Outpost24

Vulnerability Management made easy

Secure Web Applications Tactics

A Quick Start Guide

Version: 1.3

2018-06-20

Table of Contents

About this Guide

The purpose of this document is to provide users 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

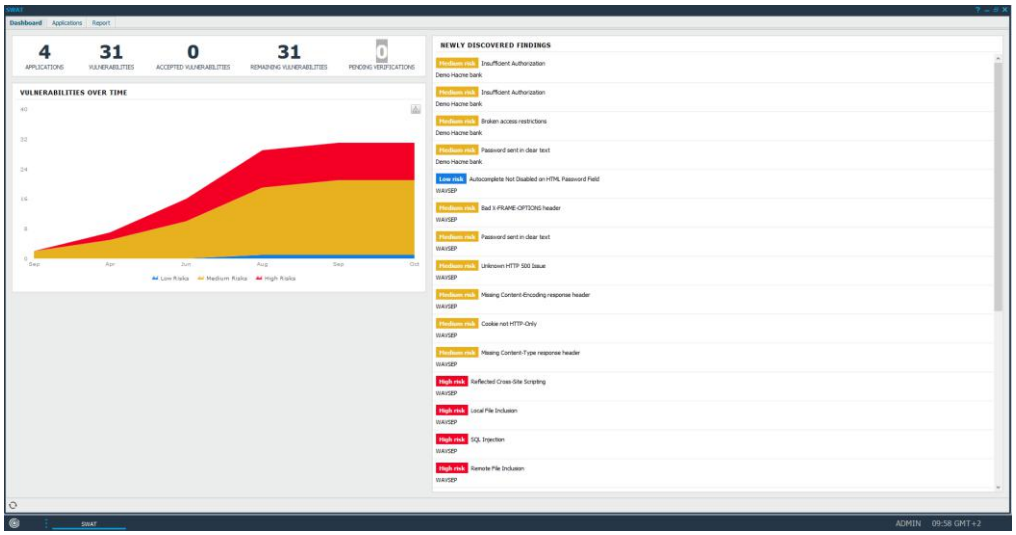
To access Outpost24 SWAT, navigate to https://outscan.outpost24.com

Please log in using your credentials.
Once logged in, go to **Menu** → **SWAT** 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.

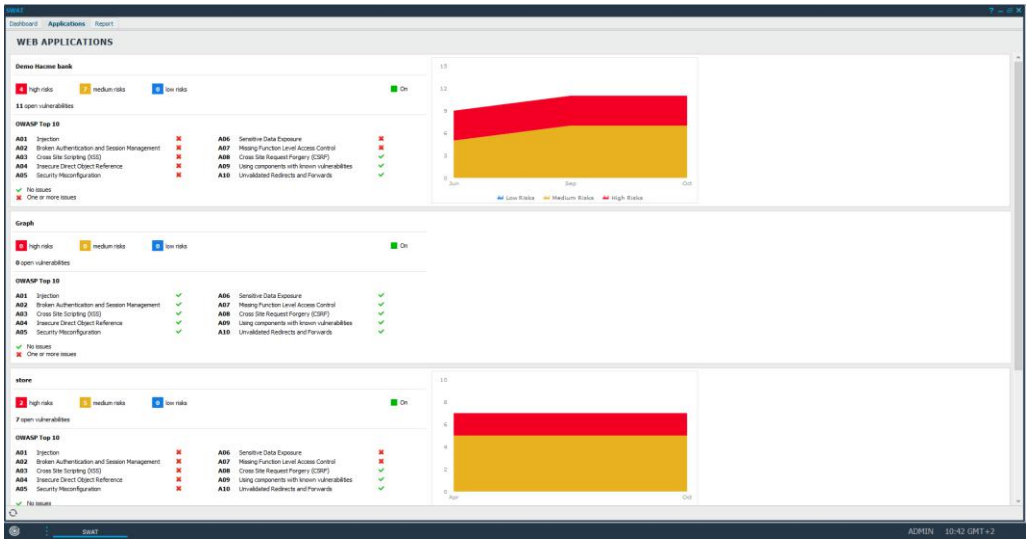


The visible options on the dashboard are listed below:

- **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.

3 Applications

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

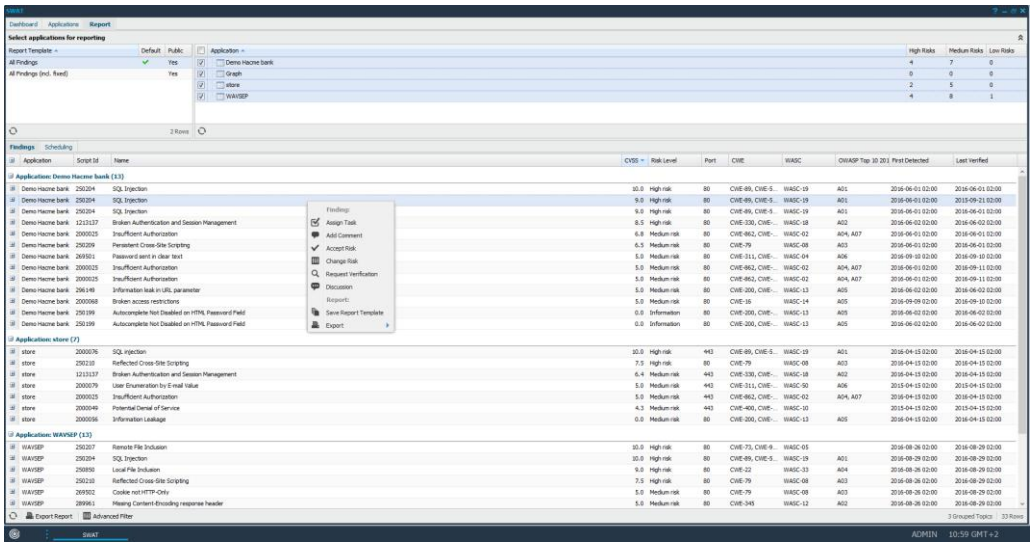


In the **Web Applications** section, it is possible to click on the web application URI or on high, medium or low risks to view the related findings.

3.1 Report

3.1.1 Findings

This section lists all the findings that were found during the web applications scan.



It is possible to perform multiple actions from the **Findings** sections. Some of the important actions are listed below.

3.1.1.1 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.

3.1.1.2 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

3.1.1.3 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.

3.1.1.4 Change Risk

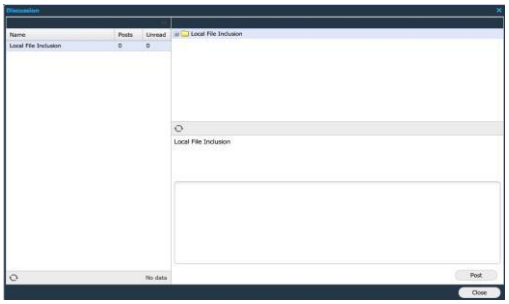
To modify the risk level associated with that vulnerability, right click on the finding and select **Change Risk**. Once selected, a window will open which allows you to select the risk level in a drop-down menu. Select the risk level that you would like to change it to and press the "Save" button. Any updated risk level will be displayed in italic font in the GUI.

3.1.1.5 Request Verification

Using Request Verification, it is possible to request for more information regarding the existence of vulnerability.

3.1.1.6 Discussion

It is possible to right click on a finding and start a discussion with Outpost24 support. The discussion window shows all discussions including previous ones in the same place.



3.1.1.7 Save Report Template

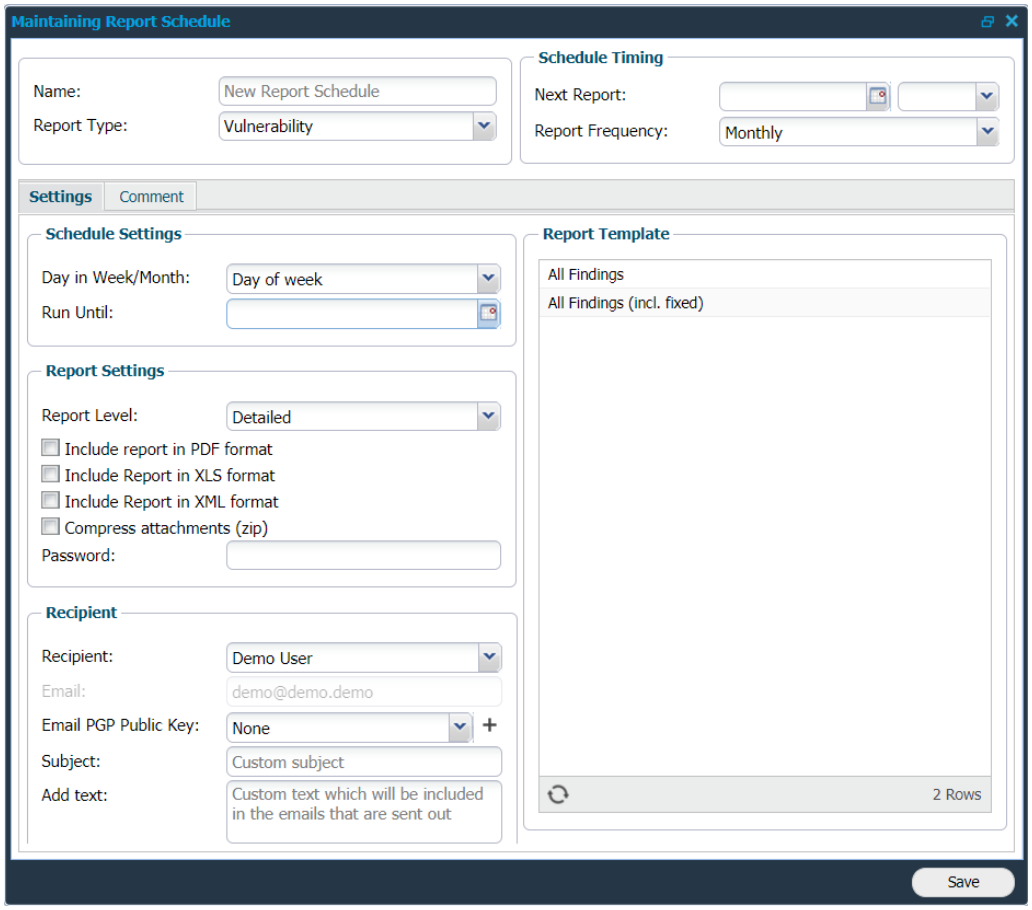
The current filter settings can be saved as a report template and be applied whenever you access the report section or schedule a report to be sent out.

3.1.1.8 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.

3.1.2 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

- **Name**: Name of the scheduled report.
- **Report Type**: Available report type is Vulnerability.

Schedule Settings

- **Day in Week/Month**: When we select 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 12 Sep-2017, the next report will be sent out on 12-Oct-2017, 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 12-Sep-2017, the next report will be sent out on 10-Oct-2017 i.e. on the second Tuesday of next month.

If scheduled report is sent out on 12-sep-2017, the day of the week is Tuesday, the day in the month is 12 and the day of week in month is second Tuesday of the 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 30-Sep-2017 for a schedule with daily frequency, then selected reported will be generated and sent every day until 30-Sep-2017. The schedule will be disabled and no report will be sent out from the next day.

Report Settings

- **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 a XLS file.
- **Include report in XML format**: Attach the report as a 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

- **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**: If desired, add a PGP Public Key to be used for encryption, when emailing the report.
- **Subject**: Custom subject for email.
- **Add text**: Custom text which will be included in the email.

Schedule Timing

- **Next Report**: The next date and time, this report should be sent to the recipient.
- **Report Frequency**: How often the report should be scheduled.

Report Template

- Select one of the saved report templates.
- Click **Save** to save the current settings of the Report Schedule.

Steps to Modify and Delete a Schedule:

- **Delete**: Will allow you to remove the report schedule that you have currently selected.
- **Edit**: To edit a schedule, right-click on it and select **Edit**.

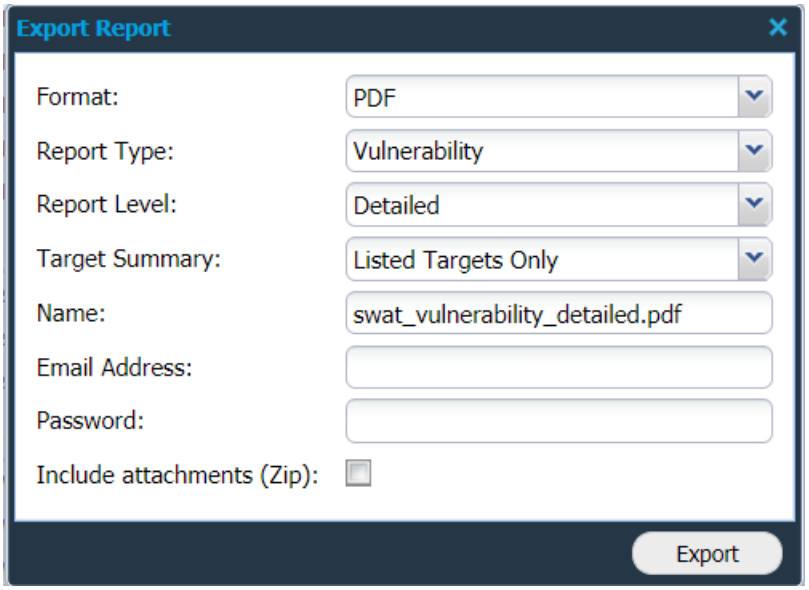
3.1.3 Discussion

You can start a discussion with the Outpost24 support team.

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

4 Export Report

A report can be exported using the **Export Report** function found in the bottom in the left corner of the Report page. It is possible to customize reports based on filtering findings that are required.



The available fields of Export Report are as described below.

4.1.1.1 Format

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

- PDF
- Excel
- XML

PDF format is the most commonly used reporting format. The reports generated in PDF format can be password protected.

The reports generated using **Excel** format have a lot of tabular information, which can be good when reporting information to an IT/Security department or similar divisions.

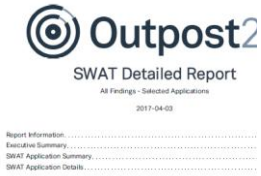
XML format is the default industry standard used for data exchange and integration. The reports generated in XML format are typically used for integration and automation.

4.1.1.2 Report Type

The default type of report generated is SWAT Vulnerability report.

4.1.1.3 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.

4.1.1.4 Target Summary

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

4.1.1.5 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.

4.1.1.6 Email Address

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

4.1.1.7 Password

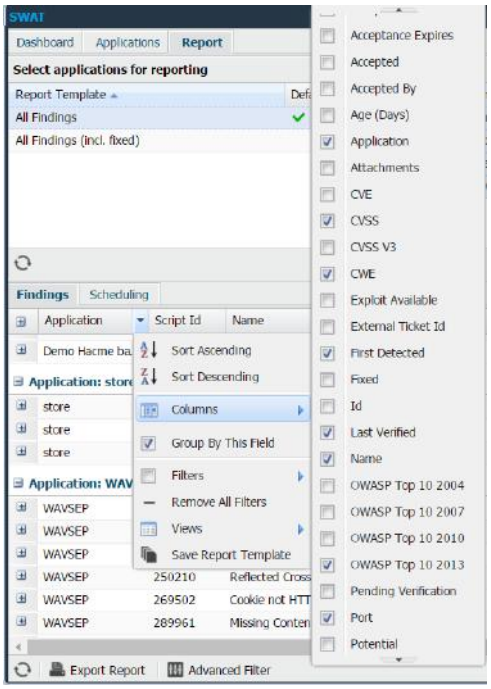
If you want the report to be password protected, you can mention a password here.

4.1.1.8 Include Attachments (Zip)

If "ticked", the exported report will be compressed with zip compression standard.

4.2 Customizing Reports based on Findings

In this drop-down menu, there is a field called **Columns** which displays all the columns available.



Select a specific column to know that information about a finding. All selected columns are displayed in the Findings grid. The available options are described below.
***Note**: The information displayed will be included in the report.*

- **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**: Informs you of which user it was that accepted the risk.
- **Added**: Flags if this entry was added after the time of the scan.
- **Age (Days)**: Displays how old the vulnerability is.
- **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**: CVE entry of the vulnerability. Entry identifier of vulnerability in Common Vulnerabilities & Exposures(CVE).
- **CVSS**: CVSS score of the vulnerability.
- **CVSS V3**: There are multiple versions of CVSS scoring. This column shows CVSS score according to V3.
- **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**: Shows the date when the vulnerability was verified on the application.
- **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.
- **OWASP Top 10 2013**: Rank in the list of 10 most critical web application security risks of 2013.
- **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**: Shows patch information related to the vulnerability if any.
- **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.

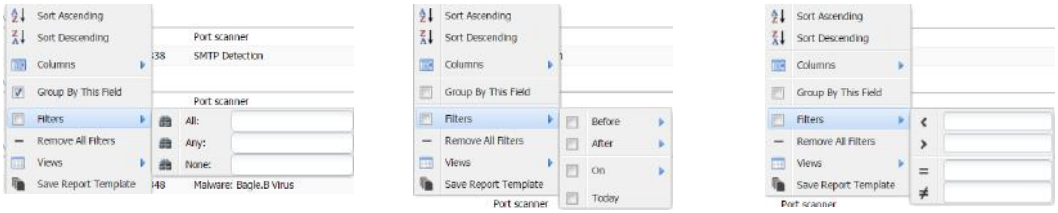
4.2.1.1 Group by this field

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.

4.2.1.2 Filters

To enable filters, open the dropdown menu and select **Filters**. Below figure shows some of the available filters.



Depending on the existing kind of data within the column which you attempt to filter, you will be presented with various options:

- **Textual**: Displays three text fields. It is possible to use all three at once to limit the results, but you can also use quotes to match an entire phrase.
  - **All**: Displays records that contain all the search words.
  - **Any**: Filters on records that contain any of the search words.
  - **None**: Excludes all records that contain any of the search words.
  - **Not Detected**: Display entries whose platform is not detected. This option is only available on Platform column.
- **Date**: Displays few of the below options based on the column selection.
  - **Before**: Display all entries before the provided date.
  - **After**: Display all entries after the provided date.
  - **On**: Display all entries on the provided date.
  - **Today**: Display all entries from today.
  - **Never**: Display all entries with value 'Never'.
- **Number**: Include and/or exclude entries dependent on numbers.
  - **<**: Filter entries on values lesser than the provided value.
  - **>**: Filter entries on values greater than the provided value.
  - **=**: Filter entries that are equal to the provided value. This field allows you to enter both ranges and comma separated list of values.
  - **≠**: Filter entries that are not equal to the provided value, this field allows you to enter both ranges and comma separated list of values.
  - **Generic**: Used to filter findings on generic ports.
- **Yes/No**: Choose to filter on either "Yes" or "No".
- **Values**: If the field contains only a small set of values, they will be listed in the filtering menu. Select those you wish to include.

- **Type**: You can filter based on the type of finding. The available types are as follows:
  - Vulnerability
  - Information
  - Port
- **Risk Level**: You can filter the findings based on the risk level.
  - **High risk**: Display all findings identified as high risk.
  - **Low risk**: Display all findings identified as low risk.
  - **Medium risk**: Display all findings identified as medium risk.
  - **Information**: Display all findings which are not identified as risks.
- **Protocol**: You can filter the findings based on protocol.
  - **ICMP**: Display all vulnerabilities those were found using ICMP.
  - **IGMP**: Display all vulnerabilities those were found using IGMP.
  - **TCP**: Display all vulnerabilities those were found using TCP.
  - **UDP**: Display all vulnerabilities those were found using UDP.
- **Verified**: You can filter the findings based on the verification status of the finding.
  - **Not verified**: Display all vulnerabilities which are still not verified.
  - **No longer present**: Display all vulnerabilities which are no longer present.
  - **Still present**: Display all vulnerabilities which are still present.
- **Vulnerability Type**: You can filter the findings based on type of the vulnerability. The different possibilities are given below:
  - Unknown
  - Dos
  - Code Execution
  - Overflow
  - Memory Corruption
  - SQL Injection
  - XSS
  - Directory Traversal
  - Http Response Splitting
  - Bypass
  - Gain Information
  - Gain Privileges
  - CSRF
  - File Inclusion
  - Information

4.2.1.3 Remove All Filters

To remove all filters, click the arrow next to the column name and select **Remove All Filters**.

4.2.1.4 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.*

Save Report Template

After adding the desired columns and respective filters, you can create a template by selecting select **Save Report template**.