**. If you wish to copy the mappings of another attribute set, then be sure to select set the Copy From Attribute Set parameter to that attribute set.

Next, optionally provide a **Description** of the attribute set. Setting the **Active Flag** parameter to **No** will create the attribute set, but not make it available when running an evaluation. Setting it to **Yes** both creates it and makes it available for evaluations.

After creating an attribute set, click on **Add Attributes** to start adding attributes to it. Search for and then select attributes to add. Click **Add Attributes** again to associate those attributes to the attribute set. Repeat this process until all required attributes are added.



To remove an attribute from an attribute set, simply click on the icon that corresponds the the attribute that you want to remove. The attribute will only be removed from the attribute set; the definition of the attribute will remain intact.

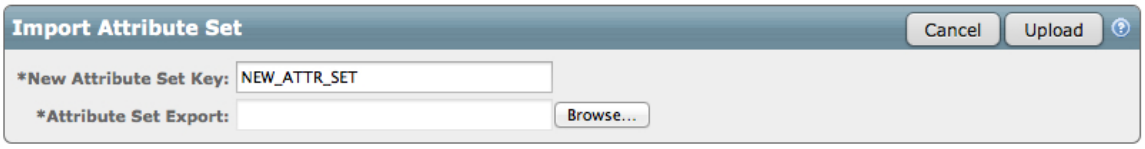


8.3.3. Exporting an Attribute Set

Attribute sets can be exported and then re-imported into the same or another instance of APEX. An attribute set can be exported by clicking on the icon in the corresponding row. This file will contain the attribute set name and details, and any associated categories, attributes and attribute values. The DEFAULT attribute set cannot be exported.

8.3.4. Importing an Attribute Set

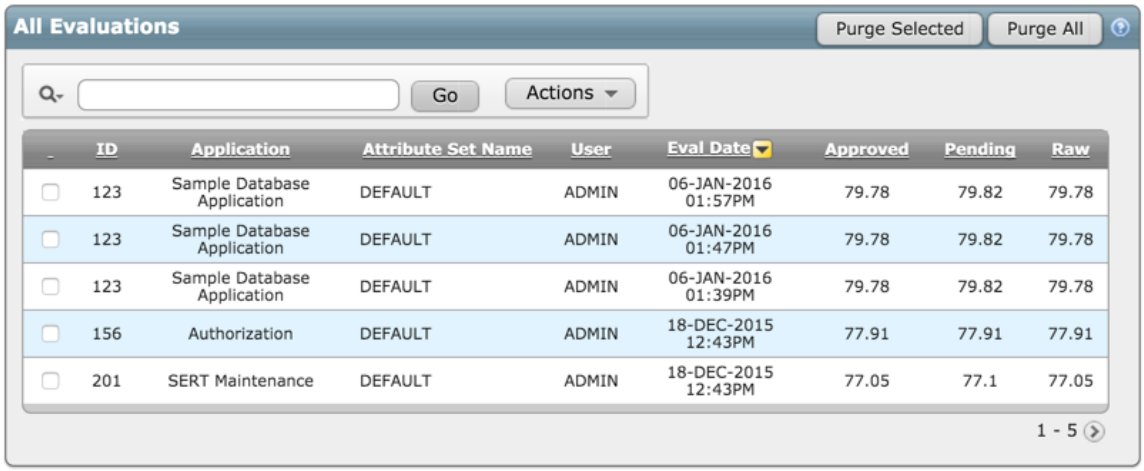
To import an attribute set, click on the **Import** button. Next, enter an **Attribute Set Key**, locate the attribute set export file and click **Upload**. Once the new attribute set is uploaded, it can be used in an application evaluation.



8.4. Purge Evaluations

An Administrator can purge evaluations that have previously run. All evaluations can be purged at once, or specific evaluations can be purged individually. This action cannot be undone.

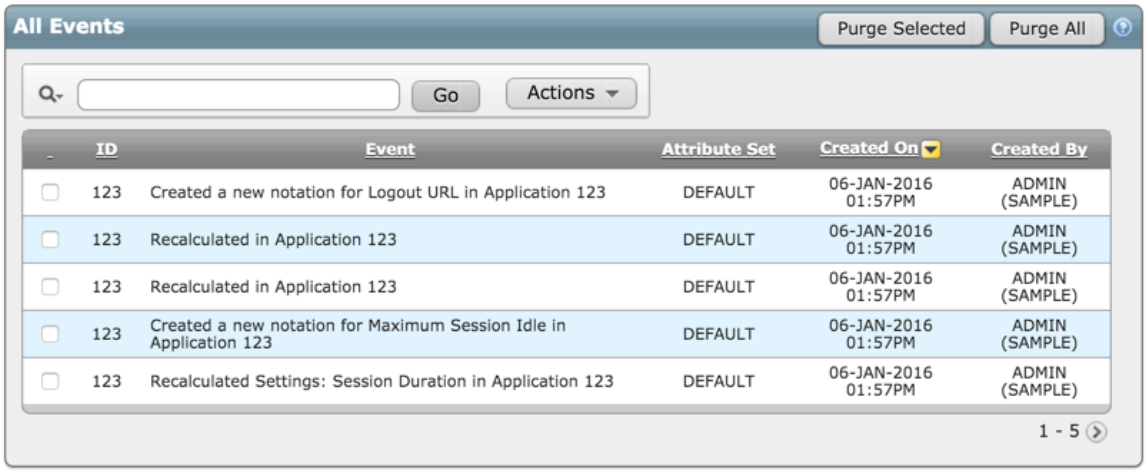
To purge all evaluations, click **Purge All**. To purge individual evaluations, select which ones you would like to purge and then click **Purge Selected**.



8.5. Purge Events

An Administrator can purge events that have previously occurred. All events can be purged at once, or specific events can be purged individually. This action cannot be undone.

To purge all events, click **Purge All**. To purge individual events, select which ones you would like to purge and then click **Purge Selected**.



8.6. Logs

The **Logs** section details any errors that have occurred during the usage of APEX-SERT. If you experience errors or other issues while using APEX-SERT, the messages that appear in the log will be vital to help troubleshoot those errors.

The only other instance where messages will be emitted into the logs is when the user preference **Record Page Views in Log** is set to Yes. This setting be used with caution as it is likely to produce and store a large amount of data in the log tables.

Logs can be purged by clicking on **Purge Logs**. This action cannot be undone, and should only be done so when the data in the logs is no longer needed.