Outpost24

Vulnerability Management made easy

Secure Web Applications Tactics

A Quick Start Guide

Version: 1.5

2019-06-24

Table of Contents

About this Guide

This document provides users with a comprehensive overview of the portal interface of Secure Web Application Tactics (SWAT). This document assumes that the reader has basic access to the OUTSCAN account with SWAT license.

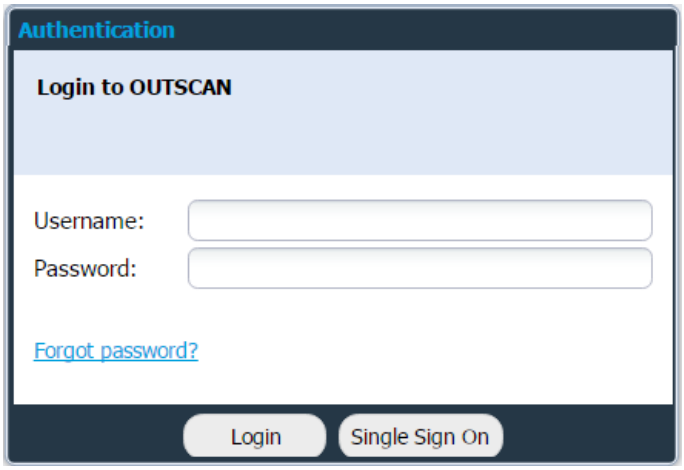
For support information, visit https://www.outpost24.com/support.

Copyright

Trademark

1 Getting Started

To launch the OUTSCAN application, navigate to https://outscan.outpost24.com
***Note**: Use HTTPS protocol.*

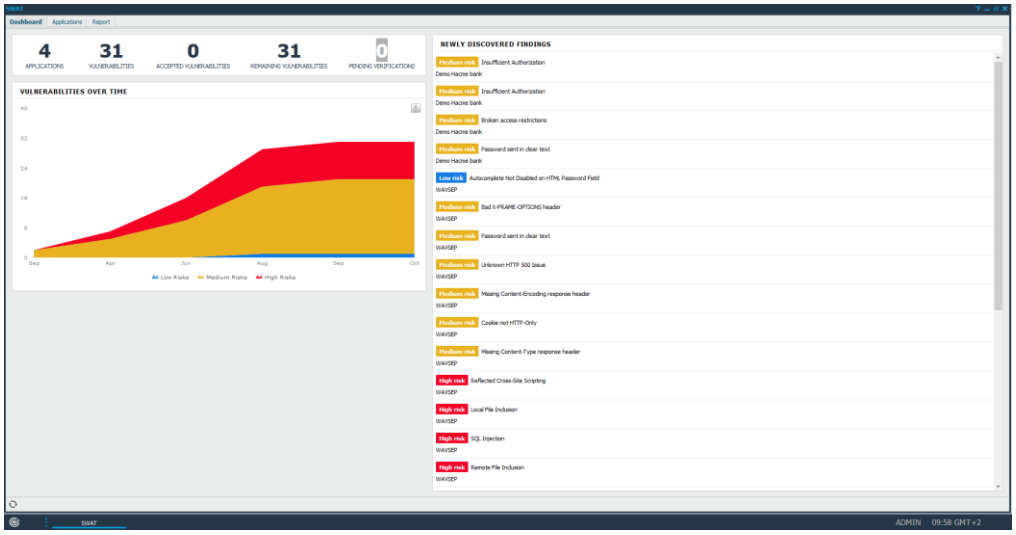


Log in using your credentials.
Once logged in, go to **Main Menu → SWAT – Classic** to open the interface.

2 SWAT

2.1 Dashboard

The **Dashboard** provides a status overview of your web applications. It displays the vulnerability trend information over time, newly discovered findings, total number of web applications in scope, total number of vulnerabilities discovered, pending false positives and total number of accepted risks. This information will be made available as soon as the onboarding process for your web applications is completed.



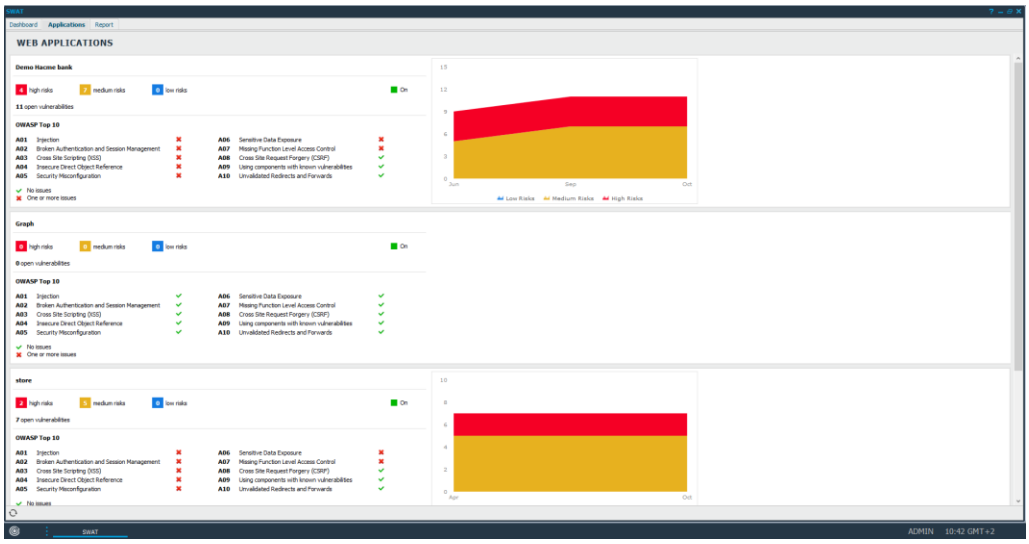
The visible options on the dashboard are listed below:

Option	Description
Applications	The number of web applications included in scope.
Vulnerabilities	Total number of vulnerabilities reported.
Accepted Vulnerabilities	Total number of accepted risks.
Pending Verifications	Total number of pending verifications.
Newly Discovered Vulnerabilities	It displays all the newly discovered vulnerabilities.
Vulnerabilities Over Time	It displays the vulnerability trend over time.

2.2 Applications

The **Applications** section displays all the web applications that are part of the scope. For each web application, the number of low, medium, and high risks reported along with the number of open vulnerabilities can be viewed.

***Note**: The information displayed in the tabs are based on the filter(s) applied in the Report tab.*

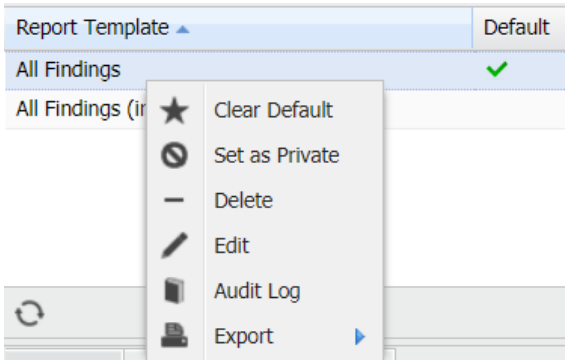


In the **Web Applications** section, it is possible to click on the web application URI or on high, medium or low risks to view the related findings.

2.3 Report

2.3.1 Selecting Report Contents

The *Select applications* for reporting grid allow you to select applications for which the report content is displayed in the bottom grid. The *Report Template* grid is used to filter the applications by defined templates and is visible only if there are any saved templates.



A template is a saved setup which includes applications, filters, grouping, and columns. This setup is applied to the **Findings** tab when a template is selected.

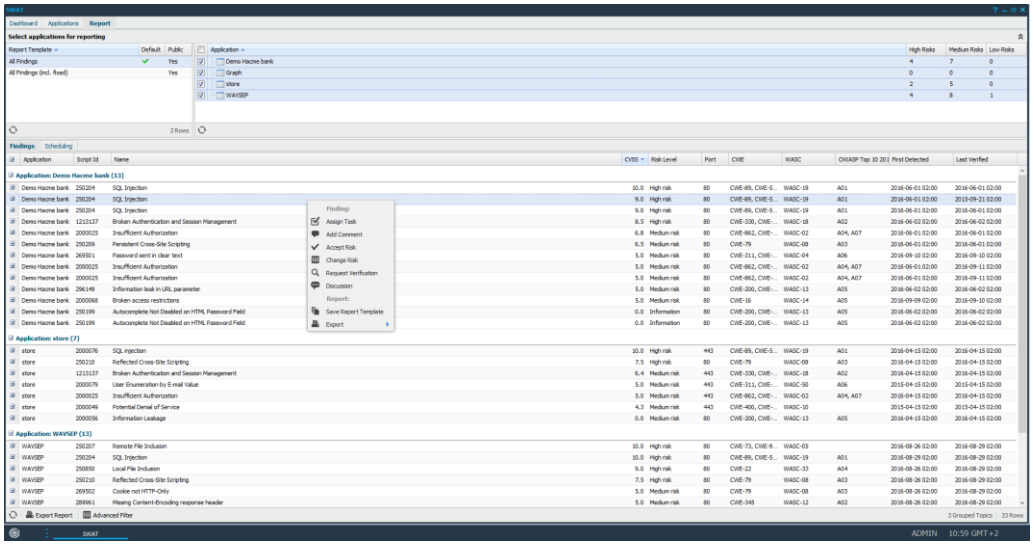
Option	Description
Set as Default/ Clear Default	To change the status of a template, right-click on the entry and select Set as Default. To clear the status, click on **Clear Default**.
Set as Private/ Set as Public	The template which is Set as Public is available for all users. If Set as Private, the template is protected from all users and viewed only by the user who created it.
Delete	Deletes the selected template.
Edit	Edits the selected template.
Audit Log	Click to view the Audit log related to that template.
Export	Click to export the template in HTML or CSV format.

If a template is marked as default, its settings are applied by default whenever the reporting section is opened.

***Note**: If the filters do not provide any entries, click on any field (column name) and create a template from there.*

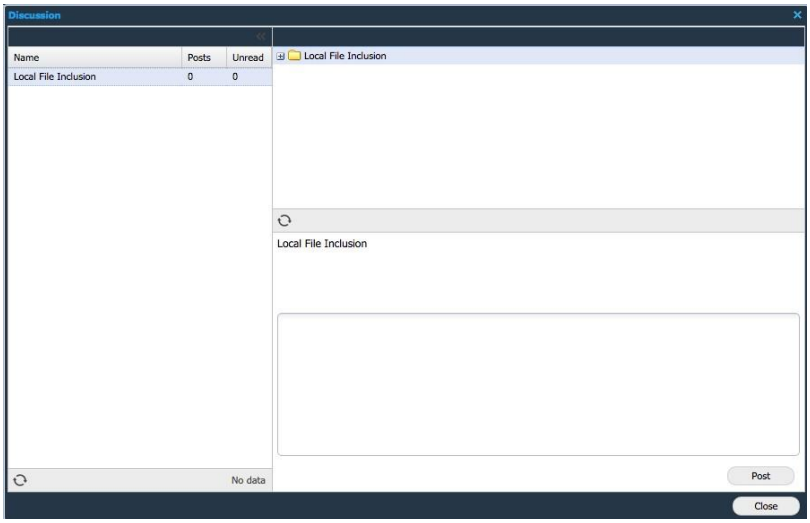
2.3.2 Findings

The **Findings** tab lists all the findings that were found during the web applications scan. Click on + located to the left of the application name, to view complete details.



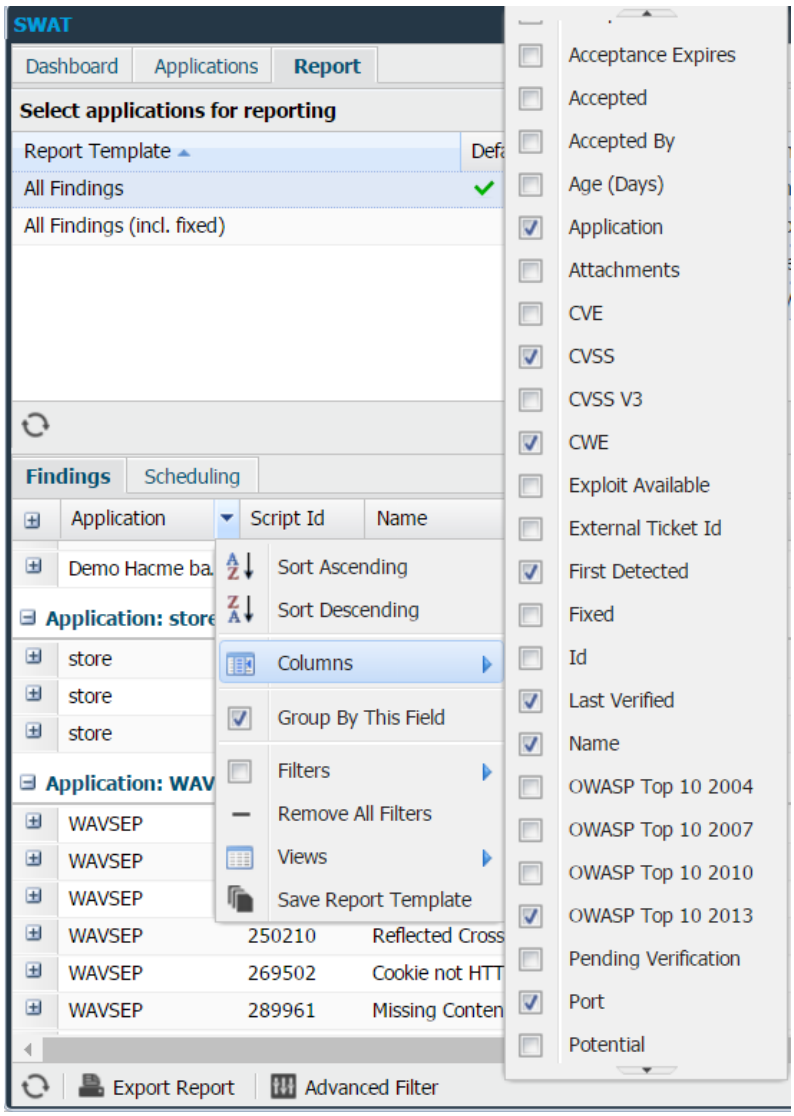
The following actions are possible when you right-click on a finding.

Option	Description
Assign Task	To assign a task based on the detected vulnerability, right click on the finding and select **Assign Task**. This lets you set the priority (with P5 being the highest). Include a due date, add an assignee, and supply additional comments. ► **Internal** - The default ticketing system which is used in OUTSCAN/HIAB. ► **External** - This can be configured using the Integrations tab (**Main Menu → Settings → Integrations**).
Add Comments	To add a comment to the vulnerability, right click on the finding and select Add **Comment**. This comment will be included in all findings of this vulnerability. The **Show Comment on Future Findings** will make it visible in all future reports.
Accept Risk	To accept the risk associated with that vulnerability, right click on the finding and select **Accept Risk**. The accepted risks show up in the finding information, dashboard and in the exported reports. It is possible to accept risk associated with a finding for a limited period (days) or forever. It is also possible to add a comment and set the risk acceptance template as a default for all the accepted risks.
Change Risk	To modify the risk level associated with that vulnerability, right click on the finding and select **Change Risk**. Once selected, a window will open which allows you to select the risk level in a drop-down menu. Select the risk level that you would like to change it to and press the Save button. Any updated risk

Option	Description
	level will be displayed in italic font in the portal interface.
Request Verification	It is possible to request more information regarding the existence of vulnerability by using the *Request Verification*.
Discussion	It is possible to right click on a finding and start a discussion with SWAT team. The discussion window shows all discussions including previous ones in the same place. 
Save Report Template	The current filter settings can be saved as a report template and be applied whenever you access the report section or schedule a report to be sent out.
Export Findings	To export the currently visible data from the grid, right click on any finding and select **Export**. It is possible to export data in CSV or HTML format.

Customizing Reports based on Findings

By clicking the arrow next to the name of any column, you are provided with a drop-down menu as shown below. Click on **Columns** to view the available columns.



Select a specific column to know that information about a finding. All selected columns are displayed in the **Findings** tab. The available options are described below.

***Note**: The information displayed is included in the report.*

Option	Description
Accept Date	Date when the risk was marked as accepted.
Acceptance Expires	The date when the risk will not be considered accepted anymore.
Accepted	Displays if the risk is accepted or not.
Accepted By	Displays the username, by whom the risk was accepted.
Age (Days)	How old is the vulnerability
Application	Application name/identifier on which this vulnerability was found.
Attachments	Number of attachments with the finding. ***Note**: Some findings need more descriptive reasoning, evidence, and/or explanations. then we need to attach some files (images, pdf etc.) with that finding.*
CVE	Common Vulnerabilities and Exposures (CVE) entry of the vulnerability.
CVSS	Common Vulnerability Scoring System (CVSS) score of the vulnerability.
CVSS V3	Score of the vulnerability according to CVSS v3.0.
CVSS V3 Security	Severity level of the vulnerability according to CVSS v3.0.
CWE	Entry identifier of vulnerability in Common Weakness Enumeration (CWE).
Exploit Available	Determines if there is a publicly available exploit present for this vulnerability.
External Ticket Id	Shows internal ticket ID, of the ticket created on external ticketing system.
First Detected	When the vulnerability was first discovered on the specific application.
Fixed	Shows if the vulnerability has been fixed.
Id	Id of the vulnerability. Should only be available for super-user/main user.
Last Verified	When the vulnerability was last verified.
Name	Name of the vulnerability.
OWASP Top 10 2004	Rank in the list of 10 most critical web application security risks of 2004.
OWASP Top 10 2007	Rank in the list of 10 most critical web application security risks of 2007.
OWASP Top 10 2010	Rank in the list of 10 most critical web application security risks of 2010.

Option	Description
OWASP Top 10 2013	Rank in the list of 10 most critical web application security risks of 2013.
OWASP Top 10 2017	Rank in the list of 10 most critical web application security risks of 2017.
Pending Verification	Shows if there is any pending verification request.
Port	Displays on which port the vulnerability was found.
Potential	Flags if this finding has been marked as a potential false positive by the system.
Risk Level	Displays the risk level of the vulnerability (High, Medium, Low, Informational).
SANS Top 25	Rank in SANS Top 25 list of most dangerous software errors.
Script ID	ID of the script which detected the vulnerability.
Solution Patches	Displays patches needed to remediate specific vulnerability. ***Note**: Applies to windows targets only.*
Task ID	Shows **Ticket ID**, if created in internal ticket system.
Ticket Assignee	Name of the assigned ticket holder.
Vulnerability Type	Displays what kind of vulnerability the finding is.
WASC	Threat classification according to Web Application Security Consortium.

Group by This Field

Most of these columns allow filtering, which gives you the option to display a subsection of all data available. To group or ungroup the grid, click the arrow next to the column name and select/deselect **Group by this field**. After grouping, all entries with similar values are displayed together in a group.

Filters

To enable filters, open the drop-down menu and select **Filters**. Depending on the type of data within the column you attempt to filter, you are presented with various options. See Filters for more details.

Views

To save the current view of the findings grid which includes current filters and displayed columns, click the arrow next to the column name and select **Save View**. After adding the view, you can either **Delete View** or directly click on the name of saved view to view the respective settings.

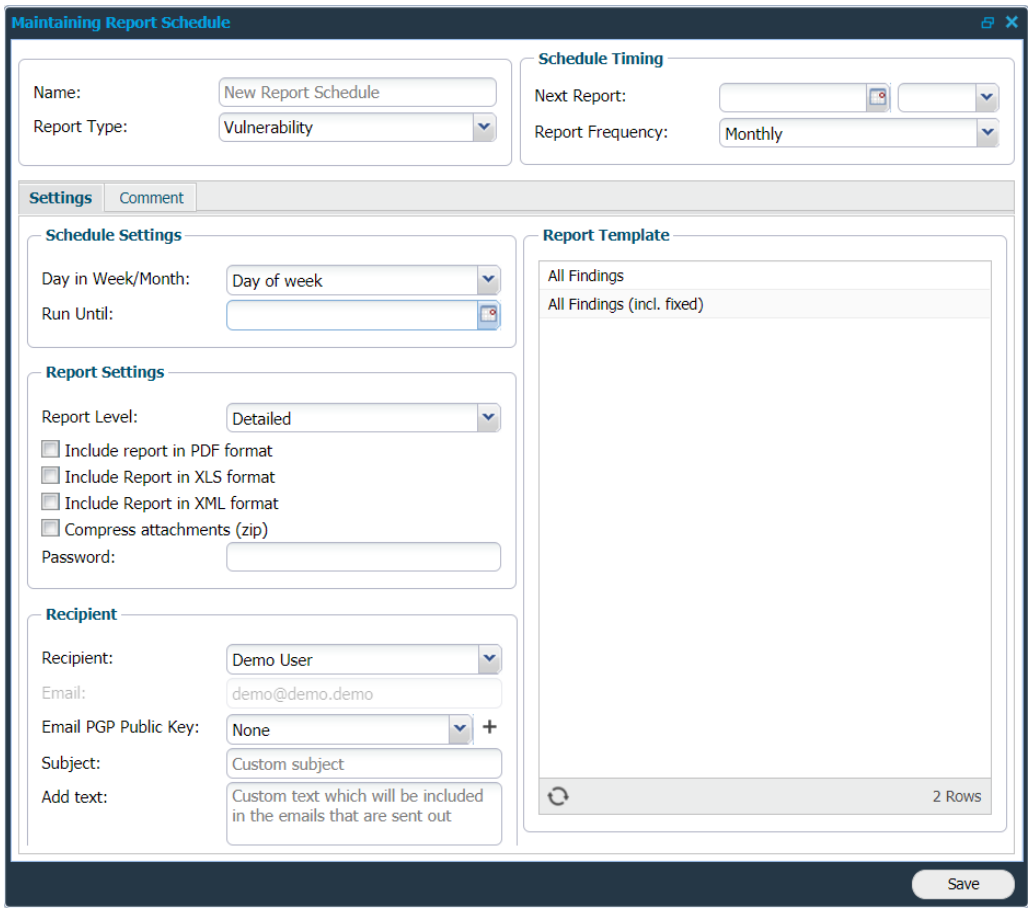
***Note**: Views are beneficial when you wish to see only selected columns. For ex: host name and risk level.*

Save Report Template

After adding the desired columns and respective filters, you can create a template by selecting **Save Report template**. This functionality allows you to save the current settings/view of Reporting Tools. Whenever you are selecting a report template, note that the latest report template is shown for the selected targets/scan job. You can either select to overwrite an old report template or create a new one.

Scheduling

The **Scheduling** tab gives you the opportunity to schedule reports to be sent out based on a report template.
Clicking **New** will open **Maintaining Report Schedule** which will present you with the following options:



Settings

Option	Description
Name	Name of the scheduled report.
Report Type	Available report type is Vulnerability.

Schedule Timings

Option	Description
Next Report	The next date and time, this report should be sent to the recipient.
Report Frequency	How often the report if scheduled.

Schedule Settings

Option	Description
Day in Week/Month	When you select the report frequency as monthly, bimonthly or quarterly, this section is enabled, and you can select any of the available options. ► **Day of week** - The schedule will be sent out on the day of the week on which it was sent out first time**.** ► **Day of month** - The schedule will be sent out on the exact date. Example: If the scheduled date is 2019-03-12, the next report will be sent out on 2019-04-12, irrespective of the day in the week. ► **Day of Week in Month** - This considers the day of week and which week in month. Example: If the scheduled date is 2019-03-12, the next report will be sent out on 2019-04-09 i.e. on the second Tuesday of next month.
Run Until	Provide a date until when the scheduled report should be sent out. Which means, the report will be generated and sent out as per the provided frequency and time in Schedule Timing until the date given in this field. If no date is set here, the schedule will be considered as to be sent forever. *Example*: *If the date is set to 2019-03-12 for a schedule with daily frequency, then selected reported will be generated and sent every day until 2019-03-12. The schedule will be disabled, and no report will be sent out from the next day.*

Report Settings

Option	Description
Report Level	Define how detailed the report should be.
Include report in PDF format	Attach the report as a PDF file.
Include report in XLS format	Attach the report as an XLS file.
Include report in XML format	Attach the report as an XML file.
Compress attachments (zip)	It allows you to create a zip attachment which decreases its size.
Password	Enter a password if you wish to export the report password protected.

Recipient

Option	Description
Recipient	Provide a name to whom you wish to send the report. Custom is only available if you have super user privileges.
E-mail PGP Public Key	► Choose Unencrypted to send an unencrypted email. ► For encrypting the email, choose from the keys available in the drop-down menu or click on + to upload a new key file. *N**ote:** An error message pops up when None is selected. You must supply a public PGP key*.
Subject	Custom subject for email.
Add text	Custom text which will be included in the email.

Report Template Grid

Choose a Report Template.

Comment

This is an optional value which allows you to add additional comments on report schedule. These are shown in **Comments** column of **Report Schedule** grid.

Select the scheduled report and click **Send Now** to send a report immediately.

Steps to Modify and Delete a Schedule

Option	Description
Delete	Allows you to remove the report schedule that you have currently selected.
Edit	To edit a schedule, right-click on it and select Edit.

2.3.3 Discussion

You can start a discussion with the SWAT team.

- Right click on a finding and start a discussion.
- The **Discussion** window shows all your discussions.

2.4 Export Report

A report can be exported using the **Export Report** option visible on the bottom left of **Reporting** window.

2.4.1 Format

A report can be exported in the most commonly and widely used document formats. The available reporting formats are:

Option	Description
PDF	This is the most commonly used reporting format. The reports generated in PDF format can be password protected.
Excel	The reports generated using excel format, have a lot of tabular information, which can be useful when reporting information to IT/Security department or similar divisions.
XML	This format is the default industry standard used for data exchange and integration. The reports generated in XML format are typically used for integration and automation.

2.4.2 Report Type

The default type of report generated is SWAT Vulnerability report.

2.4.3 Report Level

The report level helps you manage reports based on management hierarchy. It helps you generate the report based on how much information is needed and in which form. As shown in the screenshots below, the amount of information is different in the reports, thus making each report exclusive depending on functionality and audience.

There are three reporting levels:

- Detailed
- Summary
- Management

Detailed: The detailed report is the longest report that can be generated. It has in depth technical information about findings, targets, risk-levels, CVSS, report and additional information about the finding. As an example, the figure above displays the first page of a vulnerability report with level set to detailed. The report contains four chapters and has detailed information about all the vulnerabilities related to the web applications. This report is mostly directed towards web administrators and security consultants in an organization.

Summary: The summary report is the ideal sized report with report information, executive summary and SWAT application summary. This report provides just about the right information required by the IT department of any organization.

Management: The management level report gives us a brief summary of the vulnerabilities and risks reported. This executive summary gives a good graphical overview of risk level and trend. This report is ideal while reporting to higher management.

2.4.4 Target Summary

This allows you to select the targets that should be included in the summary overview of the report.

2.4.5 Name

You should mention the name of the report in this section. If you do not provide any specific name, it creates a name as per the selected options.

2.4.6 Email Address

If you want to send the report via email instead of downloading, provide the email address in this field.

2.4.7 Password

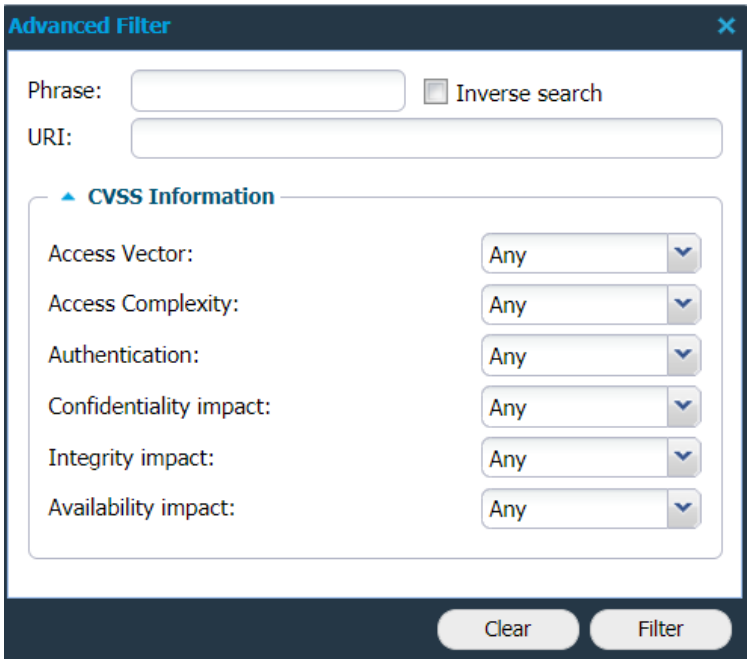
If you want the report to be password protected, you can mention a password here.

2.4.8 Include Attachments (Zip)

If selected, the exported report will be compressed with zip compression standard.
Click on **Export** button to download a report.

2.5 Advanced Filter

Along with the existing filters, you can also use **Advanced Filter** to further refine your search.



Option	Description
Phrase	Provide any key word or phrase. Searches for the given phrase in nearly 10 descriptive fields and lists all the vulnerabilities. The descriptive fields include vulnerability description, vulnerability comments, vulnerability name, script id, solution, false positive comments, gathered information, accepted risk comments, dispute comment (PCI), and explanation.
Inverse search	If enabled, searches all findings and lists vulnerabilities whose descriptive fields does not include the given phrase.
URI	Searches all findings and lists vulnerabilities based on the given URI.
CVSS Information	You can search for findings with desired CVSS Information by selecting the required fields.

After adding the required information, click on **Filter** to check to view the results. These settings also reflect in the exported reports.

To clear the enabled advanced filter settings, click on **Clear**.