Outpost24

Vulnerability Management made easy

APPSEC SCALE

User Guide

Version: 1.3

2018-03-26

Table of Contents

About This Guide

The main purpose of this document is to provide users a comprehensive overview of the portal interface of APPSEC SCALE. This document assumes that the reader has basic access to the OUTSCAN/HIAB account with APPSEC SCALE subscription.

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

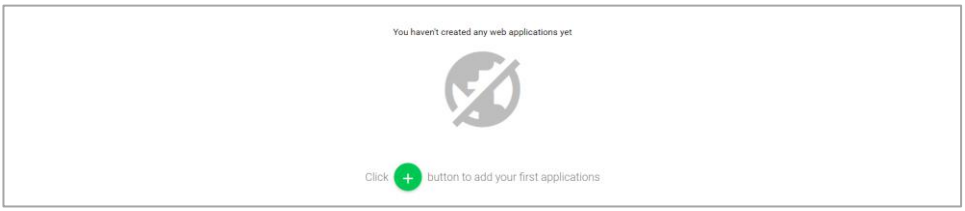
Copyright

Trademark

1 Getting Started

To launch the OUTSCAN application, navigate to https://outscan.outpost24.com.

- Log in using your credentials.
- To access the APPSEC SCALE module, go to **Menu→ APPSEC SCALE**.
- The start page of the solution is as shown below:



2 Adding Application(s)

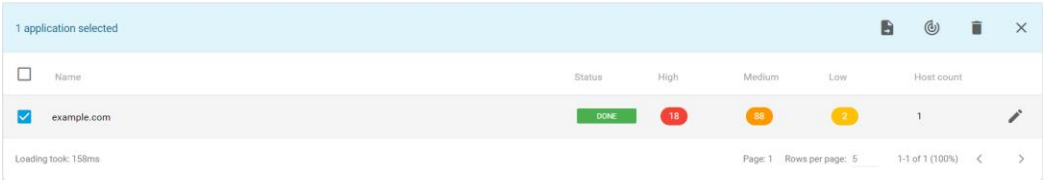
Click on **+** button to add a new web application to scan.

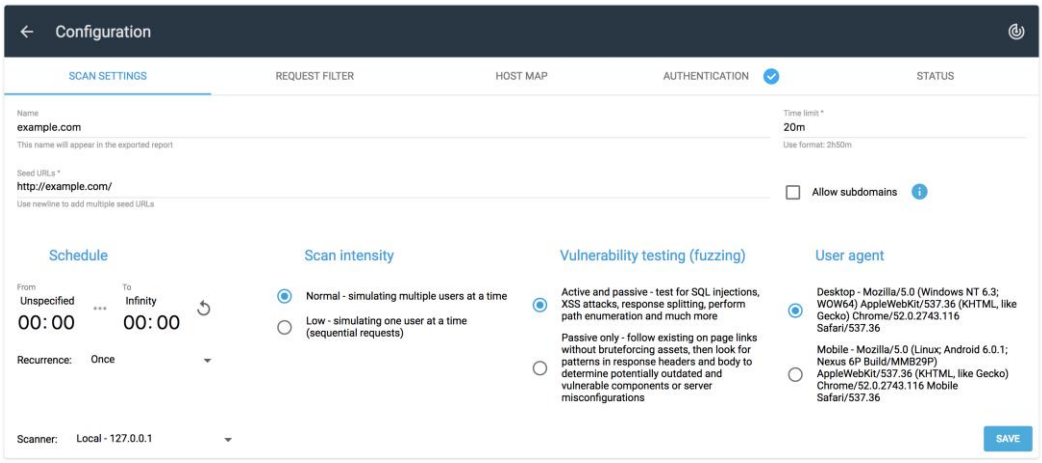
- Applications can be added as a URL, an IP address or a hostname.
- When adding more than one asset, separate them using a newline.
- After adding the target(s), click **ADD**.
- URLs not starting with http or https protocol will be prefixed with http://
- The **Choose scanner (HIAB only)** option will be visible if at least one APPSEC SCALE scanner is available.
  - The first scanner in the list is selected by default.
  - The selected scanner can be changed on the **Edit** view.

3 APPSEC SCALE Overview

After adding the target(s):

1. Click on the **edit application** symbol on the application row, to edit the configuration settings.





2. Click on a target to view the scan results.
3. To delete a selected target, click on bin icon located on top right of the window.

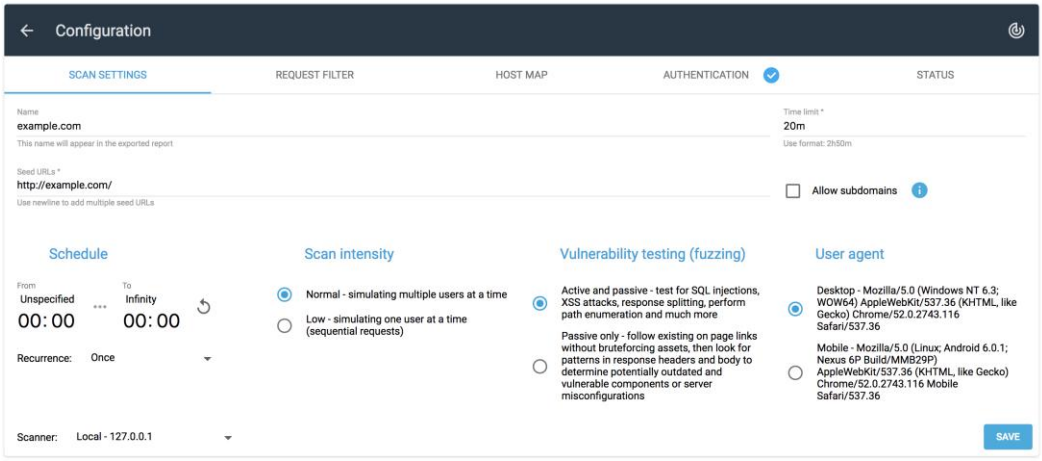
4 Configuration

The Configuration section consists of five tabs:

- Scan Settings
- Request Filter
- Host map
- Authentication
- Status

4.1 Scan Settings

The scan settings tab allows you to configure how the scan should run.



The elements of scan settings are described below:

- **Name**: Displays the name of the target you have added. This name will appear in the exported report.
- **Seed URLs**: Provide the seed URL of target. While adding multiple seed URLs, use new line after entering each URL.
- **Time limit**: Time allocated for a scan to complete. Format example: 1h10m which is the upper time limit, meaning that the scanner can finish scanning earlier if the web application is small or if the time limit is higher than the required time for scan to finish.
- **Allow subdomains**: Enable to scan all the sub domains of the target application.

Schedule

- The **From** and **To** sections of **Schedule** allows you to set a date and time span to scan the target.
- Click on  to reset the date and time settings.
- **Recurrence**: This allows you to determine how often the scan should be scheduled. Select one of the available options.

Scan Intensity

The **Scan Intensity** determines the behavior and the impact of the scanner on the target web application.

- **Normal**: This enables the scanner to crawl multiple URLs at the same time.
- **Low**: This enables the scanner to crawl one URL at a time. It is a sequential scanning.

Vulnerability Testing (Fuzzing)

Select one of the options, depending on type of scan that needs to be performed on the target application.

- **Active and passive**: By enabling this option, the scanner will perform checks for common web application vulnerabilities like test for SQL injections, XSS attacks, and much more.
- **Passive only**: Applies to finding vulnerabilities based on products that the web application is built upon. In this mode, the scanner does not send any active payloads.

User Agent

The **User Agent Identifier** you send to the server.

After enabling the required settings, click **SAVE**. You will get a popup displaying **Successfully updated**.

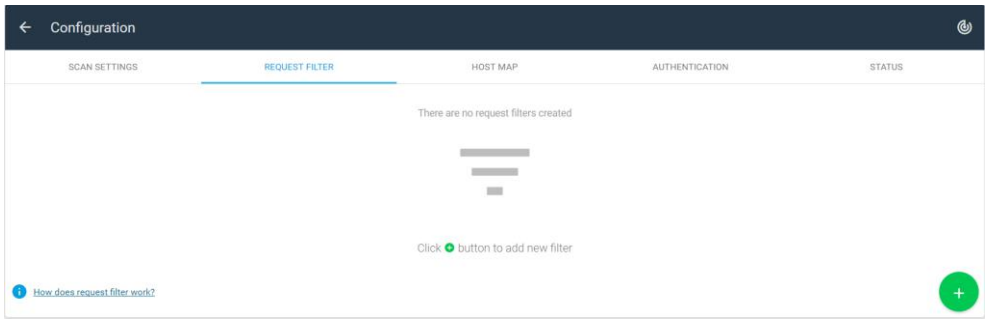
Scanner (HIAB only)

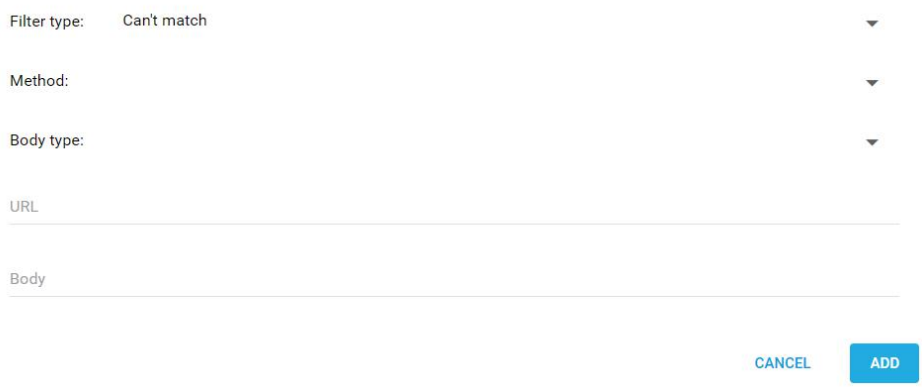
The **Scanner** drop-down list will be available if there is at least one APPSEC SCALE scanner available.

- If the application was not assigned to any scanners initially, the first one in the list will be selected by default.
- After saving the changes, it is not possible to unselect or remove the assigned scanner.

4.2 Request Filter

- To configure the filter settings, click on **+** symbol.
- To view how the **Request Filter** works, click on **i** symbol.
- If any of the options are empty, like **Method** or **Body type**, the filter matches all types of methods and body types.





The available fields of filter setting are:

Filter Type:

- **Can't match**: Black listed URLs, in other words the URLs entered here is not scanned. This is used to avoid visiting unwanted pages like the logout page or a change password function.
- **Must match**: This is used only when a predefined set of pages must be scanned. Provide the pages using regular expressions or sub-strings.

  ***Example**: If ¨.php¨ is provided as must match, it means the scanner scans only pages of ¨.php¨ file type and excludes other pages.*

Method: Optional

Select any of the supporting HTTP request methods or leave the field empty (unspecified).
The available methods are:

- GET
- POST
- DELETE
- PATCH
- PUT

Body Type: Optional

Select the desired content type from the drop-down menu, so that the request body also use the same format as query string. If you leave the field empty, it will match all the requests.

URL

Provide the URL to which the filter settings must be applied (RE2 regex matching).

Body: Optional

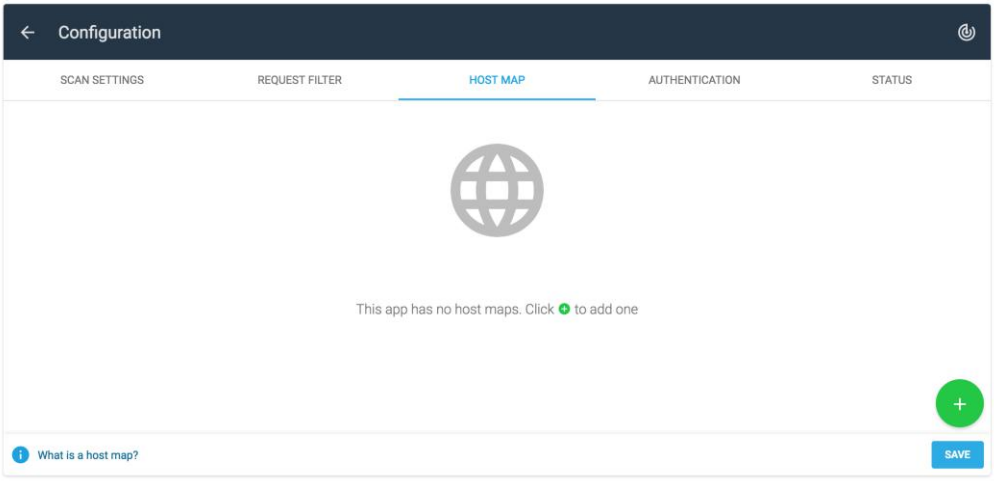
Provide the body to which the filter settings must be applied (RE2 regex matching).

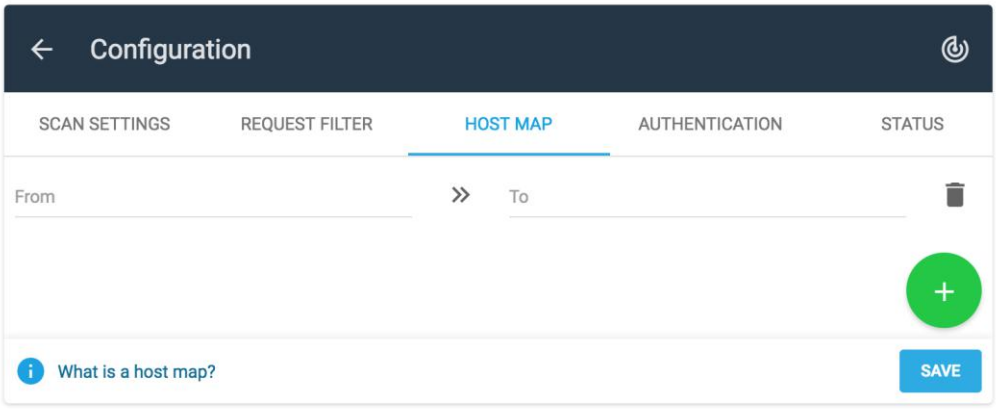
After filling the desired settings into filter configuration dialog, click **ADD**.

4.3 Host Map

The Host Map is an operating system file that maps the hostnames to IP addresses. It can be used to force certain DNS resolutions or to scan vhosts on a HTTP server where there are no DNS records for the vhosts.

To add a host map, click on **+** symbol.

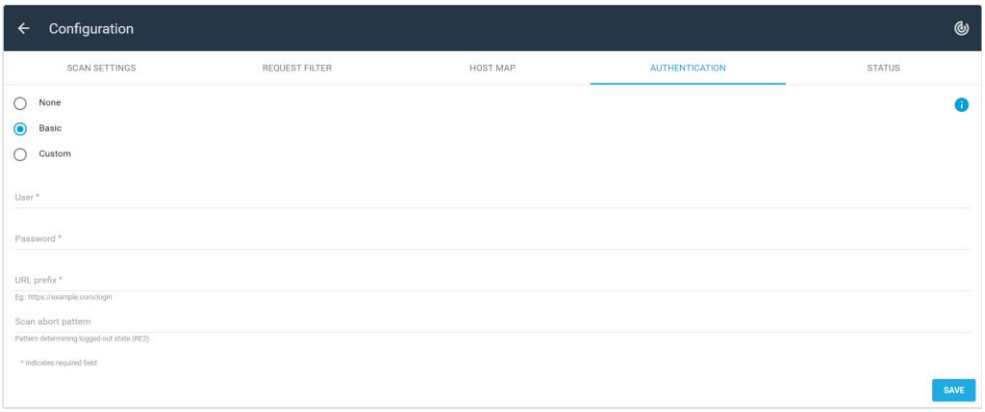




The entry in the **To** field must be a valid IPv4/IPv6 address. The IPv6 address must not be enclosed with square brackets.
***Note**: When using multiple entries in **To** section, a Round-robin selection will be applied to these entries.*

For more information, click on **What is a host map?** link. The bin icon beside the **To** section deletes the entered host map.
After entering the host map, click **SAVE**. You will get a popup displaying **Successfully updated**.

4.4 Authentication



None

Choose **None** if you wish not to have any authentication.

Basic

Choosing **Basic** authentication is appropriate when establishing an initial state of the crawled application using the WWW-Authenticate HTTP header as specified in RFC1945.

Scan Abort Pattern: To terminate a scan due to logged out state, it is recommended to specify a Scan abort pattern.

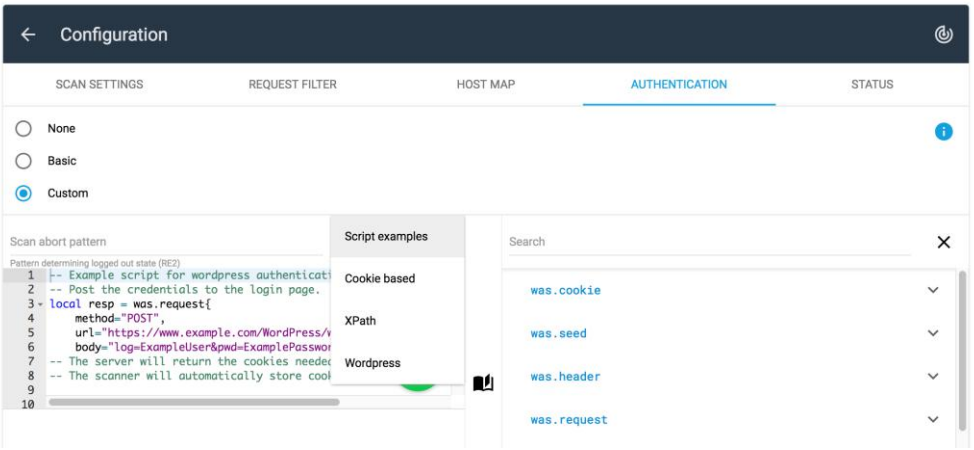
For more advanced authorization process, use Custom authentication.

Custom

Custom authentication flow provides instructions for the scan to establish a desired initial state before an actual scan starts on application's specified **Seed URLs**. The custom authentication flow provides an environment for executing Lua scripts for exchanging HTTP messages over the network, recording cookies, and providing dynamically generated seed URLs.

Some script examples are added to make it easier with Lua custom authentication script. Depending on the chosen example from the dropdown, the script input will be populated. The available examples include:

- Cookie based
- XPath
- Wordpress



Information regarding Lua can be found at https://www.lua.org/. Web application scanner specific documentation can be found by selecting the **Custom authentication** radio button.

Scan Abort Pattern: To terminate a scan due to logged out state, it is recommended to specify a Scan abort pattern.

After selecting the preferred authentication, click **SAVE**. You will get a popup displaying **Successfully updated**.

For more information, please click on **i** symbol.

4.5 Status

The **Status** tab displays the duration of the latest scan, click the **crawled URLs** button to download all crawled URLs and log showing what has been tested. If there was an error when crawling, more verbose information will be visible like, request details or authentication procedure output.

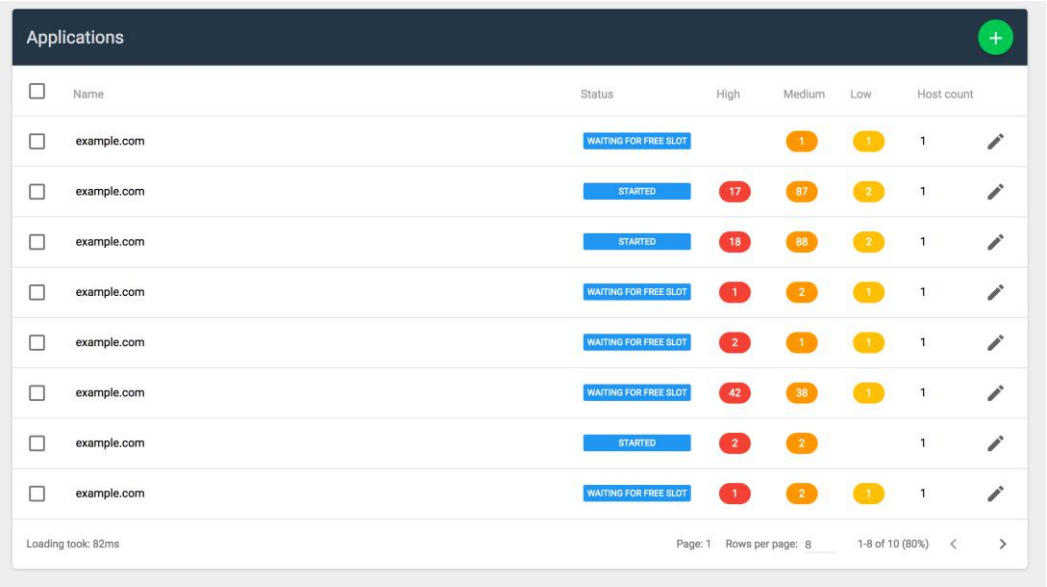
5 Performing a Scan

After configuring the settings, follow the below procedure to perform a scan:

1. Select the target
2. Click on  icon located on top right of the window
3. You will get a popup displaying **Successfully scheduled**

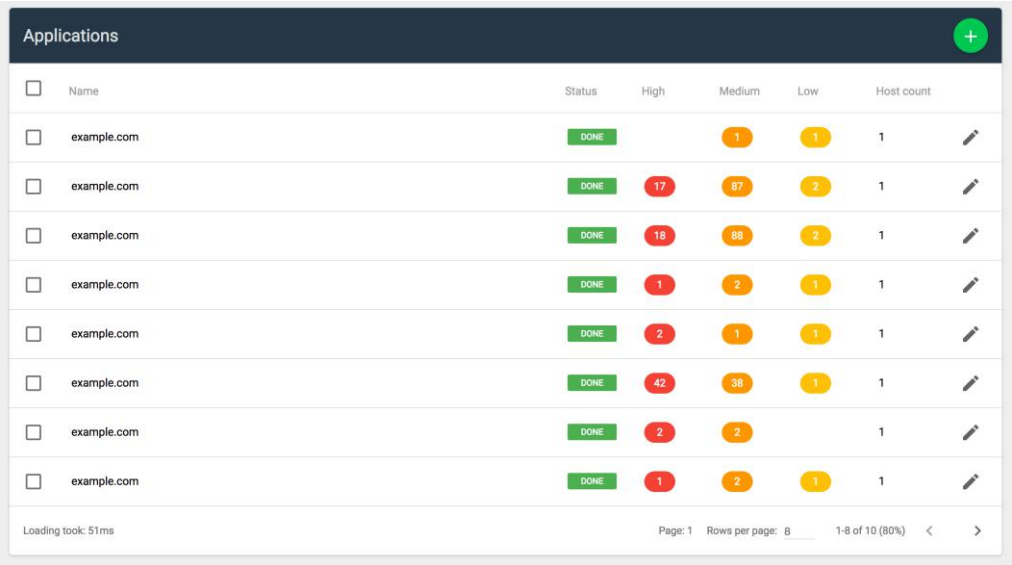
Alternatively, visit the web application you wish to scan, and press the Scan now button in the top right corner.

You can see the status of the scan in the Applications window.



Host count: Indicates how many licenses the application configuration is using.

Once the scan is completed, the status of the scan along with the risks marked as high, medium, and low are shown.

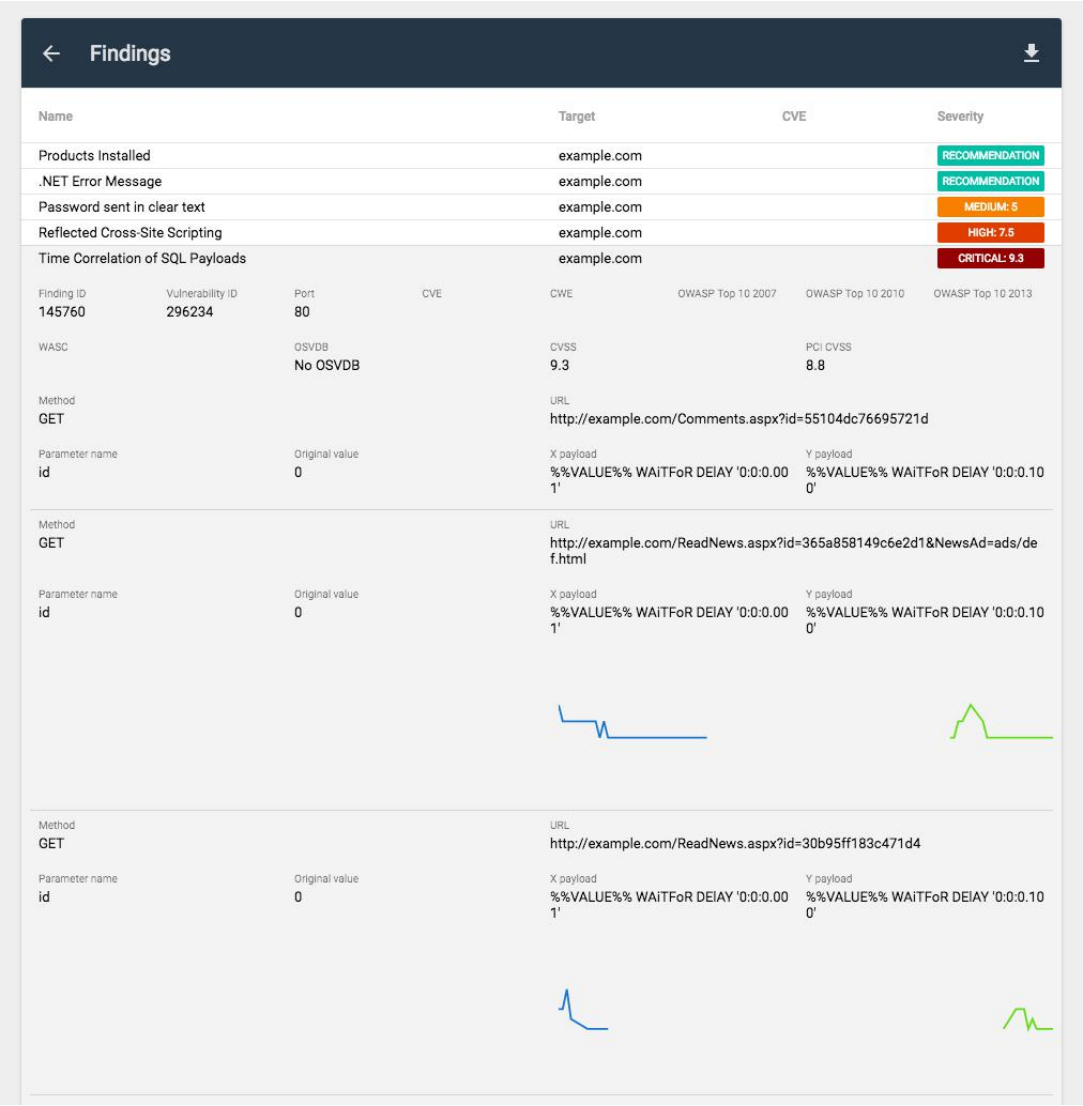


Click on the application to view the findings.

Loading took: Indicates the time taken by the server to return the result page, in other words, how long did the filtering took, or page change took.

6 Findings

The findings window lists all the risks that are found during the scan.

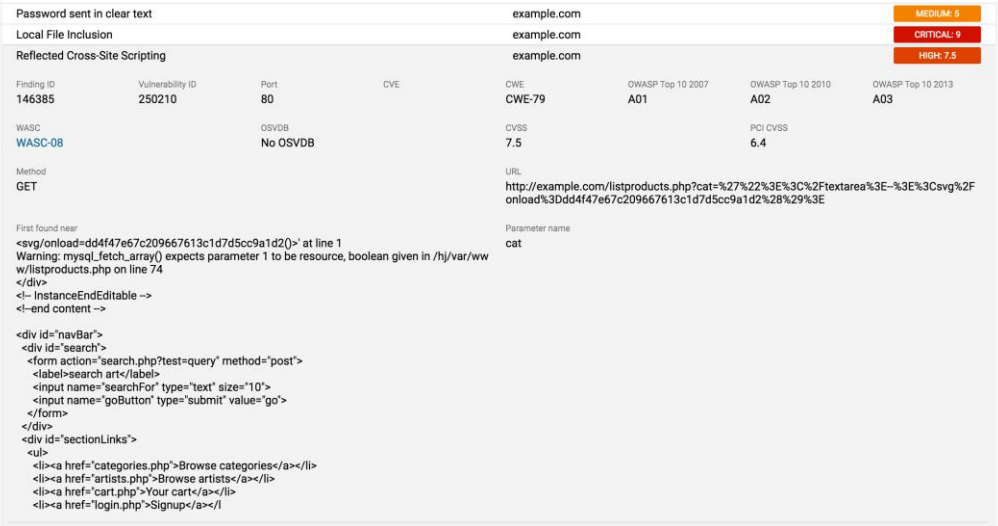


You can view the following details:

- **Name**: Displays the name of the finding.
- **Target**: Displays the host name/ application name which was scanned.
- **CVE**: Common Vulnerabilities and exposures, a catalog of known security threats.
- **Severity**: Displays the condition or the risk level of a finding.

The findings can be sorted based on their severity.

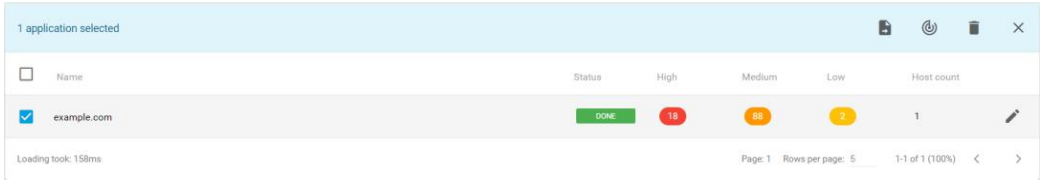
Click on a finding to view more details.



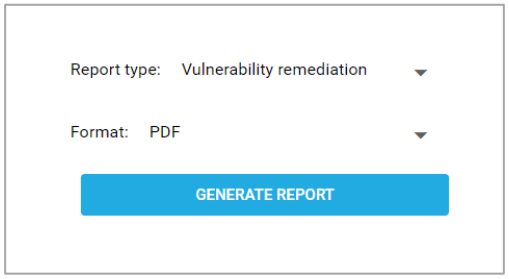
7 Export Report

To export a report:

1. Select a target from the list of applications.

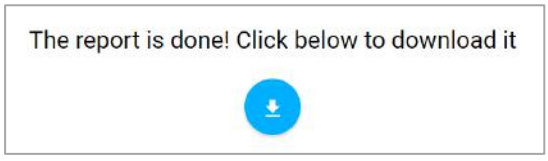


2. Click on icon located on top of the window.
3. You will be prompted with a new window.



- **Report Type**: You can generate two types of reports:
  - Vulnerability Remediation
  - Technical Details
- **Format**: A report can be exported in the most commonly and widely used document formats. The available reporting formats are as follows:
  - **PDF**: This is the most commonly used reporting format.
  - **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.

4. Select one of the options and click on **GENERATE REPORT**.



5. Click on the arrow symbol to download a local copy.

7.1 Report Types

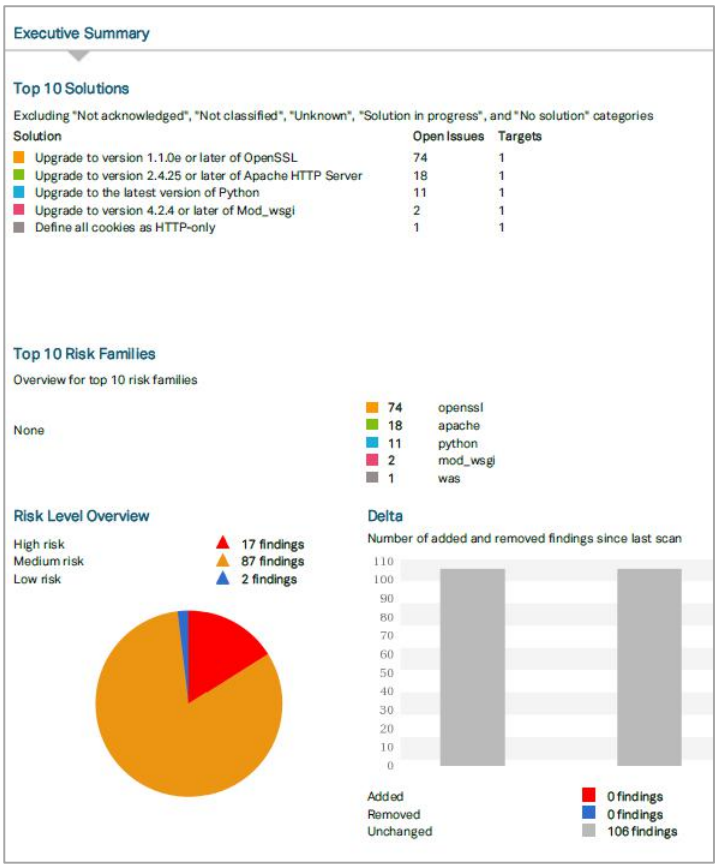
7.1.1 Vulnerability Remediation

7.1.1.1 Report Information

This section contains the generic information about the report fields as shown below.

7.1.1.2 Executive Summary

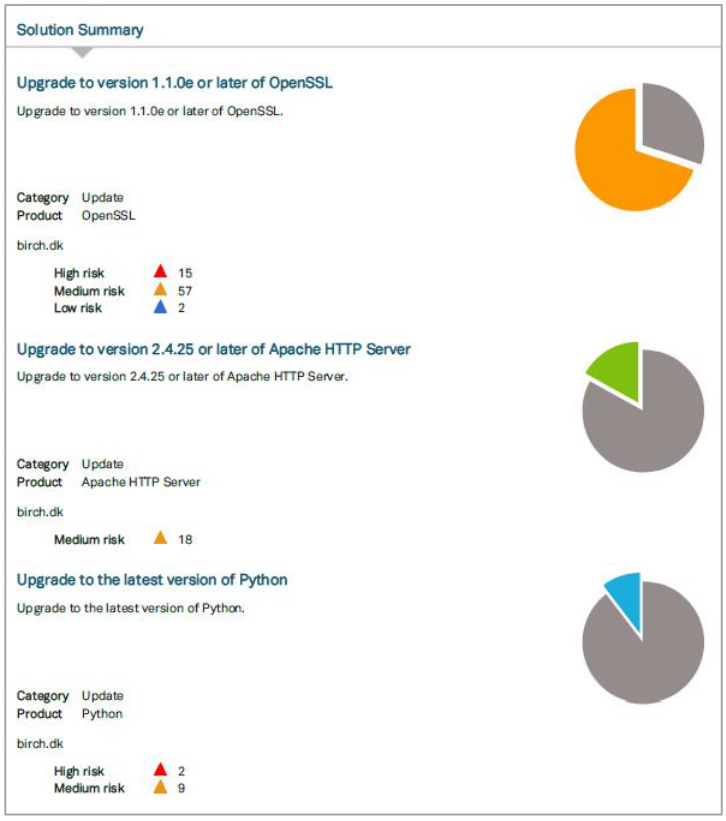
The **Executive Summary** shows the trend information, risk and solutions.



It provides us with graphical information, which is informative and useful to report findings to the top management. It is user-friendly and important section of the report. This chapter is available as default for all the report formats.

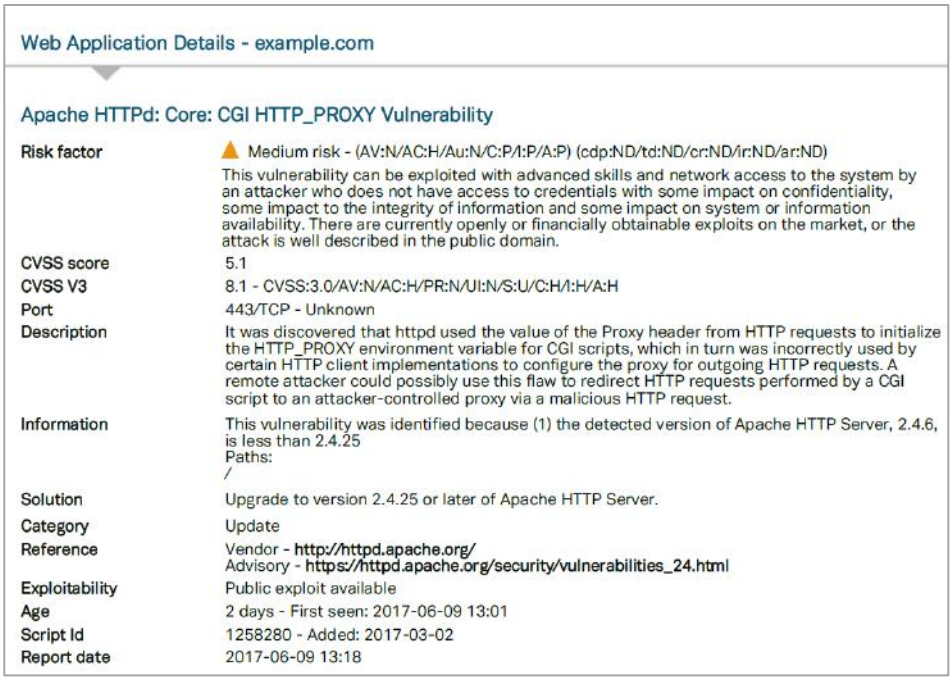
7.1.1.3 Solution Summary

This section provides the solution for the vulnerabilities with a graphical overview. The information presented here helps an organization to resolve multiple vulnerabilities and helps in planning and prioritizing tasks.



7.1.1.4 Web Application Details

This chapter provides a complete and comprehensive overview of the findings. The reported findings are explained with the help of risk factor, CVSS score, port, description of the vulnerability, and information fields. Each vulnerability has a unique script ID.

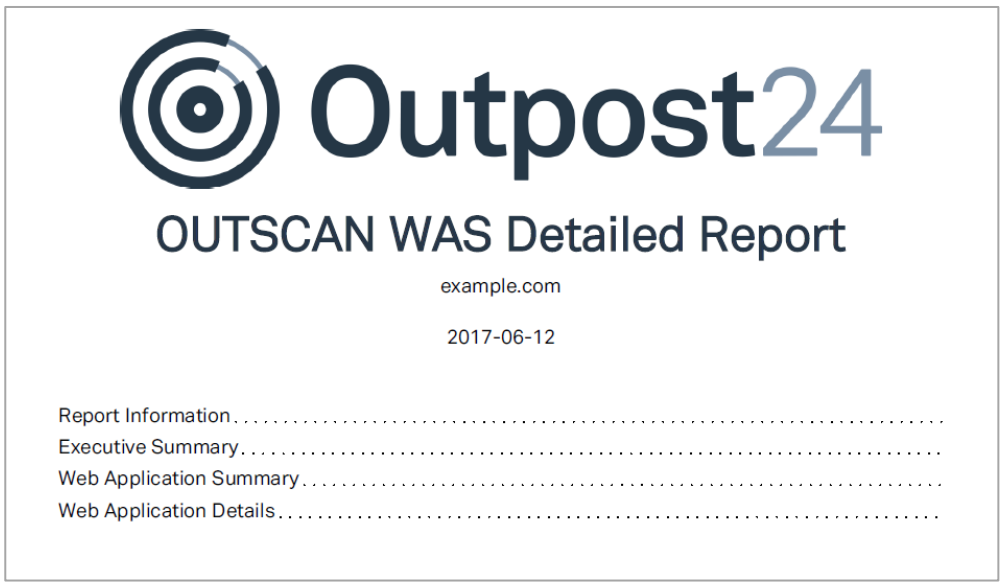


Web Application Details - example.com

Apache HTTPd: Core: CGI HTTP_PROXY Vulnerability

Risk factor	▲ Medium risk - (AV:N/AC:H/Au:N/C:P/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND) This vulnerability can be exploited with advanced skills and network access to the system by an attacker who does not have access to credentials with some impact on confidentiality, some impact to the integrity of information and some impact on system or information availability. There are currently openly or financially obtainable exploits on the market, or the attack is well described in the public domain.
CVSS score	5.1
CVSS V3	8.1 - CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Port	443/TCP - Unknown
Description	It was discovered that httpd used the value of the Proxy header from HTTP requests to initialize the HTTP_PROXY environment variable for CGI scripts, which in turn was incorrectly used by certain HTTP client implementations to configure the proxy for outgoing HTTP requests. A remote attacker could possibly use this flaw to redirect HTTP requests performed by a CGI script to an attacker-controlled proxy via a malicious HTTP request.
Information	This vulnerability was identified because (1) the detected version of Apache HTTP Server, 2.4.6, is less than 2.4.25 Paths: /
Solution	Upgrade to version 2.4.25 or later of Apache HTTP Server.
Category	Update
Reference	Vendor - http://httpd.apache.org/ Advisory - https://httpd.apache.org/security/vulnerabilities_24.html
Exploitability	Public exploit available
Age	2 days - First seen: 2017-06-09 13:01
Script Id	1258280 - Added: 2017-03-02
Report date	2017-06-09 13:18

7.1.2 Technical Details

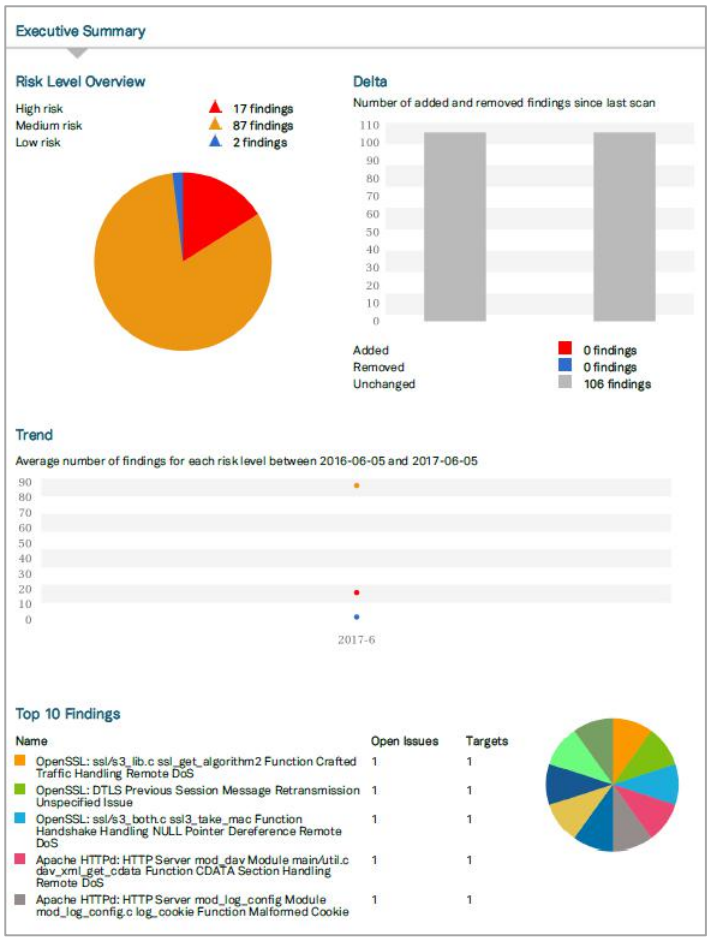


7.1.2.1 Report Information

This section contains the generic information about the report fields as shown below.

7.1.2.2 Executive Summary

The **Executive Summary** shows the trend information, risk, and solutions.



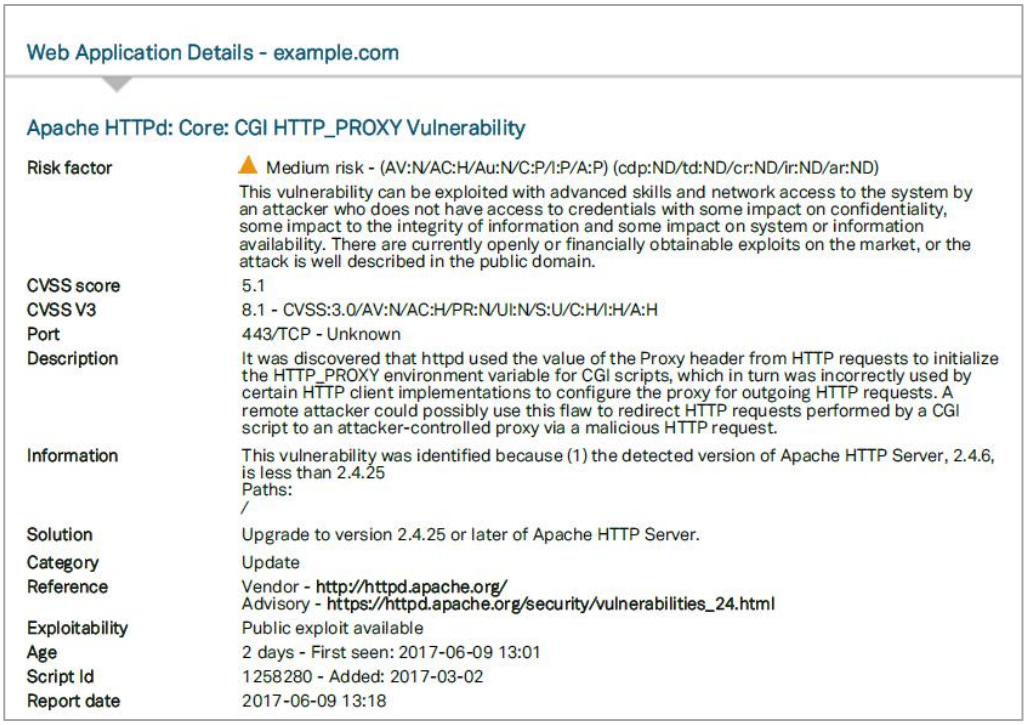
It provides us with graphical information, which is informative and useful to report findings to the top management. It is user-friendly and important section of the report. This chapter is available as default for all the report formats.

7.1.2.3 Web Application Summary

This section provides the information like, number of findings and their severity, number of virtual hosts discovered, and scanning interval.

7.1.2.4 Web Application Details

This section provides a complete and comprehensive overview of the findings. The reported findings are explained with the help of risk factor, CVSS score, port, description of the vulnerability, and information fields. Each vulnerability has a unique script ID.



Web Application Details - example.com

Apache HTTPd: Core: CGI HTTP_PROXY Vulnerability

Risk factor	▲ Medium risk - (AV:N/AC:H/Au:N/C:P/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND) This vulnerability can be exploited with advanced skills and network access to the system by an attacker who does not have access to credentials with some impact on confidentiality, some impact to the integrity of information and some impact on system or information availability. There are currently openly or financially obtainable exploits on the market, or the attack is well described in the public domain.
CVSS score	5.1
CVSS V3	8.1 - CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Port	443/TCP - Unknown
Description	It was discovered that httpd used the value of the Proxy header from HTTP requests to initialize the HTTP_PROXY environment variable for CGI scripts, which in turn was incorrectly used by certain HTTP client implementations to configure the proxy for outgoing HTTP requests. A remote attacker could possibly use this flaw to redirect HTTP requests performed by a CGI script to an attacker-controlled proxy via a malicious HTTP request.
Information	This vulnerability was identified because (1) the detected version of Apache HTTP Server, 2.4.6, is less than 2.4.25 Paths: /
Solution	Upgrade to version 2.4.25 or later of Apache HTTP Server.
Category	Update
Reference	Vendor - http://httpd.apache.org/ Advisory - https://httpd.apache.org/security/vulnerabilities_24.html
Exploitability	Public exploit available
Age	2 days - First seen: 2017-06-09 13:01
Script Id	1258280 - Added: 2017-03-02
Report date	2017-06-09 13:18