APEX-SERT

Version 5.1 Users Guide

Table of Contents

1. Preface

1.1. Audience

The *APEX-SERT Users Guide* is provided as a reference for using APEX-SERT. It is intended for any APEX application developer, development manager and those with similar roles.

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 :

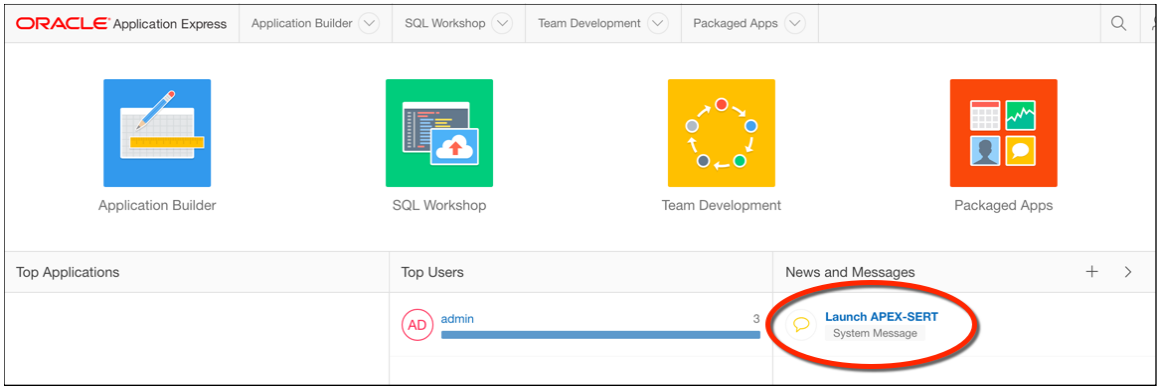
```
http://server/apex/f?p=134:10:24612647691::NO::P10_ATTRIBUTE_ID:83
```

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

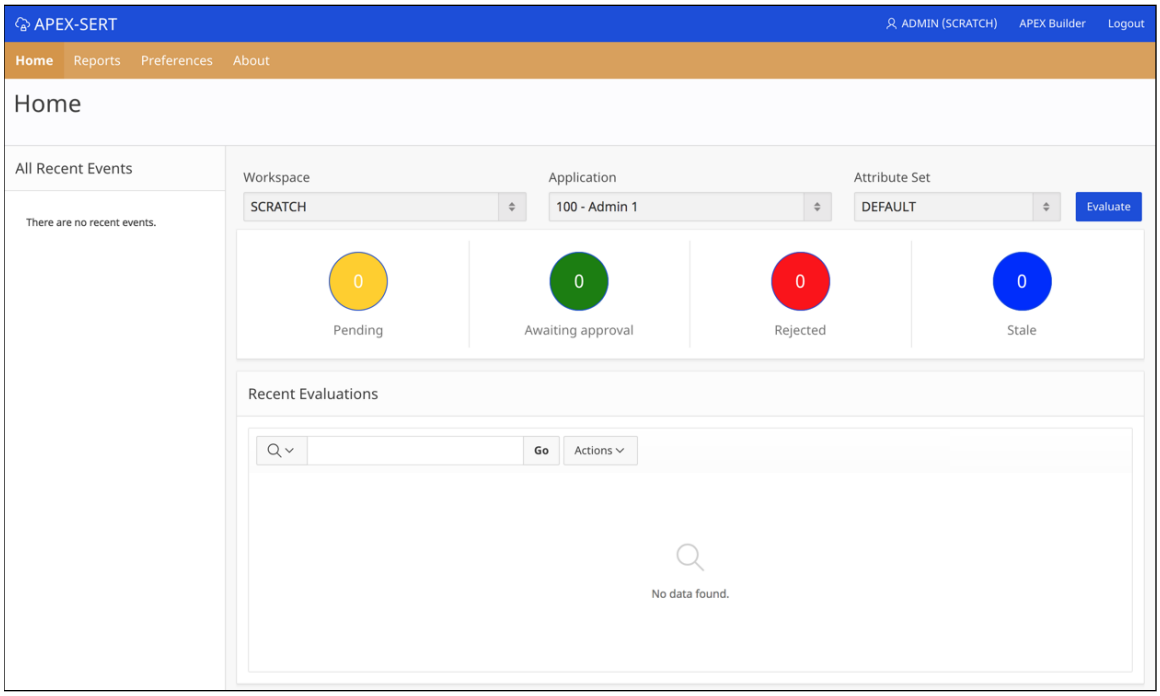
3.1. Running APEX-SERT

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:



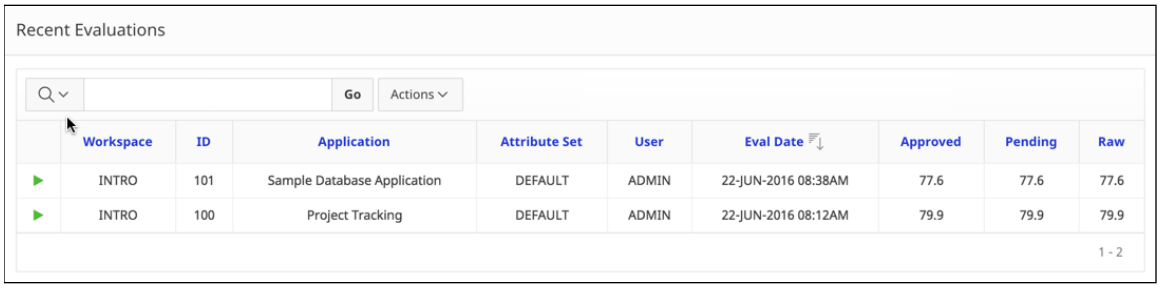
On the first launch, the home page will be quite sparse, as there have not been any evaluations run yet. As APEX-SERT is used, this page will display the high-level metrics about evaluations and exceptions.

At this point, you can start evaluating your applications immediately. Simple select a **Workspace**, **Application** and **Attribute Set** and click **Evaluate** to begin. APEX-SERT will begin evaluating your application. It may take anywhere from a couple of seconds to a minute or even longer, depending on the size of your application and processing power of your server.

3.2. Home Page

In addition to being able to evaluate applications, the Home Page of APEX-SERT contains some other details. Immediately under the list of Workspaces & Applications are four metrics. These represent a summary of all Exceptions that a user has access to. Clicking on any of the icons will display a detailed list of the Exceptions in question, and also provide a link to evaluate the corresponding application.

Next is a list of applications that have been recently evaluated, including their scores. Clicking on the green triangle will kick off an evaluation for that application.



On the left side of the page will be a list of recent activity in APEX-SERT. Things such as which applications have been evaluated, exceptions, approvals and rejections will be listed here.

Lastly, there are three links at the top of the page that will be available on all APEX-SERT pages.

First is the currently logged in user, with that user's corresponding workspace. For example, if you see **ADMIN (INTRO)**, that denotes that the user **ADMIN** from the workspace **INTRO** is currently logged in. The next link - **APEX Builder** - will return to the corresponding APEX Builder session from which APEX-SERT was launched. Finally, the **Logout** link will log out of APEX-SERT and close the browser window.

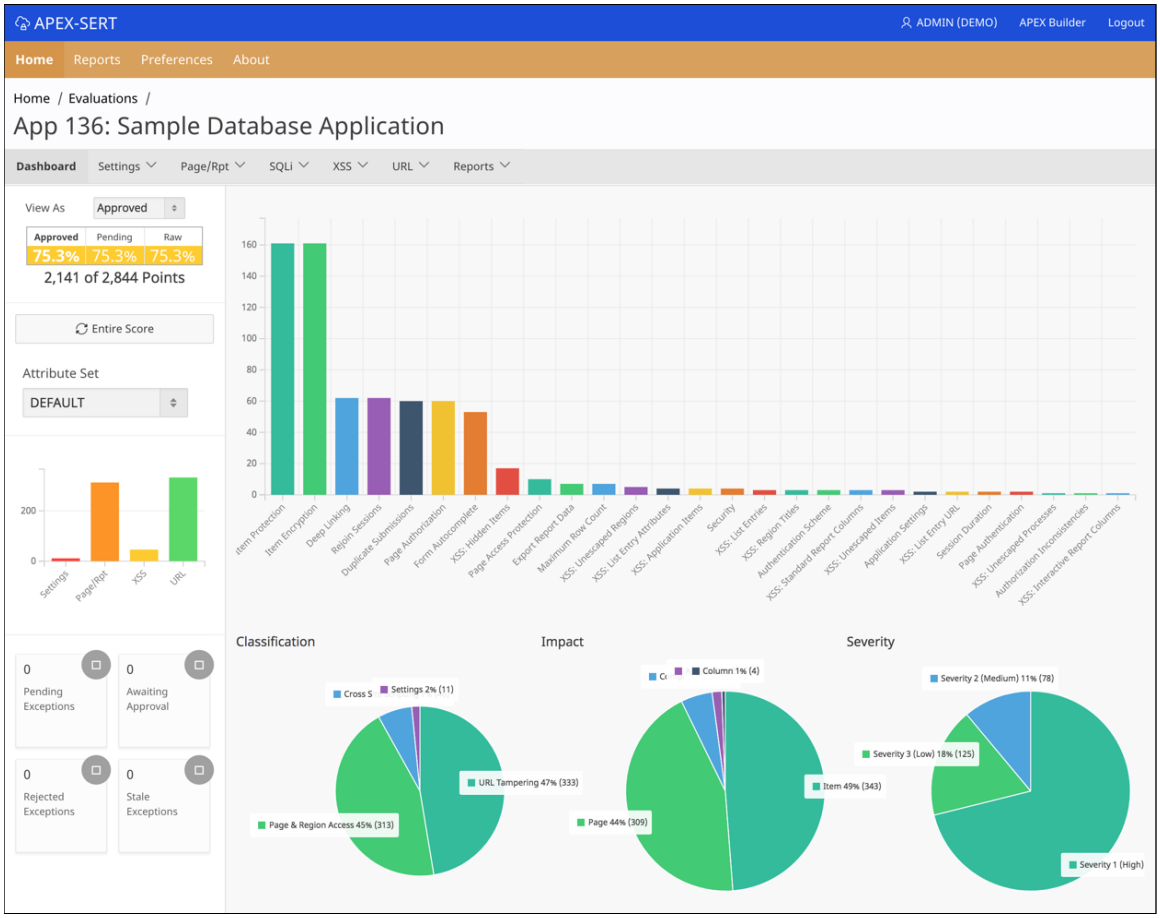
3.3. Navigation Basics

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.

3.3.1. Sidebar

The left sidebar is only used on the home page and thought an evaluation of an application. It is not used anywhere else throughout the application at all. On the home page, the sidebar will contain a list of recent events, such as which application was evaluated and by whom, as well as any exceptions that have been created, approved and/or rejected.

Within an evaluation, the left sidebar is much more complex, and serves as a mini-dashboard of sorts. Starting at the top, the first thing in the left sidebar will is a select list that allows the user to toggle between **Approved**, **Pending** and **Raw** statuses of an evaluation. Changing this value will change how APEX-SERT computes the score. For example, when Raw is selected, APEX-SERT will ignore any exceptions that have been put in place and report the corresponding score.



Below the “View As” select list are the three scores for the evaluation: **Approved**, **Pending** and **Raw**. These scores are represented by a percentage of issues that have been identified and

remedied by APEX-SERT. Immediately below the three percentage scores is the number of current and potential points for an evaluation.

Next 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 **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 **Page Score** is preferred over using **Entire Score**, especially when fixing issues outlined on the current page in APEX-SERT.

After the button or buttons is a select list containing all **Attribute Sets**. Selecting any attribute set will re-evaluate the current application using that specific attribute set. This will be a full evaluation.

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 display a modal window summarizing the component attributes.

Lastly, there is a 2x2 grid relating to exceptions for the current evaluation. Clicking on any quadrant in the grid will display the component attributes for that specific quadrant. This grid is a useful tool to see where there are exceptions that need to be approved or which are still pending from anywhere within the tool.

3.3.2. Navigation Bar

In the top-right corner of the page are the navigation bar entries. These are available from any page with APEX-SERT, and are not unlike typical APEX navigation bar entries.

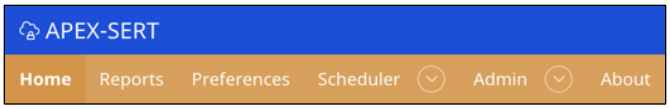
The first entry displays the currently logged in user with their corresponding workspace name in parenthesis. Next is an entry that will take the user back to the **APEX Builder,** so as long as you are evaluating an application from the same workspace that you logged in to.

If the user has the APEX-SERT Administrator role, then they will also see a link to the **APEX-SERT Admin** application. This is merely a link; they will need to provide separate credentials in order to access the application.

Lastly, there is a link to **Logout** out of APEX-SERT.

3.3.3. Tabs & Sub-Tabs

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

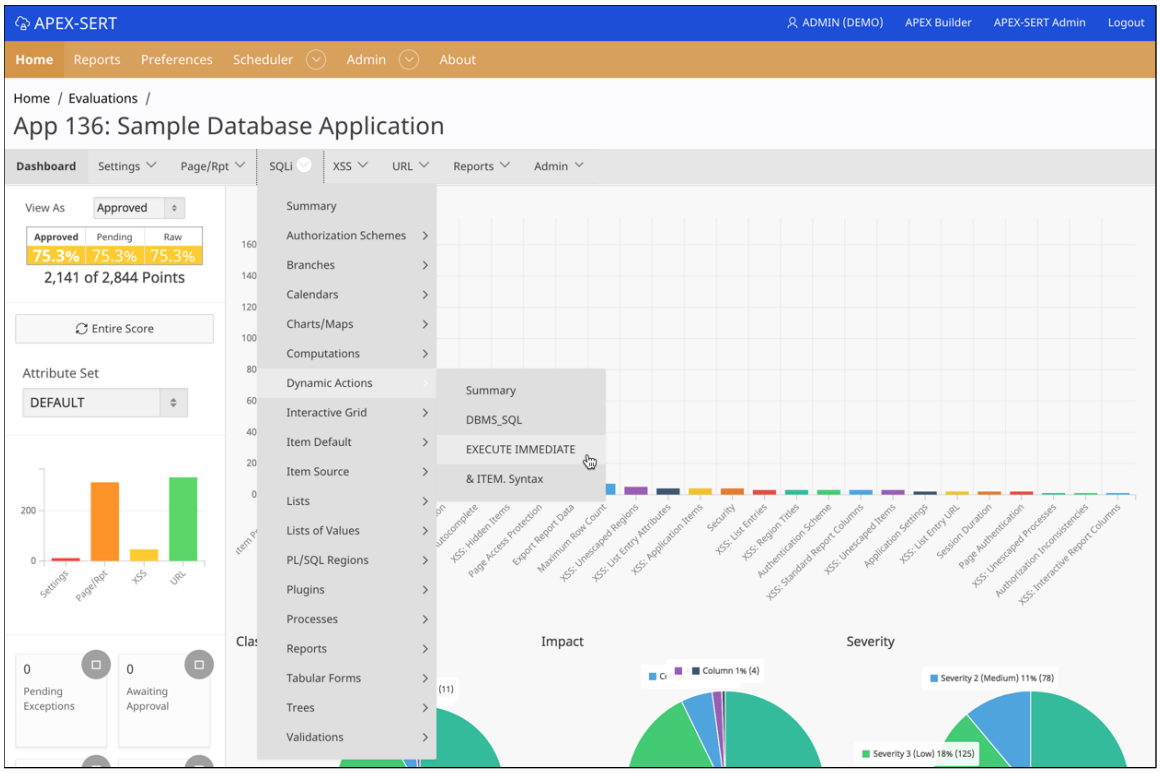


Selecting a tab will bring you to that corresponding section of APEX-SERT. Some tabs - such as **Scheduler** and **Admin** - have sub-tabs. Details for each of these sections are discussed throughout this document.

APEX-SERT also makes use of breadcrumbs throughout the application. These breadcrumbs can be used to assist with navigation.

When running an evaluation, the Application ID and Name being evaluated is displayed in bold type, just under the breadcrumbs. As the application being evaluated changes, so will this title.

Just under the Application ID and Name 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 clicked, 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.

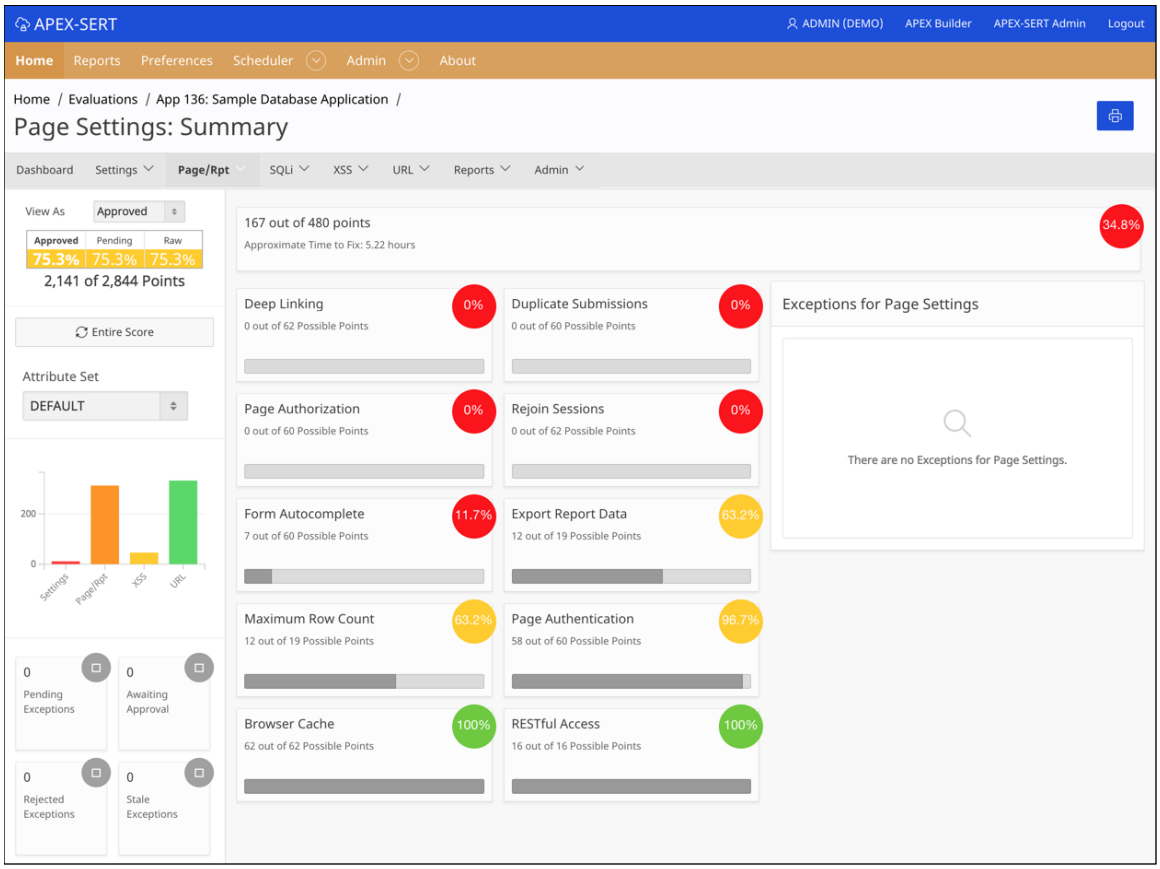


Lastly, APEX-SERT makes extensive use of APEX interactive reports, something that most developers will be very familiar with. These reports allow each user of APEX-SERT to select which columns are available, apply filters and perform other functions on a report, all without the need to get a developer 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.

Clicking on the top-level item in any sub-tab will display the classification summary page.



This page displays a scoring summary of associated attributes or categories of attributes. Clicking on either the bar chart in the left column of one of the cards will bring you to that specific attribute's page, where the discrete details of that attribute will be displayed.

Clicking on the **print** icon will produce a PDF version of this report.

The score displayed at the top of the page here represents the score only for this classification. In the above example, the score of 34.8% is derived from achieving only 167 out of a possible 480 points. The **Approximate Time to Fix** metric is also displayed here. This will give the developer an estimate as to how much time would be required to remedy the attributes that failed the evaluation.

The values displayed on this page are based on which "mode" APEX-SERT is running in. In this example, APEX-SERT is running in **Raw** mode, denoted by the label of the approved score being rendered in bold text. Selecting either **Approved** or **Pending** 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 **Workspace**, **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 size/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 ~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%. In fact, if you get a raw score of 100%, your application likely won't run at all!

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 APEX-SERT flagged an attribute as 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.

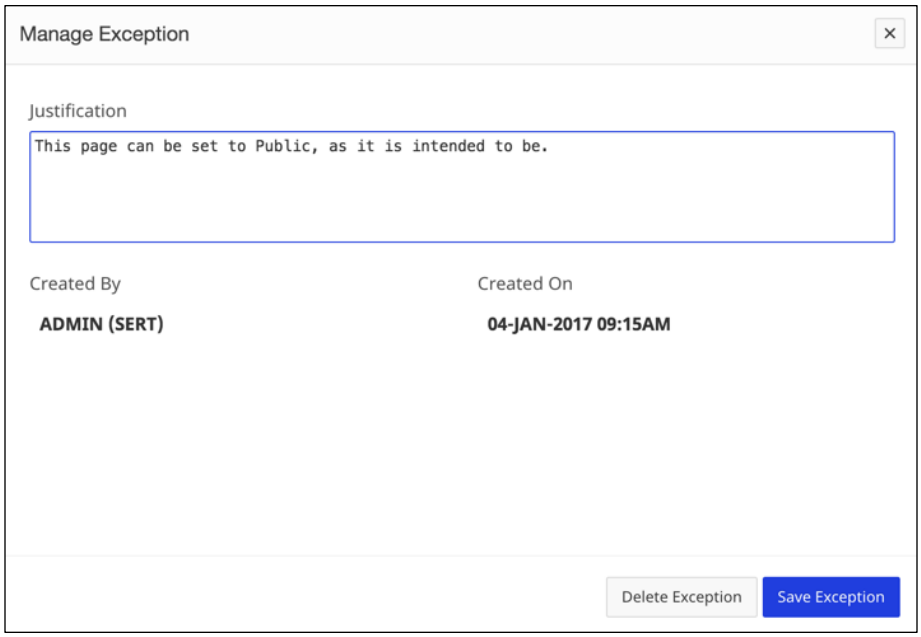
4.2.1. Creating Exceptions

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.

	Page	Page Name	Updated By	Updated On	Auth Scheme	Result		
	1	Sample Database Application	ADMIN	16-APR-2018 07:27:26 AM	MUST_NOT_BE_PUBLIC_USER	PASS	-	
	2	Customers	-	16-FEB-2017 11:11:25 AM	-	PENDING		
	3	Products	-	16-FEB-2017 11:11:25 AM	-	FAIL		
	4	Orders	-	16-FEB-2017 11:11:25 AM	-	FAIL		
	5	Sales by Month	HILARY	07-OCT-2016 08:52:23 AM	-	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, approved, rejected or deleted later.

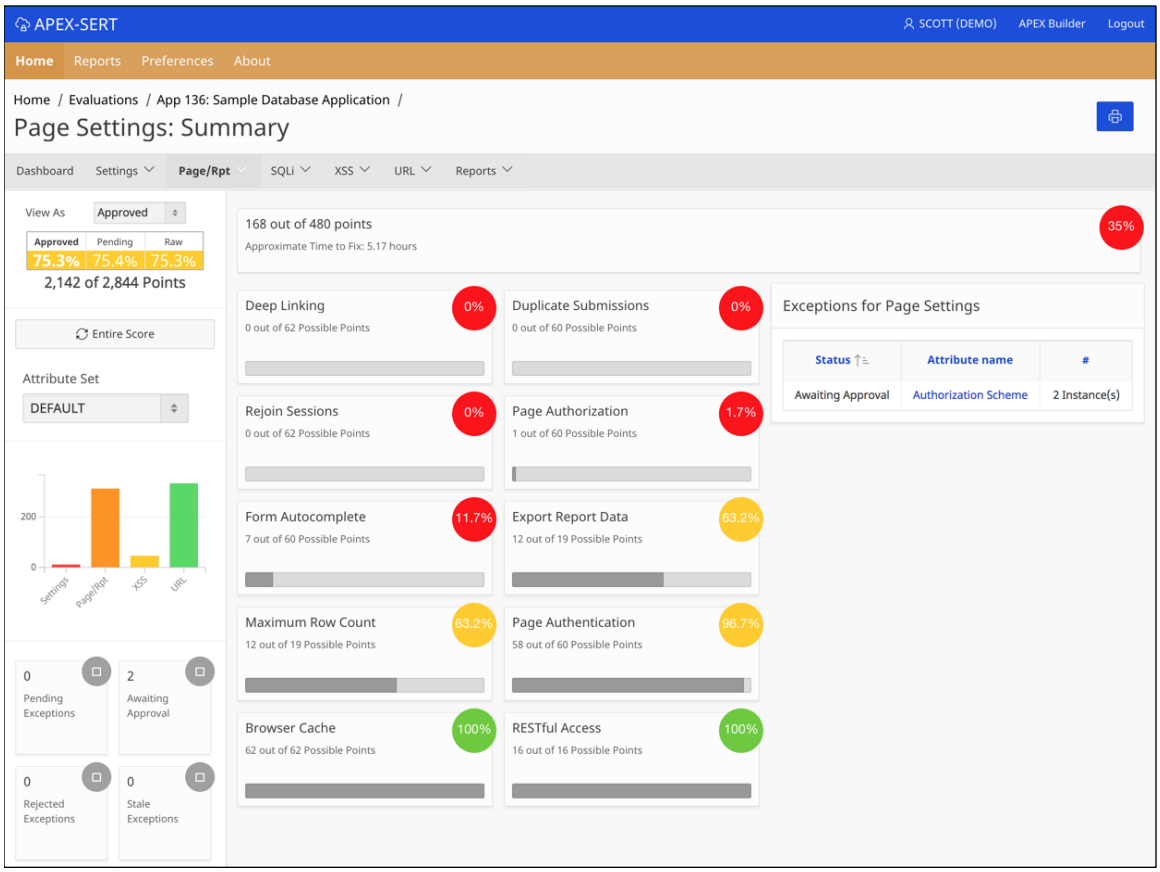
4.2.3. Approving & Rejecting Exceptions

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.

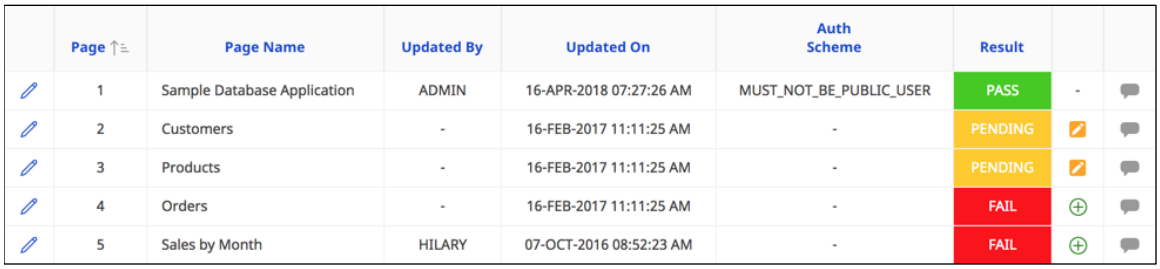
Once exceptions are created, the grid in the bottom of the left sidebar will start to display the corresponding counts of each of theirs statuses. Clicking on a quadrant will show the detail records

and allow a developer to inspect each discrete attribute that has an exception associated with it. If a developer has an Approver role, then can then either approve or reject any exception.

A list of exceptions will also be displayed on the Classification Summary page for each classification, as shown below.

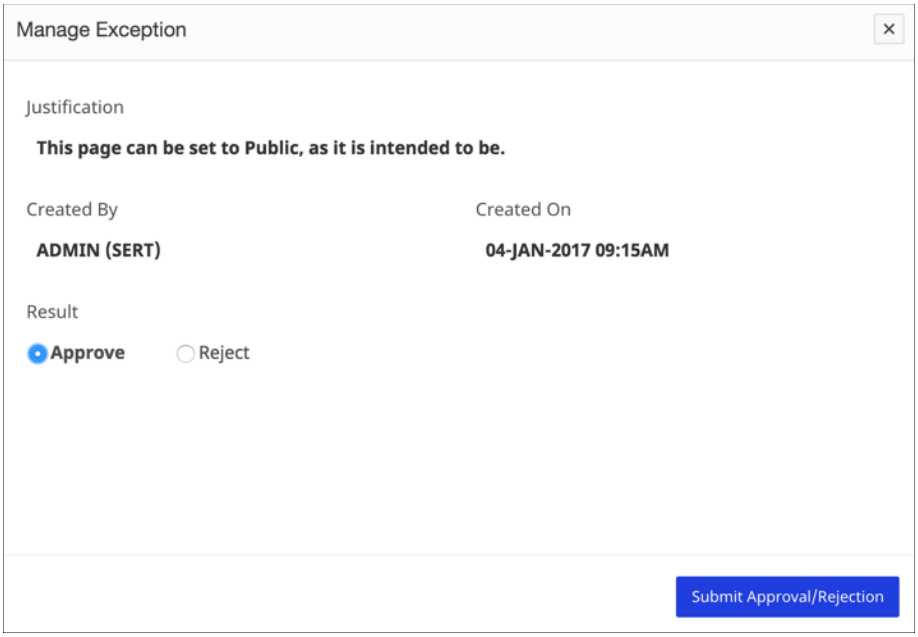


Simply click on either of the links, and you will be taken to the specific page where the exceptions have been created. If your user has the **Approver** role, then you will be able to approve exceptions, so long as they were created by someone else. It is not possible to self-approve exceptions in APEX-SERT.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



	Page	Page Name	Updated By	Updated On	Auth Scheme	Result		
	1	Sample Database Application	ADMIN	16-APR-2018 07:27:26 AM	MUST_NOT_BE_PUBLIC_USER	PASS	-	
	2	Customers	-	16-FEB-2017 11:11:25 AM	-	PENDING		
	3	Products	-	16-FEB-2017 11:11:25 AM	-	PENDING		
	4	Orders	-	16-FEB-2017 11:11:25 AM	-	FAIL		
	5	Sales by Month	HILARY	07-OCT-2016 08:52:23 AM	-	FAIL		

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.

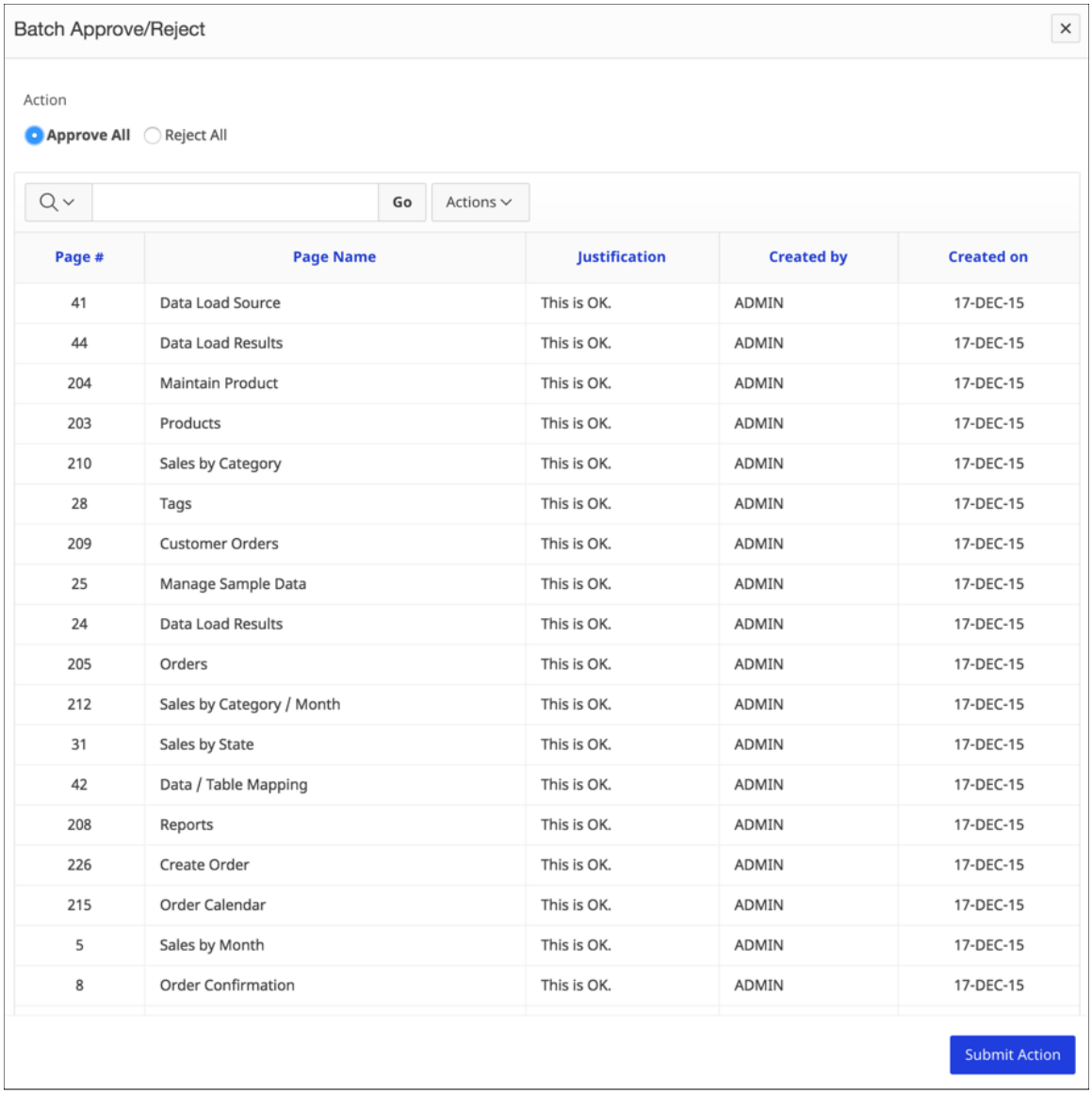
	Page	Page Name	Updated By	Updated On	Auth Scheme	Result		
	1	Sample Database Application	ADMIN	16-APR-2018 07:27:26 AM	MUST_NOT_BE_PUBLIC_USER	PASS	-	
	2	Customers	-	16-FEB-2017 11:11:25 AM	-	APPROVED		
	3	Products	-	16-FEB-2017 11:11:25 AM	-	PENDING		
	4	Orders	-	16-FEB-2017 11:11:25 AM	-	FAIL		
	5	Sales by Month	HILARY	07-OCT-2016 08:52:23 AM	-	FAIL		

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**.

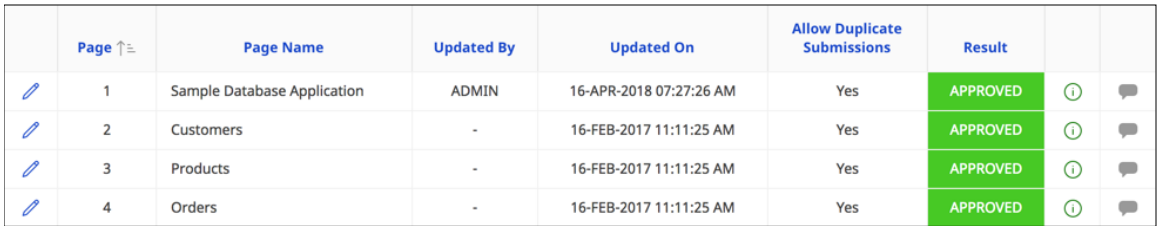
Now, when the popup disappears and the page reloads, the corresponding component's status will change from **PENDING** to **REJECTED**.

	Page	Page Name	Updated By	Updated On	Auth Scheme	Result		
	1	Sample Database Application	ADMIN	16-APR-2018 07:27:26 AM	MUST_NOT_BE_PUBLIC_USER	PASS	-	
	2	Customers	-	16-FEB-2017 11:11:25 AM	-	APPROVED		
	3	Products	-	16-FEB-2017 11:11:25 AM	-	REJECTED		
	4	Orders	-	16-FEB-2017 11:11:25 AM	-	FAIL		
	5	Sales by Month	HILARY	07-OCT-2016 08:52:23 AM	-	FAIL		

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.



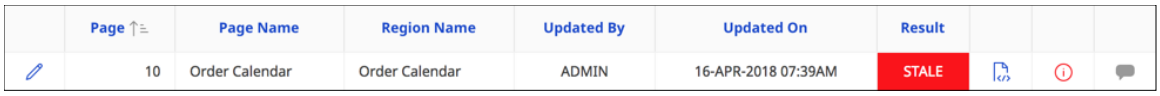
Simply choose whether to **Approve** or **Reject** all, enter a reason if rejecting, and click **Submit Action**. When the page reloads, all previously pending exceptions that were submitted by others will now be either **APPROVED** or **REJECTED**, depending on which action was selected.



4.2.4. Stale Exceptions

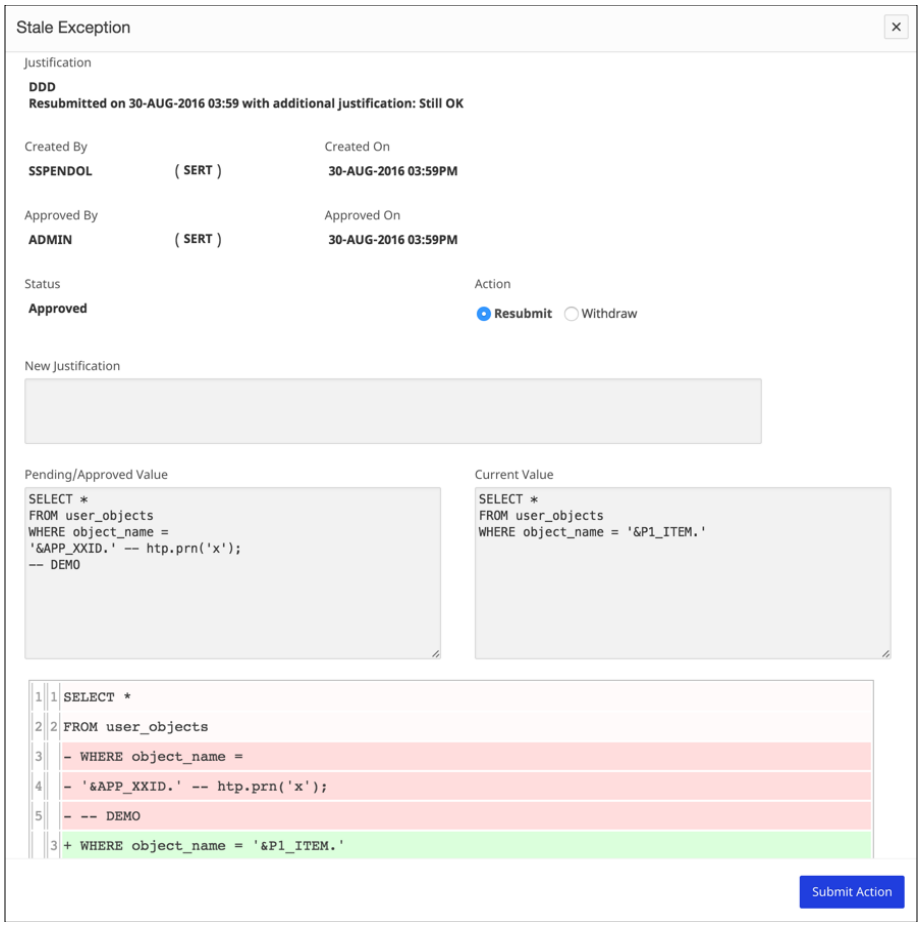
Security is not an event, but rather a process. If an exception is put in place and then approved, and then the underlying value of that attribute is changed, is the exception still valid? Perhaps not. Therefore, APEX-SERT exceptions can go "stale" if the data for which they were approved changes. This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



	Page	Page Name	Region Name	Updated By	Updated On	Result			
	10	Order Calendar	Order Calendar	ADMIN	16-APR-2018 07:39AM	STALE			

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

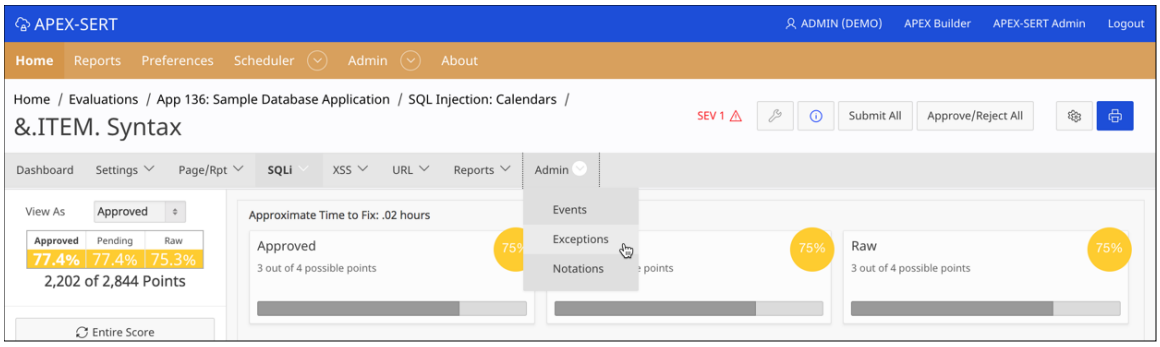


Both the value at the time the exception was submitted and the current value are displayed. Additionally, a second region will display a "diff" between the two regions, highlighting code that was added in green and code that was removed in red.

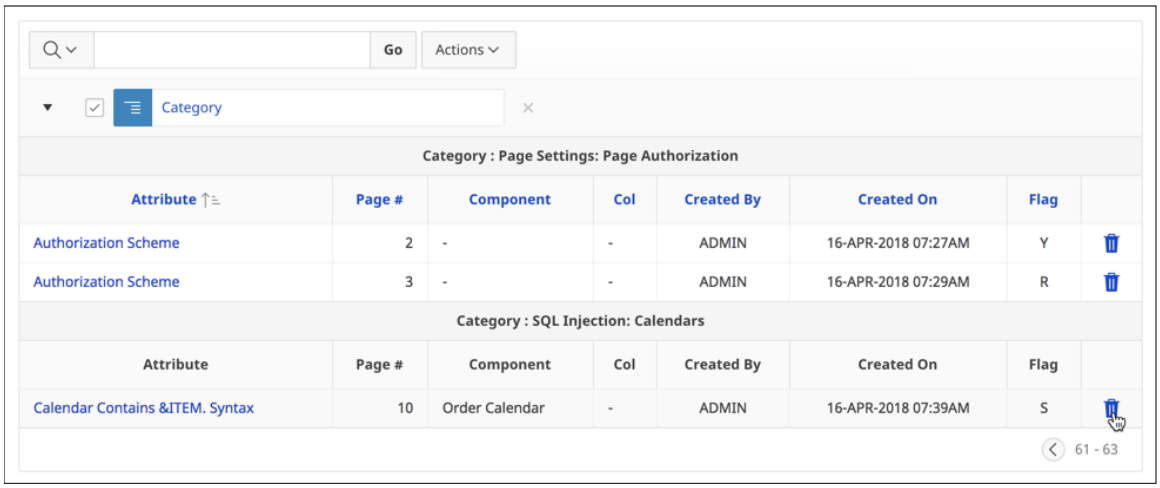
If the code change did not alter the exception, the developer can provide another justification and simply re-submit it. If the code change did, in fact, introduce a vulnerability, the developer can withdraw the exception and properly address the defect.

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

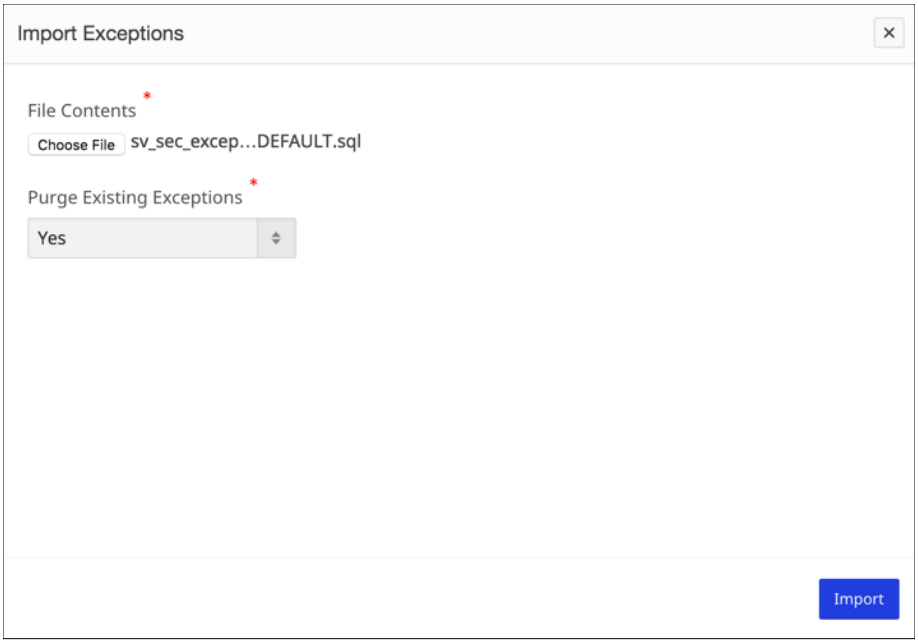
A lot of work will go into developers entering, approving and/or rejecting exceptions. As applications move from the development server to the QA server, it is important to be able to move the exceptions in tandem with the applications. Thus, APEX-SERT provides the ability for an administrator to import 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. Depending on your browser settings, the file may automatically download or you may be prompted for an action. If the later is the case, then select 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.

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.

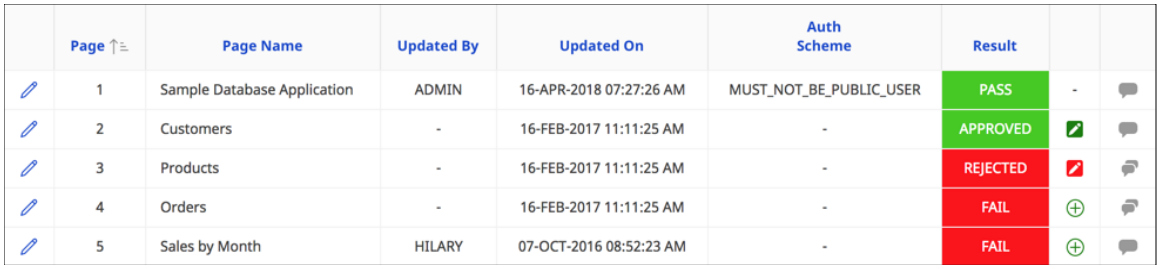
4.3. Notations

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**.

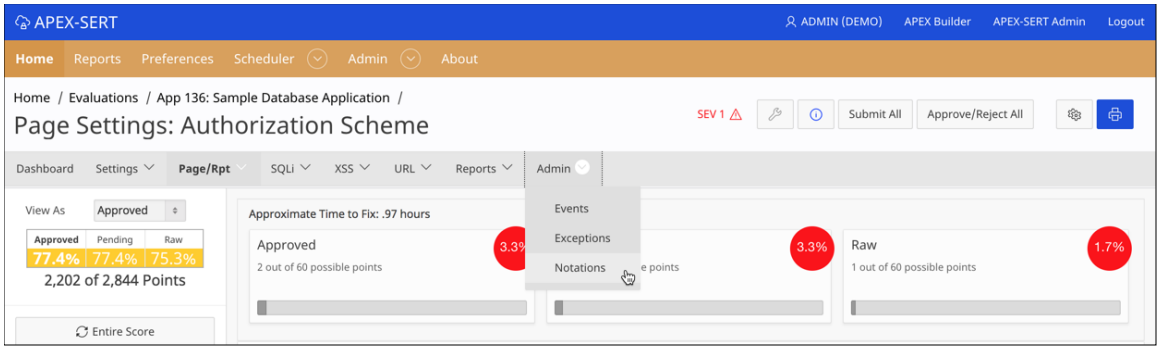
When an element has a notation, the icon will change to reflect that.



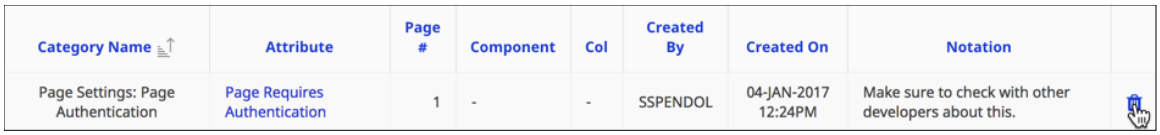
	Page	Page Name	Updated By	Updated On	Auth Scheme	Result		
	1	Sample Database Application	ADMIN	16-APR-2018 07:27:26 AM	MUST_NOT_BE_PUBLIC_USER	PASS	-	
	2	Customers	-	16-FEB-2017 11:11:25 AM	-	APPROVED		
	3	Products	-	16-FEB-2017 11:11:25 AM	-	REJECTED		
	4	Orders	-	16-FEB-2017 11:11:25 AM	-	FAIL		
	5	Sales by Month	HILARY	07-OCT-2016 08:52:23 AM	-	FAIL		

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.



Category Name	Attribute	Page #	Component	Col	Created By	Created On	Notation	
Page Settings: Page Authentication	Page Requires Authentication	1	-	-	SSPENDOL	04-JAN-2017 12:24PM	Make sure to check with other developers about this.	

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

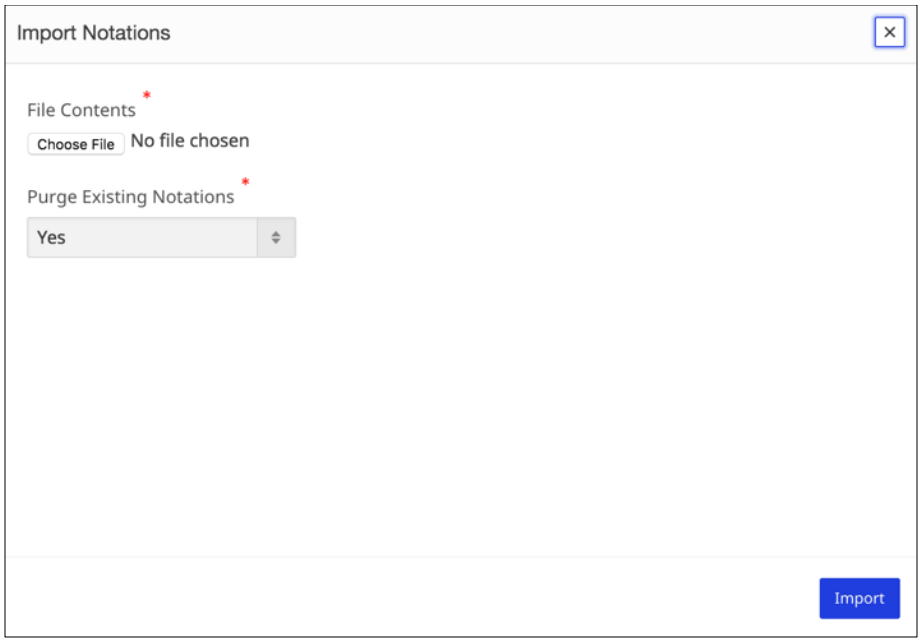
A lot of work will go into developers entering notations. As applications move from the development server to the QA server, it may be necessary to be able to move the notations in tandem with the applications. Thus, APEX-SERT provides the ability for an administrator to import and export notations,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

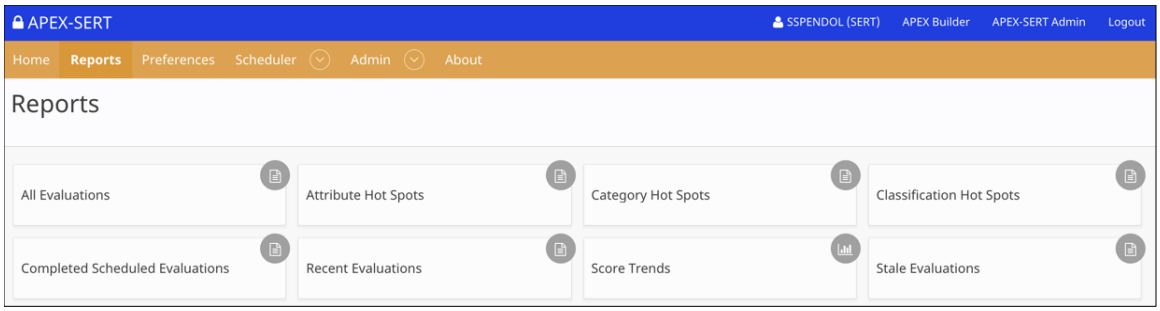
Report in APEX-SERT can be found in one of two places: at the specific application level and at the workspace level. Each type of report focuses on the specifics of the evaluation of the application or evaluations across multiple applications, respectively.

All reports in APEX-SERT can also be printed in PDF format. APEX-SERT uses PL/FPDF, a free open source PDF library to print well-formatted PDF reports without any additional software or server components.

Each report can further be configured by clicking on the gear icon. Here, the columns can be selected or de-selected, as well as length, alignment and display order defined.

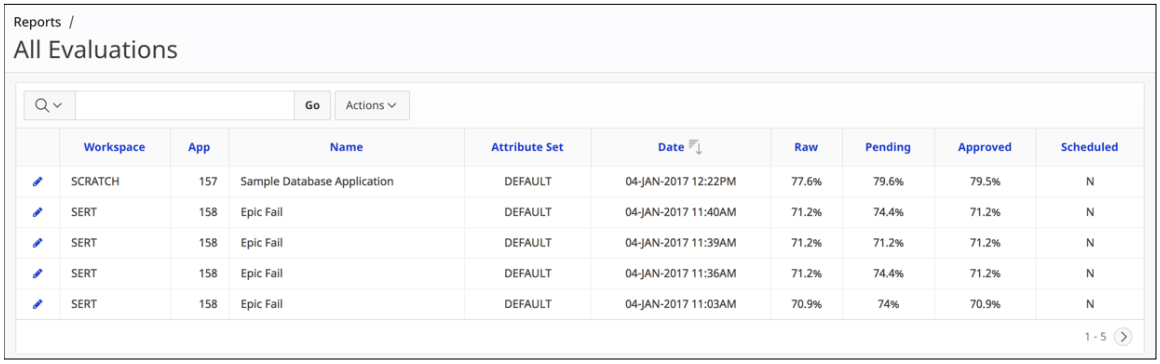
5.1. Workspace Reports

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.



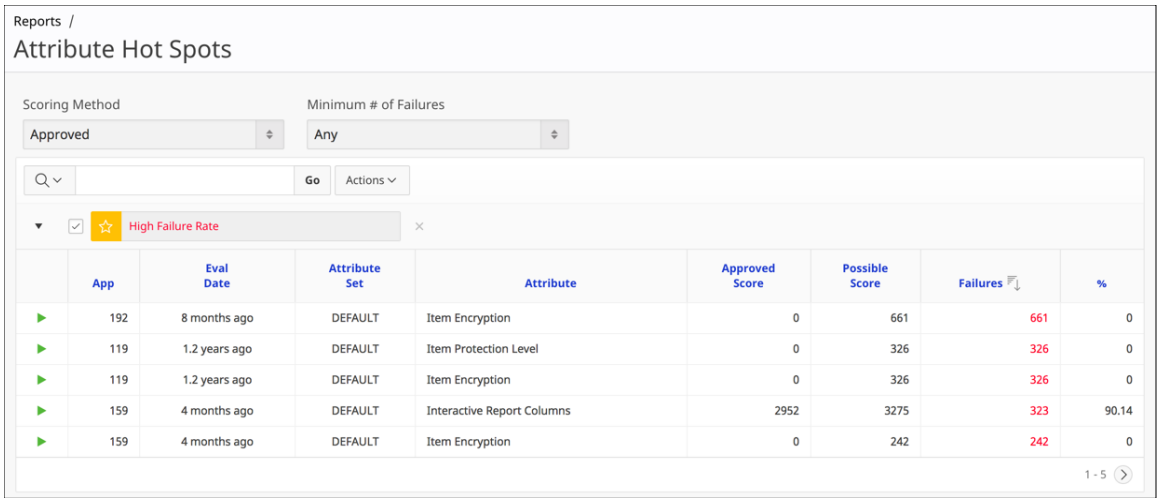
5.1.1. All Evaluations

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.



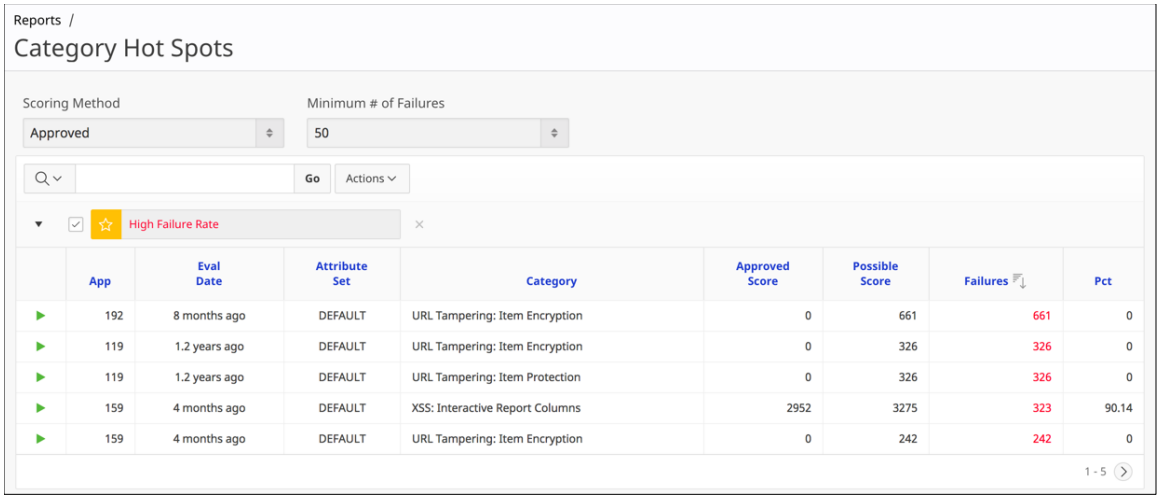
5.1.2. Attribute Hot Spots

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.



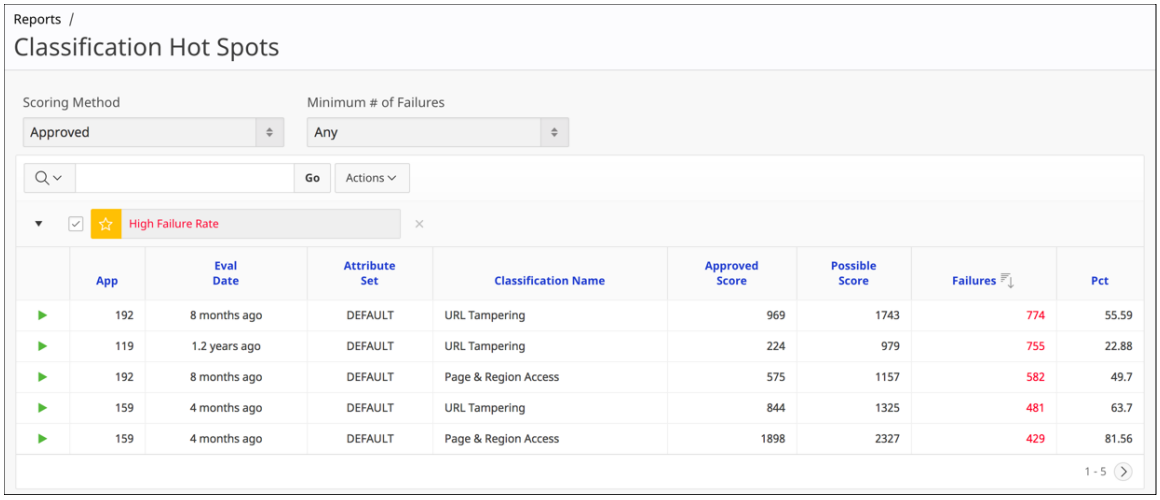
5.1.3. Category Hot Spots

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.



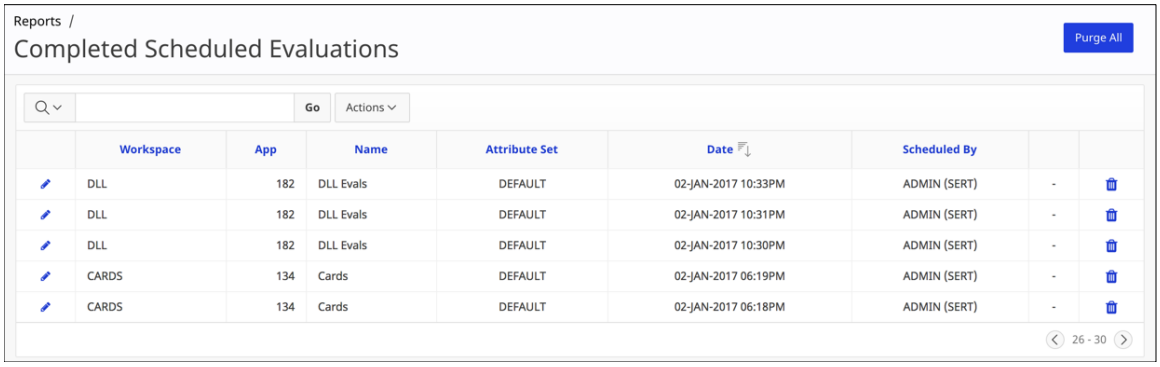
5.1.4. Classification Hot Spots

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. Completed Scheduled Evaluations

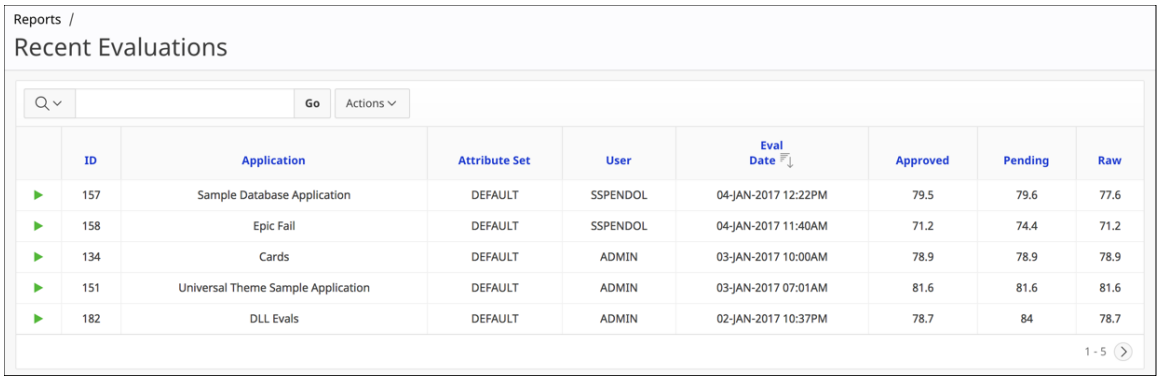
The Completed Scheduled Evaluations report shows all completed scheduled evaluations.



Clicking on the edit pencil will display more details about the evaluation. Further details can be displayed by clicking on the corresponding classification and categories.

5.1.6. 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.

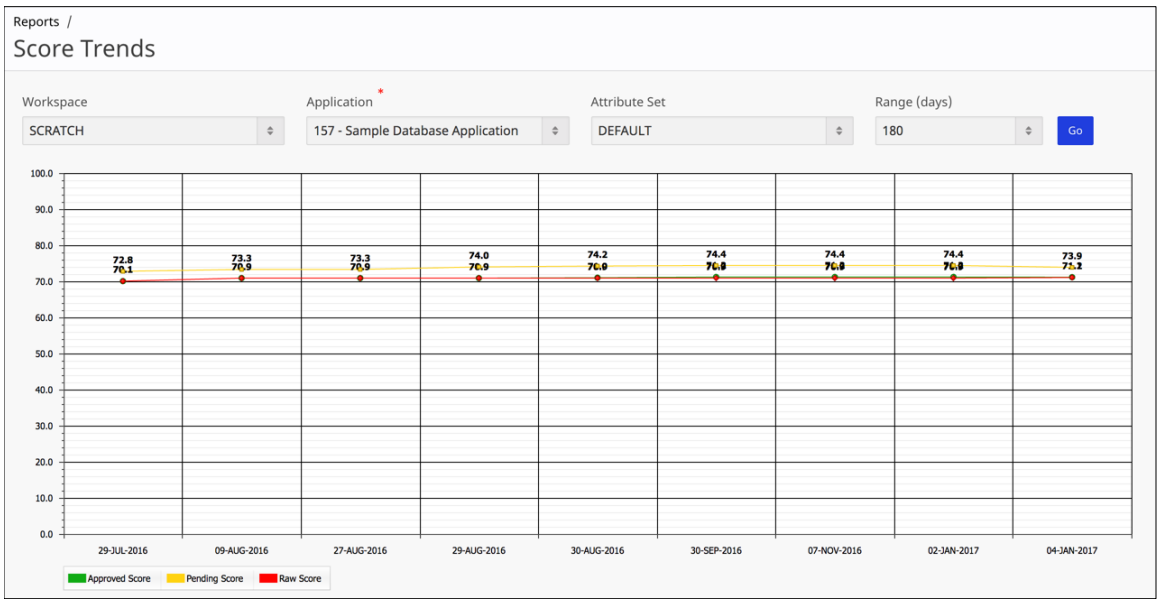


	ID	Application	Attribute Set	User	Eval Date	Approved	Pending	Raw
▶	157	Sample Database Application	DEFAULT	SSPENDOL	04-JAN-2017 12:22PM	79.5	79.6	77.6
▶	158	Epic Fail	DEFAULT	SSPENDOL	04-JAN-2017 11:40AM	71.2	74.4	71.2
▶	134	Cards	DEFAULT	ADMIN	03-JAN-2017 10:00AM	78.9	78.9	78.9
▶	151	Universal Theme Sample Application	DEFAULT	ADMIN	03-JAN-2017 07:01AM	81.6	81.6	81.6
▶	182	DLL Evals	DEFAULT	ADMIN	02-JAN-2017 10:37PM	78.7	84	78.7

1 - 5

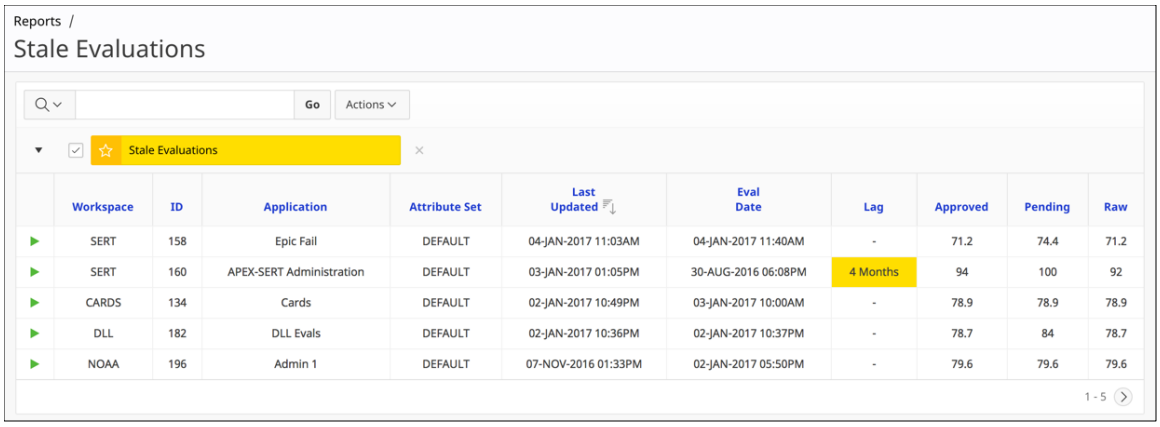
5.1.7. Score Trends

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



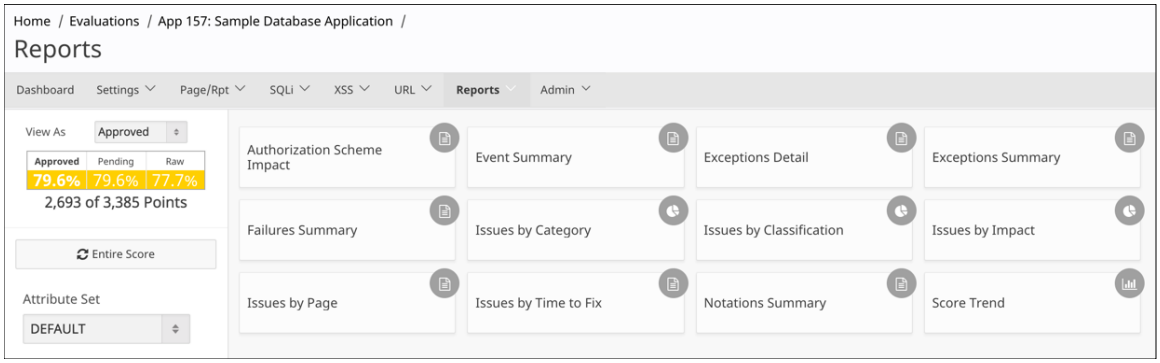
5.1.8. Stale Evaluations

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.



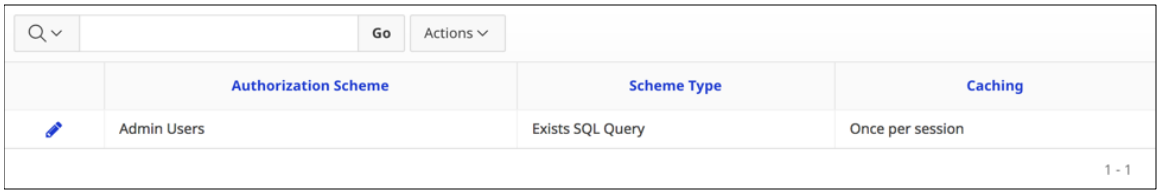
5.2. Application Reports

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.

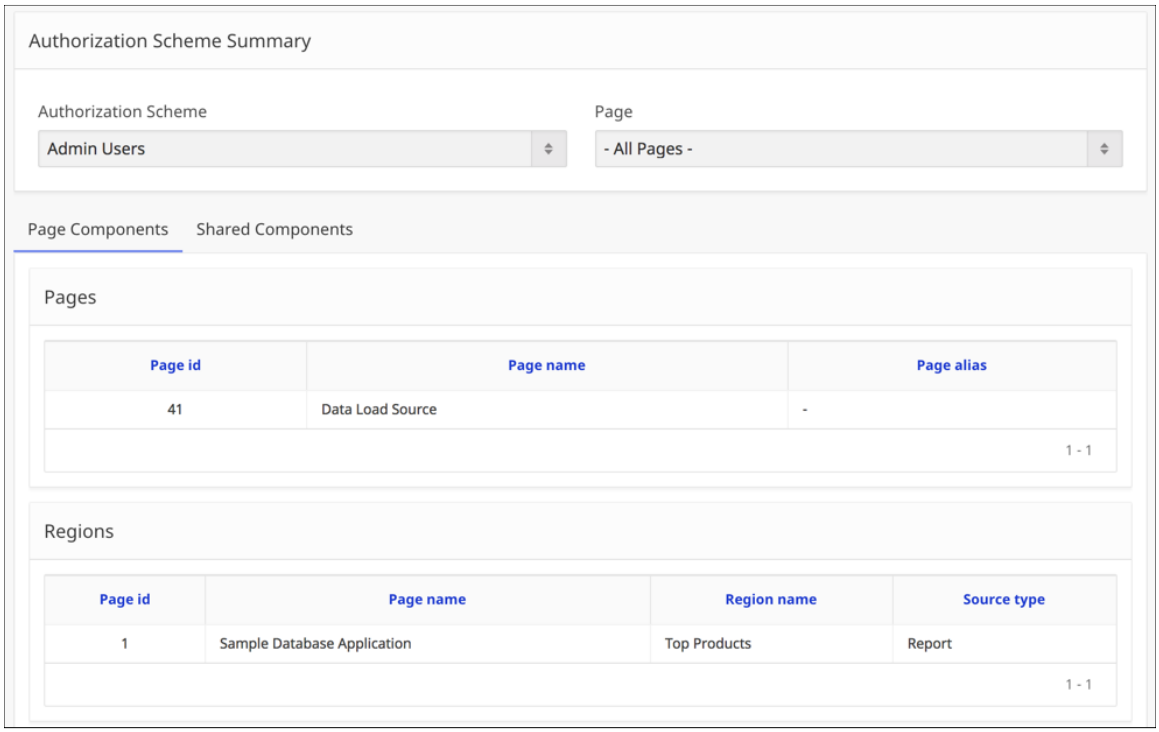


5.2.1. Authorization Scheme Impact

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

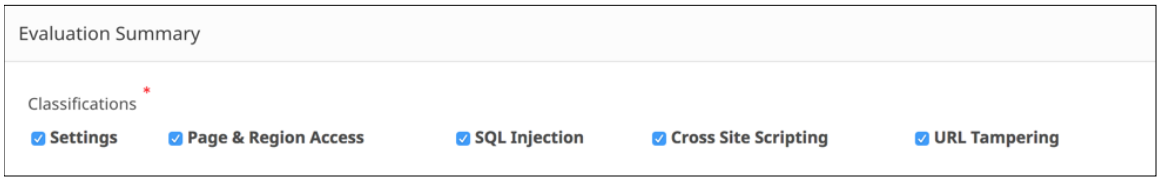


Clicking on the edit icon will display the results of the report. From this screen, the report can be filtered based on either the **Authorization Scheme** and **Page**. Additionally, there are two sub-tabs that can be toggled: **Page Components** and **Shared Components**.



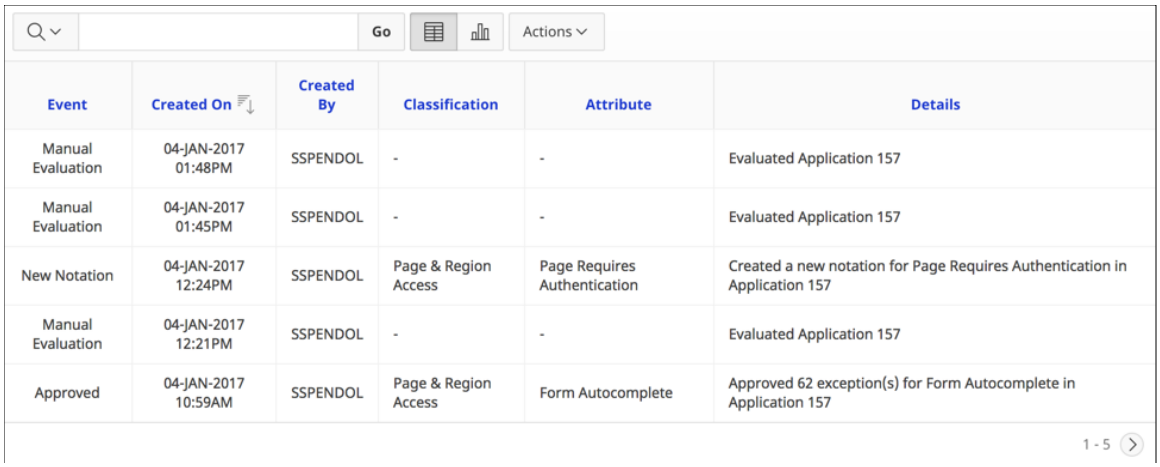
5.2.2. Evaluation Summary

The Evaluation Summary report is the only report that is PDF-only. Simply select which Classification(s) to include and click the **printer** icon to run the report.



5.2.3. 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.

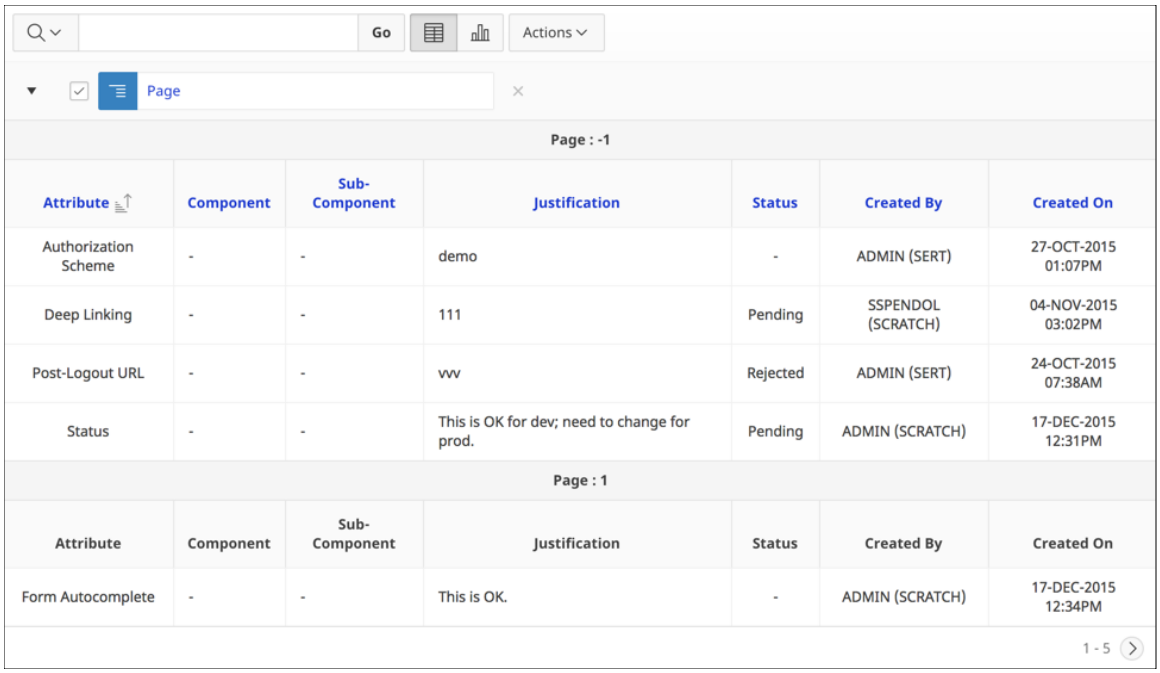


Event	Created On	Created By	Classification	Attribute	Details
Manual Evaluation	04-JAN-2017 01:48PM	SSPENDOL	-	-	Evaluated Application 157
Manual Evaluation	04-JAN-2017 01:45PM	SSPENDOL	-	-	Evaluated Application 157
New Notation	04-JAN-2017 12:24PM	SSPENDOL	Page & Region Access	Page Requires Authentication	Created a new notation for Page Requires Authentication in Application 157
Manual Evaluation	04-JAN-2017 12:21PM	SSPENDOL	-	-	Evaluated Application 157
Approved	04-JAN-2017 10:59AM	SSPENDOL	Page & Region Access	Form Autocomplete	Approved 62 exception(s) for Form Autocomplete in Application 157

1 - 5

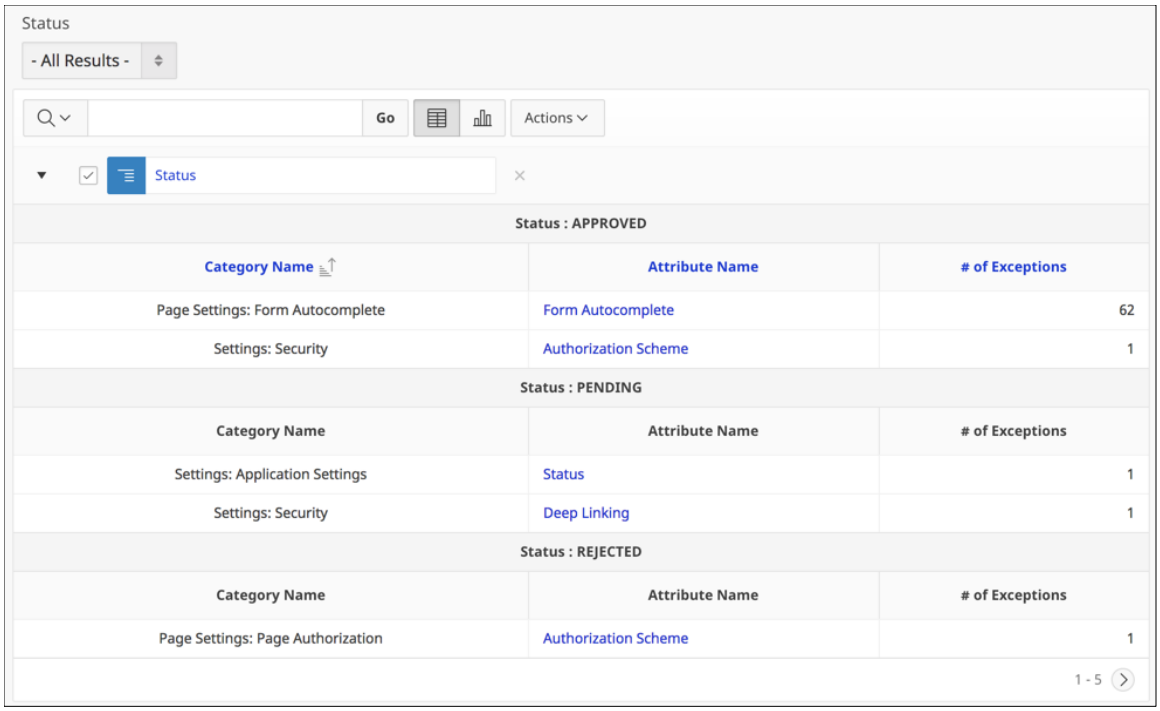
5.2.4. Exceptions Detail

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



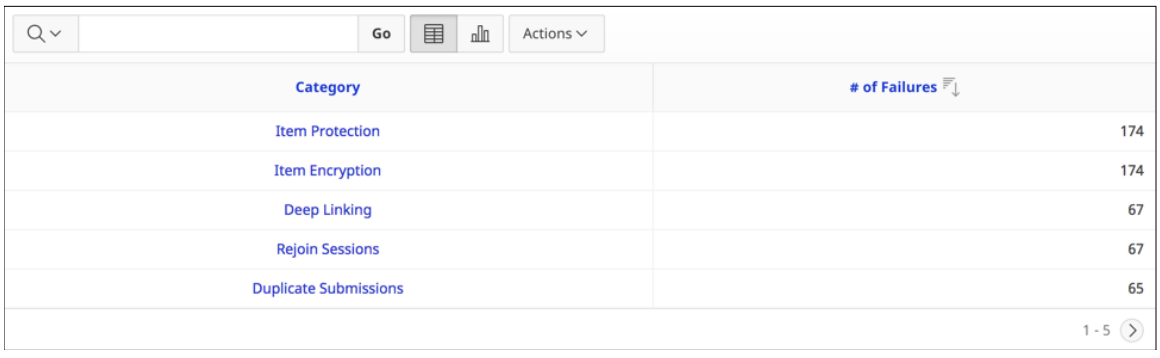
5.2.5. Exceptions Summary

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



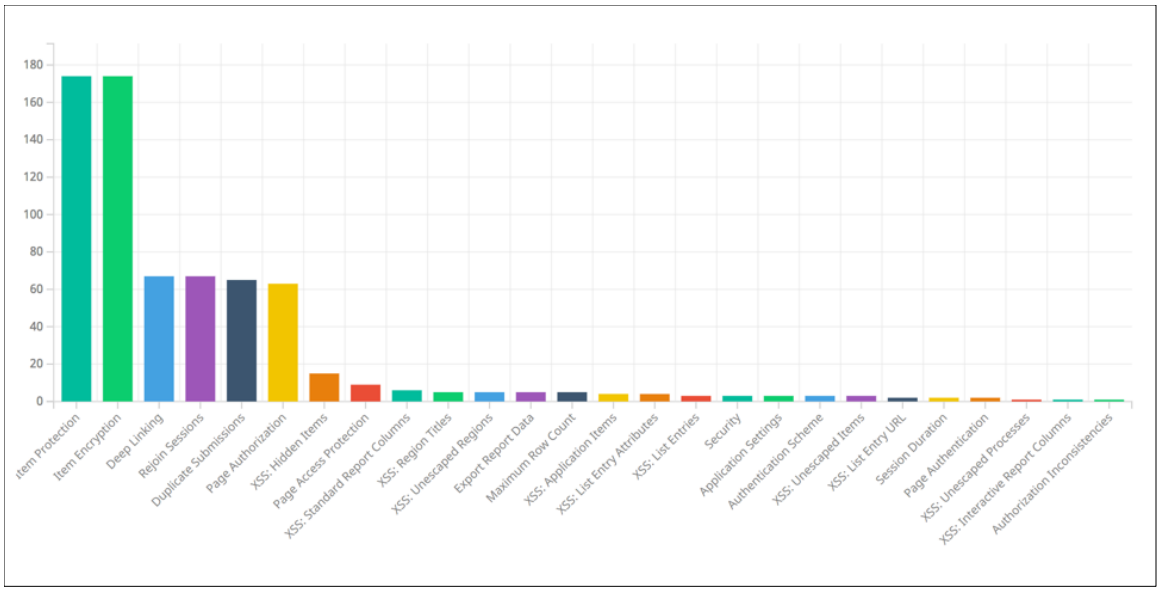
5.2.6. Failures Summary

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.



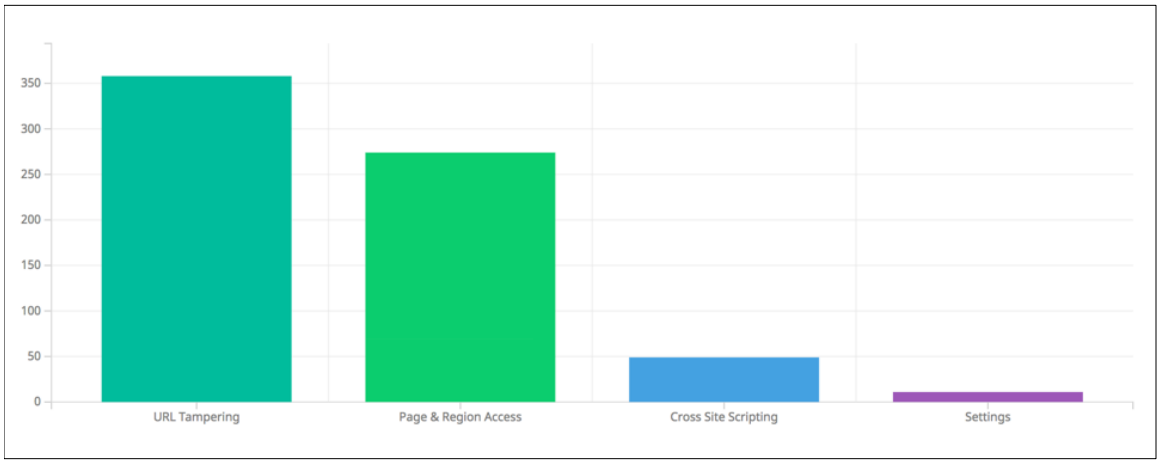
5.2.7. Issues by Category

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



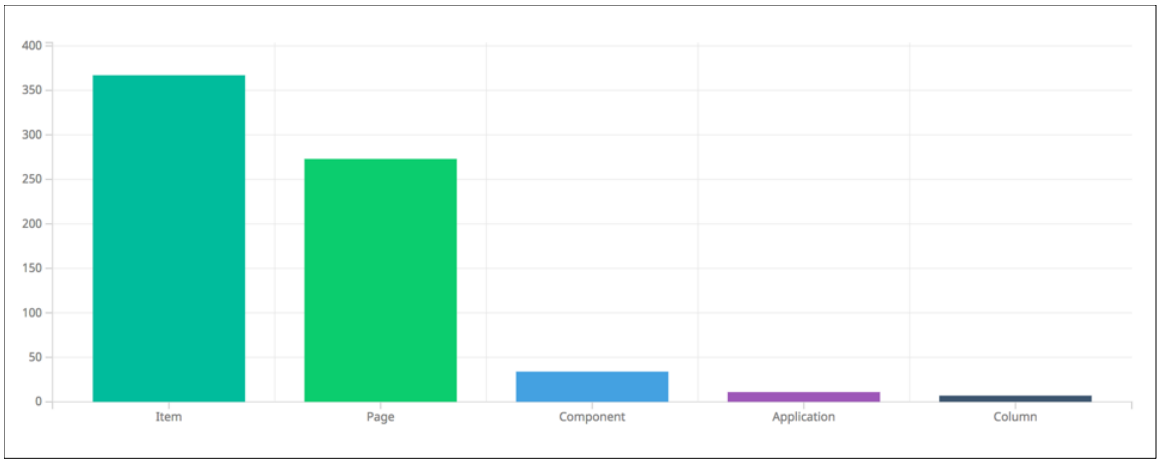
5.2.8. Issues by Classification

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



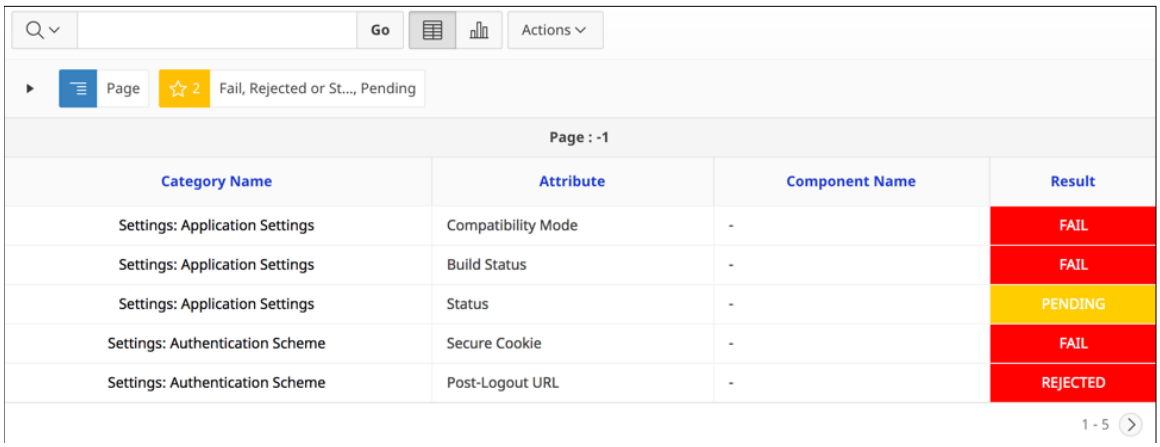
5.2.9. Issues by Impact

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



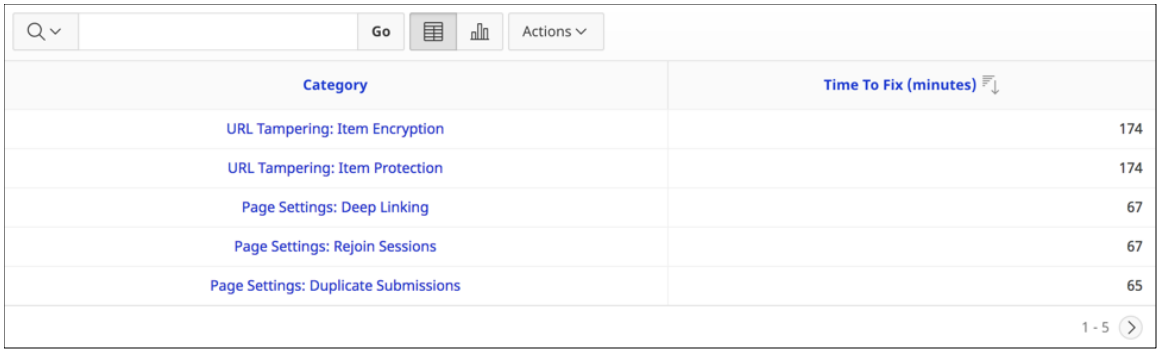
5.2.10. Issues by Page

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



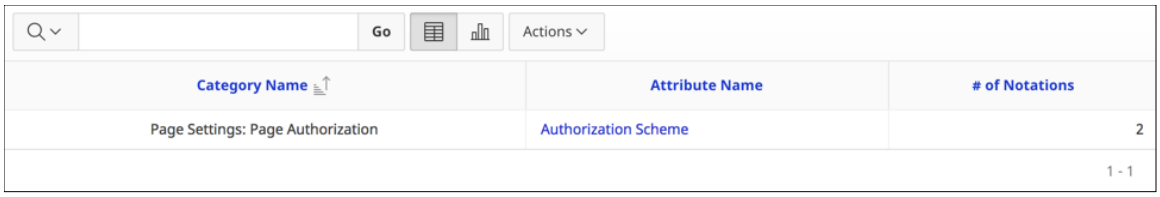
5.2.11. Issues by Time to Fix

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



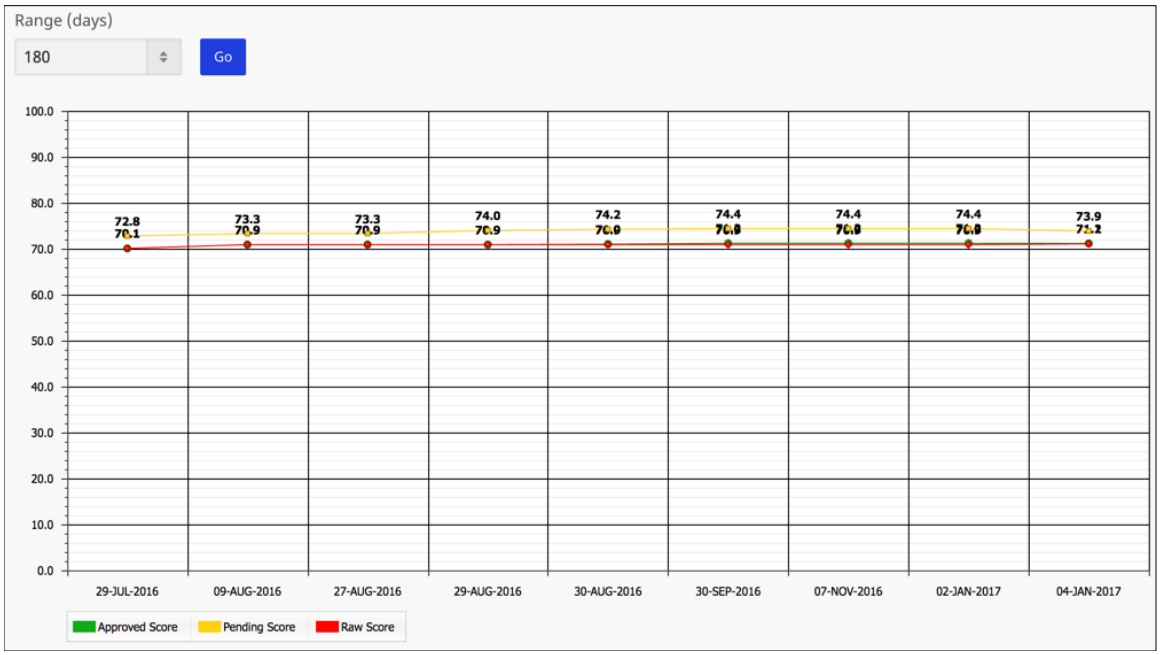
5.2.12. Notations Summary

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.



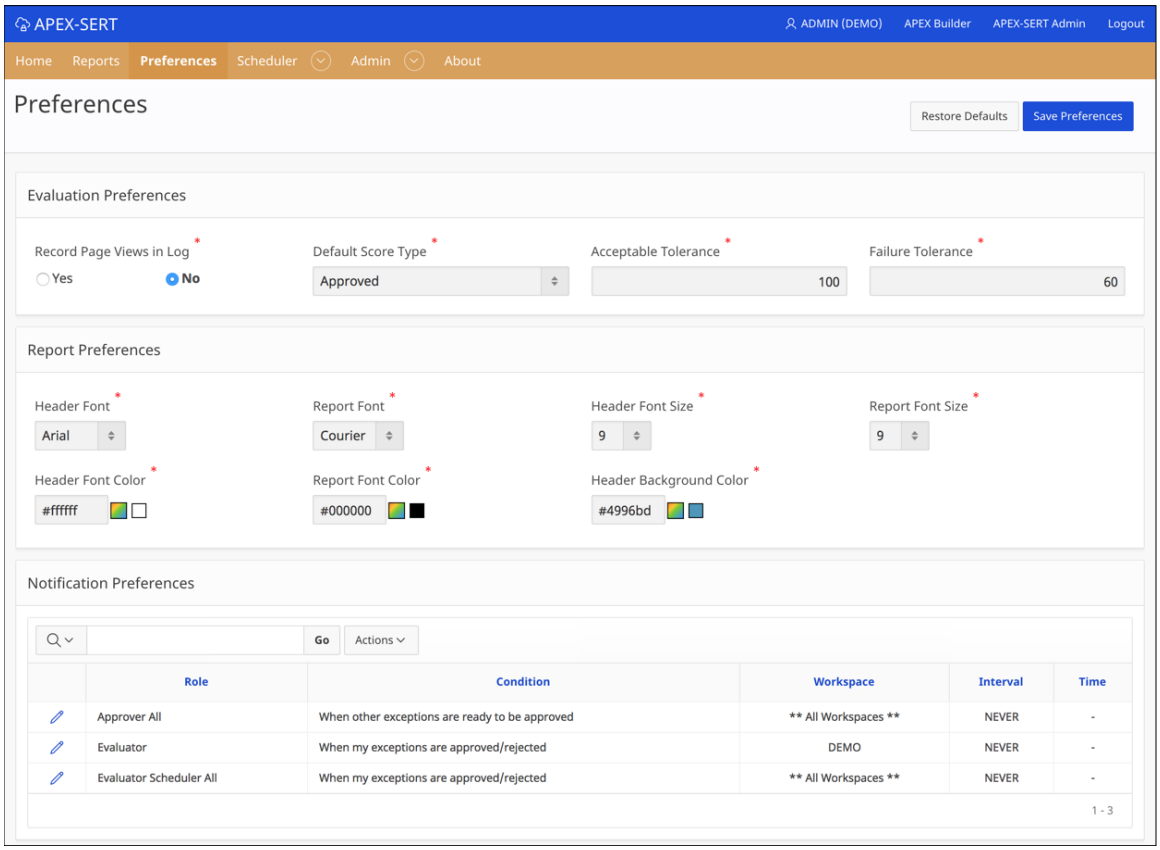
5.2.13. Score Trend

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, as well as printing preferences. All preferences are located in the main **Preferences** tab.



Notice: Notification Preferences are currently not enabled and will be added in an upcoming release/ patch.

7. Scheduling Evaluations

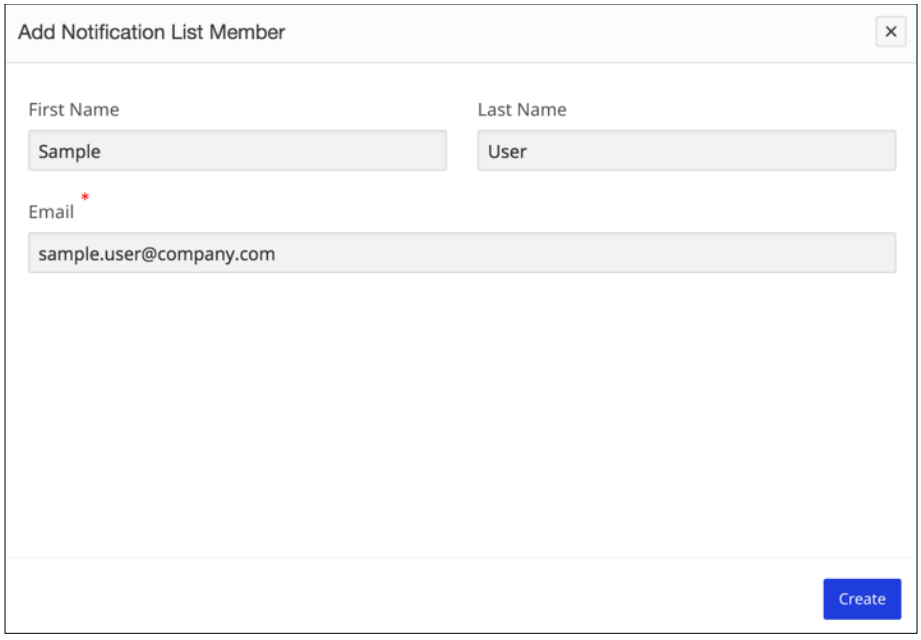
APEX-SERT allows granted either the **Evaluate & Schedule in All Workspaces** or **Schedule in a Specific Workspace** role to schedule an evaluation to be run on either a weekly or daily basis. Evaluations can only be run for one of the three scoring methods: Approved, Pending or Raw. Results of scheduled 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 to have a corresponding APEX workspace account.

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

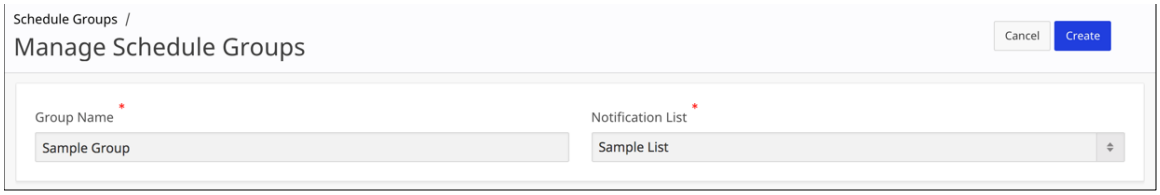
Now that the list is created, click **Add Member** to add a recipient. Enter the user's first and last name and e-mail address that they wish to receive notifications and click **Create**. Repeat this process for each user that needs to be added to the list.



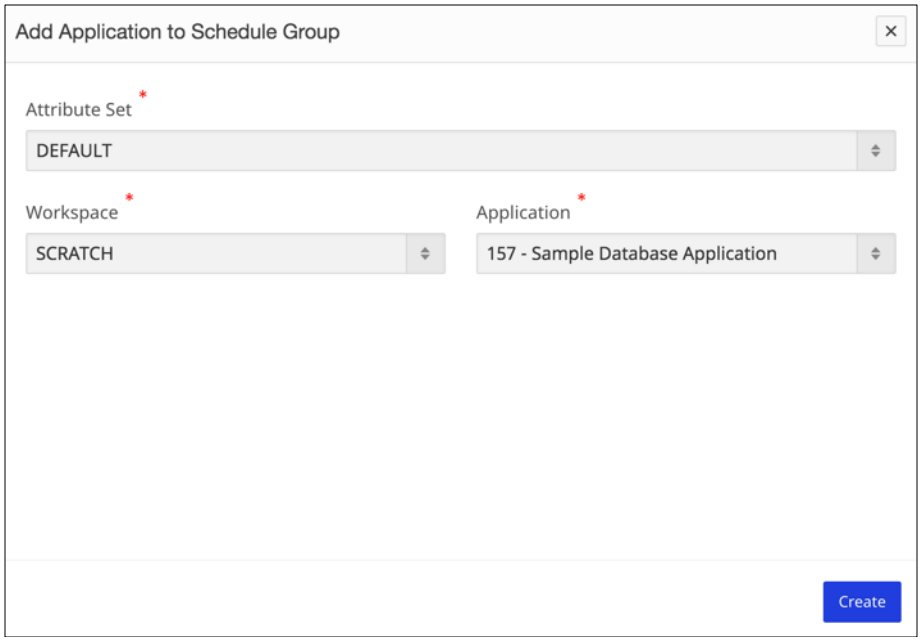
7.2. Scheduling Groups

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 **Schedule Groups** sub-tab from the **Scheduler** tab. Next, click on the **Create** button. On the next page, enter a value for the **Group Name** and select a **Notification List**. Click **Create** to create the **Schedule Group**.



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**.

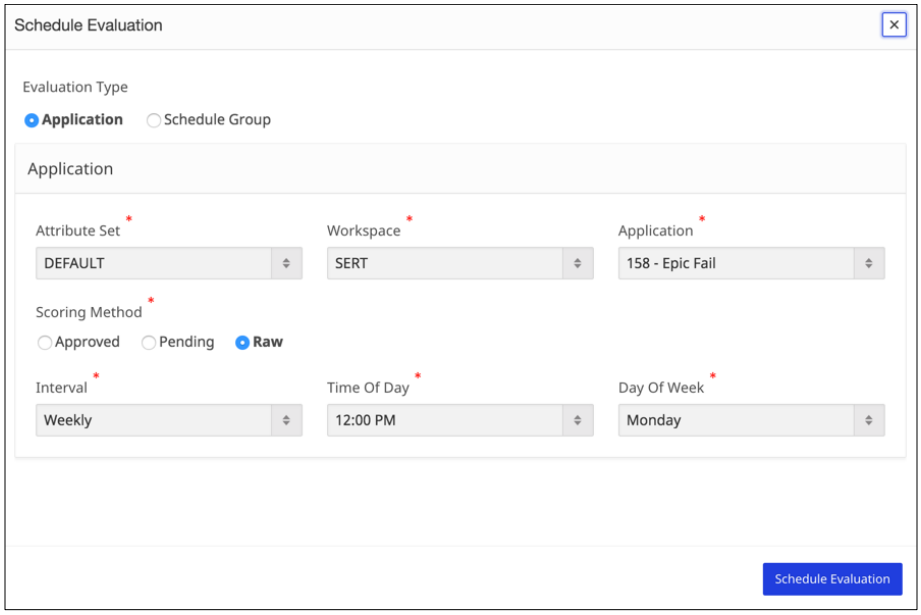


7.3. Scheduling an Evaluation

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**.

To schedule an evaluation, click on the **Scheduler** sub-tab from the **Scheduler** tab. Next, click on the **Schedule Evaluation** button. A modal window will render which will contain details on the evaluation to be scheduled.



7.3.1. Single Application

To schedule a single application, select the corresponding **Attribute Set**, **Workspace** and **Application**. Next, set which **Scoring Method** you wish to use for the evaluation. Finally, select the **Interval** that you wish to evaluate the application. If **Weekly** is selected, then **Day of Week** will also need to be specified. If **Daily** is selected, only **Time of Day** will be required.

Once all choices have been made, click **Schedule Evaluation** to schedule it. The application should now display as part of the **Scheduled Individual Evaluations** report.

7.3.2. Schedule Group

To schedule a **Schedule Group**, start by changing the **Evaluation Type** to **Schedule Group**. Once the page refreshes, select the **Schedule Group** and **Interval**. If **Weekly** is selected, then **Day of Week** will also need to be specified. If **Daily** is selected, only **Time of Day** will be required.

Once all choices have been made, click **Schedule Evaluation** to schedule it. The application should now display as part of the **Scheduled Group Evaluations** report.

7.3.3. Removing Scheduled Evaluations

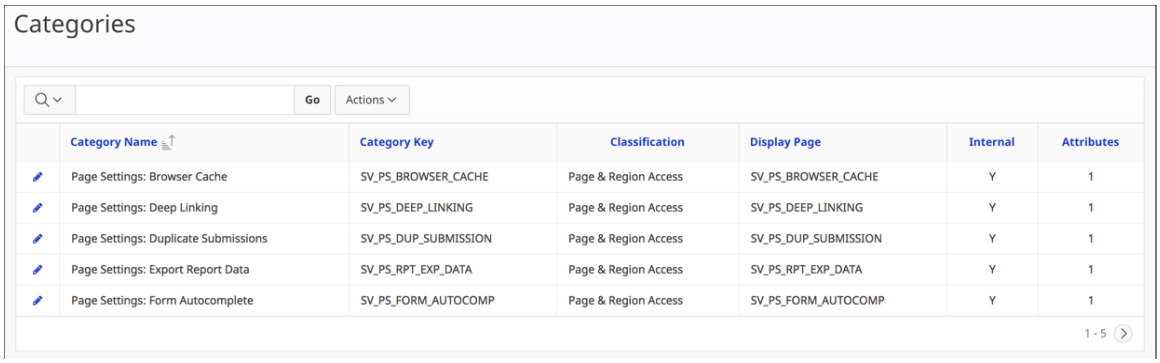
To remove a scheduled evaluation - either an individual or group - simply click the trash can icon next to the corresponding application. No further evaluations for that application or group will occur.

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

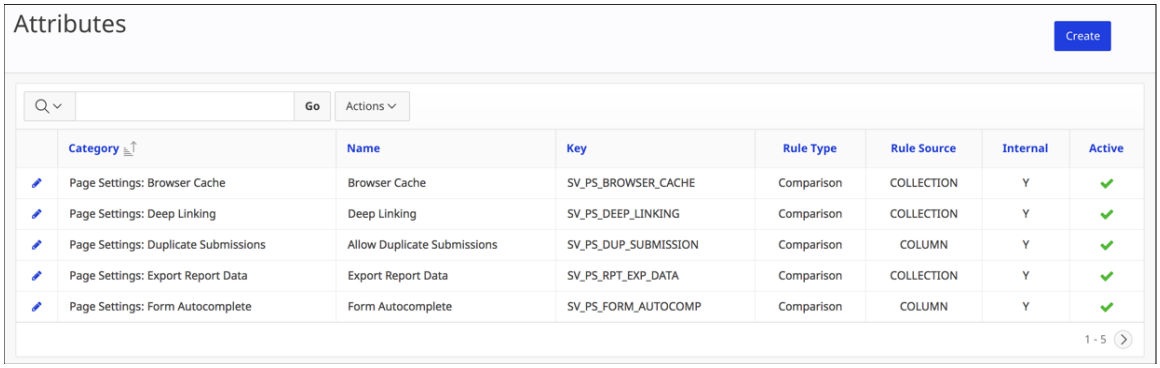
Attributes in APEX-SERT are grouped into **Categories**. Some categories have as few as 1 associated attribute, while others have upwards of 15 or more. Categories cannot be modified nor created in APEX-SERT.



While it is possible to edit a **Category**, no changes can be made to any of them.

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.



Category	Name	Key	Rule Type	Rule Source	Internal	Active
Page Settings: Browser Cache	Browser Cache	SV_PS_BROWSER_CACHE	Comparison	COLLECTION	Y	✔
Page Settings: Deep Linking	Deep Linking	SV_PS_DEEP_LINKING	Comparison	COLLECTION	Y	✔
Page Settings: Duplicate Submissions	Allow Duplicate Submissions	SV_PS_DUP_SUBMISSION	Comparison	COLUMN	Y	✔
Page Settings: Export Report Data	Export Report Data	SV_PS_RPT_EXP_DATA	Comparison	COLLECTION	Y	✔
Page Settings: Form Autocomplete	Form Autocomplete	SV_PS_FORM_AUTOCOMP	Comparison	COLUMN	Y	✔

1 - 5

APEX-SERT provides the capability to create custom Attributes. However, due to the complexity of this action, it is not included in this guide at this time.

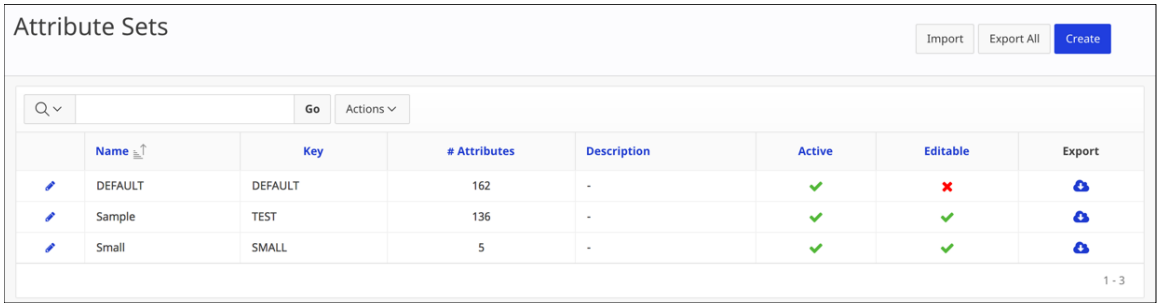
8.3. Attribute Sets

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

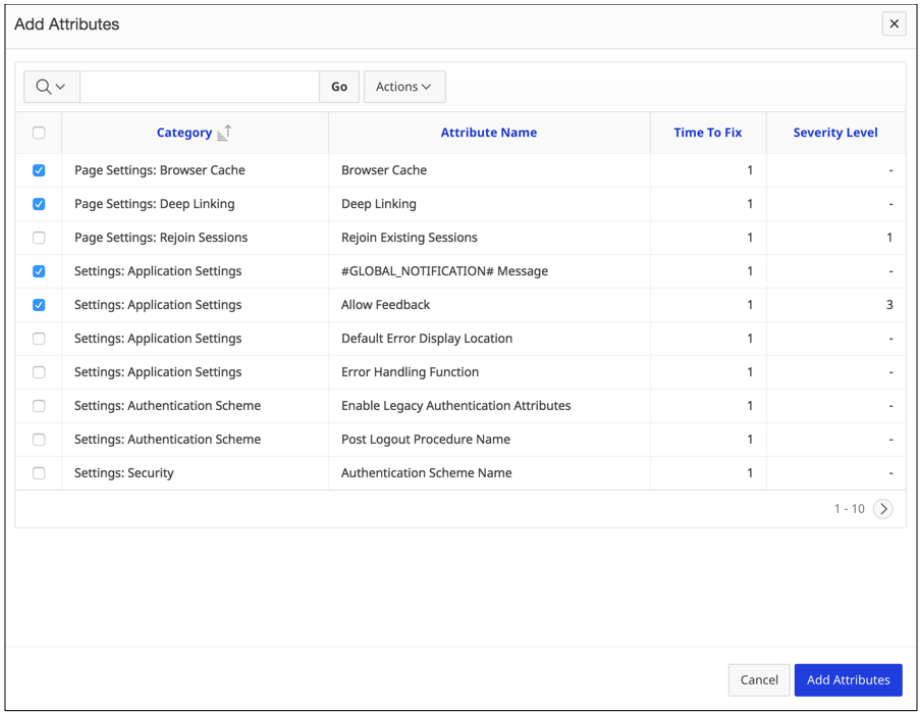
To create an attribute set, click on the **Create** button. Next, specify the new attribute set **Name** and **Key**. If you wish to copy the mappings of another attribute set, then be sure to select set the **Copy From Attribute Set** parameter to that attribute set.

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.

8.3.3. Managing an Attribute Set

Once an **Attribute Set** is created, attributes can be added to it. If an existing **Attribute Set** was copied, there may already be **Attributes** associated with it.

To associate additional **Attributes** with 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.

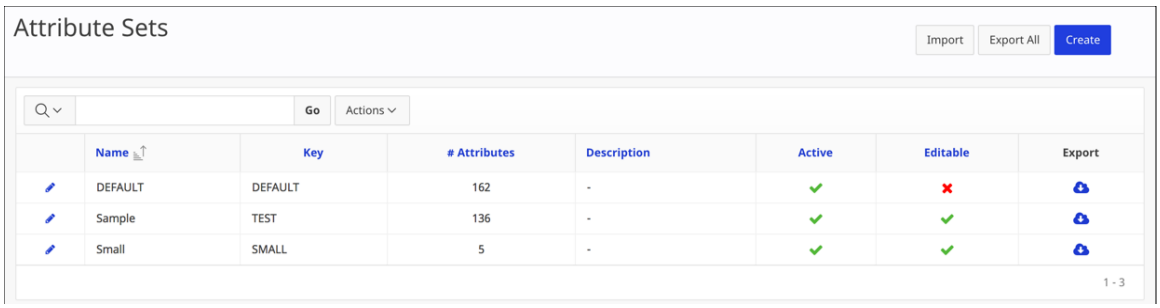


To remove an attribute from an attribute set, simply click on the icon that corresponds the the attribute that you want to remove. The attribute will only be removed from the attribute set; the definition of the attribute will remain intact.

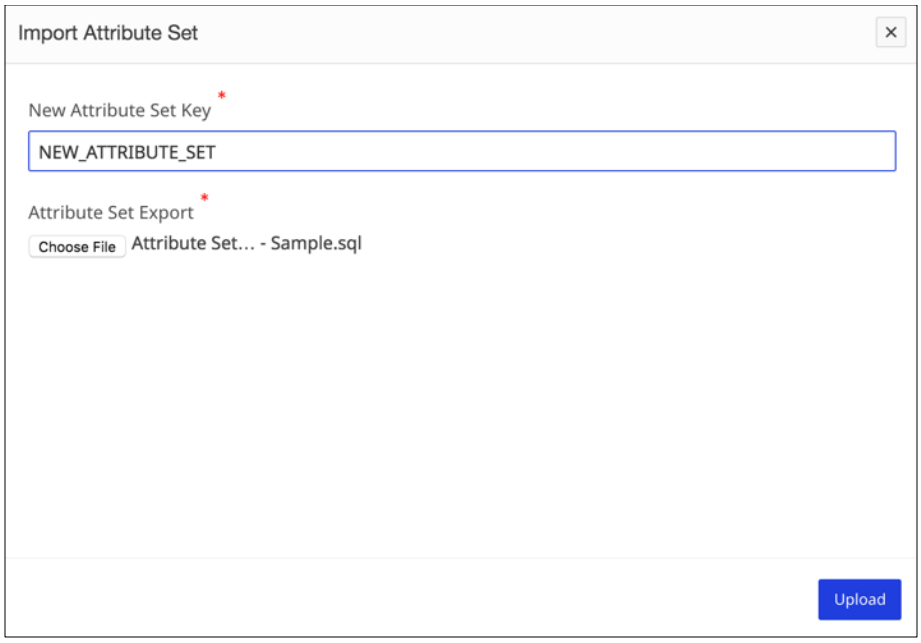
To change either the **Time to Fix**, **Severity Level** or **Active Flag** value of an **Attribute**, edit the attribute by clicking on the pencil icon. The values set will apply only to a specific **Attribute** in a specific **Attribute Set**.

8.3.4. Exporting & Importing 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 or edited.



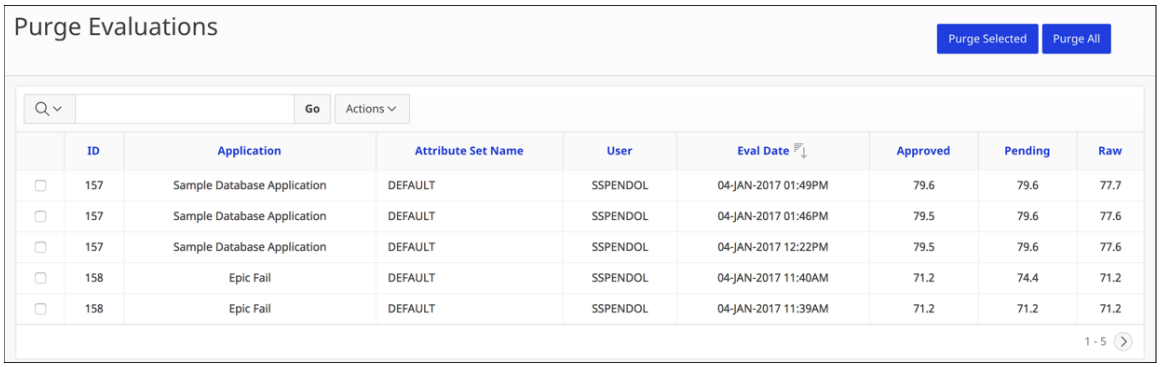
To import an attribute set, click on the **Import** button. Next, enter an **Attribute Set Key**, locate the attribute set export file and click **Upload**. Once the new attribute set is uploaded, it can be used in an application evaluation.



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.

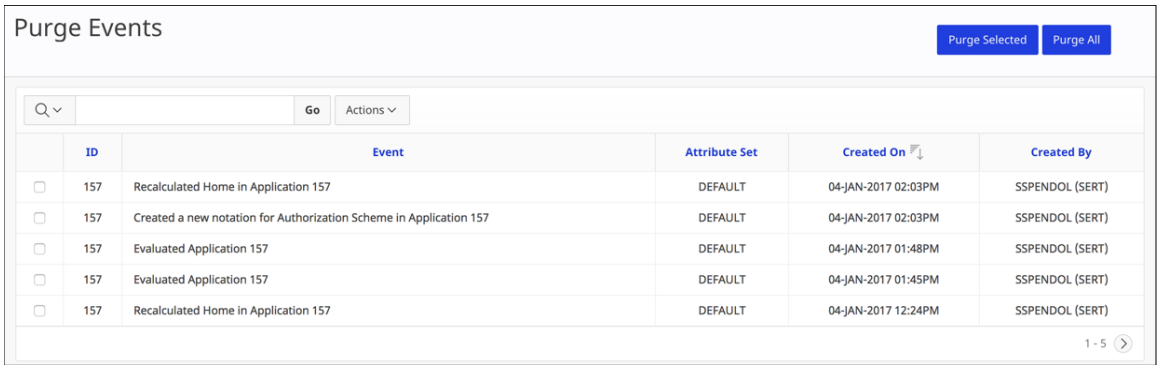
To purge all evaluations, click **Purge All**. To purge individual evaluations, select which ones you would like to purge and then click **Purge Selected**.



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.