nemasis®-DAST

User Guide

Product Version: 14.0.1000.118

Document Version: NDAST-UG-1404

Any technical documentation provided by MicroWorld is copyrighted and owned by MicroWorld. Although MicroWorld makes every effort to ensure that this information is accurate, MicroWorld will not be liable for any errors or omission of facts contained herein. This user guide may include typographical errors, technical or other inaccuracies.

MicroWorld does not offer any warranty to this user guide's accuracy or use. Any use of the user guide or the information contained therein is at the risk of the user. MicroWorld reserves the right to make changes without any prior notice. No part of this user guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MicroWorld Technologies Incorporated.

The terms MicroWorld, MicroWorld logo, Nemasis, and Nemasis logo are trademarks of MicroWorld. All other product names referenced in this user guide are trademarks or registered trademarks of their respective companies and are hereby acknowledged. MicroWorld disclaims proprietary interest in the trademarks and names of others.

The product described in this user guide is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Technical Support:	support@nemasisva.com
Sales:	sales@nemasisva.com
Live Chat:	http://www.nemasisva.com/english/livechat.asp
Printed By:	MicroWorld Technologies Incorporated
Date:	March 2020

Contents

Introduction

The Nemasis is a Vulnerability Management Suite that detects vulnerabilities in your network and provides accurate solution to fix it. It assists you in managing your organization's overall governance, risk and compliance with regulations. The Nemasis is designed to keep you and your organization safe from the cybersecurity threats and make sure you are protected 24x7.

Nemasis DAST scans vulnerabilities of websites and web applications (Internal and Public facing). It identifies the vulnerabilities but also finds the security issues within them in the running state and provides recommendations to mitigate the vulnerabilities. It runs on operating code to detect issues with requests, responses, scripting, data injection, sessions, authentication, and more. It will enumerate ALL the webpages on a specific domain and give a report on possible surface attacks that could occur because of error in programming or error in giving wrong permissions to various areas of your website.

Following are key benefits of Nemasis DAST:

- Follows OWASP compliances (2013 and 2017) with live provision of them on dashboard and exportable reports for Audit purposes.
- Scanners are built with a crawl and attack architecture.
- Scan for hidden and other exploitable vulnerabilities (XSS, SQL injection, and other listed in OWASP Top 10).
- Comprehensive application coverage with advanced attack methodologies.
- Compatible with web applications built on PHP, ASP, Java, and many more.
- Complete Audit Services and recommendations for improvement (PCI-DSS status, GDPR status, WHOIS Audit, Domain Audit, Blacklist Audit, Malware Check, Copycat Domain Audit, SSL Audit, MongoDB Audit) for dedicated audit purposes.

Scope and Purpose

The purpose of this User Guide is to provide readers an understanding of the Nemasis DAST Console and guidance on the best way to use it. This User Guide will prove useful for whoever is involved in developing, monitoring, or learning about the Nemasis DAST. Hereinafter the application Nemasis DAST will be referred as Nemasis.

The User Guide covers processes of creating a scan task, running the scan task, generating the report, and fixing the discovered vulnerabilities. If you are familiar with managing vulnerabilities, the User Guide will be easy to understand. If you are not familiar, please read more about it on the internet as this User Guide does not offer in-depth information.

It is recommended that you read this User Guide side by side as you operate the Nemasis console. Please note that this User Guide does not cover the installation process.

Supported Platforms/Browsers for Nemasis - VMS

Supported Devices/Systems / Heterogeneous Platforms/ applications

- Network devices
- Virtual systems: VMware, Microsoft Hyper-V, and Oracle Virtual Box
- Operating systems: Windows, Mac, and Linux
- Databases: Oracle and SQL Server
- Web applications: Web servers, web services
- IPv4/hybrid networks

Browsers (with HTML5 support)

- Google Chrome (Recommended)
- Mozilla Firefox
- Mozilla Firefox ESR
- Safari
- Safari for iOS

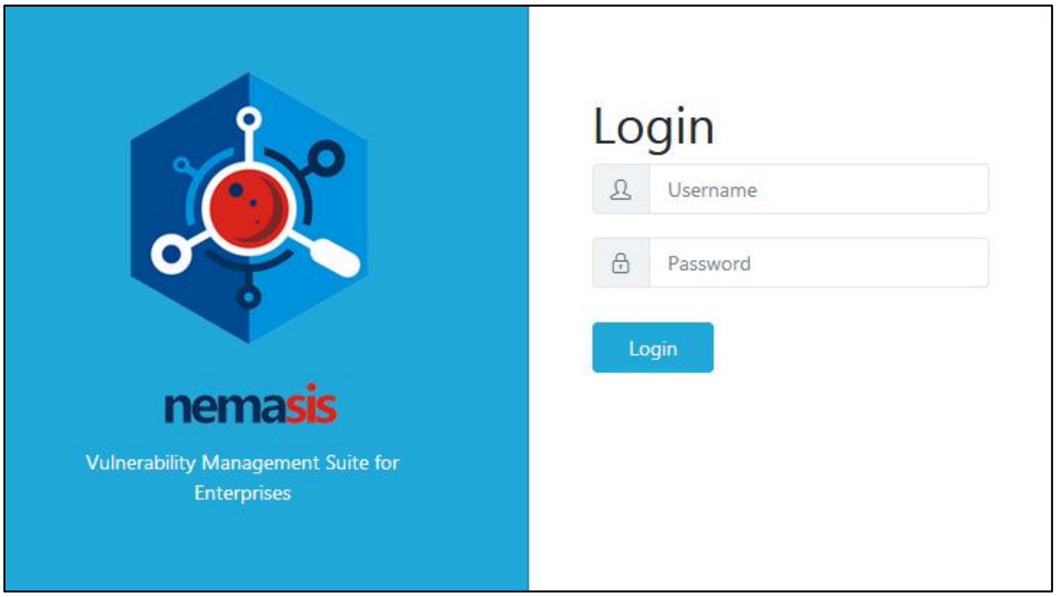
Minimum System Requirements

- 64-bit Debian based Linux OS
- 2 CPUs
- 8 GB RAM
- 50 GB HDD

Login

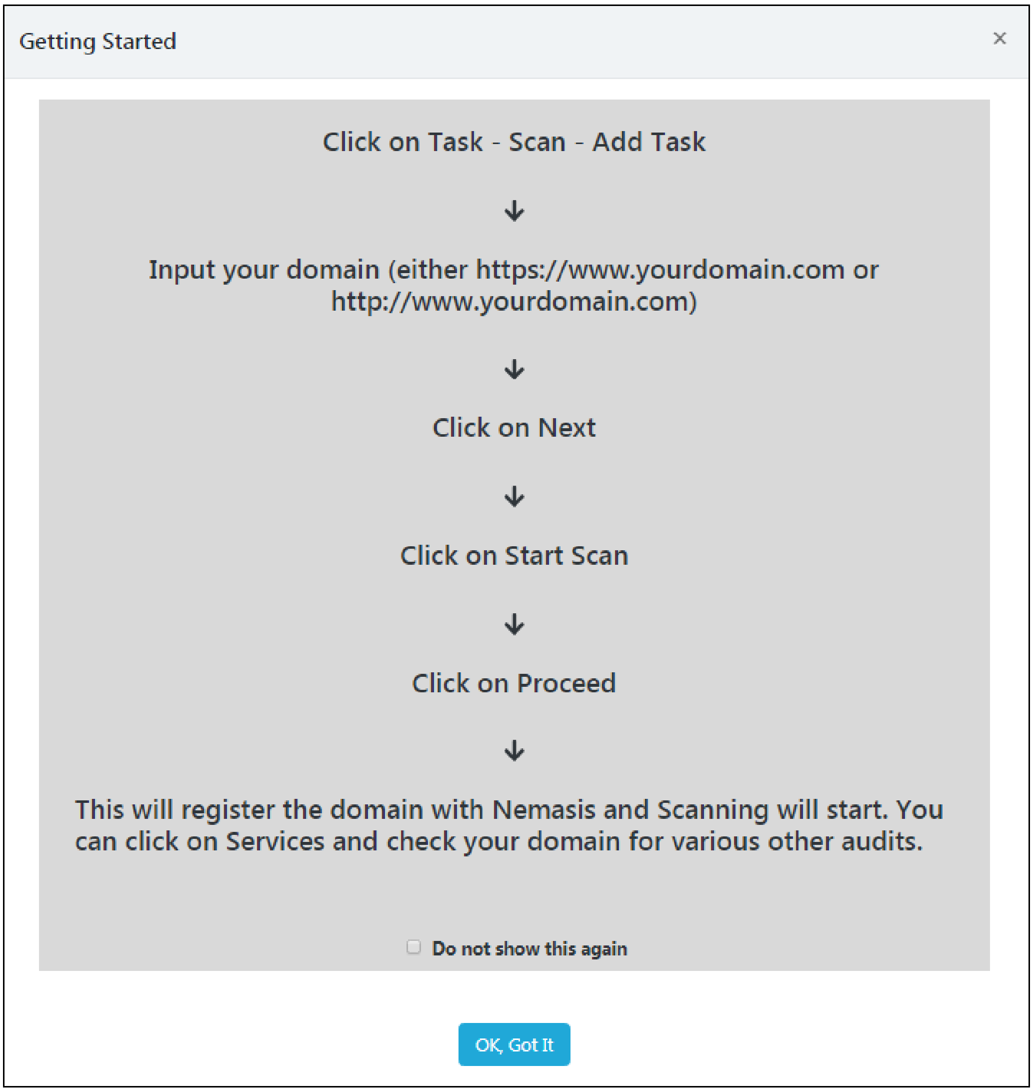
To log in to the Nemasis console, perform the following steps:

1. Launch the browser.
2. Enter the following URL
   https://<IP address of the Nemasis installed system>:10442.
   Nemasis console page appears.



3. Enter the default login credentials **Username** – admin, **Password** – admin and then click **Login**.

After logging in to the Nemasis, you are presented with the following pop-up window.



Getting Started ×

Click on Task - Scan - Add Task

↓

Input your domain (either https://www.yourdomain.com or http://www.yourdomain.com)

↓

Click on Next

↓

Click on Start Scan

↓

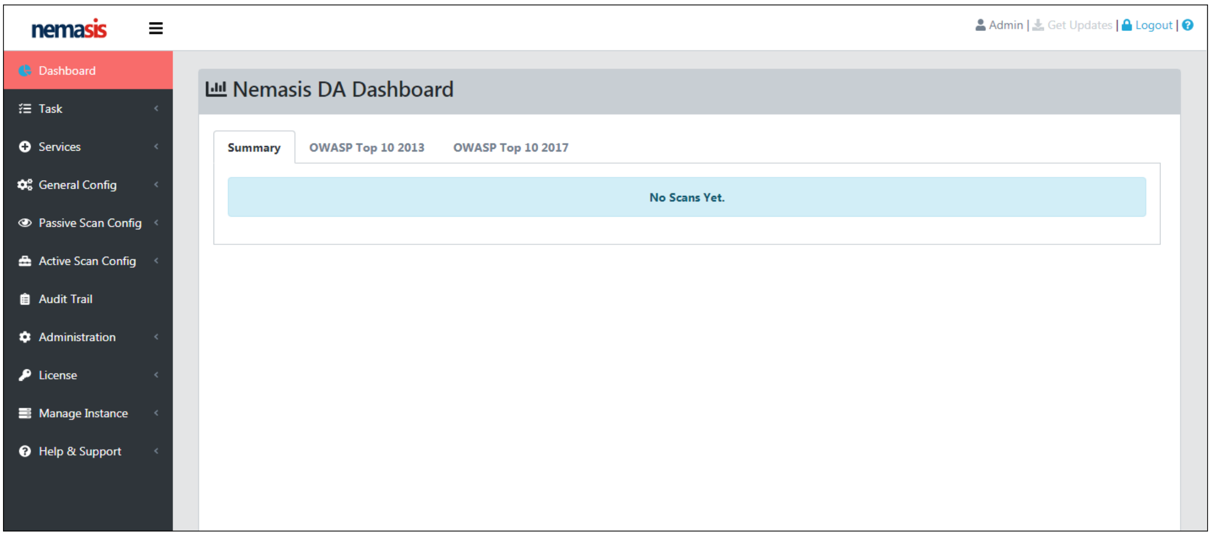
Click on Proceed

↓

This will register the domain with Nemasis and Scanning will start. You can click on Services and check your domain for various other audits.

□ Do not show this again

Click on **OK, Got it**. The screen will be displayed with blank Dashboard window.



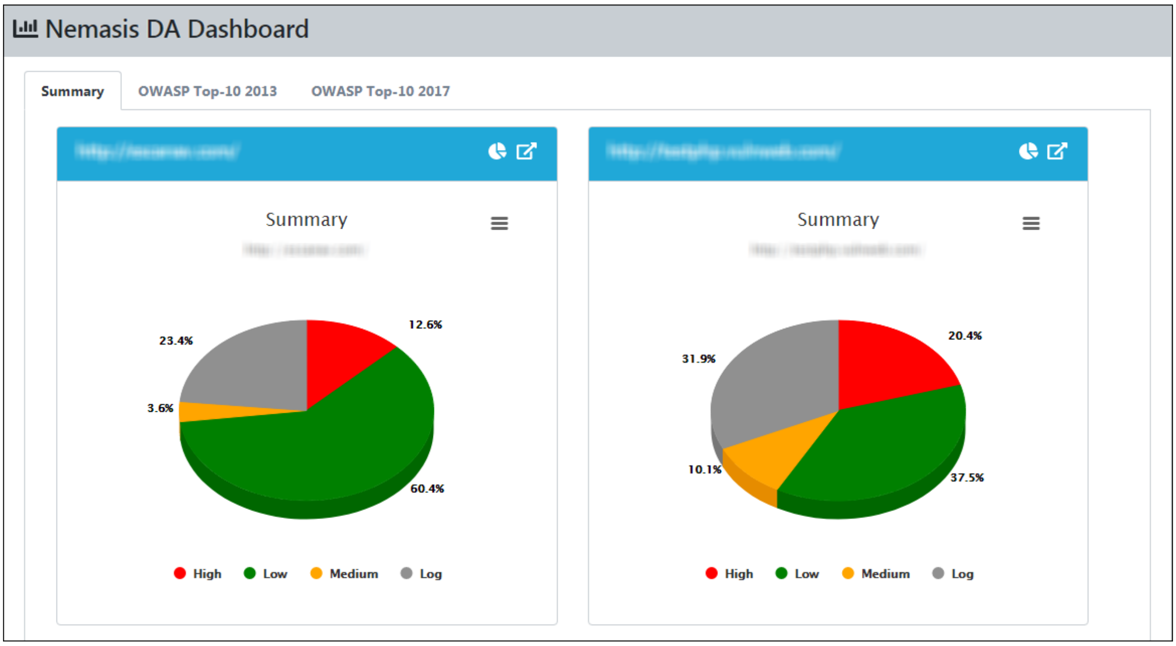
No Scans Yet.

The console tree on the left side contains following modules:

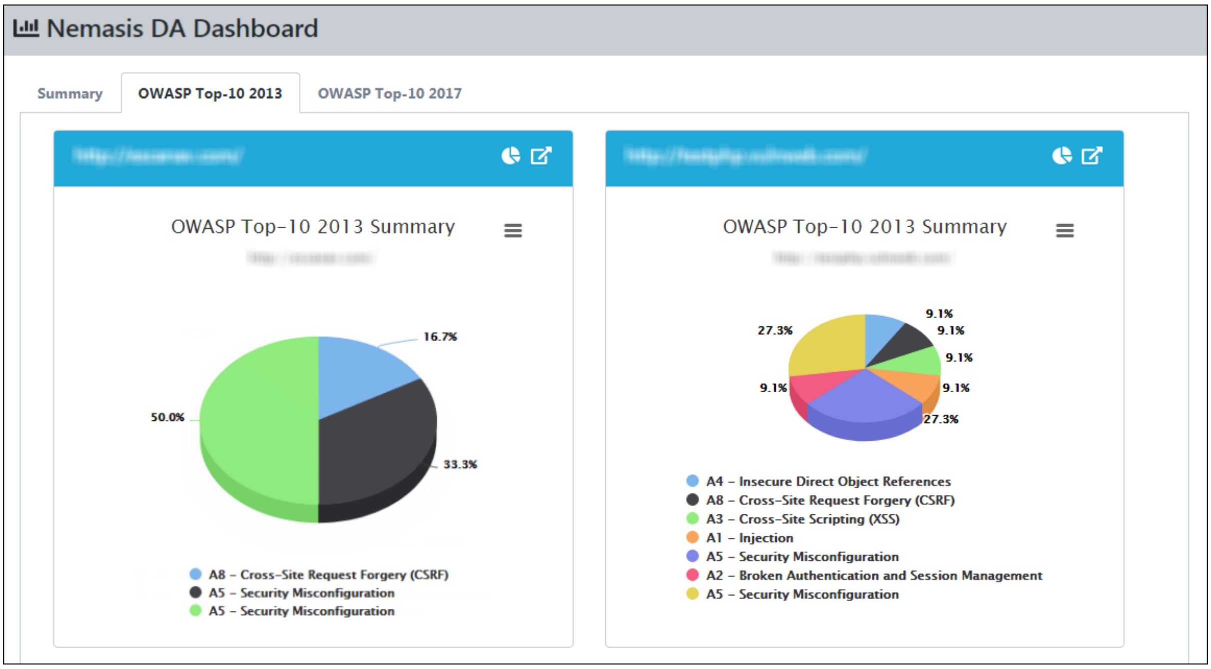
- **Dashboard**
- **Task**
- **Services**
- **General Config**
- **Passive Scan Config**
- **Active Scan Config**
- **Audit Trail**
- **Administration**
- **License**
- **Manage Instance**
- **Help & Support**

Dashboard

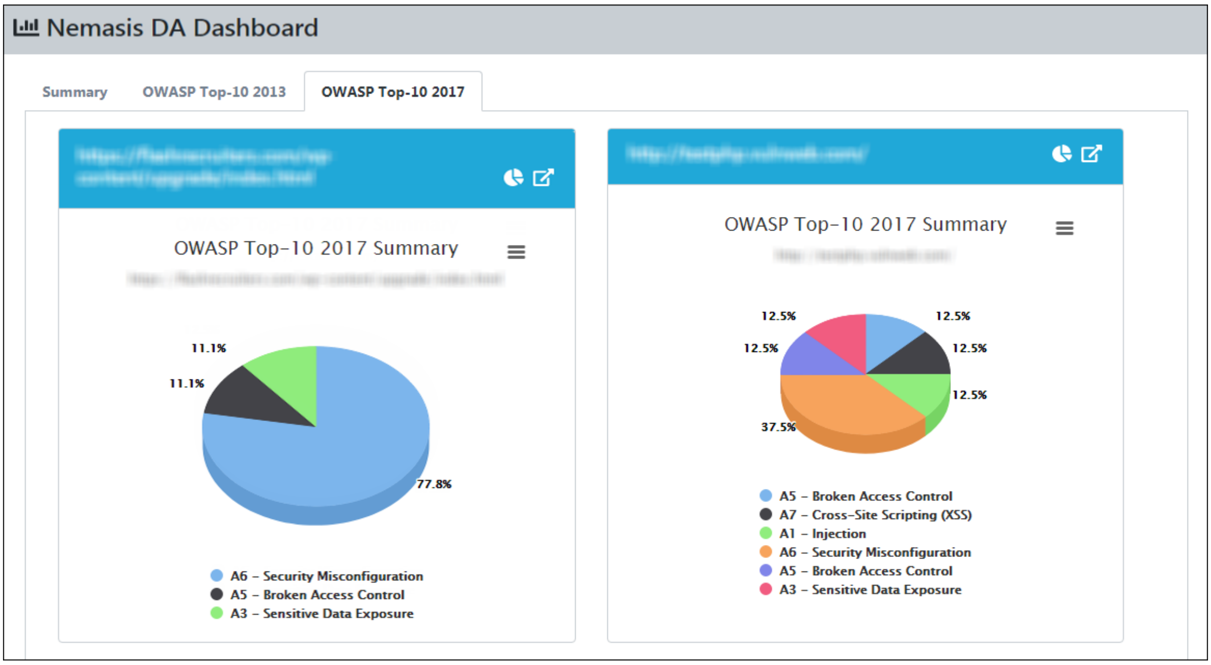
The Dashboard module displays overall scan results in interactive pie charts. By clicking in pie charts you can view the specific information.



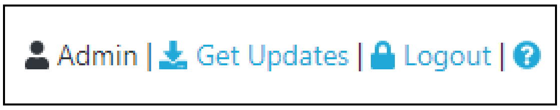
You can view overall result of vulnerabilities based on OWASP 2013 standard.


Nemasis DA Dashboard
Summary
OWASP Top-10 2013
OWASP Top-10 2017
OWASP Top-10 2013 Summary
16.7%
50.0%
33.3%
A8 – Cross-Site Request Forgery (CSRF)
A5 – Security Misconfiguration
A5 – Security Misconfiguration
OWASP Top-10 2013 Summary
9.1%
27.3%
9.1%
9.1%
9.1%
9.1%
27.3%
A4 – Insecure Direct Object References
A8 – Cross-Site Request Forgery (CSRF)
A3 – Cross-Site Scripting (XSS)
A1 – Injection
A5 – Security Misconfiguration
A2 – Broken Authentication and Session Management
A5 – Security Misconfiguration

You can view overall result of vulnerabilities based on OWASP 2017 standard.


Nemasis DA Dashboard
Summary
OWASP Top-10 2013
OWASP Top-10 2017
OWASP Top-10 2017 Summary
11.1%
11.1%
77.8%
A6 – Security Misconfiguration
A5 – Broken Access Control
A3 – Sensitive Data Exposure
OWASP Top-10 2017 Summary
12.5%
12.5%
12.5%
12.5%
12.5%
37.5%
A5 – Broken Access Control
A7 – Cross-Site Scripting (XSS)
A1 – Injection
A6 – Security Misconfiguration
A5 – Broken Access Control
A3 – Sensitive Data Exposure

In the top right corner, there are additional options.

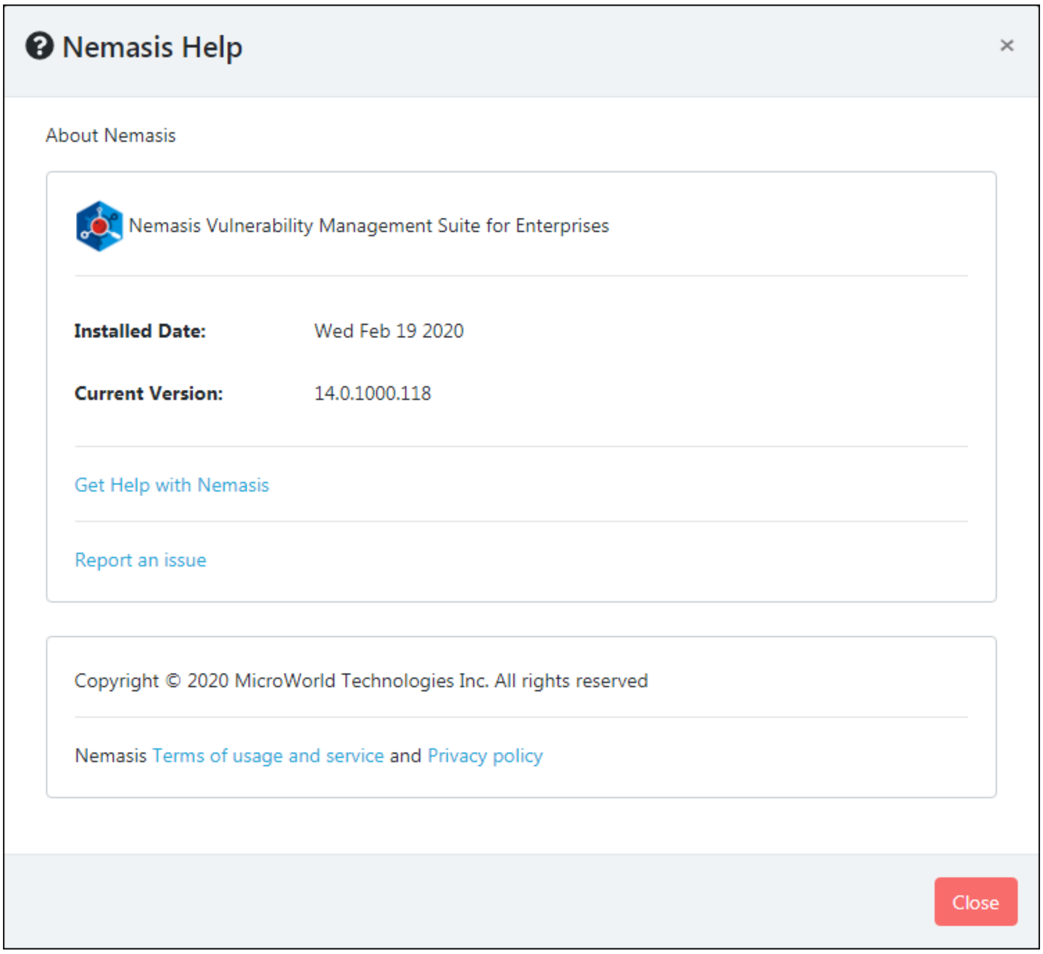


Get Updates
Clicking **Get Updates** will initiate the download of the new database for Nemasis.

Logout
Clicking **Logout** will log you out of the Nemasis console.

Nemasis Help ?

Clicking ? displays the Nemasis Help pop-up.



Nemasis Help

About Nemasis

Nemasis Vulnerability Management Suite for Enterprises

Installed Date: Wed Feb 19 2020

Current Version: 14.0.1000.118

Get Help with Nemasis

Report an issue

Copyright © 2020 MicroWorld Technologies Inc. All rights reserved

Nemasis Terms of usage and service and Privacy policy

The pop-up displays your Nemasis Installed Date and the Current Version in use. By clicking **Get Help with Nemasis** you can get the assistance required for Nemasis. If you are facing any issue with the Nemasis, click **Report an issue**. You will be redirected to the Nemasis Support webpage where you can report your issue and get it solved quickly. You can read about Nemasis **Terms of Usage and Service** and **Privacy Policy** by clicking the respective links.

Task

The Task module contains **Scan** and **Link Scan** submodules.

Scan

The Scan module lets you run scan for finding vulnerabilities in your web applications or websites. As Nemasis is built with crawl and attack architecture. Once the scan is started it will automatically crawl and attack. Commonly, crawling is referred as Spider Scan and attack is referred as Active Scan.

The Spider Scan is used to find new resources (URLs) on a specific site automatically. It starts with a list of URLs to visit, called seeds, depending on how the spider starts. The Spider then visits these URLs, identifies all the hyperlinks in the page and adds them to the list of URLs to visit. This process goes on recursively as long as new resources are discovered. The Spider makes a request to fetch the resources during the processing of an URL and then parses the responses.

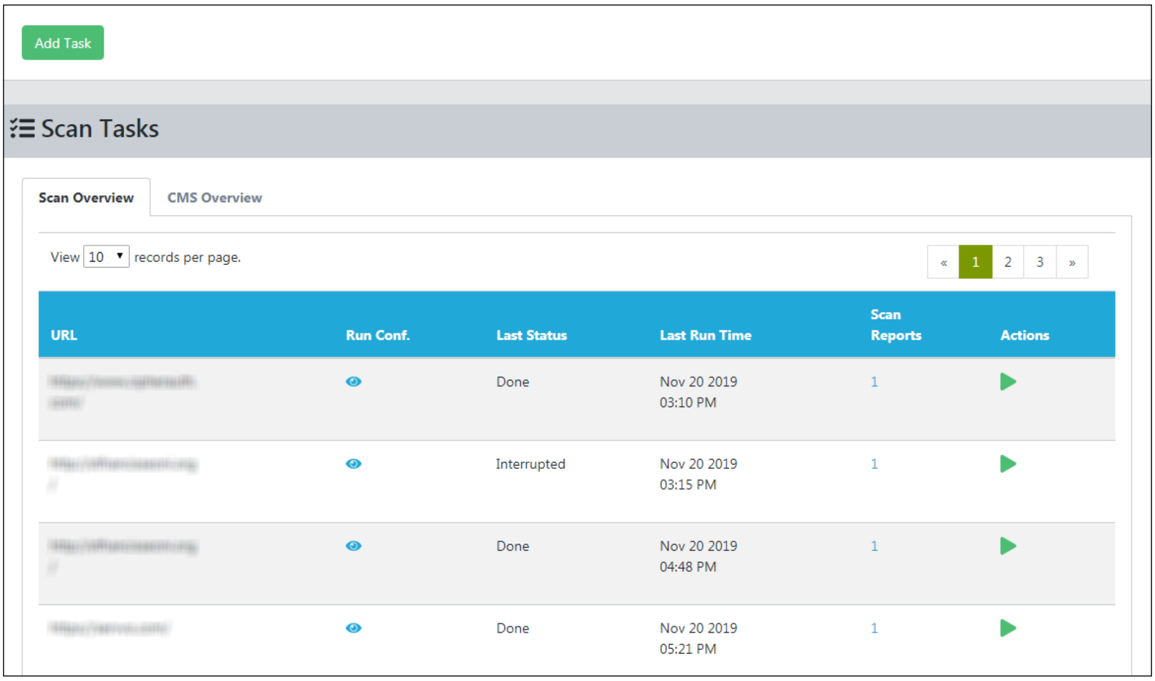
The Active scan usually tries to identify potential vulnerabilities by using known attacks against the target. It should be noted that only certain type of vulnerabilities can be detected. It is a kind of penetration testing that will be performed on the domain. This scan will only list the number of URLs and then perform the scan. Due to this it is mandatory to perform crawling before performing attack.

There are following tabs:

- Scan Overview
- CMS Overview

Scan Overview

Scan Overview tab displays the URL, Run Conf., Last Status, Last Run Time, Scan Reports, and Actions.



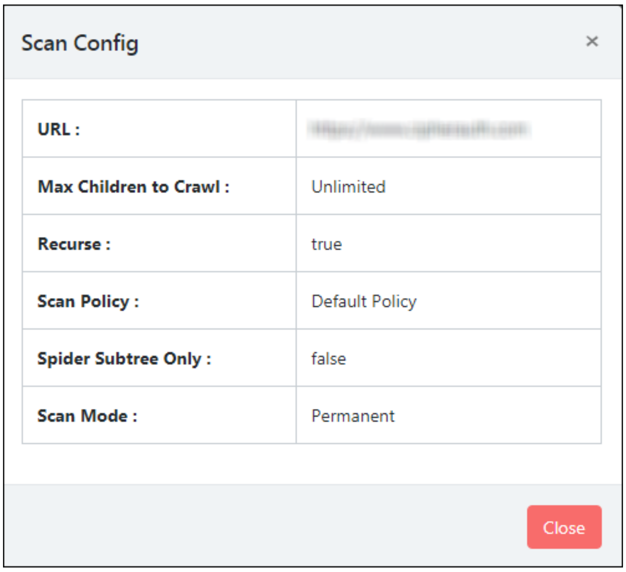
URL	Run Conf.	Last Status	Last Run Time	Scan Reports	Actions
[redacted]	👁	Done	Nov 20 2019 03:10 PM	1	▶
[redacted]	👁	Interrupted	Nov 20 2019 03:15 PM	1	▶
[redacted]	👁	Done	Nov 20 2019 04:48 PM	1	▶
[redacted]	👁	Done	Nov 20 2019 05:21 PM	1	▶

URL

Displays the URL

Run Conf.

Run Conf. is a clickable icon (👁), which gives you details of the scan configuration such as URL, recurse, max children crawled, and spider subtree.



URL :	[redacted]
Max Children to Crawl :	Unlimited
Recurse :	true
Scan Policy :	Default Policy
Spider Subtree Only :	false
Scan Mode :	Permanent

Last Status

Displays the status of the last run scan. If a scan is in Running status then, if it displays,

- 🕷 Performing spider scan!!
- ⚡ Performing active scan!!

Last Run Time

Displays the run time of the last run scan

Scan Reports

Displays the numbers of reports generated

Actions

Clicking icons in the Actions column lets you take actions regarding a Scan.

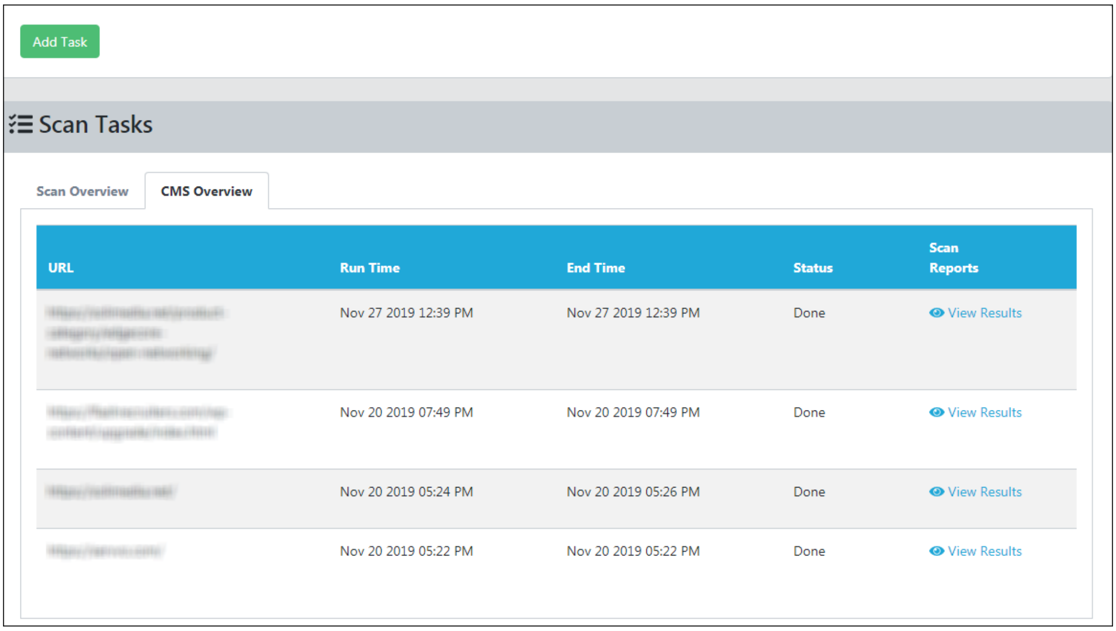
- ▶ Start Scan
- ■ Stop Scan
- ❚❚ Pause Scan

Note	You can see the details of active scan's progress by hovering the mouse over it. Clicking it displays a list of scanning rules currently running and rules that were skipped.

CMS Overview

The Nemasis provides a CMS vulnerability scanner to run the vulnerability tests for different versions of WordPress. It lists down the detected vulnerabilities and the remediation instructions along with technical information.

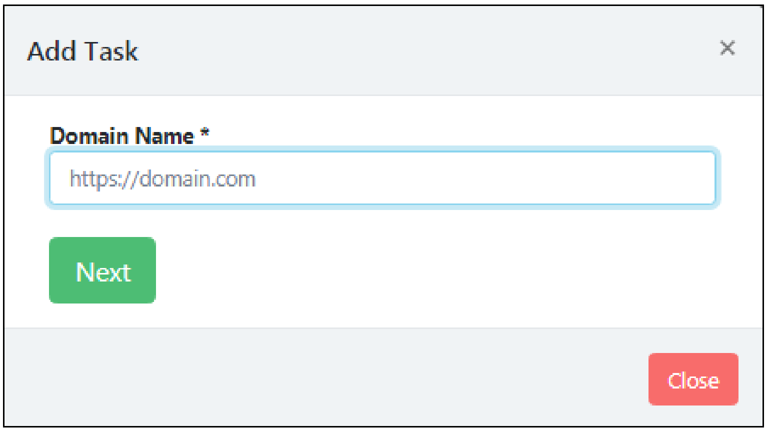
CMS Overview tab displays the URL if it is found to be a CMS, Run Time, End Time, Status, and Scan Reports.



URL	Run Time	End Time	Status	Scan Reports
[redacted]	Nov 27 2019 12:39 PM	Nov 27 2019 12:39 PM	Done	View Results
[redacted]	Nov 20 2019 07:49 PM	Nov 20 2019 07:49 PM	Done	View Results
[redacted]	Nov 20 2019 05:24 PM	Nov 20 2019 05:26 PM	Done	View Results
[redacted]	Nov 20 2019 05:22 PM	Nov 20 2019 05:22 PM	Done	View Results

Adding a Task

1. To add a scan task, click **Add Task**.
   Add task window appears.

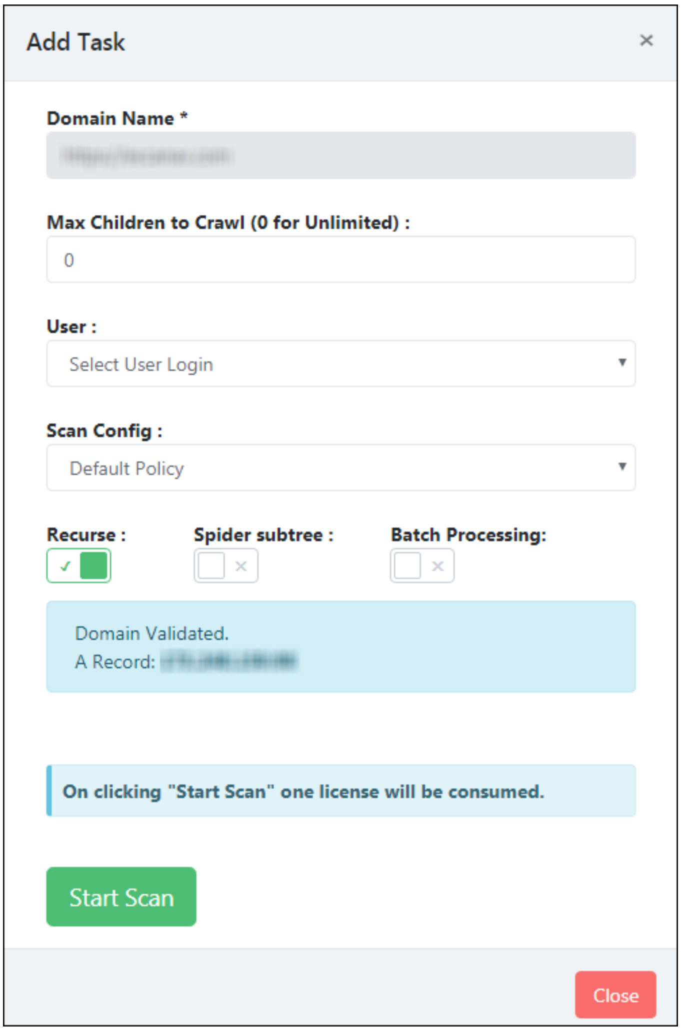


Add Task

Domain Name *

https://domain.com

2. Enter the domain name for the scan.
3. Click **Next**. Add task window extends.



Add Task

Domain Name *

[redacted]

Max Children to Crawl (0 for Unlimited) :

0

User :

Select User Login

Scan Config :

Default Policy

Recurse : ✓ Spider subtree : □ Batch Processing: □

Domain Validated.
A Record: [redacted]

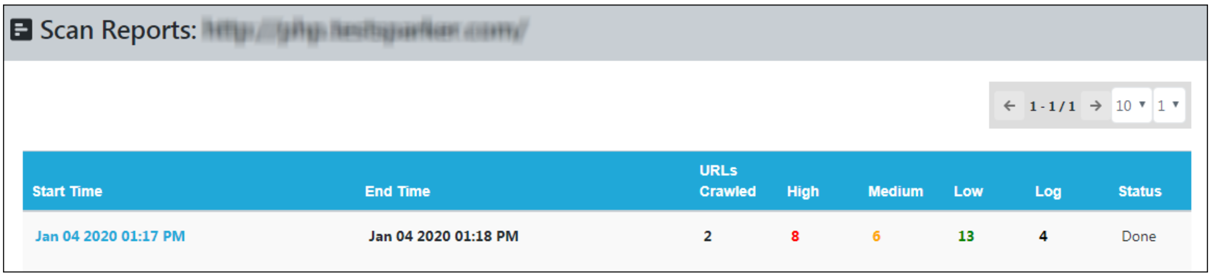
On clicking "Start Scan" one license will be consumed.

4. Enter the following details:
    - **Maximum Children to Crawl (0 for Unlimited)**
    - Select a **User**. Learn more about User by clicking **here**.
    - Select a **Scan Config**. Learn more about Scan policy by clicking **here**.
5. Configure the following toggle options:
    - **Recurse** option is used to seed the spider for all the selected nodes. It is enabled by default.
    - **Spider subtree** option will allow spider to access resources that under the beginning point (URI). It is disabled by default.
    - **Batch Processing** option sets limit to the spider to crawl for 10000 vulnerabilities and start performing Active Scan. It is disabled by default while creating task.
6. Click **Start Scan**. The scan will be initiated.

Note	In Trail version, **Batch Processing** is enabled by default.

Viewing a Report

To view the report of the performed scan, click on numbers below the **Scan Reports** column. You will be able to view the **Reports**, which has **Start Time**, **End Time**, **URL Crawled**, the number of vulnerabilities found based on severity score (**High**, **Medium**, **Low**, and **Log**) and **Status** of the scan.

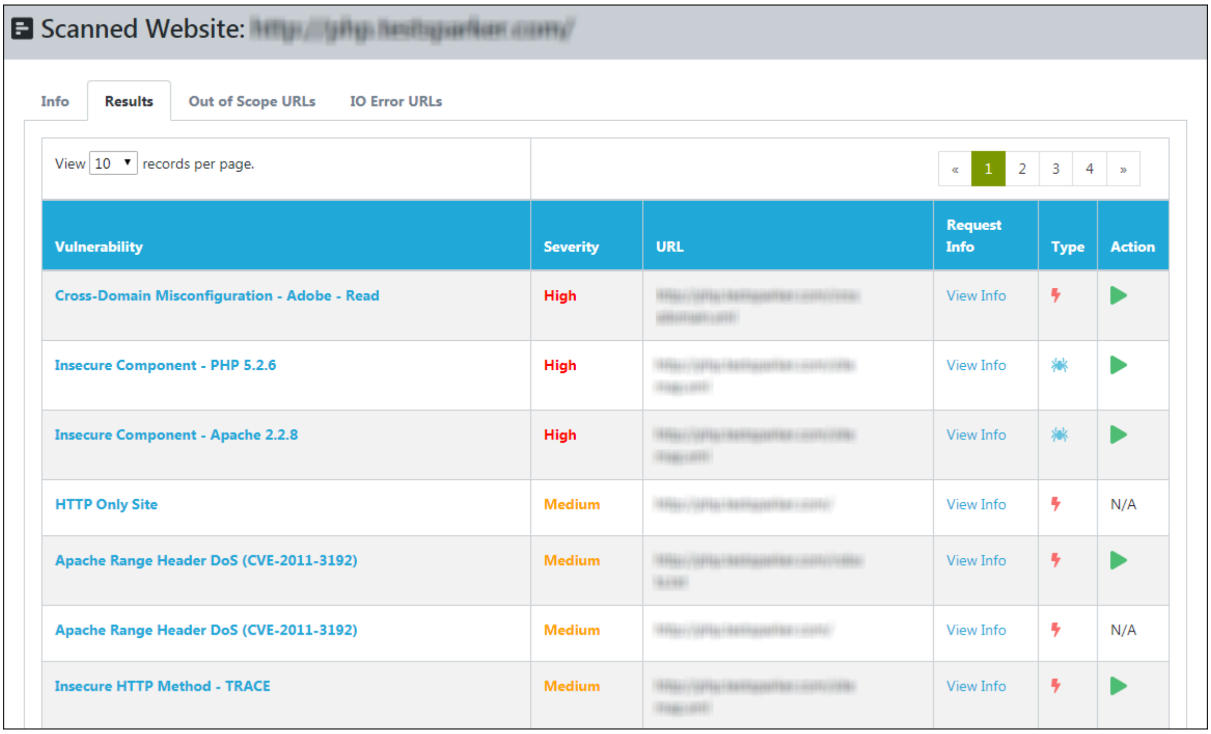


Scan Reports: [redacted]

← 1 - 1 / 1 → 10 ▾ 1 ▾

Start Time	End Time	URLs Crawled	High	Medium	Low	Log	Status
Jan 04 2020 01:17 PM	Jan 04 2020 01:18 PM	2	8	6	13	4	Done

To get the details of the particular scan, select report under **Start Time** column. The **Results** tab displays list of vulnerabilities found and their severity score, page URL, Request Info, and type for each of it. You can also get the view of vulnerabilities found according to the risk score.



Scanned Website: [redacted]

View 10 ▾ records per page.

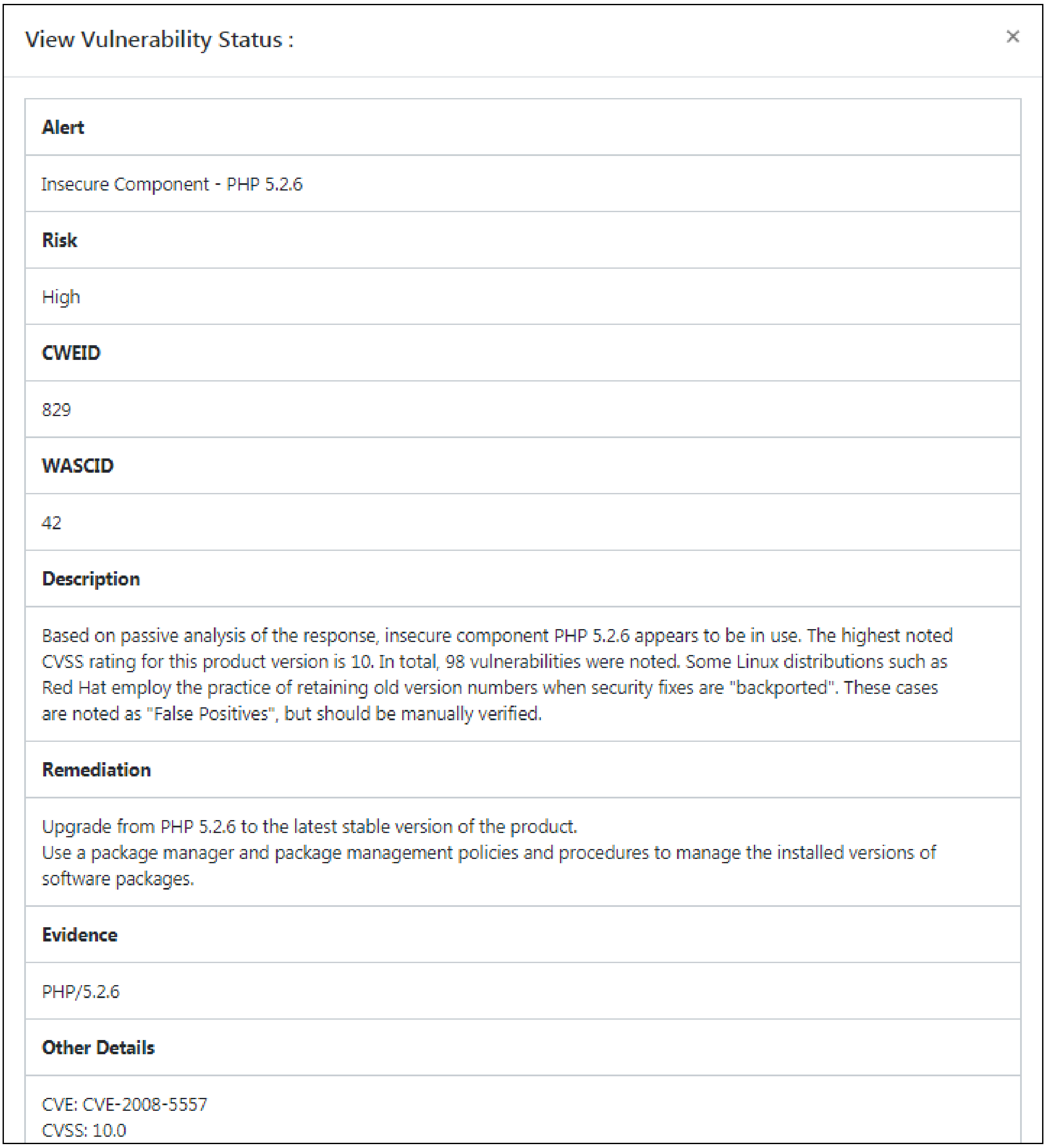
« 1 2 3 4 »

Vulnerability	Severity	URL	Request Info	Type	Action
Cross-Domain Misconfiguration - Adobe - Read	High	[redacted]	View Info	⚡	▶
Insecure Component - PHP 5.2.6	High	[redacted]	View Info	🕷	▶
Insecure Component - Apache 2.2.8	High	[redacted]	View Info	🕷	▶
HTTP Only Site	Medium	[redacted]	View Info	⚡	N/A
Apache Range Header DoS (CVE-2011-3192)	Medium	[redacted]	View Info	⚡	▶
Apache Range Header DoS (CVE-2011-3192)	Medium	[redacted]	View Info	⚡	N/A
Insecure HTTP Method - TRACE	Medium	[redacted]	View Info	⚡	▶

Type column will give the detail of vulnerability during which scan it was found.

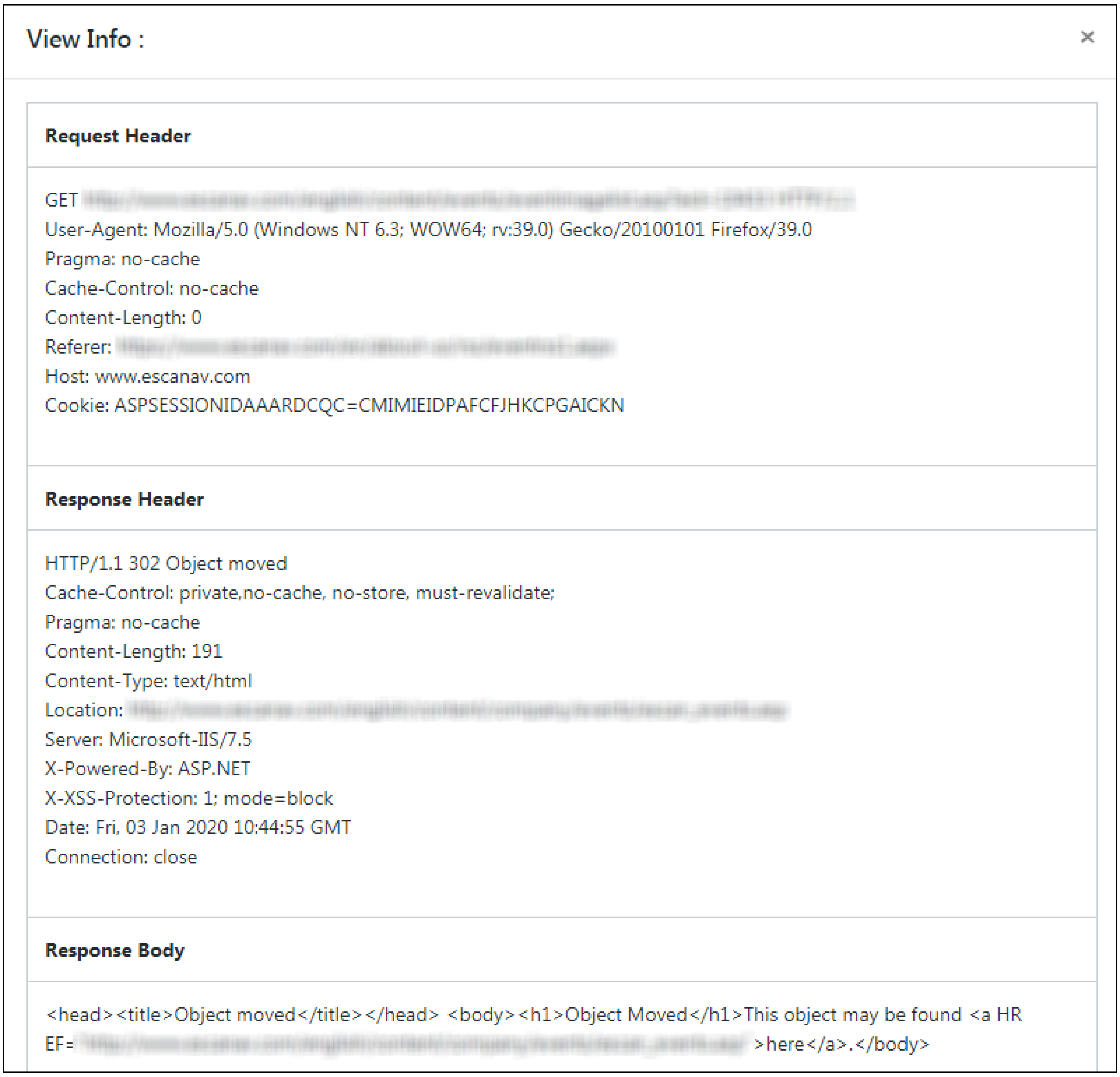
- 🕷 Spider scan
- ⚡ Active scan

To get detailed report for all the vulnerabilities found, click on the name of the vulnerability in the **Vulnerability** column. The report will include Alert, Risk, CWEID, WASCID, Descriptions, Remediation, Evidence, Other Details, and References for the vulnerability found.



Alert
Insecure Component - PHP 5.2.6
Risk
High
CWEID
829
WASCID
42
Description
Based on passive analysis of the response, insecure component PHP 5.2.6 appears to be in use. The highest noted CVSS rating for this product version is 10. In total, 98 vulnerabilities were noted. Some Linux distributions such as Red Hat employ the practice of retaining old version numbers when security fixes are "backported". These cases are noted as "False Positives", but should be manually verified.
Remediation
Upgrade from PHP 5.2.6 to the latest stable version of the product. Use a package manager and package management policies and procedures to manage the installed versions of software packages.
Evidence
PHP/5.2.6
Other Details
CVE: CVE-2008-5557 CVSS: 10.0

To get details of response status for all vulnerabilities, click on **View Info** in the **Request Info** column. It will contain following Request Header, Request Body, Response Header, and Response Body sections.



Request Header

GET [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: [redacted]
Host: www.escanav.com
Cookie: ASPSESSIONIDAAARDCQC=CMIMIEIDPAFCFJHKCPGAICKN

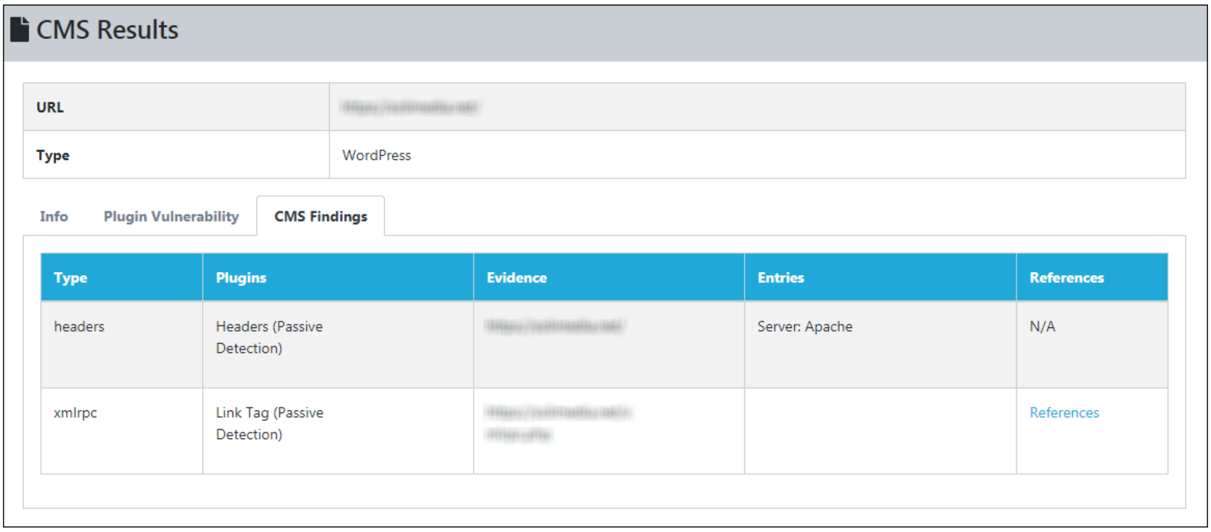
Response Header

HTTP/1.1 302 Object moved
Cache-Control: private,no-cache, no-store, must-revalidate;
Pragma: no-cache
Content-Length: 191
Content-Type: text/html
Location: [redacted]
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
X-XSS-Protection: 1; mode=block
Date: Fri, 03 Jan 2020 10:44:55 GMT
Connection: close

Response Body

<head><title>Object moved</title></head> <body><h1>Object Moved</h1>This object may be found <a HR
EF= [redacted] >here</a>.</body>

In CMS tab, you can view the Scan Reports of CMS URL, click View Results under Scan Reports, CMS Results gets displayed.

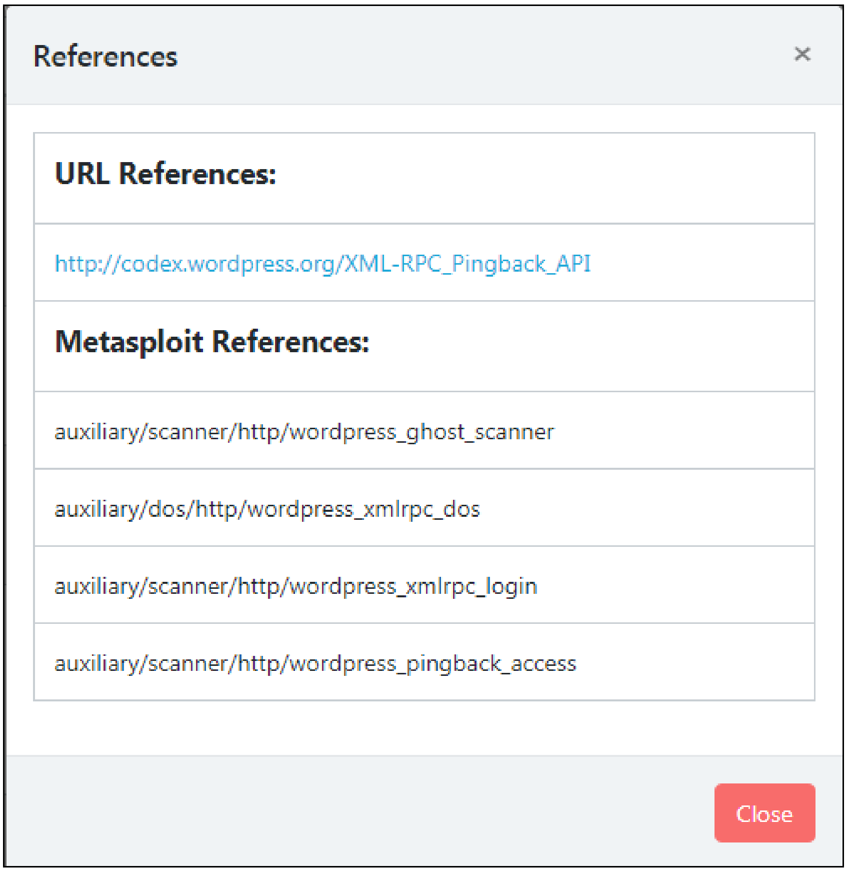


CMS Results

URL	[redacted]
Type	WordPress

Type	Plugins	Evidence	Entries	References
headers	Headers (Passive Detection)	[redacted]	Server: Apache	N/A
xmlrpc	Link Tag (Passive Detection)	[redacted]		References

To view the References, click on it.



References

URL References:

http://codex.wordpress.org/XML-RPC_Pingback_API

Metasploit References:

auxiliary/scanner/http/wordpress_ghost_scanner

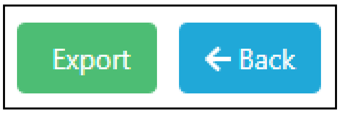
auxiliary/dos/http/wordpress_xmlrpc_dos

auxiliary/scanner/http/wordpress_xmlrpc_login

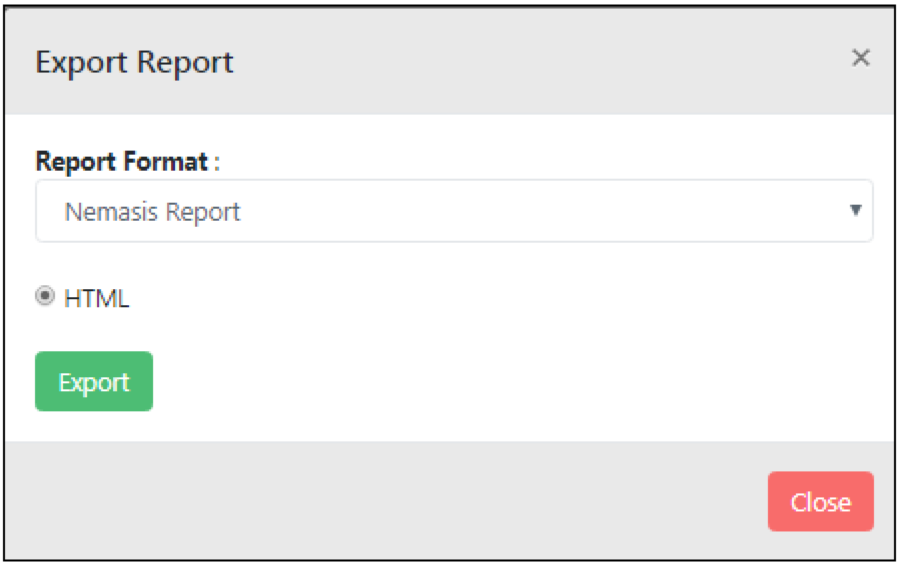
auxiliary/scanner/http/wordpress_pingback_access

Exporting a report

You can export **Scan Report**. To export the report, click **Export** on the right-hand side corner of the **Results** tab.



Export Report window appears, select **Report Format** and **HTML** and click **OK**.



Report Format : Nemasis Report

● HTML

The report will be downloaded in the HTML format.

Report Format

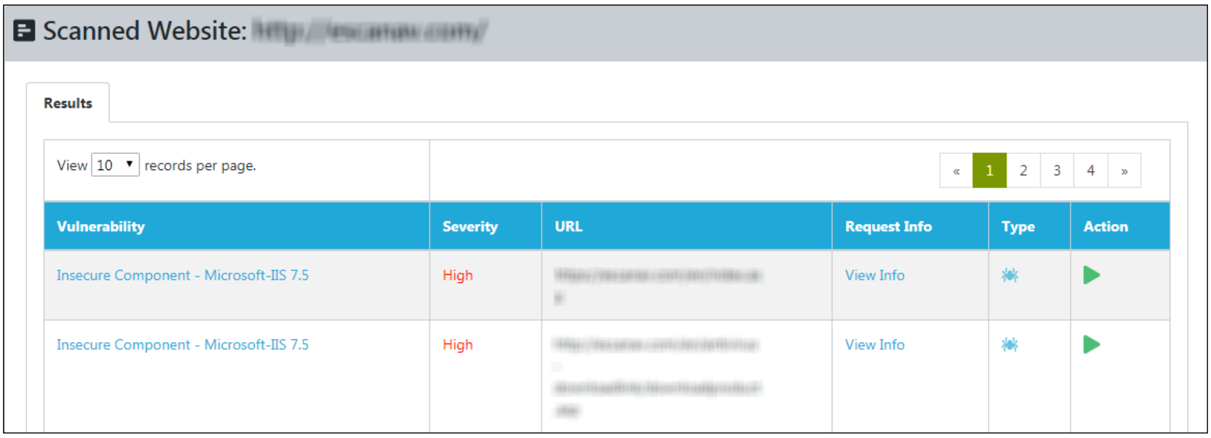
- Nemasis Report
- OWASP Top-10 2013
- OWASP Top-10 2017
- PCI-DSS Compliance

Link Scan

The **Link Scan** submodule lets you scan specific URL from the domain for all the vulnerabilities.

Scanning a specific URL

To scan a specific URL link, you can select the link from the **Scan Task** list. You can choose a specific URL from the reports of the scanned domains. Once you select the URL to be scanned, click ▶ icon from the **Action** tab.



Scanned Website: [redacted]

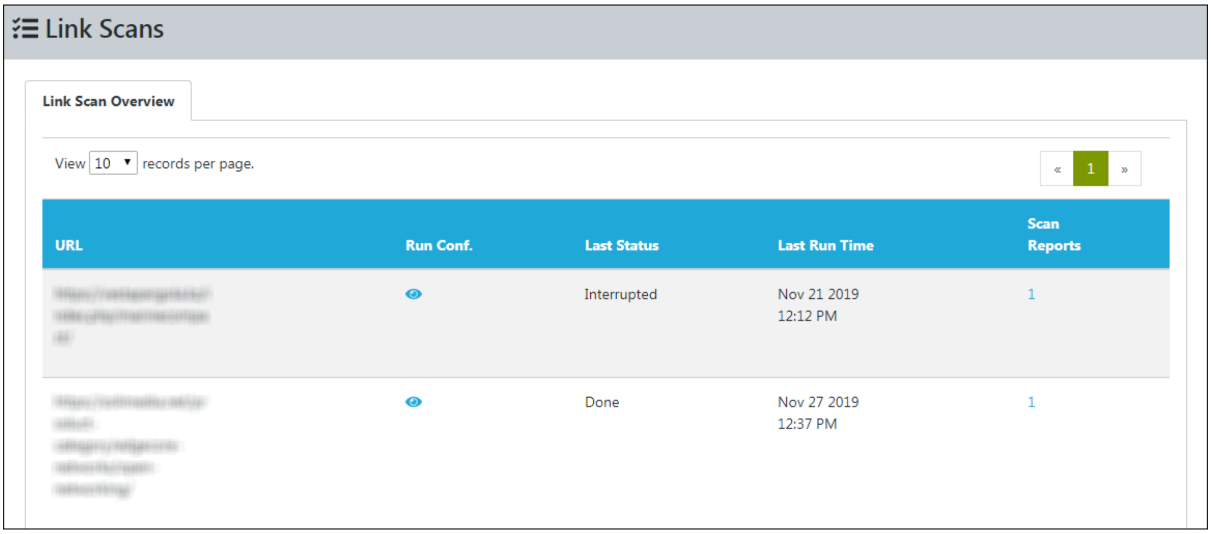
Results

View 10 ▾ records per page.

« 1 2 3 4 »

Vulnerability	Severity	URL	Request Info	Type	Action
Insecure Component - Microsoft-IIS 7.5	High	[redacted]	View Info	✱	▶
Insecure Component - Microsoft-IIS 7.5	High	[redacted]	View Info	✱	▶

After the scan is initiated, it will redirect to **Link Scan** page and in **Link Scan Overview** tab you can view the generated report once the scan is completed.



Link Scans

Link Scan Overview

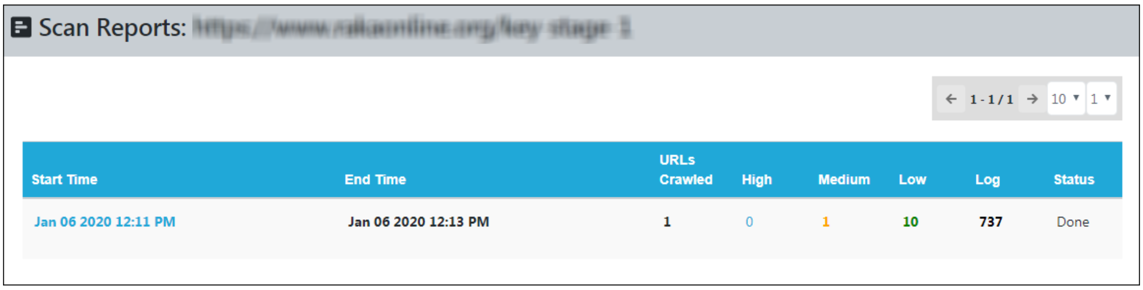
View 10 ▾ records per page.

« 1 »

URL	Run Conf.	Last Status	Last Run Time	Scan Reports
[redacted]	👁	Interrupted	Nov 21 2019 12:12 PM	1
[redacted]	👁	Done	Nov 27 2019 12:37 PM	1

Viewing a Report

To view the report of the performed scan, click on numbers below the **Scan Reports** column. You will be able to view the **Reports**, which has **Start Time**, **End Time**, **URLs Crawled**, the number of vulnerabilities found based on severity score (**High**, **Medium**, **Low**, and **Log**) and **Status** of the scan.

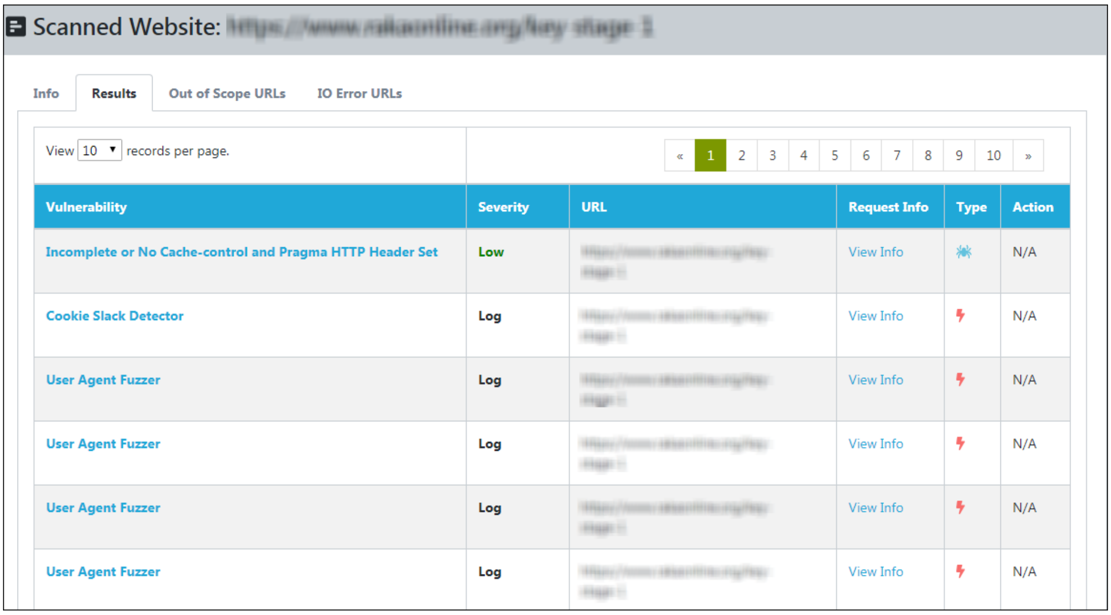


Scan Reports: [redacted]

← 1 - 1 / 1 → 10 ▾ 1 ▾

Start Time	End Time	URLs Crawled	High	Medium	Low	Log	Status
Jan 06 2020 12:11 PM	Jan 06 2020 12:13 PM	1	0	1	10	737	Done

To get the details of the particular scan, select report under Start Time column. The Results tab displays list of vulnerabilities found and their severity score, page URL, request info, and type for each of it. You can also get the view of vulnerabilities found according to the risk score.



Scanned Website: [redacted]

Vulnerability	Severity	URL	Request Info	Type	Action
Incomplete or No Cache-control and Pragma HTTP Header Set	Low	[redacted]	View Info	🐞	N/A
Cookie Slack Detector	Log	[redacted]	View Info	⚡	N/A
User Agent Fuzzer	Log	[redacted]	View Info	⚡	N/A
User Agent Fuzzer	Log	[redacted]	View Info	⚡	N/A
User Agent Fuzzer	Log	[redacted]	View Info	⚡	N/A
User Agent Fuzzer	Log	[redacted]	View Info	⚡	N/A

To get detailed report for all the vulnerabilities found, click on the name of the vulnerability in the **Vulnerability** column. The report will include Alert, Risk, CWEID, WASCID, Descriptions, Remediation, Evidence, Other Details, and References for the vulnerability found. To get details of response status for all vulnerabilities, click on the **Request Info** column. It will contain following Request Header, Request Body, Response Header, and Response Body sections.

You can download the report in HTML format by clicking on **Export** button at right-hand side corner.

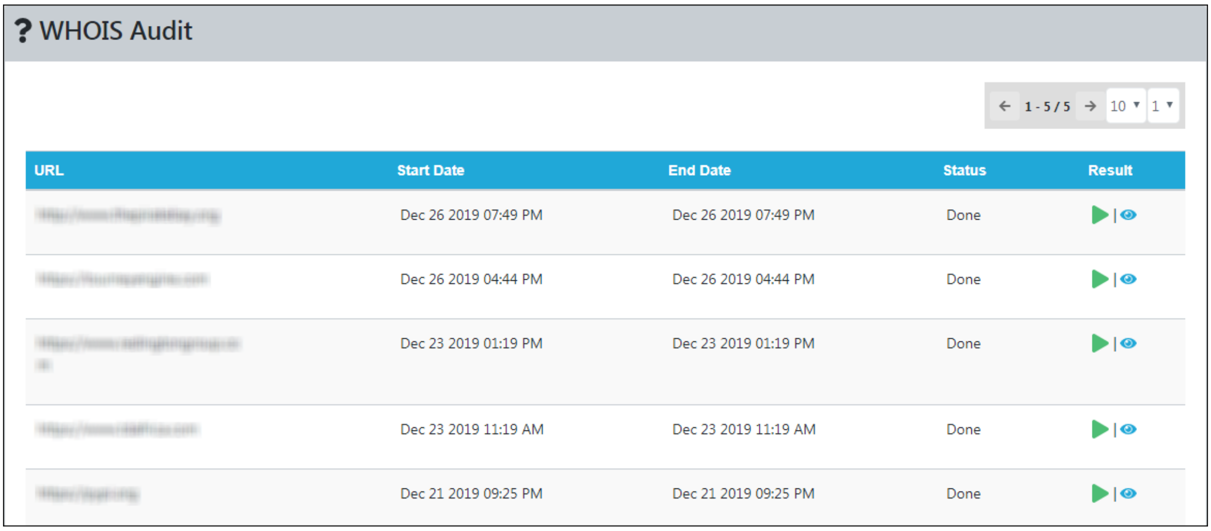
Services

The Service module contains **WHOIS Audit**, **Domain Audit**, **SSL Audit**, **BlackList Audit**, **Malware Check**, **SEO Analytics**, **Copycat Domains**, and **Mongo Audit** submodules.

WHOIS Audit

The WHOIS Audit module lets user to scan and generate the audit report of a specific domain for Extensible Provisioning Protocol (EPP) domain status codes. This audit helps users to recognize EPP status codes so that they can clarify is it safe from domain name hijacking, unauthorized modification from both client and server, and phishing attacks. By getting this report, users can keep a track on their domain's status.

This module displays the **URL**, **Start Date**, **End Date, Status**, and **Result** of the audit.

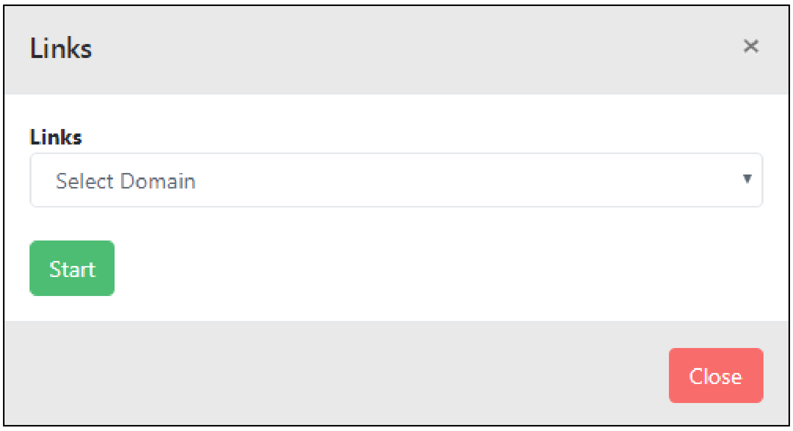


? WHOIS Audit

URL	Start Date	End Date	Status	Result
[illegible]	Dec 26 2019 07:49 PM	Dec 26 2019 07:49 PM	Done	▶ | 👁
[illegible]	Dec 26 2019 04:44 PM	Dec 26 2019 04:44 PM	Done	▶ | 👁
[illegible]	Dec 23 2019 01:19 PM	Dec 23 2019 01:19 PM	Done	▶ | 👁
[illegible]	Dec 23 2019 11:19 AM	Dec 23 2019 11:19 AM	Done	▶ | 👁
[illegible]	Dec 21 2019 09:25 PM	Dec 21 2019 09:25 PM	Done	▶ | 👁

Adding a WHOIS Audit

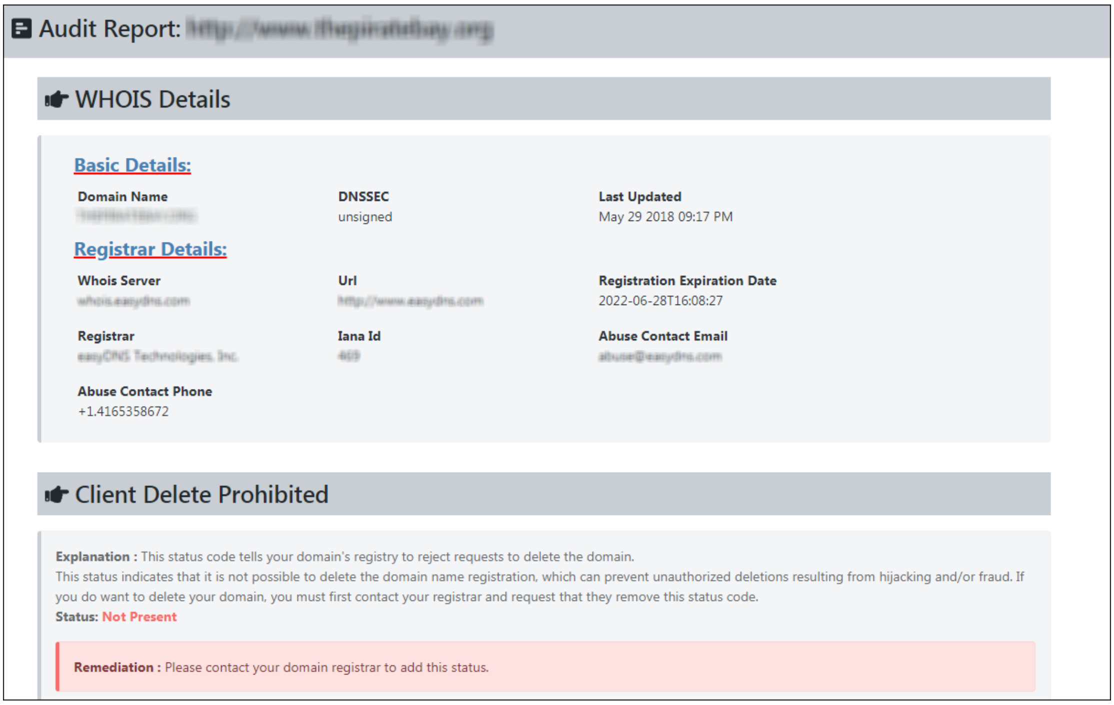
1. To add WHOIS audit, click **Add**.
   Links window appears.



2. Select domain from the dropdown menu.
3. Click **Start**. The WHOIS audit scan will be initiated.

Viewing a Report

To view a report of a particular domain, click on the 👁 icon on the **Result** column.



Audit Report: [redacted]

WHOIS Details

Basic Details:

Domain Name	DNSSEC	Last Updated
[redacted]	unsigned	May 29 2018 09:17 PM

Registrar Details:

Whois Server	Url	Registration Expiration Date
[redacted]	[redacted]	2022-06-28T16:08:27
Registrar	**Iana Id**	**Abuse Contact Email**
[redacted]	[redacted]	[redacted]
Abuse Contact Phone		
+1.4165358672		

Client Delete Prohibited

Explanation : This status code tells your domain's registry to reject requests to delete the domain.
This status indicates that it is not possible to delete the domain name registration, which can prevent unauthorized deletions resulting from hijacking and/or fraud. If you do want to delete your domain, you must first contact your registrar and request that they remove this status code.
Status: Not Present

Remediation : Please contact your domain registrar to add this status.

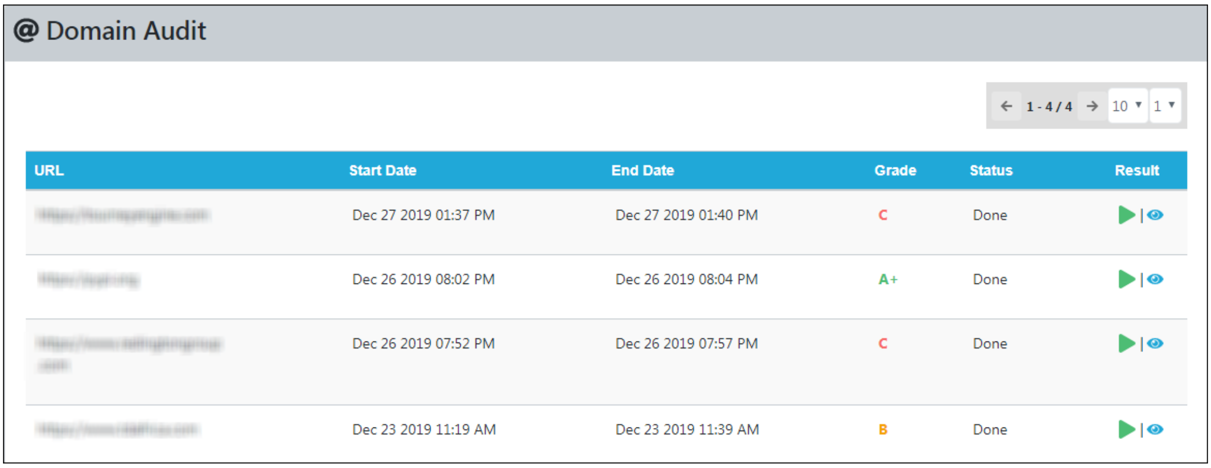
To export the audit report, click **Export** on the left-hand side corner. The report gets exported in HTML format.

Domain Audit

The Domain Audit service lets user to scan and generate the audit report of web pages of the domain along with Grade of the domain. The audit will consist summary of HTTP Response, Web Application Firewall (WAF), Server Signature, Content Encoding, and more. The Grade of the domain is based on the following rules:

- GDPR Security Analysis
- PCI DSS Security Analysis
- HTTP Headers Security Analysis
- Content Security Policy Analysis
- CMS Security Analysis

This module displays the **URL**, **Start Date**, **End Date**, **Grade**, **Status**, and **Result** of the audit.

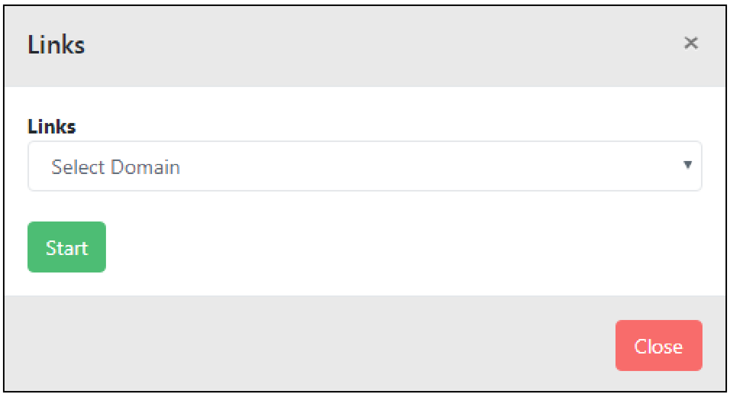


@ Domain Audit

URL	Start Date	End Date	Grade	Status	Result
[redacted]	Dec 27 2019 01:37 PM	Dec 27 2019 01:40 PM	C	Done	▶ | 👁
[redacted]	Dec 26 2019 08:02 PM	Dec 26 2019 08:04 PM	A+	Done	▶ | 👁
[redacted]	Dec 26 2019 07:52 PM	Dec 26 2019 07:57 PM	C	Done	▶ | 👁
[redacted]	Dec 23 2019 11:19 AM	Dec 23 2019 11:39 AM	B	Done	▶ | 👁

Adding a Domain Audit

1. To add Domain audit, click **Add**.
   Links window appears.



Links ×

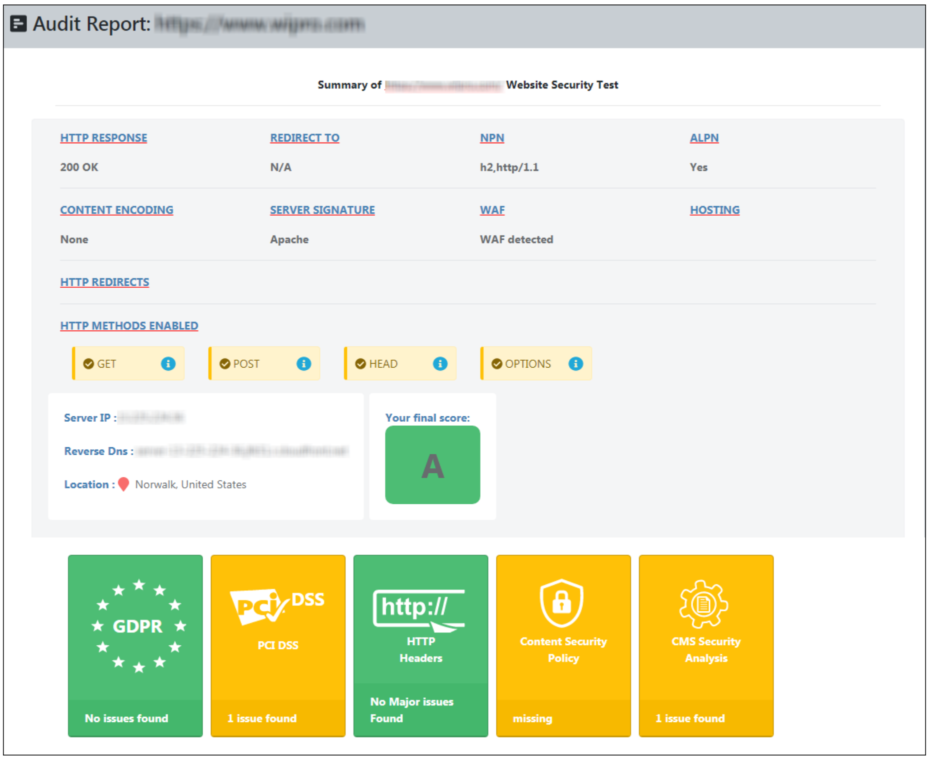
Links

Select Domain ▾

2. Select domain from the dropdown menu.
3. Click **Start**. The Domain audit scan will be initiated.

Viewing a Report

To view the audit report on the console, click 👁 icon on the **Result** column. To get more details on the vulnerabilities found, click ℹ icon on the console.



Audit Report: [redacted]

Summary of [redacted] Website Security Test

HTTP RESPONSE	REDIRECT TO	NPN	ALPN
200 OK	N/A	h2,http/1.1	Yes
CONTENT ENCODING	SERVER SIGNATURE	WAF	HOSTING
None	Apache	WAF detected	

HTTP REDIRECTS

HTTP METHODS ENABLED

✓ GET ℹ ✓ POST ℹ ✓ HEAD ℹ ✓ OPTIONS ℹ

Server IP : [redacted]

Reverse Dns : [redacted]

Location : Norwalk, United States

Your final score: A

GDPR	PCI DSS	HTTP Headers	Content Security Policy	CMS Security Analysis
No issues found	1 issue found	No Major issues Found	missing	1 issue found

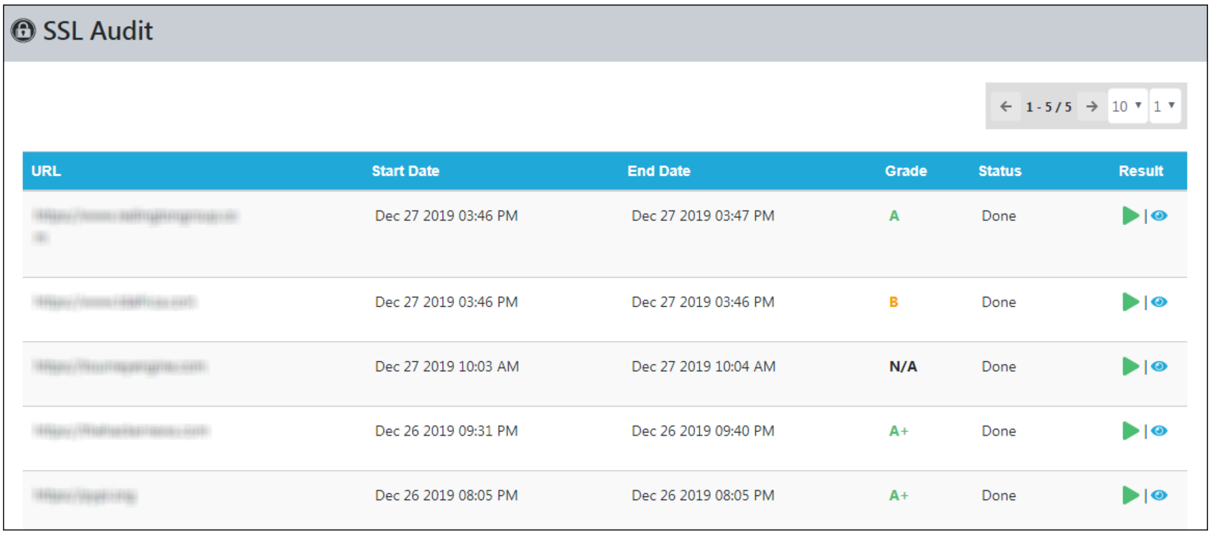
To export the audit report, click **Export** on the left-hand side corner. The report gets exported in HTML format.

SSL Audit

The SSL Audit service lets user to scan and generate the audit report of SSL for web servers. It does the deep analysis of the configuration of SSL certificate for the domain along with the detailed information about the security parameters.

Nemasis will check the latest vulnerabilities and misconfigurations in SSL settings. For example, certificate issuer, validity, algorithm used to sign, protocol details, cipher suites, handshake simulation, and more. It will also Grade the domain based on the vulnerabilities, misconfigurations, and so on.

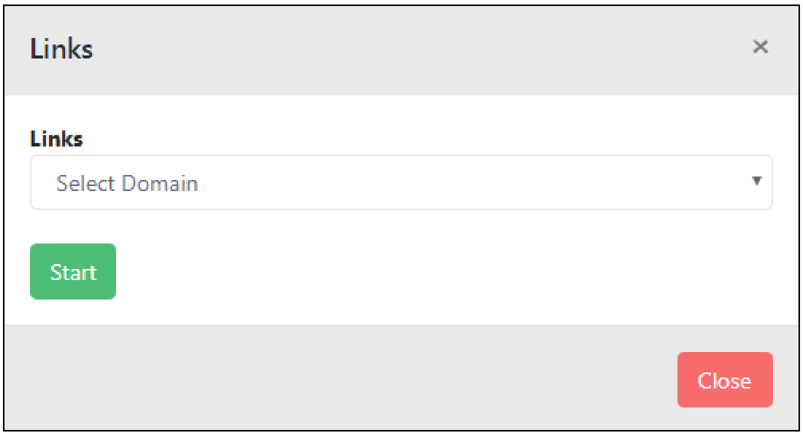
This module displays the **URL**, **Start Date**, **End Date, Grade**, **Status**, and **Result** of the audit.



URL	Start Date	End Date	Grade	Status	Result
[redacted]	Dec 27 2019 03:46 PM	Dec 27 2019 03:47 PM	A	Done	▶ | 👁
[redacted]	Dec 27 2019 03:46 PM	Dec 27 2019 03:46 PM	B	Done	▶ | 👁
[redacted]	Dec 27 2019 10:03 AM	Dec 27 2019 10:04 AM	N/A	Done	▶ | 👁
[redacted]	Dec 26 2019 09:31 PM	Dec 26 2019 09:40 PM	A+	Done	▶ | 👁
[redacted]	Dec 26 2019 08:05 PM	Dec 26 2019 08:05 PM	A+	Done	▶ | 👁

Adding a SSL Audit

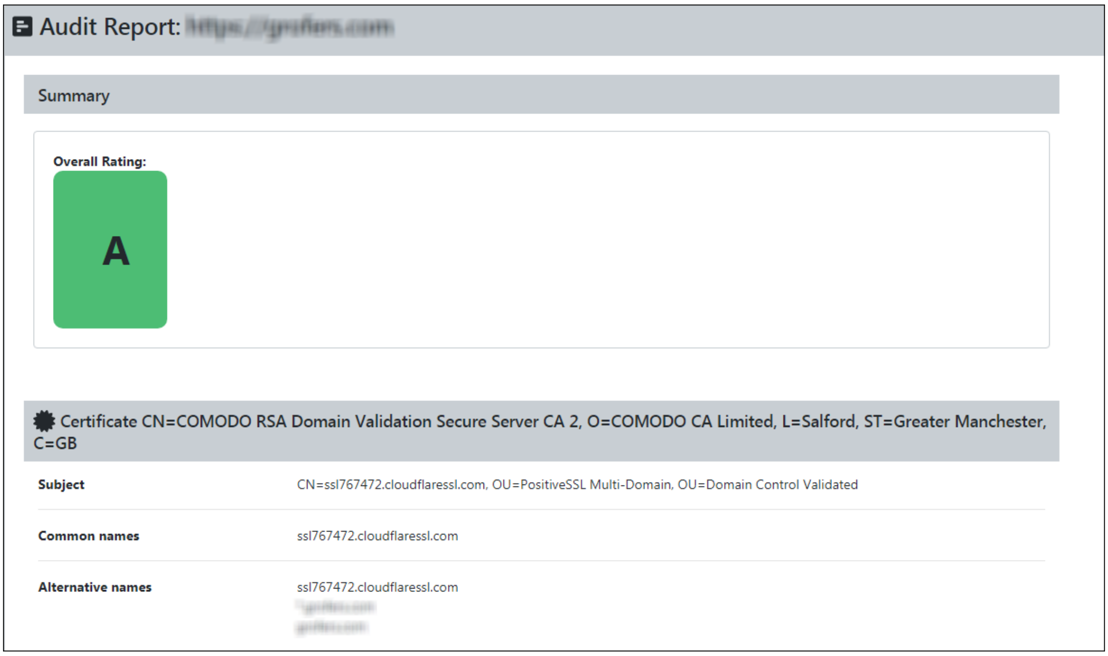
1. To add SSL audit, click **Add**.
   Links window appears.



2. Select domain from the dropdown menu.
3. Click **Start**. The SSL audit scan will be initiated.

Viewing a Report

To view the audit report on the console, click 👁 icon on the **Result** column.



Audit Report: [redacted]

Summary

Overall Rating:

A

Certificate CN=COMODO RSA Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB

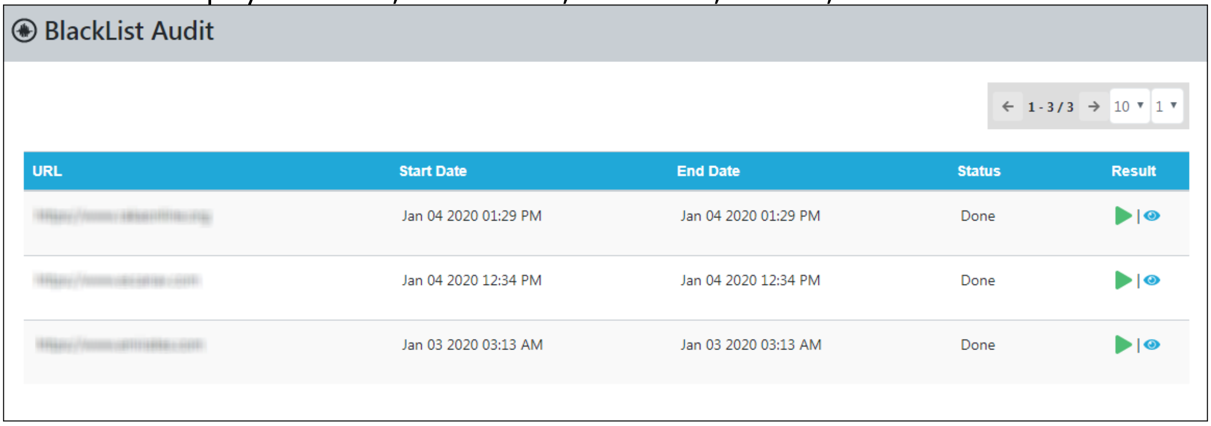
Subject	CN=ssl767472.cloudflaressl.com, OU=PositiveSSL Multi-Domain, OU=Domain Control Validated
Common names	ssl767472.cloudflaressl.com
Alternative names	ssl767472.cloudflaressl.com [redacted] [redacted]

To export the audit report, click **Export** on the left-hand side corner. The report gets exported in HTML format.

BlackList Audit

The BlackList Audit service lets user to scan and generate the audit report of DNS Real-time Blackhole List (RBL). Nemasis send the DNS queries and gathers data. It will then test the server's IP address over multiple DNS based email blacklists.

This module displays the **URL**, **Start Date**, **End Date**, **Status**, and **Result** of the audit.

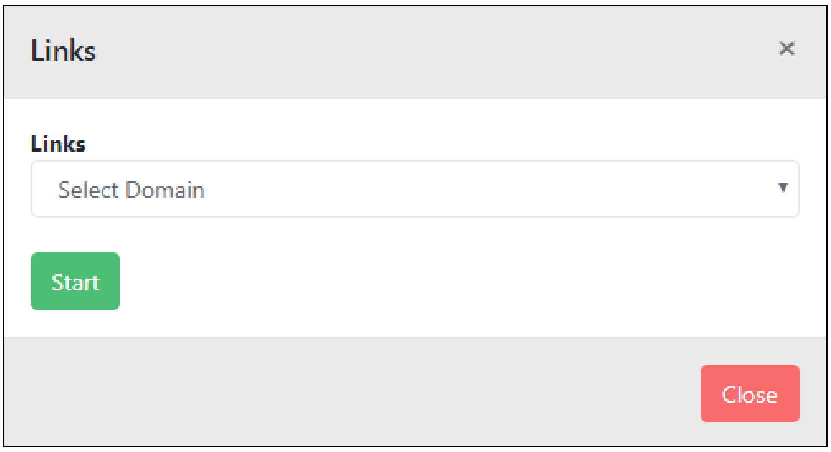


BlackList Audit

URL	Start Date	End Date	Status	Result
[redacted]	Jan 04 2020 01:29 PM	Jan 04 2020 01:29 PM	Done	▶ | 👁
[redacted]	Jan 04 2020 12:34 PM	Jan 04 2020 12:34 PM	Done	▶ | 👁
[redacted]	Jan 03 2020 03:13 AM	Jan 03 2020 03:13 AM	Done	▶ | 👁

Adding a BlackList Audit

1. To add a BlackList audit, click **Add**.
   Links window appears.



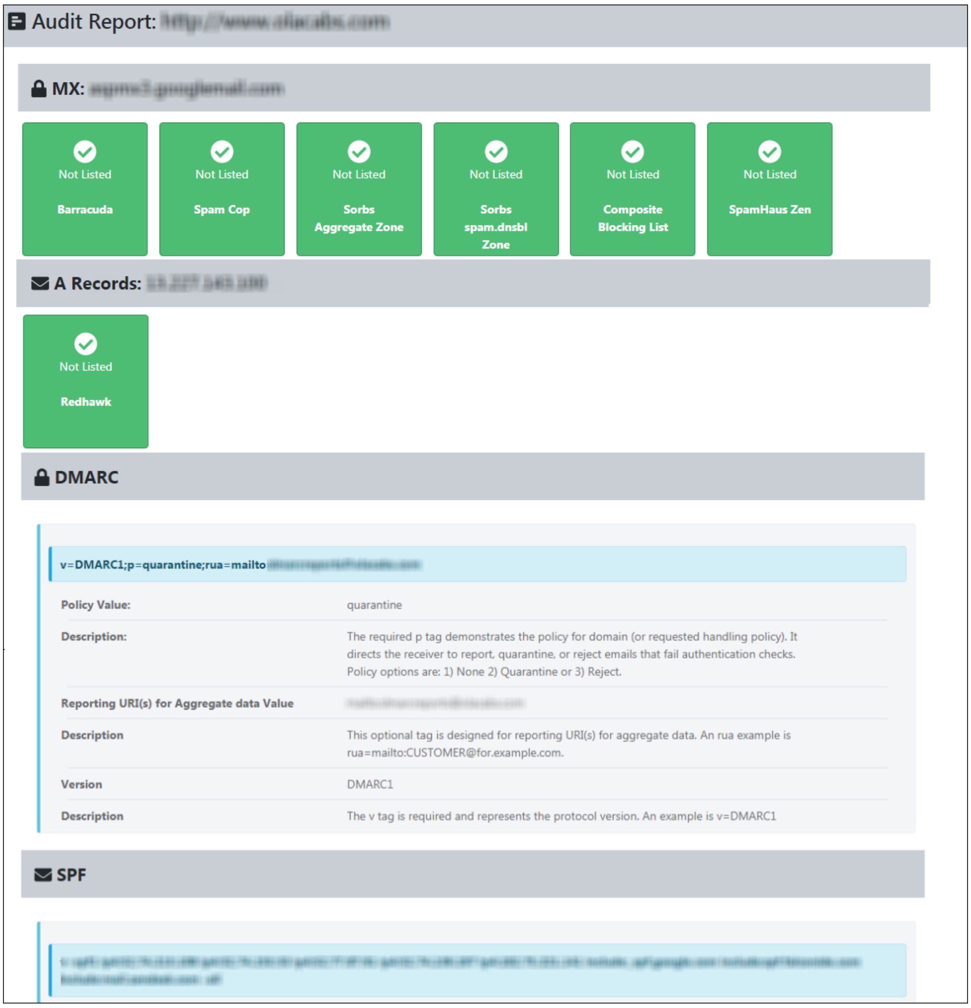
2. Select domain from the dropdown menu.
3. Click **Start**. The BlackList audit scan will be initiated.

Viewing a Report

To view the audit report, click 👁 on the **Result** column. This will have following tabs:

- MX Records
- A Records
- DMARC
- SPF
- Open Relay
- TLS
- PTR

By analyzing DMARC data, user can view sources are sending on behalf of your domain, and also ensures that all the legitimate sending sources are compliant with SPF, DKIM, and DMARC that have a positive impact on email delivery. Using Nemasis, with a single click you will get information from more than 150 blacklists on whether the domain is blacklisted or not.



Audit Report: [redacted]

MX: [redacted]

✓ Not Listed Barracuda

✓ Not Listed Spam Cop

✓ Not Listed Sorbs Aggregate Zone

✓ Not Listed Sorbs spam.dnsbl Zone

✓ Not Listed Composite Blocking List

✓ Not Listed SpamHaus Zen

A Records: [redacted]

✓ Not Listed Redhawk

DMARC

v=DMARC1;p=quarantine;rua=mailto [redacted]

Policy Value:	quarantine
Description:	The required p tag demonstrates the policy for domain (or requested handling policy). It directs the receiver to report, quarantine, or reject emails that fail authentication checks. Policy options are: 1) None 2) Quarantine or 3) Reject.
Reporting URI(s) for Aggregate data Value	[redacted]
Description	This optional tag is designed for reporting URI(s) for aggregate data. An rua example is rua=mailto:CUSTOMER@for.example.com.
Version	DMARC1
Description	The v tag is required and represents the protocol version. An example is v=DMARC1

SPF

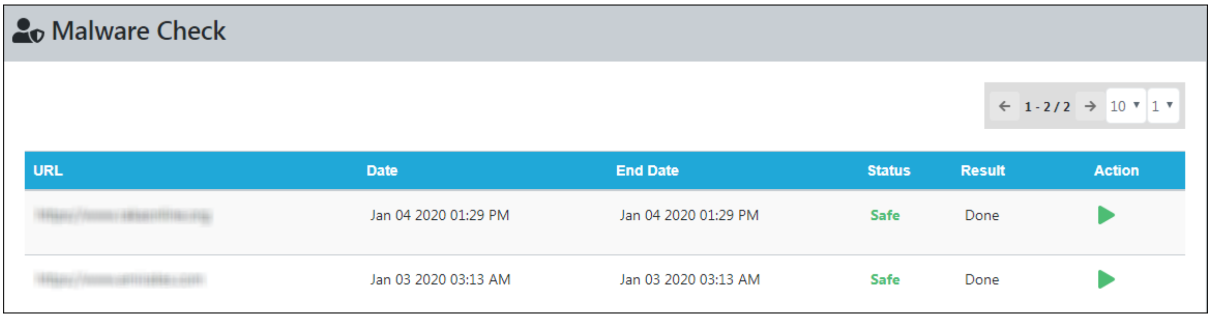
[redacted]

To export the audit report, click **Export** on the left-hand side corner. The report gets exported in HTML format.

Malware Check

Nemasis Malware Check helps to find out "is the site safe". This helps to find if your domains are unsafe and having malicious content, which can harm you by stealing and using sensitive information for phishing.

This module displays the **URL**, **Start Date**, **End Date**, **Status**, **Result**, and **Action** of the audit.

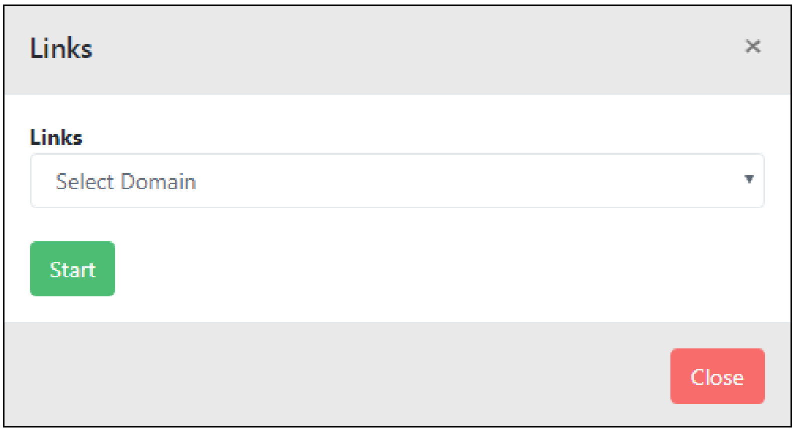


Malware Check

URL	Date	End Date	Status	Result	Action
[redacted]	Jan 04 2020 01:29 PM	Jan 04 2020 01:29 PM	Safe	Done	▶
[redacted]	Jan 03 2020 03:13 AM	Jan 03 2020 03:13 AM	Safe	Done	▶

Adding a Malware Check

1. To add a Malware Check, click **Add**.
   Links window appears.



Links

Links: Select Domain ▾

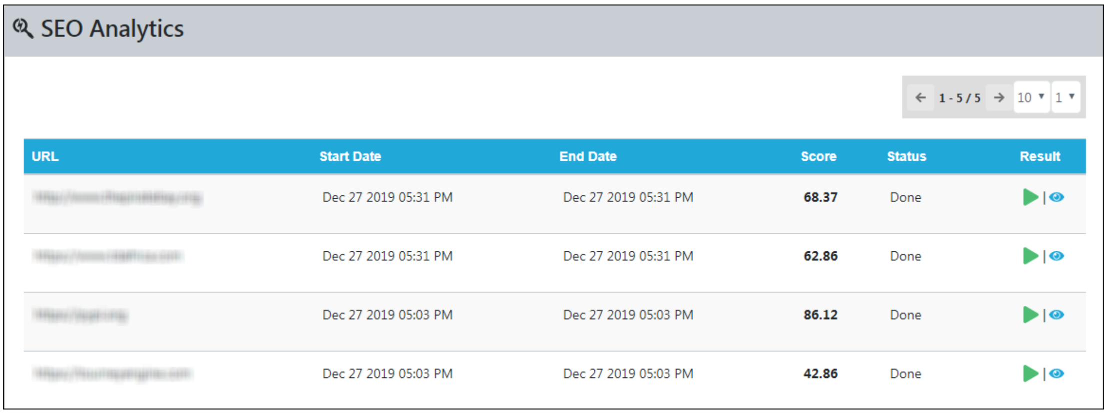
2. Select domain from the dropdown menu.
3. Click **Start**. The Malware check will be initiated.

SEO Analytics

SEO is required to rank your domain higher, extend the reach, drive traffic, and achieve the business goals. Nemasis SEO Analytics tests your website based on performance such as request, speed, SEO matrics, and more. It will also check if your website is mobile-friendly in terms of responsiveness and viewport settings.

Nemasis will check content of the website through factors like page titles and meta descriptions. It will also check the SSL certificates. This serves as a way to prove to visitors that your site is both authentic and safe for contact information submissions. Each report consists of Basic Info, Mobile, Backlinks, Social Presence, Branding, Security, Indexing, Content, Technologies, and Performance sections.

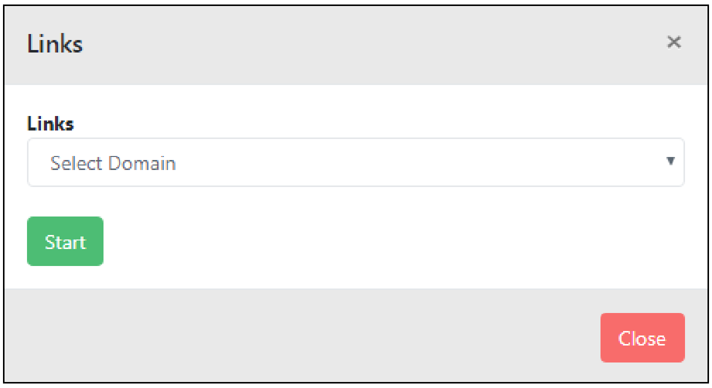
This module displays the **URL**, **Start Date**, **End Date**, **Score, Status**, and **Result** of the analysis.



URL	Start Date	End Date	Score	Status	Result
[redacted]	Dec 27 2019 05:31 PM	Dec 27 2019 05:31 PM	68.37	Done	▶ | 👁
[redacted]	Dec 27 2019 05:31 PM	Dec 27 2019 05:31 PM	62.86	Done	▶ | 👁
[redacted]	Dec 27 2019 05:03 PM	Dec 27 2019 05:03 PM	86.12	Done	▶ | 👁
[redacted]	Dec 27 2019 05:03 PM	Dec 27 2019 05:03 PM	42.86	Done	▶ | 👁

Adding a SEO Analytics

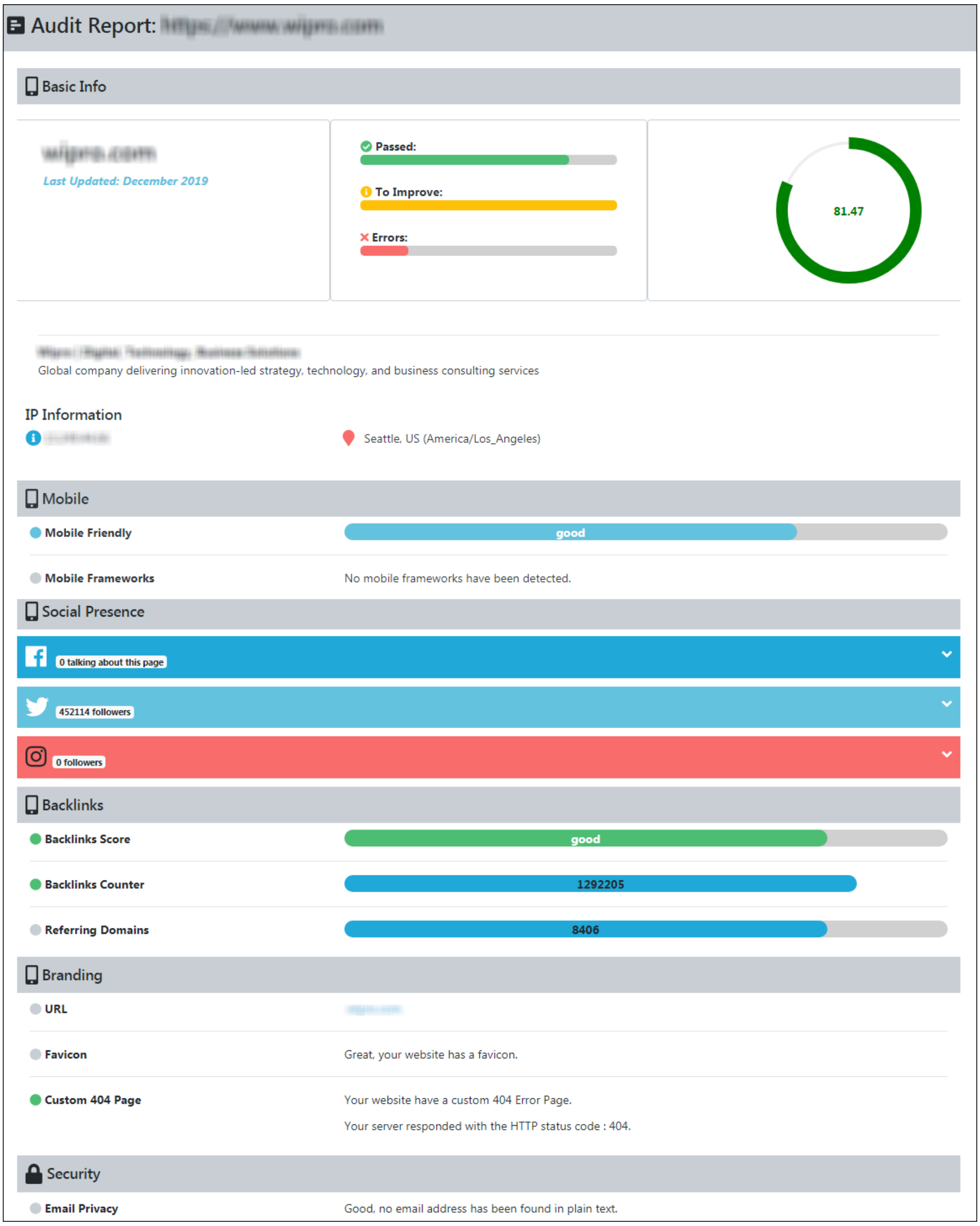
1. To add a SEO Analytics, click **Add**.
   Links window appears.



2. Select domain the dropdown menu.
3. Click **Start**. The SEO audit scan will be initiated.

Viewing a Report

To view the audit report of a particular domain, click on the 👁 icon on the **Result** column. To get more details on the vulnerabilities found, click ℹ icon on the console.



Audit Report: [redacted]

Basic Info

[redacted]
Last Updated: December 2019

✓ Passed:
❗ To Improve:
✕ Errors:

[redacted]
Global company delivering innovation-led strategy, technology, and business consulting services

IP Information
ℹ [redacted]
Seattle, US (America/Los_Angeles)

Mobile

● Mobile Friendly	good
● Mobile Frameworks	No mobile frameworks have been detected.

Social Presence

0 talking about this page

452114 followers

0 followers

Backlinks

● Backlinks Score	good
● Backlinks Counter	1292205
● Referring Domains	8406

Branding

● URL	[redacted]
● Favicon	Great, your website has a favicon.
● Custom 404 Page	Your website have a custom 404 Error Page. Your server responded with the HTTP status code : 404.

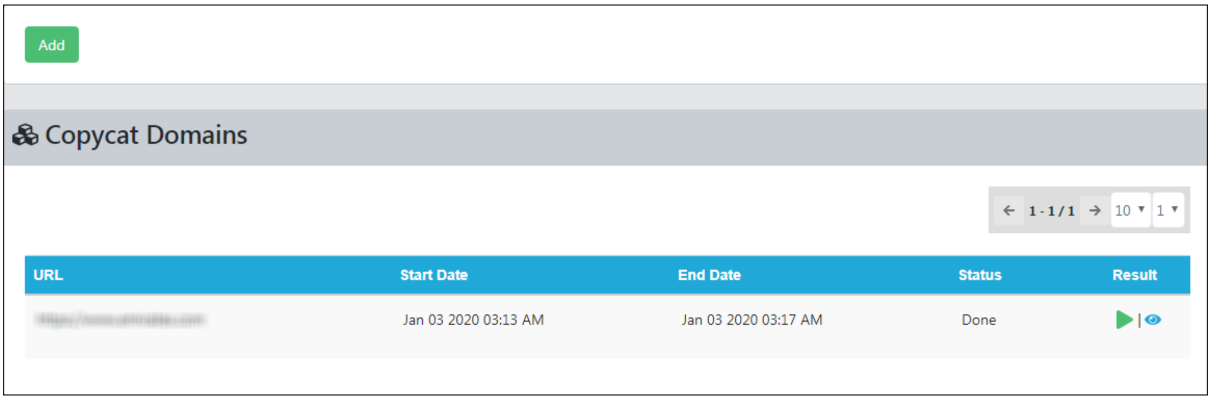
Security

● Email Privacy	Good, no email address has been found in plain text.

To export the audit report, click **Export** on the left-hand side corner. The report gets exported in HTML format.

Copycat Domains

The **Copycat Domains** service scans the domain and look for all the similar domain names. This will help to find out the phishing domains that might be similar to your domain.
This module displays the **URL**, **Start Date**, **End Date**, **Status**, and **Result** of the analysis.



Add

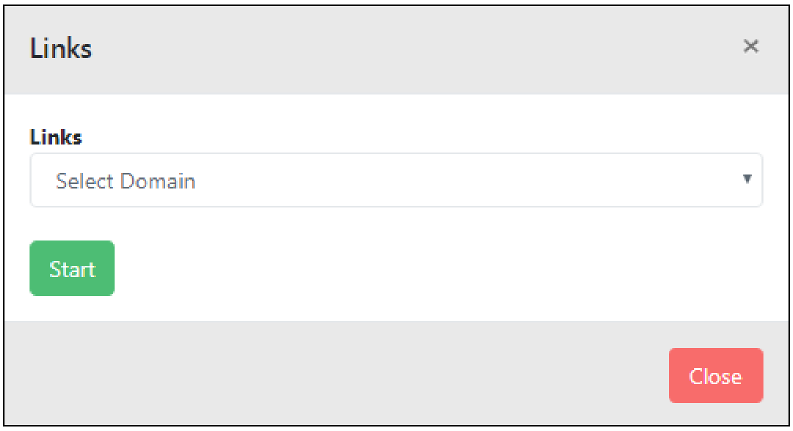
Copycat Domains

← 1 - 1 / 1 → 10 ▾ 1 ▾

URL	Start Date	End Date	Status	Result
[redacted]	Jan 03 2020 03:13 AM	Jan 03 2020 03:17 AM	Done	▶ | 👁

Adding a Copycat Domains

1. To add a Copycat Domains, click **Add**.
   Links window appears.



Links ×

Links

Select Domain ▾

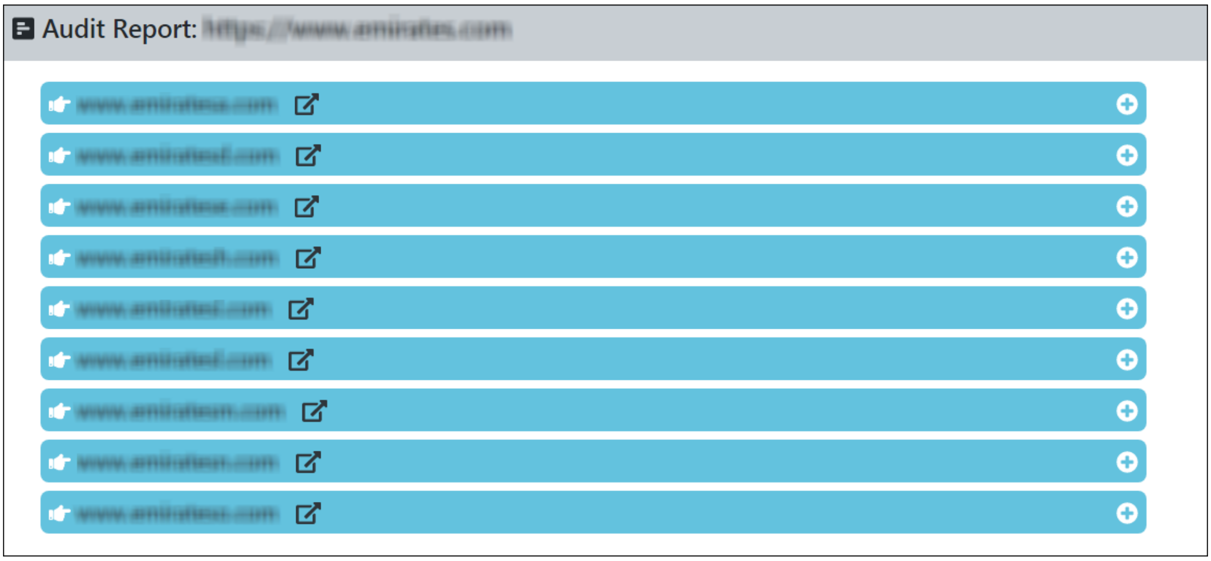
Start

Close

2. Select domain the dropdown menu.
3. Click **Start**. The Copycat Domains scan will be initiated.

Viewing a Report

To view the audit report of a particular domain, click on the 👁 icon on the **Result** column.



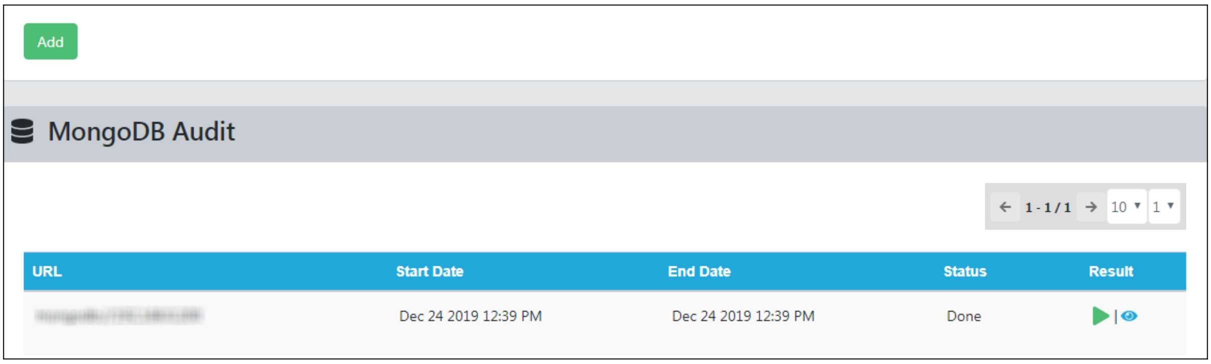
Audit Report: [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

To export the audit report, click **Export** on the left-hand side corner. The report gets exported in HTML format.

MongoDB Audit

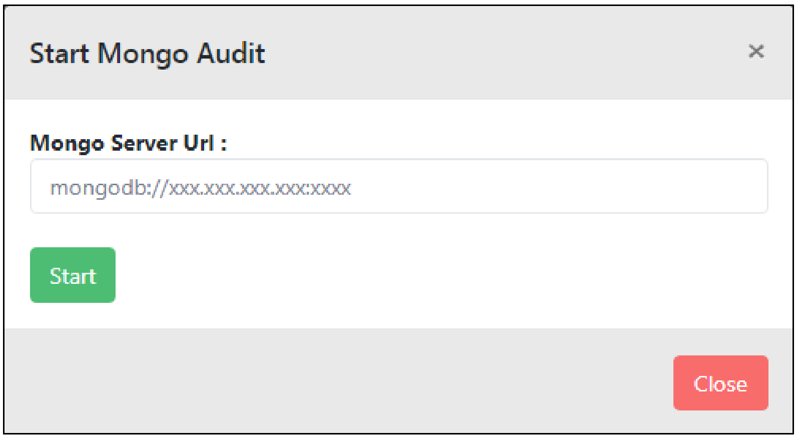
The MongoDB Audit service lets users to scan and generate an audit report of Mongo Server, which helps to strengthen the security of MongoDB. This will scan all the security issues, misconfigurations, and standard protocols of the Mongo servers.
This module displays the **URL**, **Start Date**, **End Date**, **Status**, and **Result** of the analysis.



URL	Start Date	End Date	Status	Result
[redacted]	Dec 24 2019 12:39 PM	Dec 24 2019 12:39 PM	Done	▶ | 👁

Adding a MongoDB Audit

1. To add a MongoDB audit, click **Add**.
   Start MongoDB Audit appears.

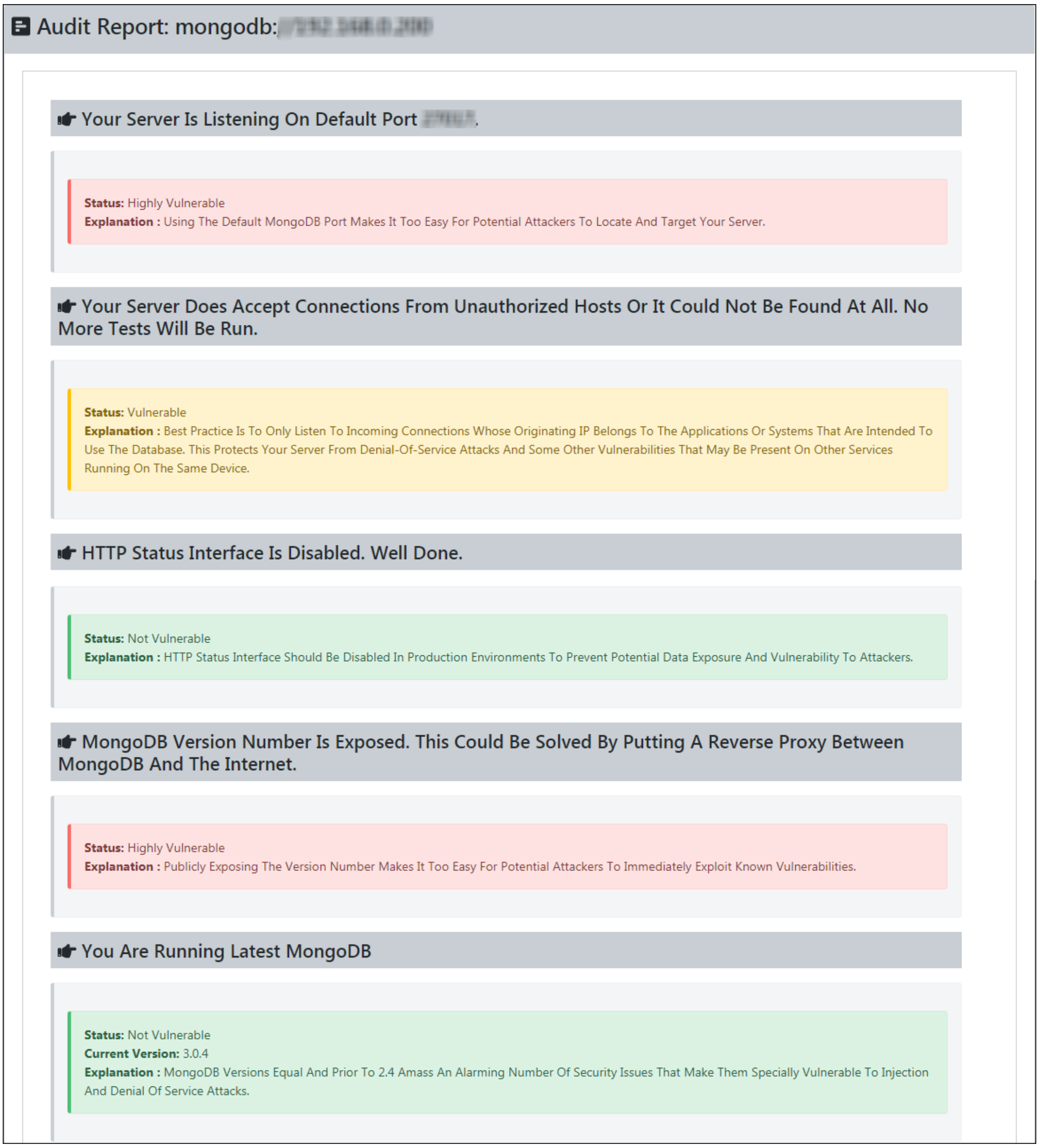

Start Mongo Audit

Mongo Server Url : mongodb://xxx.xxx.xxx.xxx:xxxx

2. Enter **Mongo Server Url**.
3. Click **Start**. The Mongo audit scan will be initiated.

Viewing a Report

To view the audit report of a particular Mongo server, click on the 👁 icon on the **Result** column.



Audit Report: mongodb:[redacted]

Your Server Is Listening On Default Port [redacted].

Status: Highly Vulnerable
Explanation : Using The Default MongoDB Port Makes It Too Easy For Potential Attackers To Locate And Target Your Server.

Your Server Does Accept Connections From Unauthorized Hosts Or It Could Not Be Found At All. No More Tests Will Be Run.

Status: Vulnerable
Explanation : Best Practice Is To Only Listen To Incoming Connections Whose Originating IP Belongs To The Applications Or Systems That Are Intended To Use The Database. This Protects Your Server From Denial-Of-Service Attacks And Some Other Vulnerabilities That May Be Present On Other Services Running On The Same Device.

HTTP Status Interface Is Disabled. Well Done.

Status: Not Vulnerable
Explanation : HTTP Status Interface Should Be Disabled In Production Environments To Prevent Potential Data Exposure And Vulnerability To Attackers.

MongoDB Version Number Is Exposed. This Could Be Solved By Putting A Reverse Proxy Between MongoDB And The Internet.

Status: Highly Vulnerable
Explanation : Publicly Exposing The Version Number Makes It Too Easy For Potential Attackers To Immediately Exploit Known Vulnerabilities.

You Are Running Latest MongoDB

Status: Not Vulnerable
Current Version: 3.0.4
Explanation : MongoDB Versions Equal And Prior To 2.4 Amass An Alarming Number Of Security Issues That Make Them Specially Vulnerable To Injection And Denial Of Service Attacks.

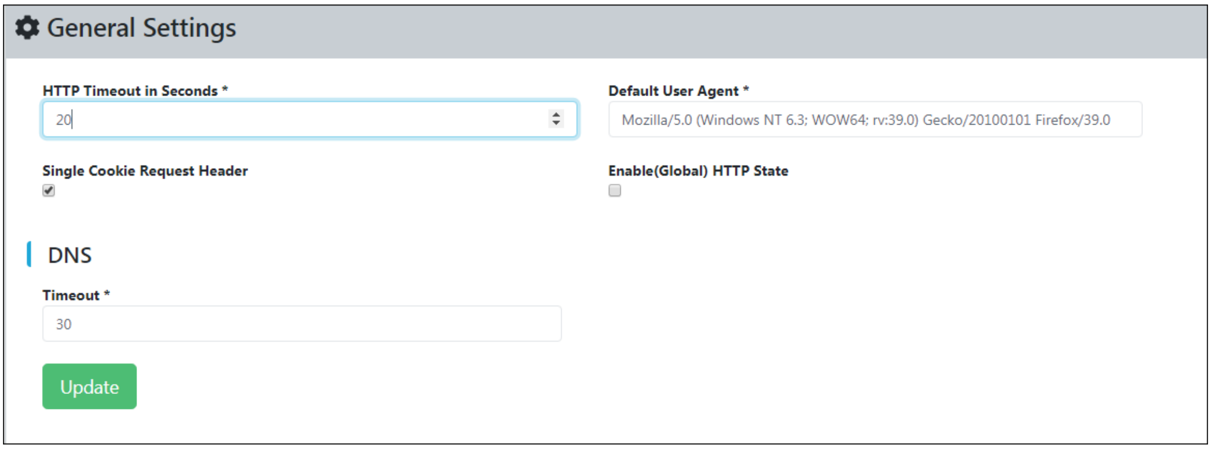
To export the audit report, click **Export** on the left-hand side corner. The report gets exported in HTML format.

General Config

The General Config module contains **General Setting**, **Proxy Setting**, **Context**, **Anti-CSRF Tokens**, and **SMTP** submodules.

General Setting

The **General Setting** submodule allows you to update timeout, name of the default user, single cookie request (Enable/Disable), HTTP state (Enable/Disable), and Time to Live (TTL) setting for DNS.



General Settings

HTTP Timeout in Seconds *: 20

Default User Agent *: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0

Single Cookie Request Header ☑

Enable(Global) HTTP State □

DNS

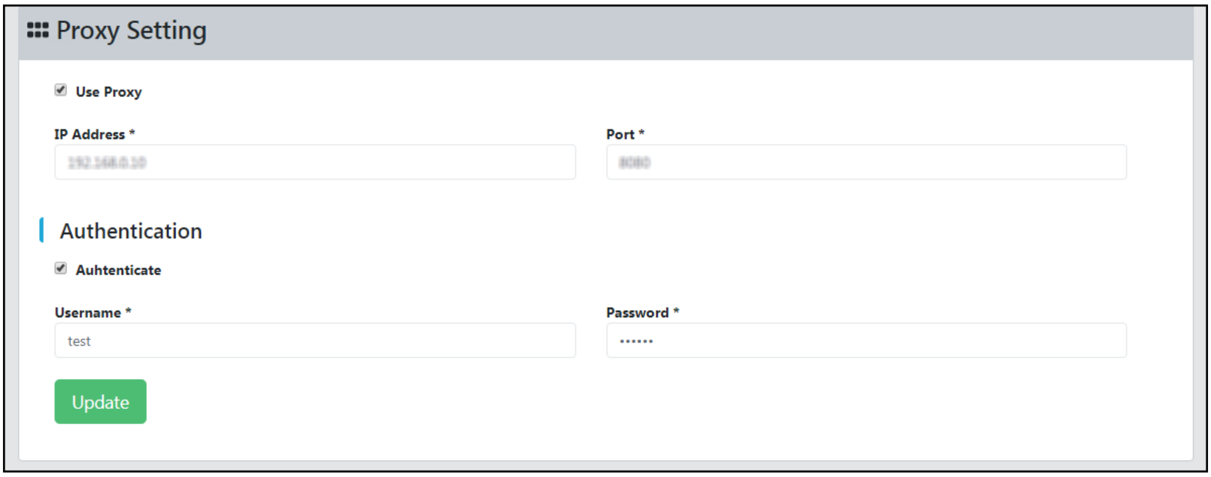
Timeout *: 30

By default, **Timeout in seconds** is set to 20 seconds and **TTL Successful Queries** for DNS is set to 30 seconds. Also, Single Cookie request header is enabled by default.

Proxy Setting

Proxy setting is a way of being anonymous on the internet or to access information that is not accessible in your country/region. Though it won't make you 100% anonymous, it still protects your identity. Proxies are just IP addresses of different machines in different regions that pass your request and make the content available to you.

The Proxy Setting submodule allows you to update the proxy IP address and port. You can also add authentication setting such as **Authenticate Outgoing Proxy Server**, **Prompt for credentials**, add **IP / Domain**, **Username**, and **Password**.



Proxy Setting

☑ Use Proxy

IP Address * [redacted]

Port * [redacted]

Authentication

☑ Auhtenticate

Username * test

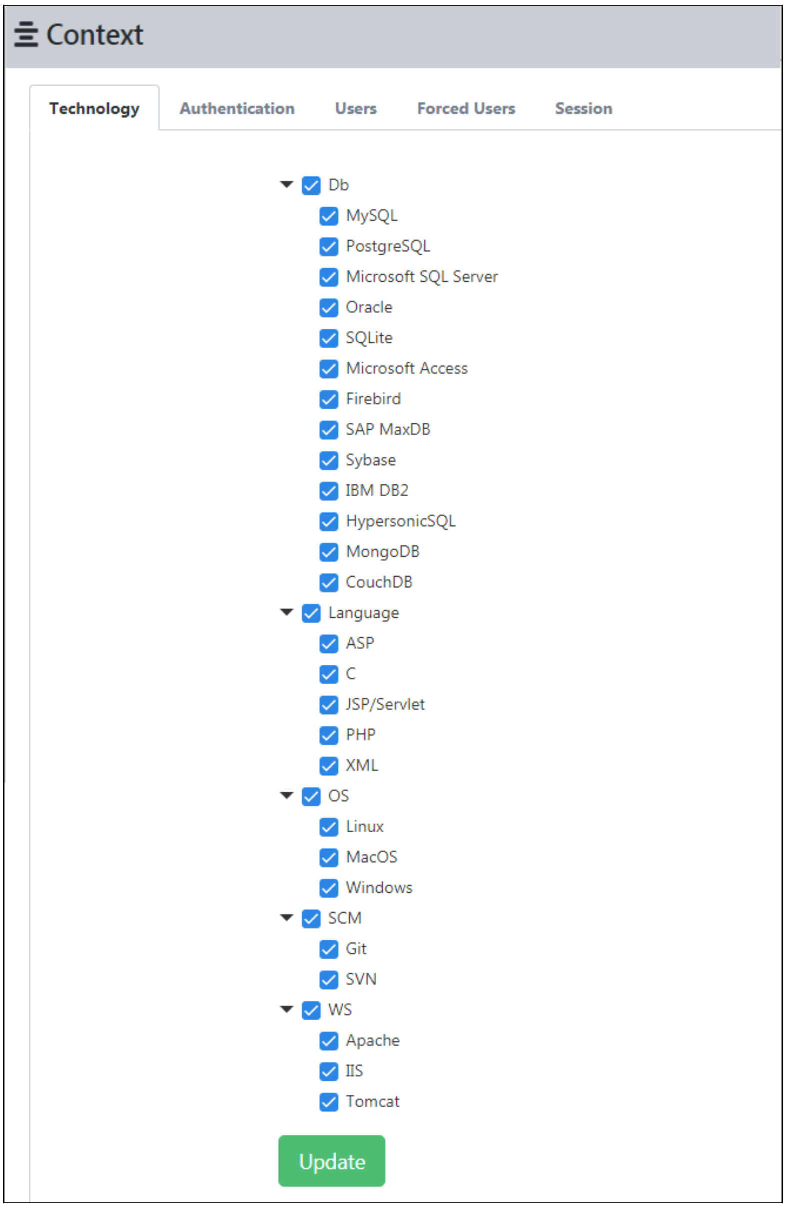
Password * ••••••

Context

Context should be defined as per your specific need but it should correspond to your web application. Define different context for each web application to create a new testing system and also to set a scope where you can test each one of them accordingly.

Technology

This tab enables you to specify the technology used in the context (if known). All the technologies are included by default. You can speed up the active scanning by excluding the technologies (if known) that are not used in the context. It has different types of technology used for web applications like database, language, OS, web servers, and many more.



Context

Technology | Authentication | Users | Forced Users | Session

- ☑ Db
  - ☑ MySQL
  - ☑ PostgreSQL
  - ☑ Microsoft SQL Server
  - ☑ Oracle
  - ☑ SQLite
  - ☑ Microsoft Access
  - ☑ Firebird
  - ☑ SAP MaxDB
  - ☑ Sybase
  - ☑ IBM DB2
  - ☑ HypersonicSQL
  - ☑ MongoDB
  - ☑ CouchDB
- ☑ Language
  - ☑ ASP
  - ☑ C
  - ☑ JSP/Servlet
  - ☑ PHP
  - ☑ XML
- ☑ OS
  - ☑ Linux
  - ☑ MacOS
  - ☑ Windows
- ☑ SCM
  - ☑ Git
  - ☑ SVN
- ☑ WS
  - ☑ Apache
  - ☑ IIS
  - ☑ Tomcat

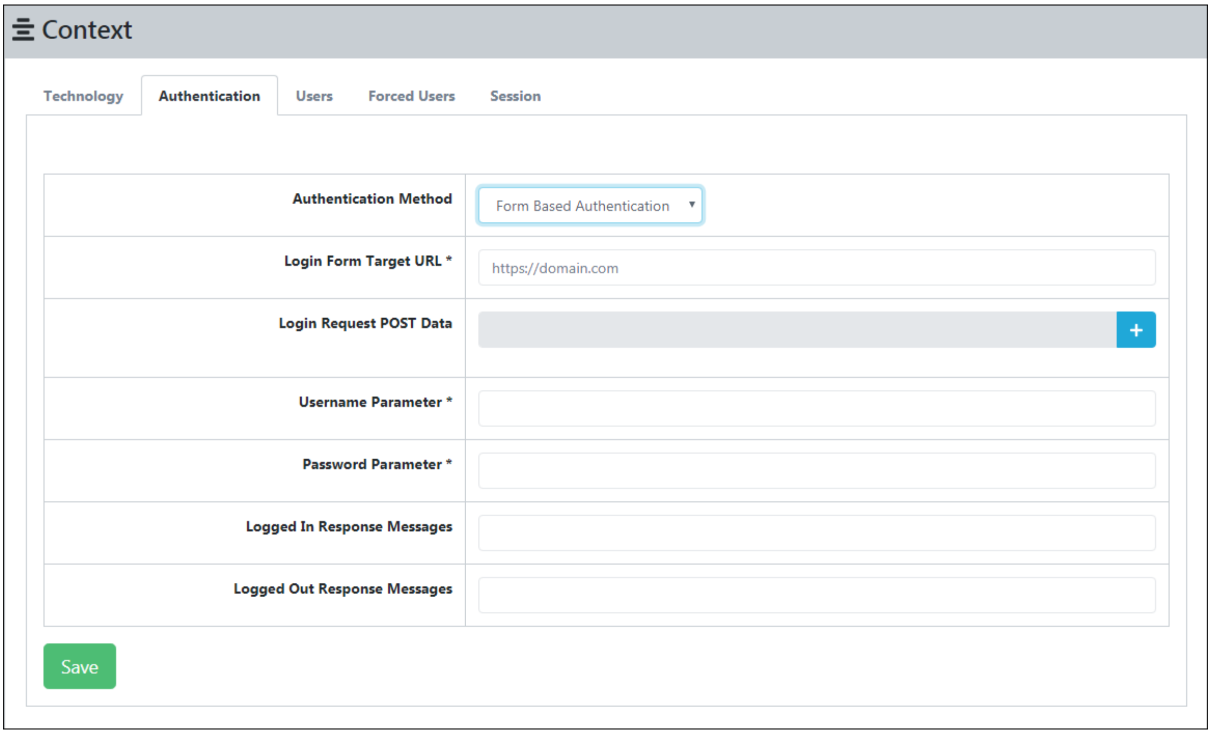
Authentication

This tab allows you to configure the authentication for the context. By selecting an authentication method you can configure the options present in specific authentication method. There are following types of authentications:

- **Form Based Authentication**
- **HTTP Authentication**

Form Based Authentication

Enter the login URL and the parameter supplied to the username and password to which login request is performed. If Login Request POST Data is entered, then the login request is performed as an HTTP POST, otherwise it is performed as an HTTP GET.



Context

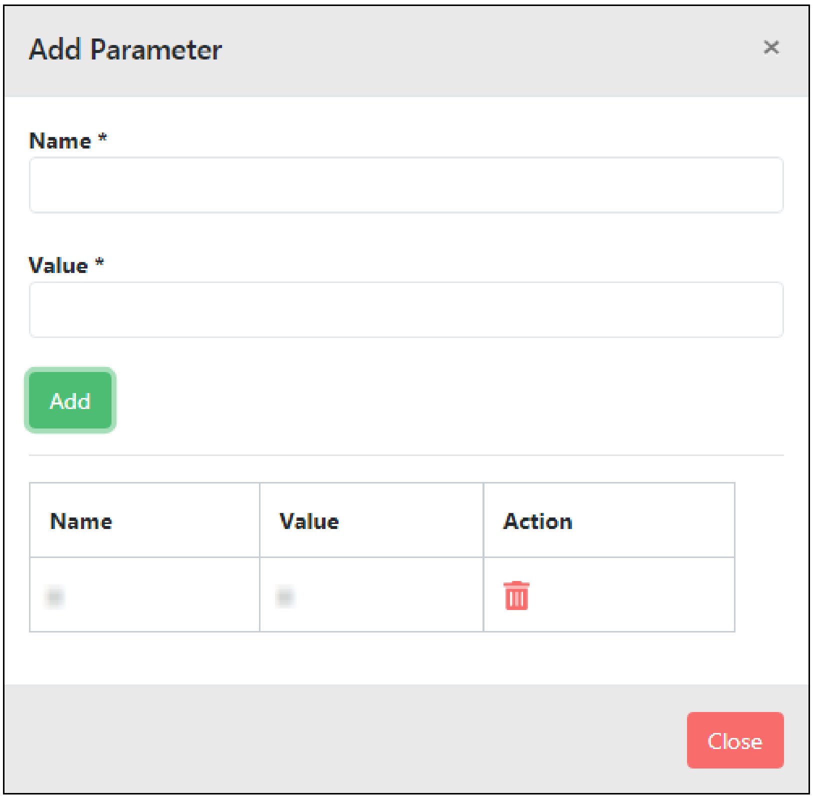
Technology | Authentication | Users | Forced Users | Session

Authentication Method	Form Based Authentication ▾
Login Form Target URL *	https://domain.com
Login Request POST Data	+
Username Parameter *	
Password Parameter *	
Logged In Response Messages	
Logged Out Response Messages	

Save

To add **Login Request POST Data**, follow the steps given below:

1. Click +.
   Add Parameter window appears.
2. Enter **Name** and **Value** for your post data.
3. After entering the details, click **Add.**



Add Parameter ×

Name *

Value *

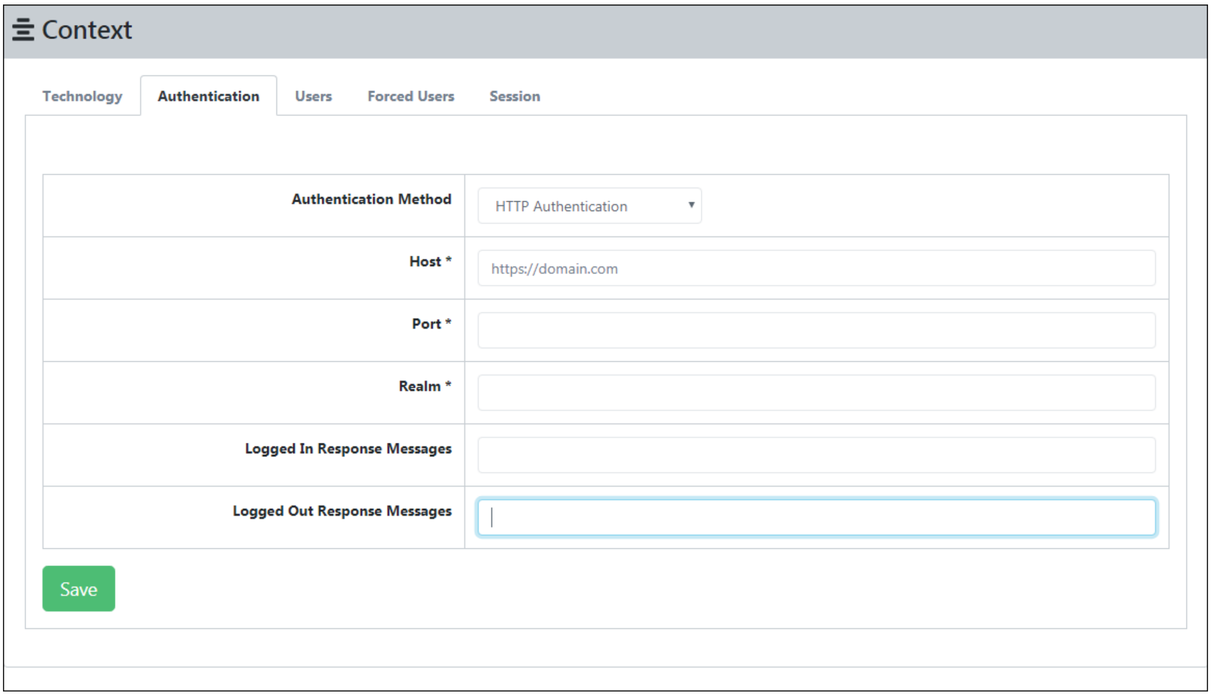
Name	Value	Action
[illegible]	[illegible]	🗑

Note	You can add maximum of 3 parameters in the **Login Request POST Data.**

To delete a parameter, click 🗑.

HTTP Authentication

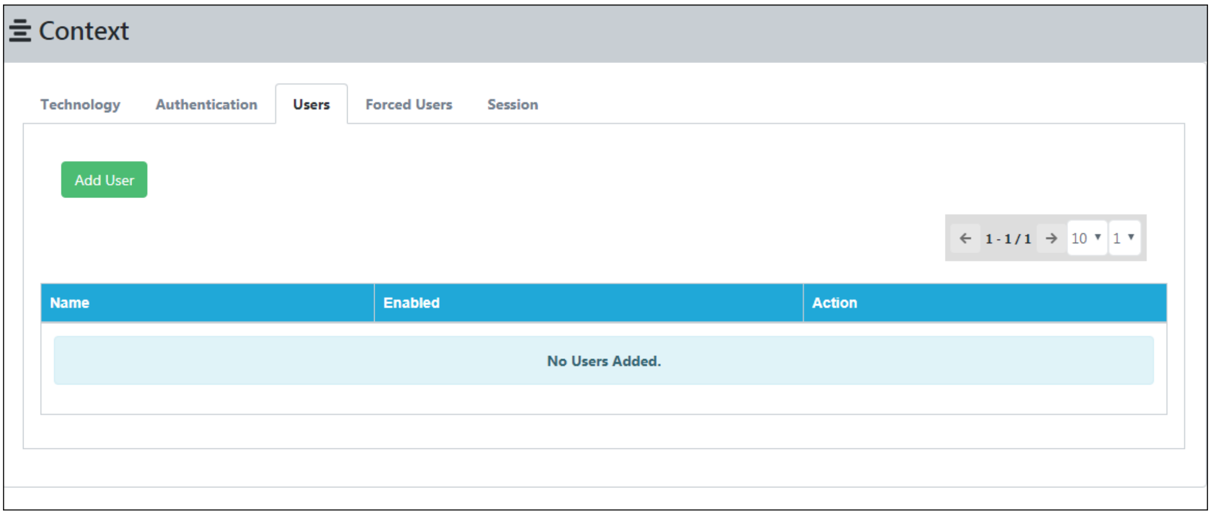
This method is to authenticate HTTP by means of HTTP message headers. You can configure it by entering Host, Port, and Realm the credentials along with login and logout message.



Authentication Method	HTTP Authentication
Host *	https://domain.com
Port *	
Realm *	
Logged In Response Messages	
Logged Out Response Messages	

Users

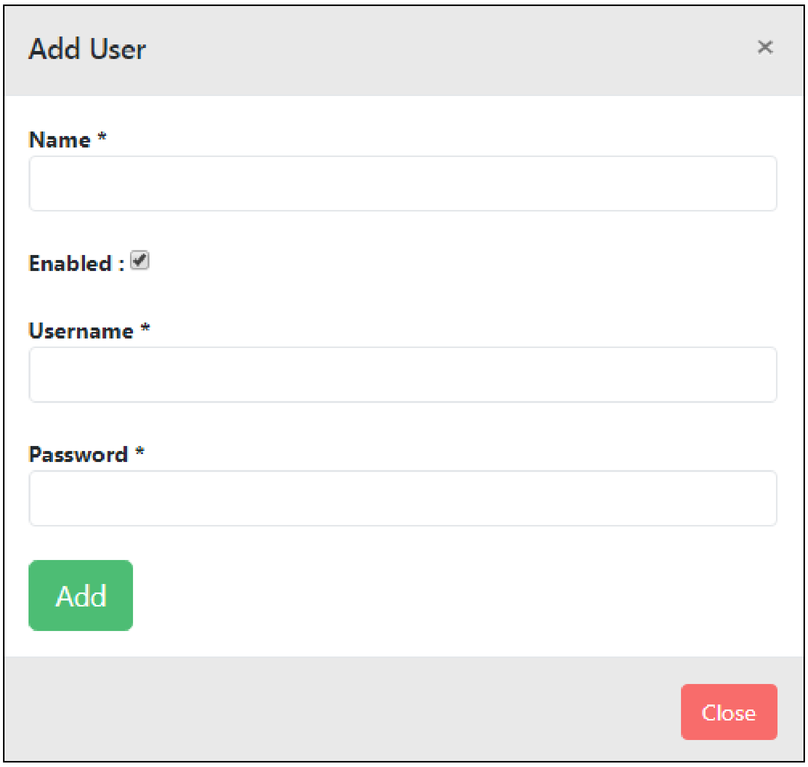
This tab enables you to add users that can be used throughout the application for different activities.



Name	Enabled	Action
No Users Added.		

Adding a User

1. To add a User, click **Add**.
   Add User window appears.

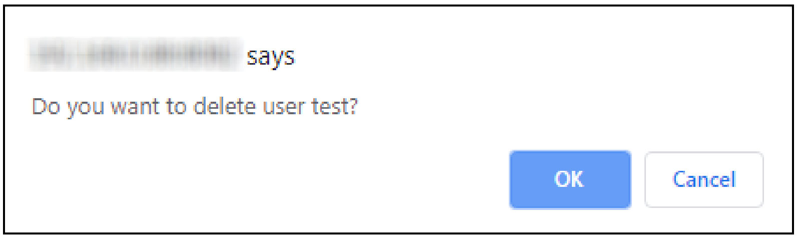


2. Enter the details for **Name**, **Username**, and **Password** field.
3. Click **Add.** The user will be added to the list.

Deleting a User

To delete a User, follow the steps given below:

1. In the Actions column, click 🗑.
   A delete confirmation prompt appears.



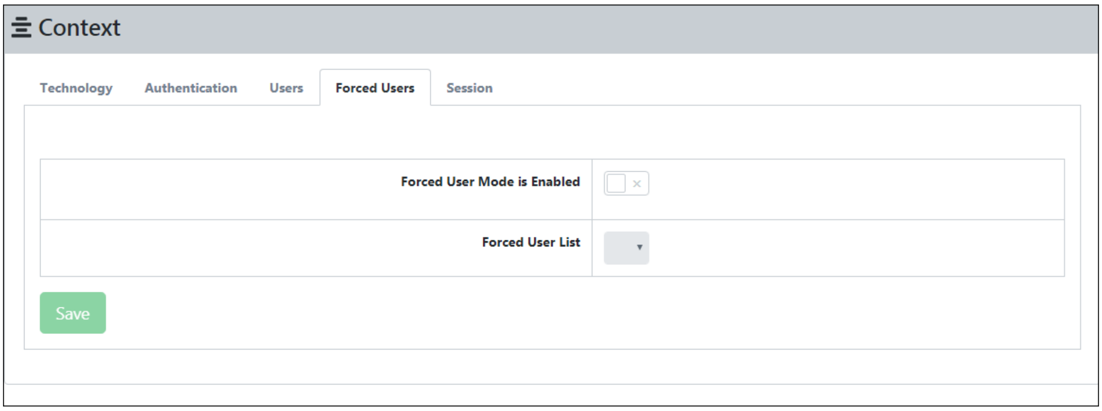
[redacted] says

Do you want to delete user test?

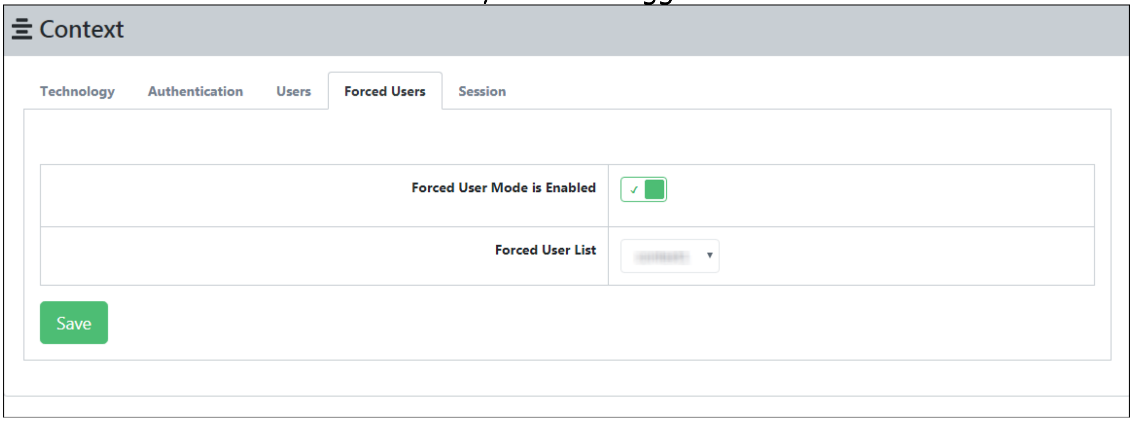
2. Click **OK**. The user will be deleted.

Forced Users

This tab lets you enable the forced user mode that allows the user to login into your web applications forcefully while performing a scan.



1. To enable the Forced User Mode, click the toggle.

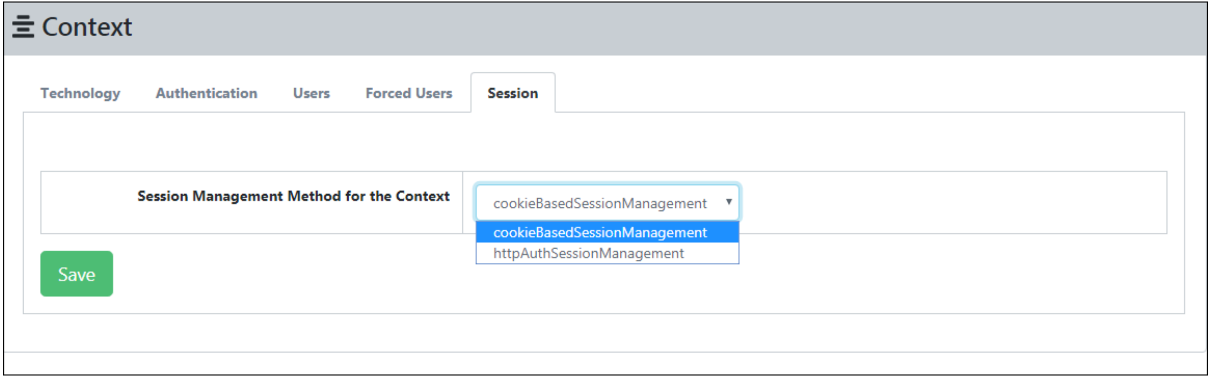


2. Forced User List gets enabled. Select the user from the dropdown menu. Click **Save**.

Note	**Forced User** option can be enabled only if a user in the Users tab is in enabled state.

Session

This tab allows you to manage context Session Management. On the Session tab you can select the Session Management method.



Session Management Method for the Context: cookieBasedSessionManagement

cookieBasedSessionManagement
httpAuthSessionManagement

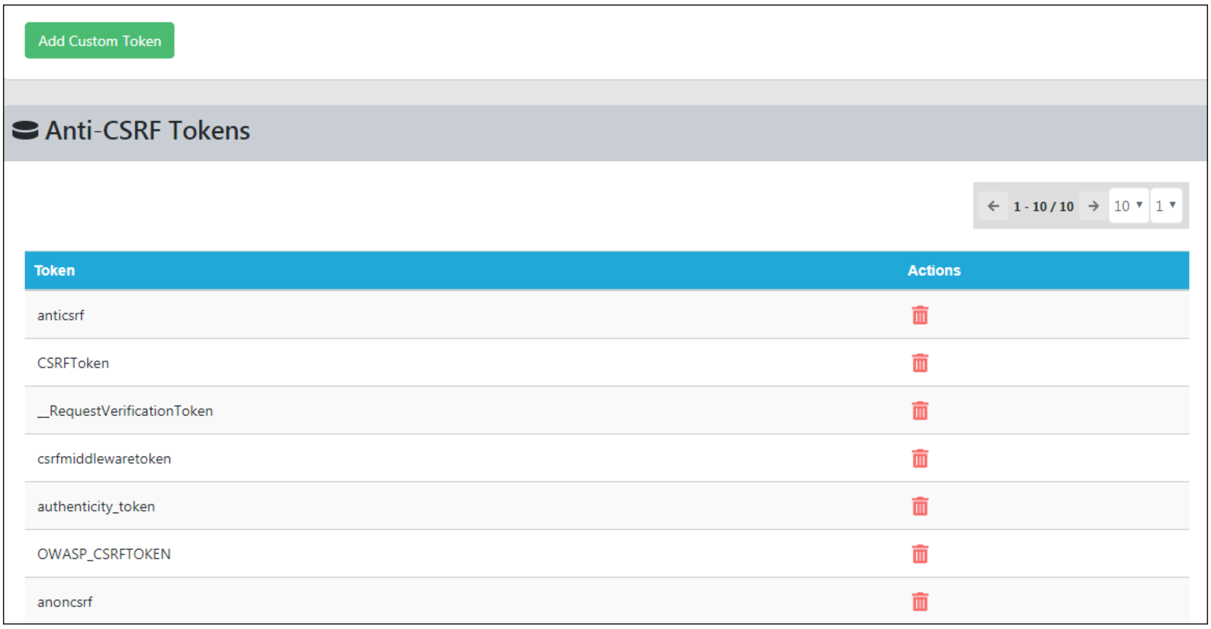
cookieBasedSessionManagement
This method is used to track the session through cookies.

httpAuthSessionManagement
This method is used to track the session through HTTP request header.

Anti CSRF Tokens

Cross-Site Request Forgery (CSRF) is an attack that forces a website or web application to send an HTTP request to a target destination without their insight or intent in order to perform an activity as the victim. Anti-CSRF tokens are random parameters used to protect a website or web application against CSRF attacks. Nemasis detects Anti-CSRF tokens using specific HTTP headers related to HSTS (HTTP Strict Transport Security). The Anti-CSRF token will be the specific HTTP Header name related to HSTS in the token name field.

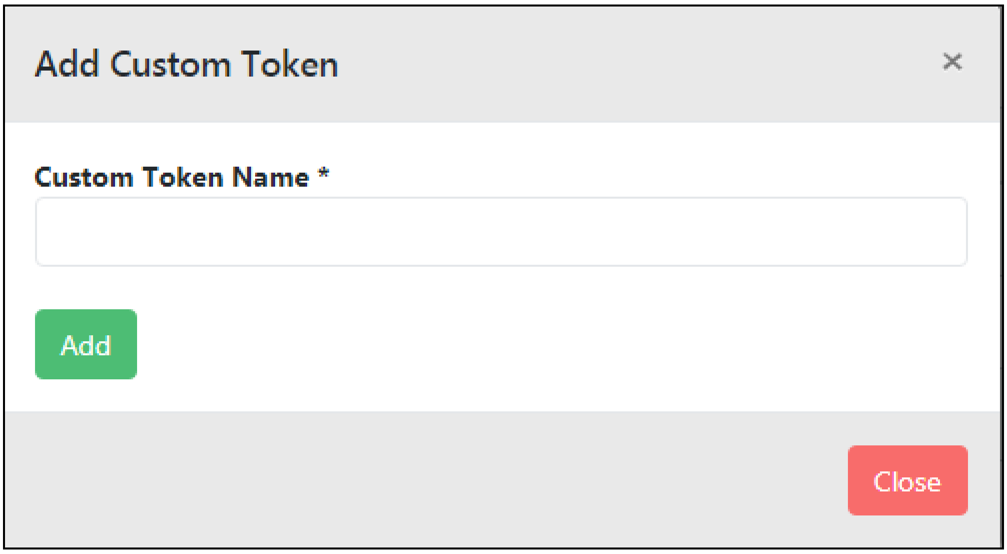
The **Anti CSRF Tokens** submodule will allow you to add these attributes for your web application.



Token	Actions
anticsrf	🗑
CSRFToken	🗑
__RequestVerificationToken	🗑
csrfmiddlewaretoken	🗑
authenticity_token	🗑
OWASP_CSRFTOKEN	🗑
anoncsrf	🗑

Adding an Anti-CSRF Token

1. To add an Anti-CSRF Token, click **Add Custom Token**.
   Add Custom Token window appears.



Add Custom Token

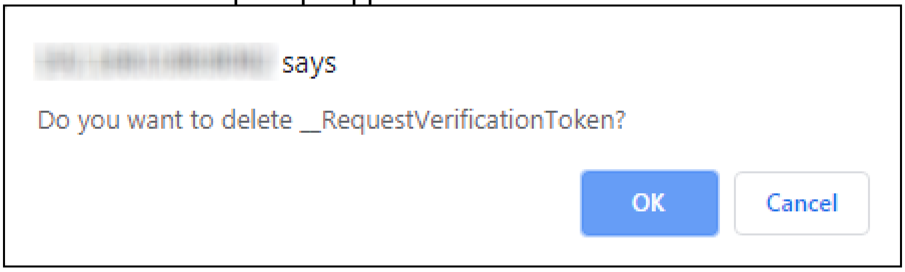
Custom Token Name *

2. Enter token name in the **Custom Token Name** field.
3. Click **Add.**
   The token will be added to the Anti-CSRF Tokens list.

Deleting an Anti-CSRF Token

To delete an Anti-CSRF token, perform the following steps:

1. In the Actions column, click on 🗑.
   A delete confirmation prompt appears.



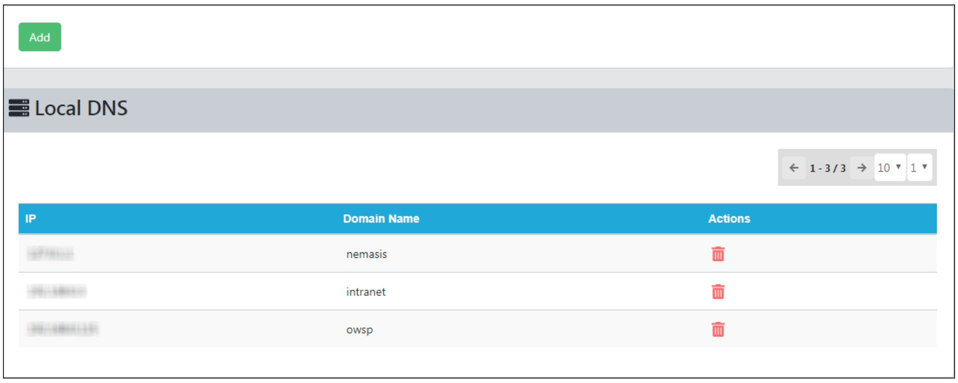
[redacted] says

Do you want to delete __RequestVerificationToken?

2. Click **OK**. The Anti-CSRF token will be deleted.

Local DNS

Through this submodule, user can scan intranet websites (locally hosted) by adding DNS name. You need to provide an internal IP address along with a domain name for the intranet websites. After adding the scan, Nemasis will look for the IP address associated with the domain name in its local DNS cache, which stores DNS information that you have saved in your system recently. If it is present locally, then the intranet website will be scanned.

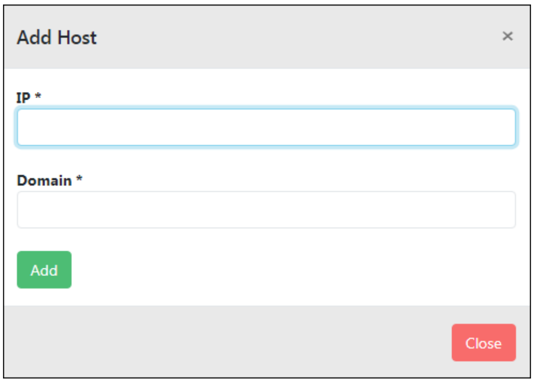


IP	Domain Name	Actions
[redacted]	nemasis	🗑
[redacted]	intranet	🗑
[redacted]	owsp	🗑

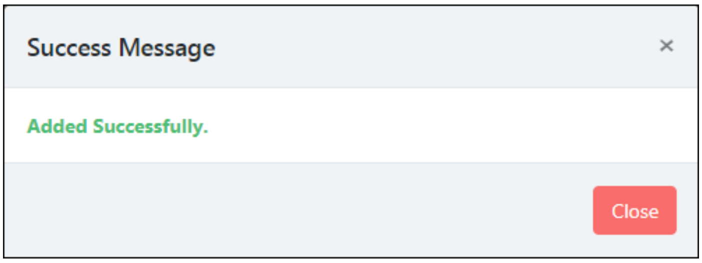
Adding local DNS

To add local DNS follow the below steps:

1. Click **Add**. Add Host window appears.



2. Enter an internal IP address along with the domain name of the intra-websites and click **Add**. The domain will be added successfully.



Success Message

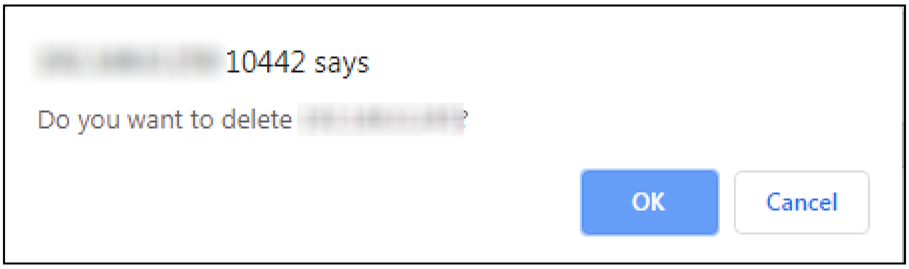
Added Successfully.

3. After adding local DNS, you can start scanning the intra- websites. Learn more about adding a scan task by clicking **here**.

Deleting local DNS

To delete Local DNS follow the below steps:

1. In the Actions column, click 🗑.
   A delete confirmation prompt appears.



[redacted]10442 says

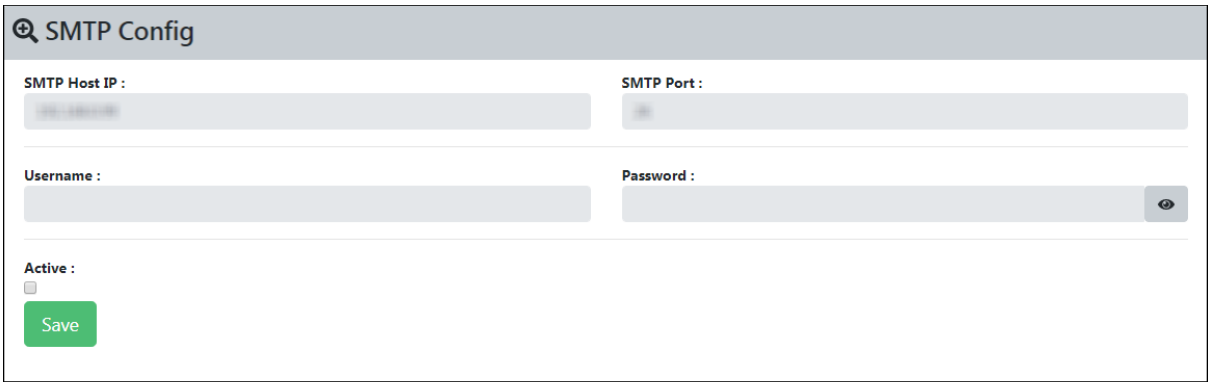
Do you want to delete [redacted]?

2. Click **OK**. The local DNS will be deleted.

Note	For more details on **Scanning Intra-Websites on Nemasis DAST**, click here.

SMTP

With SMTP submodule, you provide SMTP server access and allow Nemasis to send emails.



SMTP Config

SMTP Host IP :

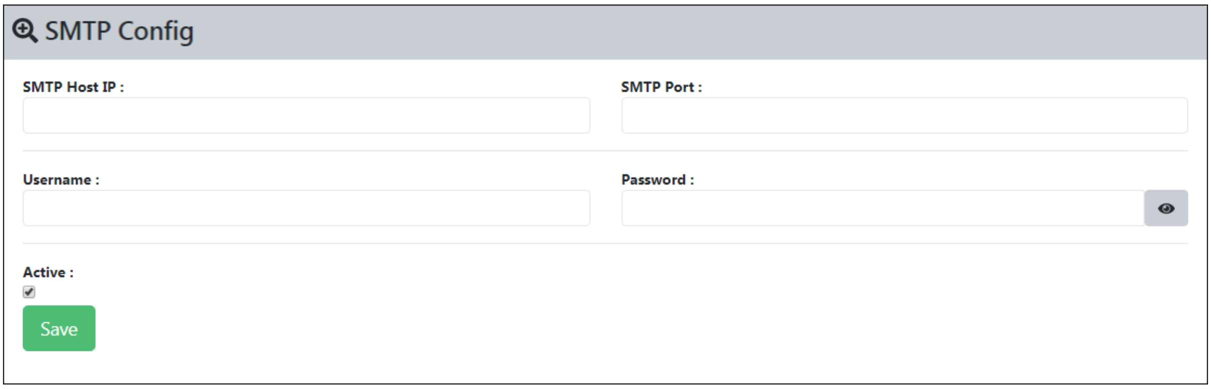
SMTP Port :

Username :

Password :

Active :
□

Select the **Active** checkbox. This will enable all the fields.



SMTP Config

SMTP Host IP :

SMTP Port :

Username :

Password :

Active :
☑

SMTP Host IP
Enter IP address of system on which the SMTP server is installed.

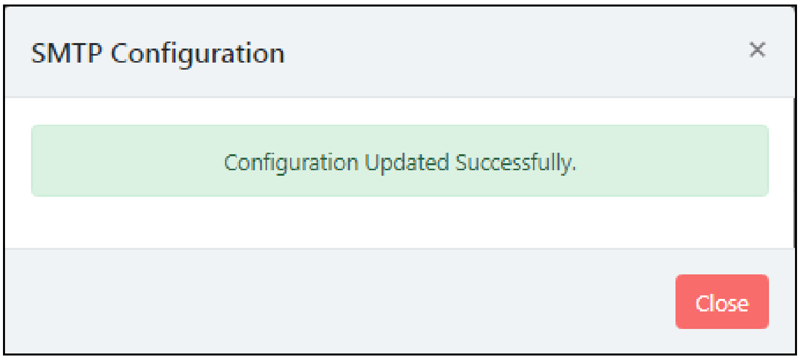
SMTP Port
Enter the SMTP Port number.

Username/Password
If required, enter your SMTP server's login credentials in the respective fields.

- SMTP Password is visible.

-SMTP Password is hidden.

After filling all the details, click **Save**. A success message appears.



SMTP Configuration

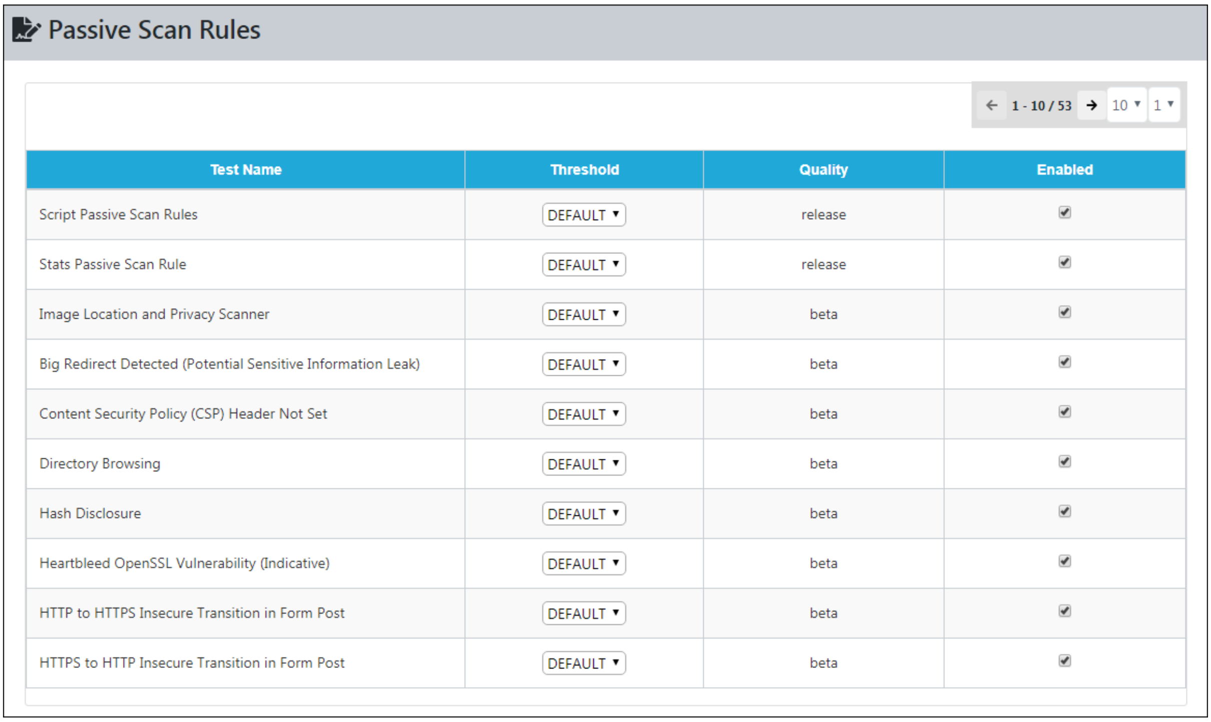
Configuration Updated Successfully.

Passive Scan Config

The Passive Scan Config module contains **Passive Scan Rules** and **Spider Scan Rules** submodules.

Passive Scan Rules

By standard, Nemasis passively checks all HTTP messages sent to the web application being tested (requests and responses). Passive scanning does not change any request or response in any manner and is therefore secure to use. Passive scanning can be used to add tags and raise alerts for potential threats automatically, by using a set of rules that are provided by default.
The Passive Config can be configured using **Passive Scan Rules**.



Passive Scan Rules

Test Name	Threshold	Quality	Enabled
Script Passive Scan Rules	DEFAULT ▾	release	☑
Stats Passive Scan Rule	DEFAULT ▾	release	☑
Image Location and Privacy Scanner	DEFAULT ▾	beta	☑
Big Redirect Detected (Potential Sensitive Information Leak)	DEFAULT ▾	beta	☑
Content Security Policy (CSP) Header Not Set	DEFAULT ▾	beta	☑
Directory Browsing	DEFAULT ▾	beta	☑
Hash Disclosure	DEFAULT ▾	beta	☑
Heartbleed OpenSSL Vulnerability (Indicative)	DEFAULT ▾	beta	☑
HTTP to HTTPS Insecure Transition in Form Post	DEFAULT ▾	beta	☑
HTTPS to HTTP Insecure Transition in Form Post	DEFAULT ▾	beta	☑

Test Name
This list contains the test/rule name.

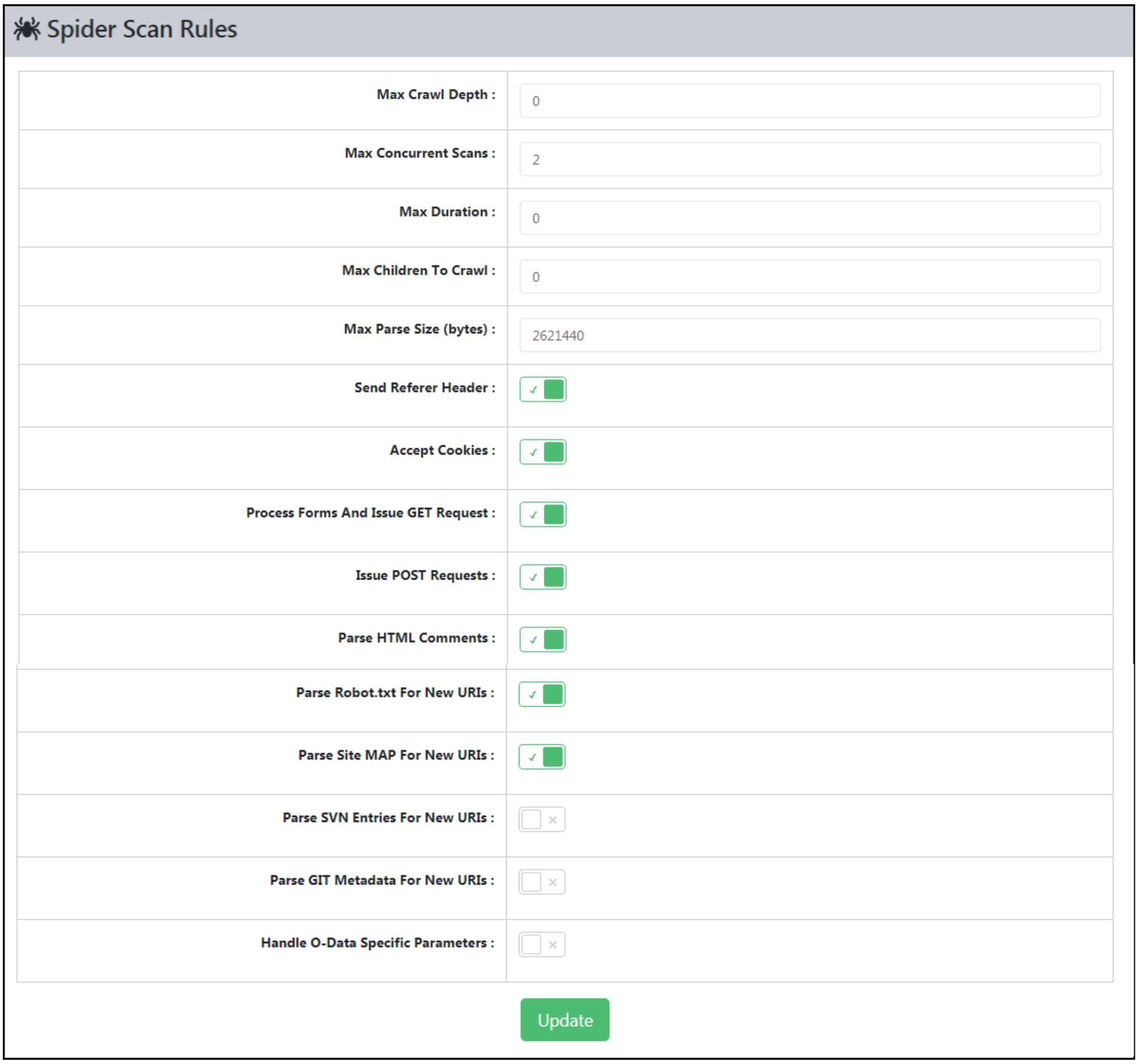
Threshold
This feature lets you configure the testing manner of potential vulnerabilities.
The dropdown contains following options:

- **OFF**: The test will not run.
- **DEFAULT**: The test will run in default mode.
- **Low**: The test will detect maximum potential threats, which may increase the number of false positives.
- **Medium:** The test will detect a moderate number of potential threats.
- **High**: The test will detect minimum potential threats, which may result in missing of real threats, that is, false negative.

Enabled
Select the checkbox to enable or disable the specific test.

Spider Scan Rules

This submodule allows you to configure the Spider Scan option. Modifying these options will also affect the running spider.



Spider Scan Rules

Max Crawl Depth :	0
Max Concurrent Scans :	2
Max Duration :	0
Max Children To Crawl :	0
Max Parse Size (bytes) :	2621440
Send Referer Header :	☑
Accept Cookies :	☑
Process Forms And Issue GET Request :	☑
Issue POST Requests :	☑
Parse HTML Comments :	☑
Parse Robot.txt For New URIs :	☑
Parse Site MAP For New URIs :	☑
Parse SVN Entries For New URIs :	☐
Parse GIT Metadata For New URIs :	☐
Handle O-Data Specific Parameters :	☐

Max Crawl Depth

This parameter sets the maximum depth in the crawling process where a page or website must be found for processing. The spider does not collect and parse resources (URLs) found deeper than this level. The value zero indicates unlimited depth.

Max Concurrent Scans

This number sets the maximum number of scans used in the crawling process. Changing this parameter has no impact on ongoing crawling.

Max Duration
This parameter sets the maximum period of time that the spider should crawl. It is measured in minutes, zero (the default time), which means that the spider will run until it has found all of the links that it is able to.

Max Children to Crawl
This parameter limits the max number of children that are allowed to crawl at every node. This is useful for data-driven apps that have large numbers of 'pages' that run on the same code but has different data. By default, the value is set as zero.

Max Parse Size (bytes)
This parameter sets the maximum size (in bytes) that may be parsed for a response. This allows the spider to skip the big responses/files.

Send Referer Header
This option sends the spider request with "Referer" header. By default, it is enabled.

Accept Cookies
This option helps you enable or disable to accept cookies while performing spider scan. The spider handles any cookies obtained from the server and sends it back accordingly if this option is enabled. If this option is disabled, the spider will not accept any cookies. By default, it is enabled.

Process Forms and Issue GET Request
This parameter decides the spider's behavior when it comes across HTML forms during the crawling process. If this parameter is disabled then, the spider skips the HTML forms. And if enabled, the HTML forms with HTTP GET methods will be submitted with auto generated values. It is enabled by default.

Issue POST Requests
In order to configure this option **Process Forms and Issue GET Request** should be enabled. As described in the previous option, this option is used when the spider encounters the HTML forms with the HTTP POST methods. This option is enabled by default.

Parse HTML Comments
This option decides whether the spider should crawl the HTML comments while searching for links to resources. Only the resources found in the valid HTML comments tag will be crawled. It is enabled by default.

Parse robot.txt for New URIs
This option decides whether the spider should crawl the robots.txt files found on websites while searching for links to resources. This option does not define whether the spider should follow the robots.txt file rules. It is enabled by default.

Parse SiteMAP for New URIs

This option allows you to parse the sitemap for all the new URIs for links. This option is enabled by default.

Parse SVN Entries for New URIs

Subversion is an open-source version control system used to manage the collections of files that make up software projects. This option allows you to parse the Subversion (SVN) entries for all the new URIs. This option is disabled by default.

Parse GIT Meta-data for new URIs

This option allows you to parse the GIT metadata for all the new URIs. This option is disabled by default.

Handle O-Data Specific Parameters

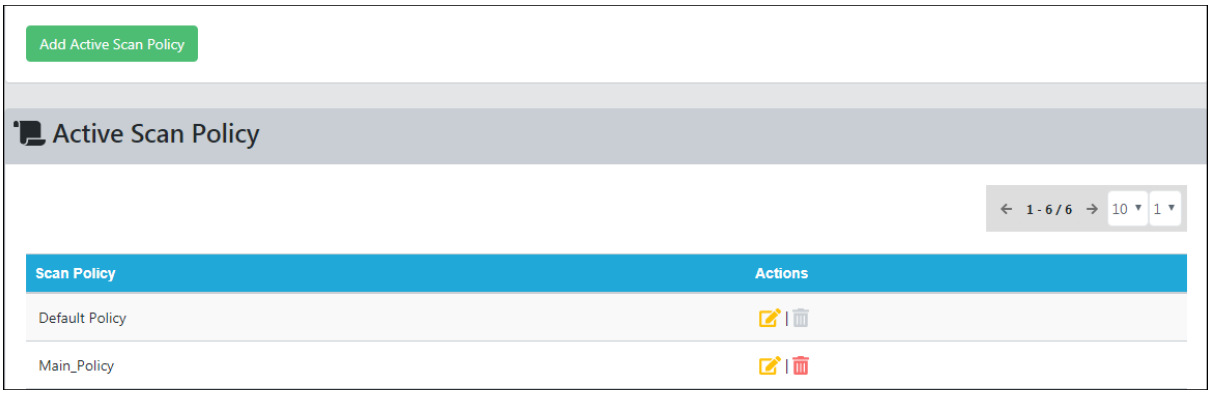
This option allows you to process the O-Data specific parameter, that is, resource identifiers according to the specific-defined rules. This option is disabled by default.

Active Scan Config

The Active Scan Config contains **Active Scan Policies**, **Active Scan Settings**, **Active Scan Input**, **Rules Manager**, and **Replacer Manager** submodules.

Active Scan Policies

An active scan policy lets you define the rules to be followed during an Active scan. You can configure these rules for their attack strength, alert threshold type and whether they should be active or inactive.

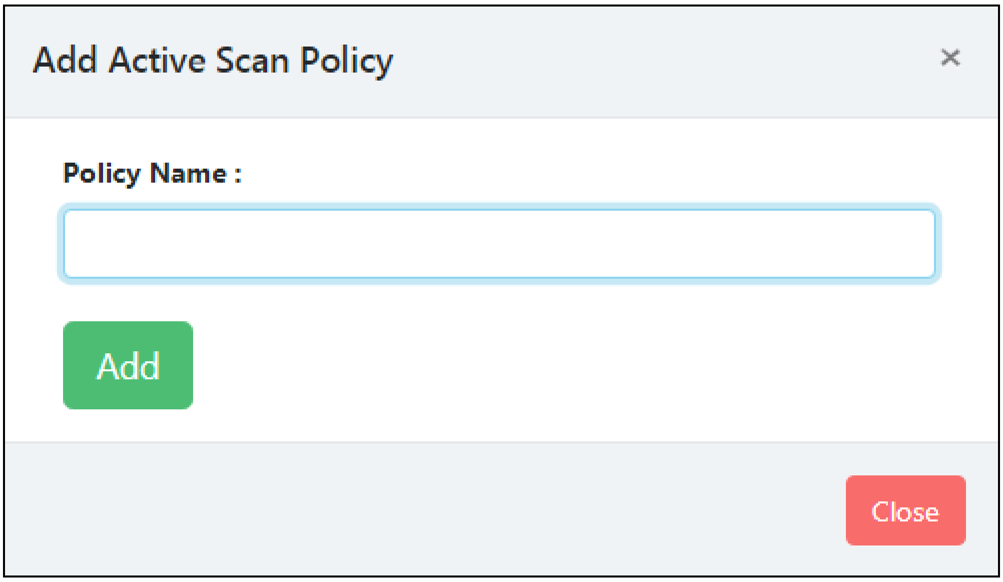


Scan Policy	Actions
Default Policy	✎ | 🗑
Main_Policy	✎ | 🗑

Adding an Active Scan Policy

To add an Active Scan Policy, follow the steps are given below:

1. Click **Add Active Scan Policy**.
   Add Scan Policy window appears.

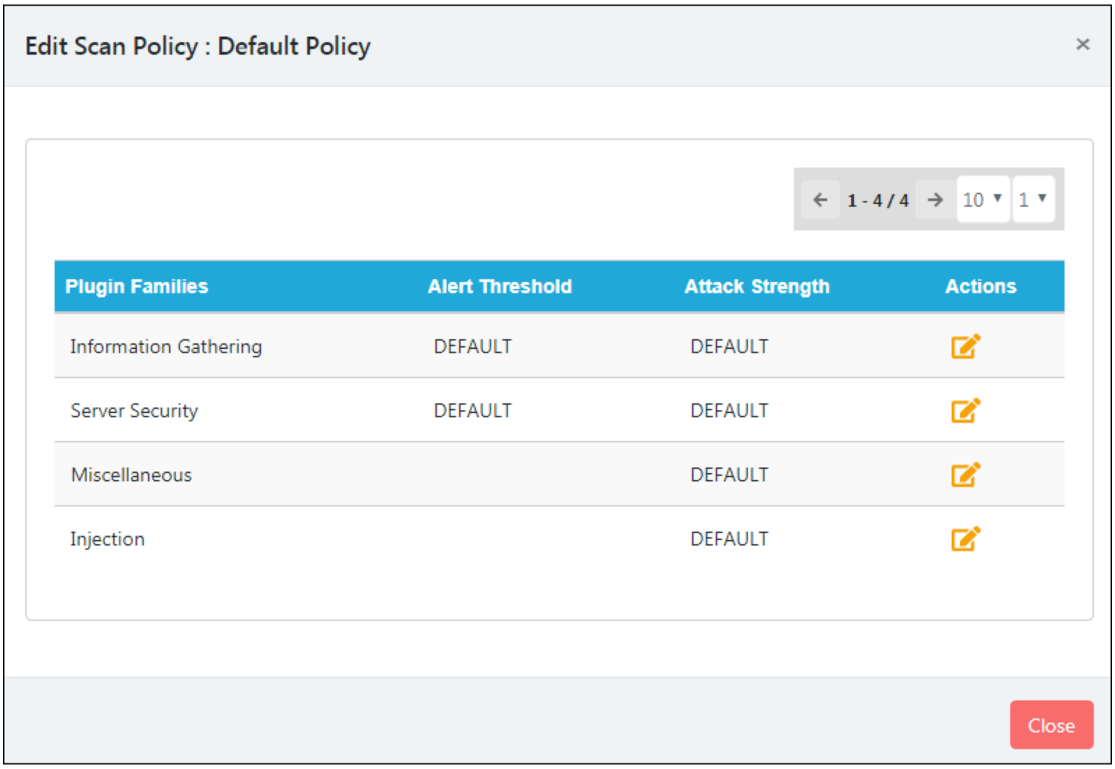


2. Enter the name of the scan policy and then click **Add Scan Policy**.
   The policy will be added with default policy rules pre-defined by Nemasis DA.

Editing a Scan Policy

To edit a Scan Policy, follow the steps given below:

1. In the **Actions** column, click ✎.
   The Edit Scan Policy window appears.



Edit Scan Policy : Default Policy

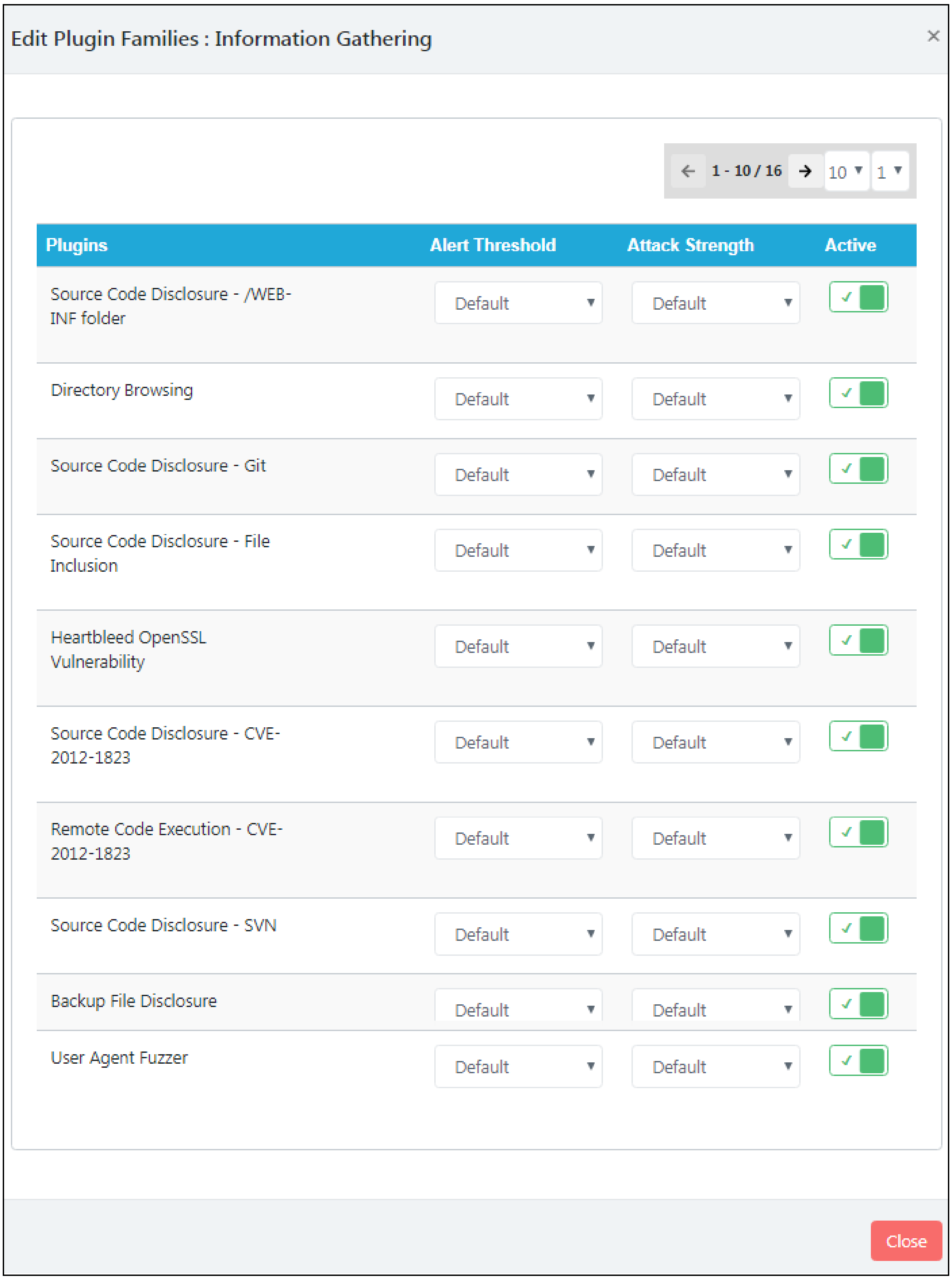
Plugin Families	Alert Threshold	Attack Strength	Actions
Information Gathering	DEFAULT	DEFAULT	✎
Server Security	DEFAULT	DEFAULT	✎
Miscellaneous		DEFAULT	✎
Injection		DEFAULT	✎

   It displays the list of **Plugin Families** names, **Alert Threshold**, **Attack Strength**, and **Actions** columns.
   This window consists of default Plugin Families with following pre-defined plugins by Nemasis: **Information Gathering**, **Server Security**, **Miscellaneous**, and **Injection**.

3. You can further edit each Plugin Family according to your need as each of them has different sets of pre-defined plugins.

Information Gathering

You can edit the Information Gathering plugin family by clicking ✎. You can configure the **Alert Threshold**, **Attack Strength**, and the status (**Active**) of each plugin present in it.



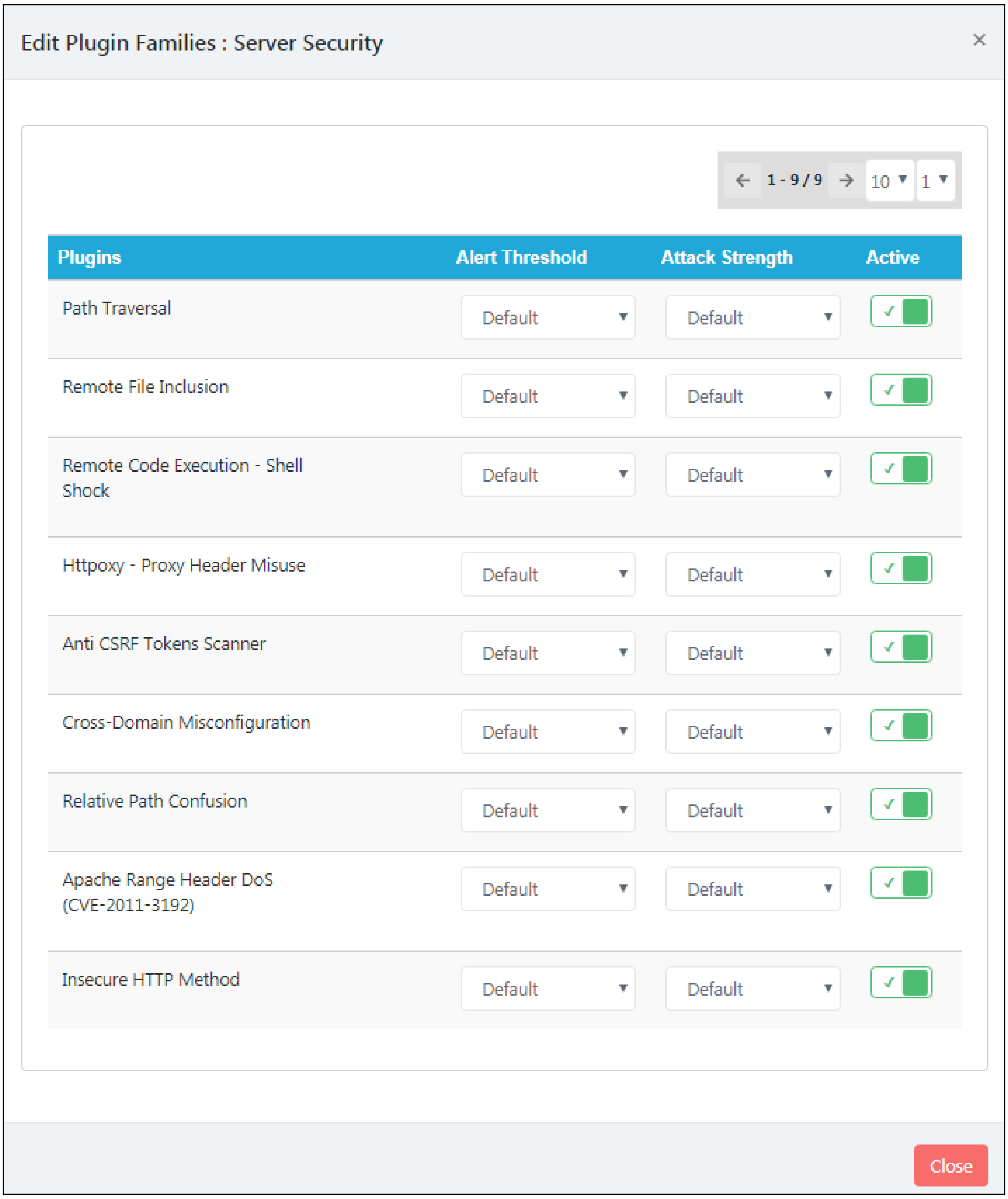
Edit Plugin Families : Information Gathering

Plugins	Alert Threshold	Attack Strength	Active
Source Code Disclosure - /WEB-INF folder	Default ▾	Default ▾	✓
Directory Browsing	Default ▾	Default ▾	✓
Source Code Disclosure - Git	Default ▾	Default ▾	✓
Source Code Disclosure - File Inclusion	Default ▾	Default ▾	✓
Heartbleed OpenSSL Vulnerability	Default ▾	Default ▾	✓
Source Code Disclosure - CVE-2012-1823	Default ▾	Default ▾	✓
Remote Code Execution - CVE-2012-1823	Default ▾	Default ▾	✓
Source Code Disclosure - SVN	Default ▾	Default ▾	✓
Backup File Disclosure	Default ▾	Default ▾	✓
User Agent Fuzzer	Default ▾	Default ▾	✓

The **Alert Threshold** can be set to **OFF**, **Default**, **Low**, **Medium**, and **High**. The **Attack Strength** can be set to **OFF**, **Default**, **Low**, **Medium**, **High**, and **Insane**. Change the status of plugin by enabling the toggle. You will also see the **Plugin Quality** of each plugin, namely, **Release**, **Beta**, and **Alpha**.

Server Security

You can edit the Server Security plugin family by clicking 📝. You can configure the **Alert Threshold**, **Attack Strength**, and the status (**Active**) of each plugin present in it.



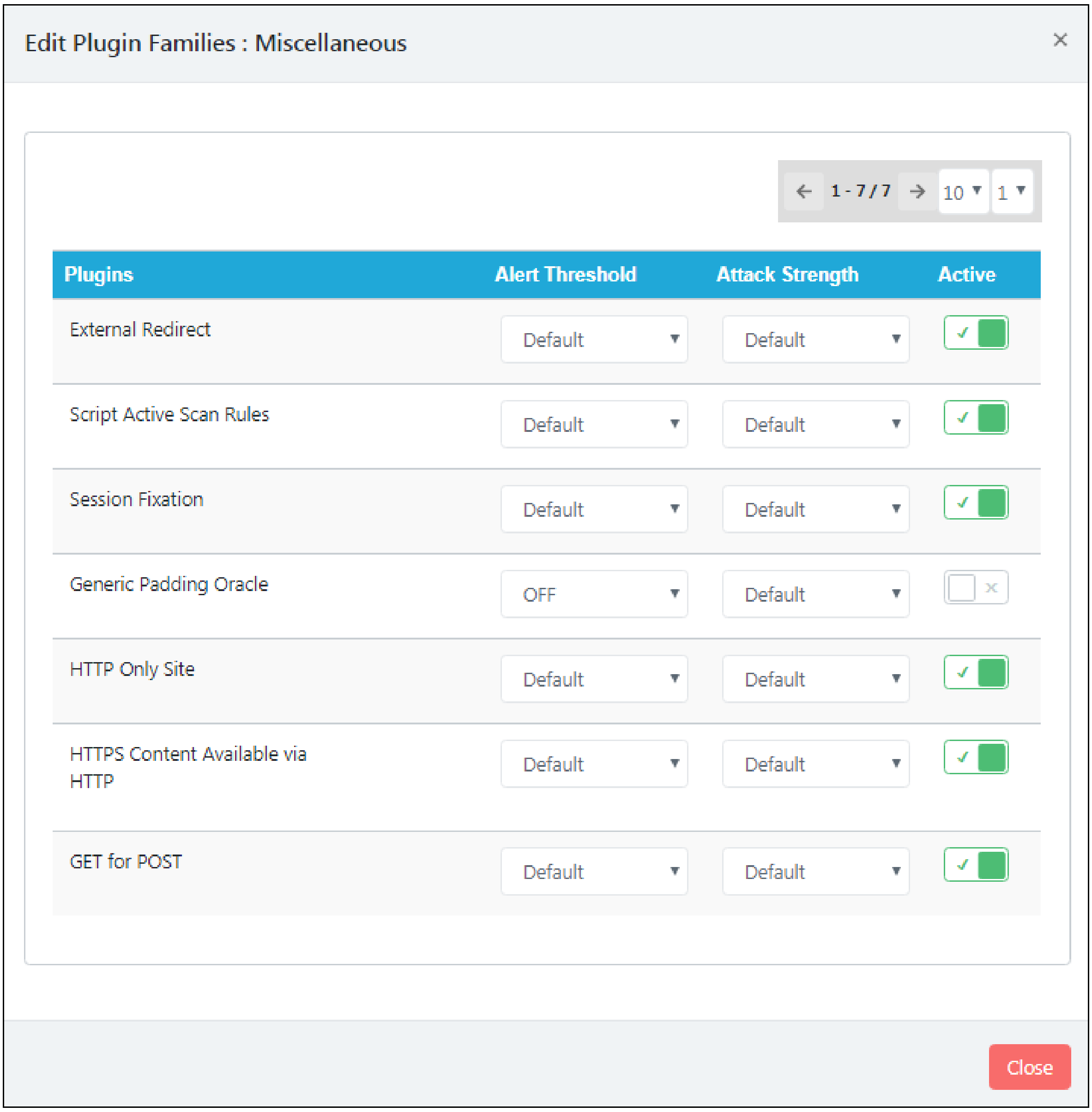
Edit Plugin Families : Server Security

Plugins	Alert Threshold	Attack Strength	Active
Path Traversal	Default ▾	Default ▾	✓
Remote File Inclusion	Default ▾	Default ▾	✓
Remote Code Execution - Shell Shock	Default ▾	Default ▾	✓
Httpoxy - Proxy Header Misuse	Default ▾	Default ▾	✓
Anti CSRF Tokens Scanner	Default ▾	Default ▾	✓
Cross-Domain Misconfiguration	Default ▾	Default ▾	✓
Relative Path Confusion	Default ▾	Default ▾	✓
Apache Range Header DoS (CVE-2011-3192)	Default ▾	Default ▾	✓
Insecure HTTP Method	Default ▾	Default ▾	✓

The **Alert Threshold** can be set to **OFF**, **Default**, **Low**, **Medium**, and **High**. The **Attack Strength** can be set to **OFF**, **Default**, **Low**, **Medium**, **High**, and **Insane**. Change the status of the plugin by enabling the toggle. You will also see the **Plugin Quality** of each plugin, namely, **Release**, **Beta**, and **Alpha**.

Miscellaneous

You can edit the Miscellaneous plugin family by clicking ✎. You can configure the **Alert Threshold**, **Attack Strength**, and the status (**Active**) of each plugin present in it.



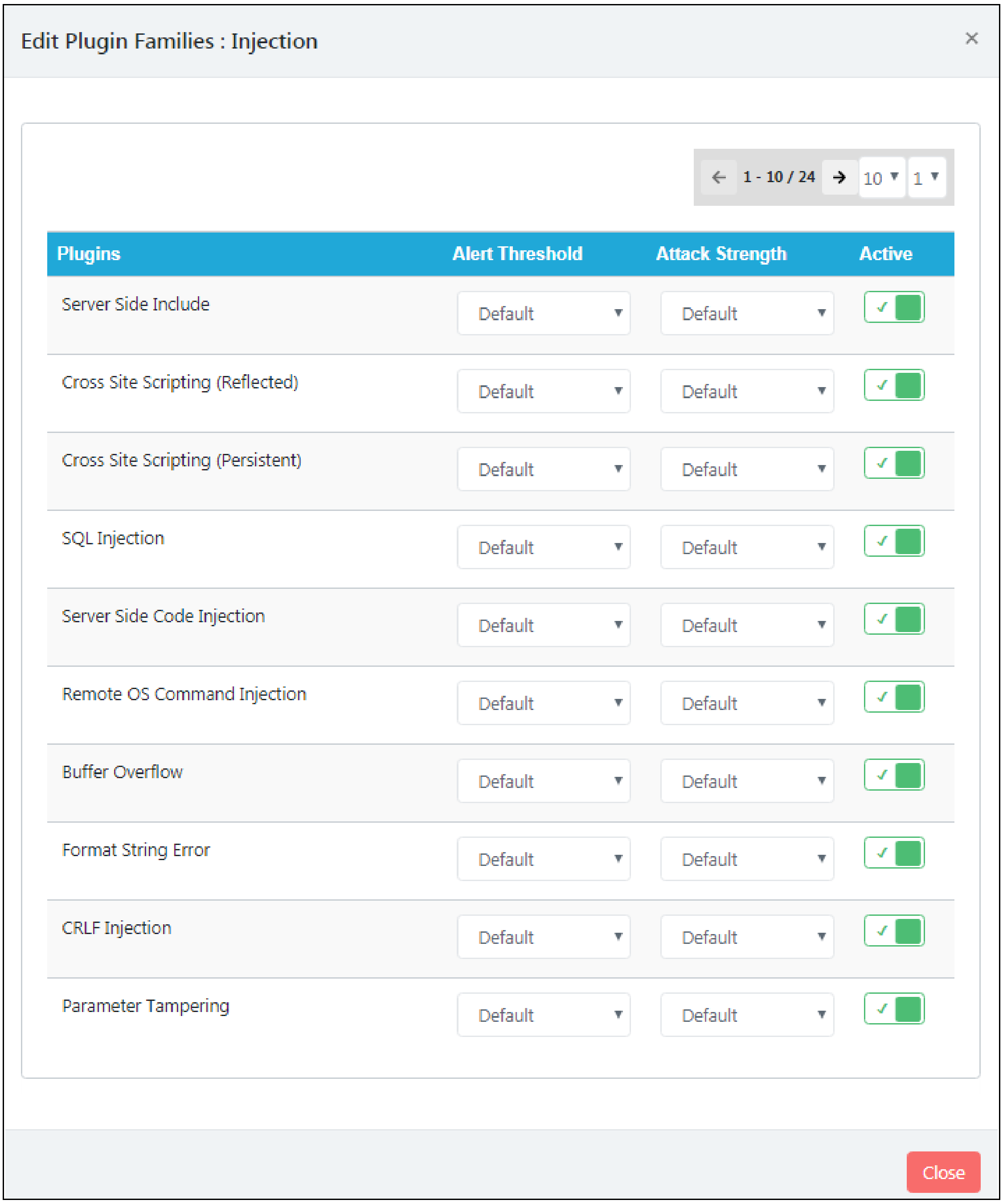
Edit Plugin Families : Miscellaneous

Plugins	Alert Threshold	Attack Strength	Active
External Redirect	Default ▾	Default ▾	✓
Script Active Scan Rules	Default ▾	Default ▾	✓
Session Fixation	Default ▾	Default ▾	✓
Generic Padding Oracle	OFF ▾	Default ▾	✗
HTTP Only Site	Default ▾	Default ▾	✓
HTTPS Content Available via HTTP	Default ▾	Default ▾	✓
GET for POST	Default ▾	Default ▾	✓

The **Alert Threshold** can be set to **OFF**, **Default**, **Low**, **Medium**, and **High**. The **Attack Strength** can be set to **OFF**, **Default**, **Low**, **Medium**, **High**, and **Insane**. Change the status of plugin by enabling the toggle. You will also see the **Plugin Quality** of each plugin, namely, **Release**, **Beta**, and **Alpha**.

Injection

You can edit the Injection plugin family by clicking ✎. You can configure the **Alert Threshold**, **Attack Strength**, and the status (**Active**) of each plugin present in it.



Edit Plugin Families : Injection

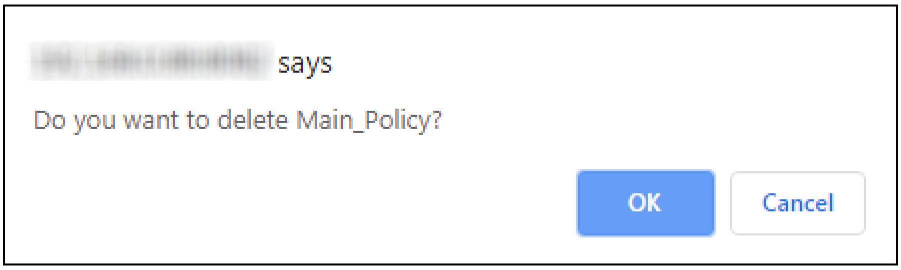
Plugins	Alert Threshold	Attack Strength	Active
Server Side Include	Default	Default	✓
Cross Site Scripting (Reflected)	Default	Default	✓
Cross Site Scripting (Persistent)	Default	Default	✓
SQL Injection	Default	Default	✓
Server Side Code Injection	Default	Default	✓
Remote OS Command Injection	Default	Default	✓
Buffer Overflow	Default	Default	✓
Format String Error	Default	Default	✓
CRLF Injection	Default	Default	✓
Parameter Tampering	Default	Default	✓

The **Alert Threshold** can be set to **OFF**, **Default**, **Low**, **Medium**, and **High**. The **Attack Strength** can be set to **OFF**, **Default**, **Low**, **Medium**, **High**, and **Insane**. Change the status of plugin by enabling the toggle. You will also see the **Plugin Quality** of each plugin, namely, **Release**, **Beta**, and **Alpha**.

Deleting a Scan Policy

To delete a Scan Policy, follow the steps given below:

1. In the **Actions** column, click 🗑.
   A delete confirmation prompt appears.



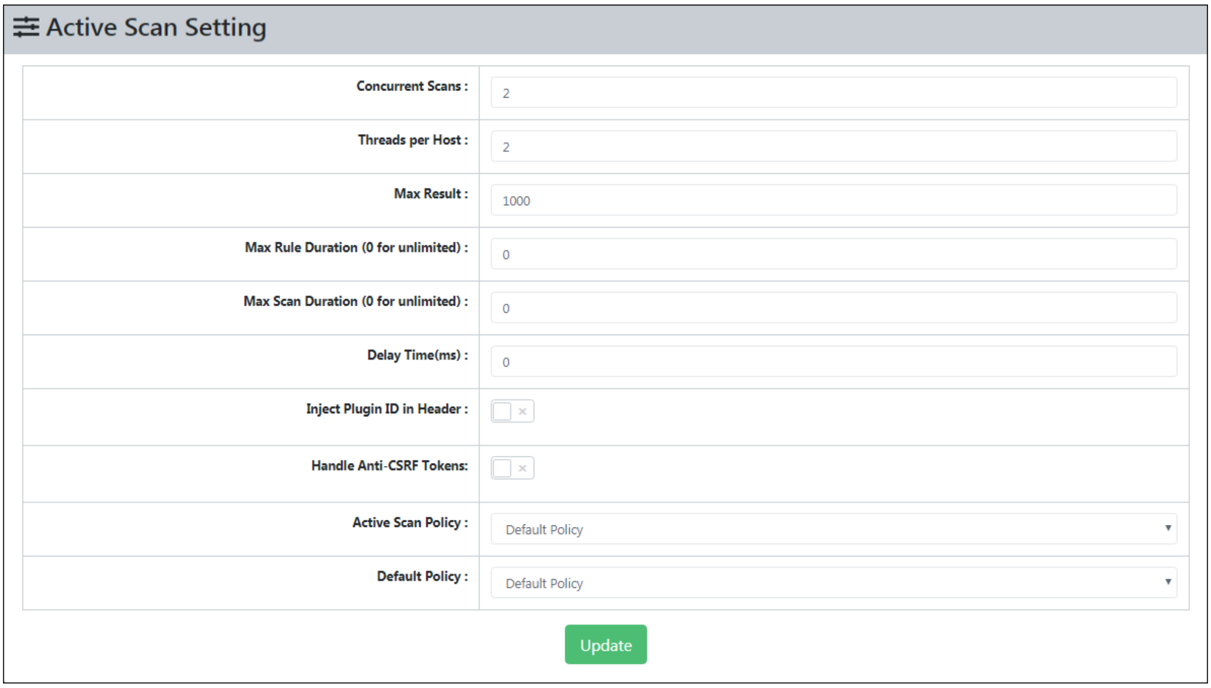
[redacted] says

Do you want to delete Main_Policy?

2. Click **OK**. The Scan Policy report will be deleted.

Active Scan Settings

This submodule allows you to configure and update the active scan option.



Active Scan Setting

Concurrent Scans :	2
Threads per Host :	2
Max Result :	1000
Max Rule Duration (0 for unlimited) :	0
Max Scan Duration (0 for unlimited) :	0
Delay Time(ms) :	0
Inject Plugin ID in Header :	☐ ×
Handle Anti-CSRF Tokens:	☐ ×
Active Scan Policy :	Default Policy ▾
Default Policy :	Default Policy ▾

Concurrent Scans
This option allows you to define the maximum number of hosts that will be scanned at the same time. If the scan is running for multiple systems at the same time, Nemasis appliance may get negatively affected.

Threads per Host
This option allows you to define the number of threads the scanner will use per host. If you increase the number of threads, it will speed up the scan but the target host and the Nemasis appliance may get negatively affected.

Max Result
This option allows you to define the number of results that will be stored. Maximum results you can store are up to 1000.

Max Rule Duration (0 for unlimited)
This option allows you to set the maximum duration for any individual rule can run. It is defined in minutes and zero minute means no limit. This can be used to avoid unnecessary time-consuming rules.

Max Scan Duration (0 for unlimited)
This option allows you to set the maximum duration that the entire scan can run. It is defined in minutes and zero minute means no limit. This can be used to complete the scan in a set time.

Delay Time (ms)

This option allows you to define the delay between each request in milliseconds. When you set this option to a non-zero value, the time taken by Active scan will increase with respect to the value. But the target host will be less affected.

Inject Plugin ID in header

If this option is enabled, the active scanner will inject the Plugin ID in header request while sending the HTTP requests. This option is disabled by default.

Handle Anti-CSRF

If this option is enabled, then the active scanner will try to request the Anti-CSRF tokens automatically when required. This option disabled by default.

Attack Policy

This option is used to select the Scan Policy that will be used for scanning in Active Scan. Here the Scan Policy used can be defined in the **Active Scan Policy** module. Learn more about User by clicking **here**.

Default Policy

This option is used to select the Scan Policy that is used by default when you start an Active Scan.

Active Scan Input

This submodule allows you to configure the Active Scan input vectors. It consists of elements that will be attacked by the active scanner. Scanning each and every element will be time consuming, but missing some element may result in missing some vulnerabilities. Refer to Figure .

This module contains following tabs:

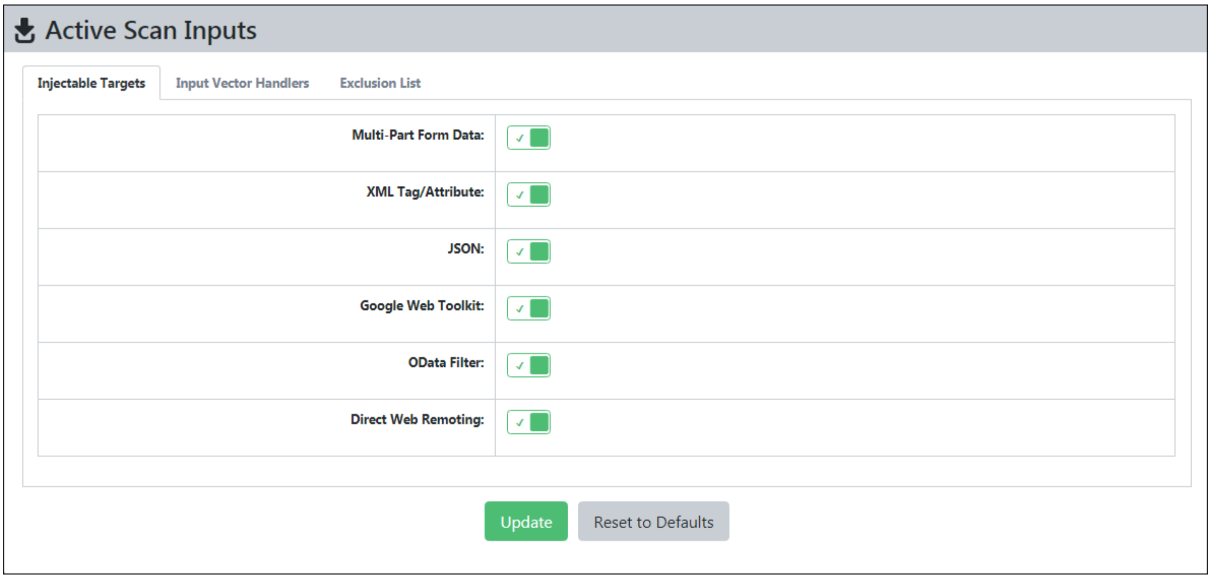
- **Injectable Targets**
- **Input Vector Handlers**
- **Exclusion List**

After you made changes, click **Update** to save changes.

To restore the default settings, click **Reset to Default**.

Injectable Targets

During an Active Scan, the scanner scans the pre-defined data formats to find vulnerabilities. The Injectable Targets tab lets you to configure the different data formats. Click the toggle to enable or disable for data injection.



Multi-Part Form Data: ✓

XML Tag/Attribute: ✓

JSON: ✓

Google Web Toolkit: ✓

OData Filter: ✓

Direct Web Remoting: ✓

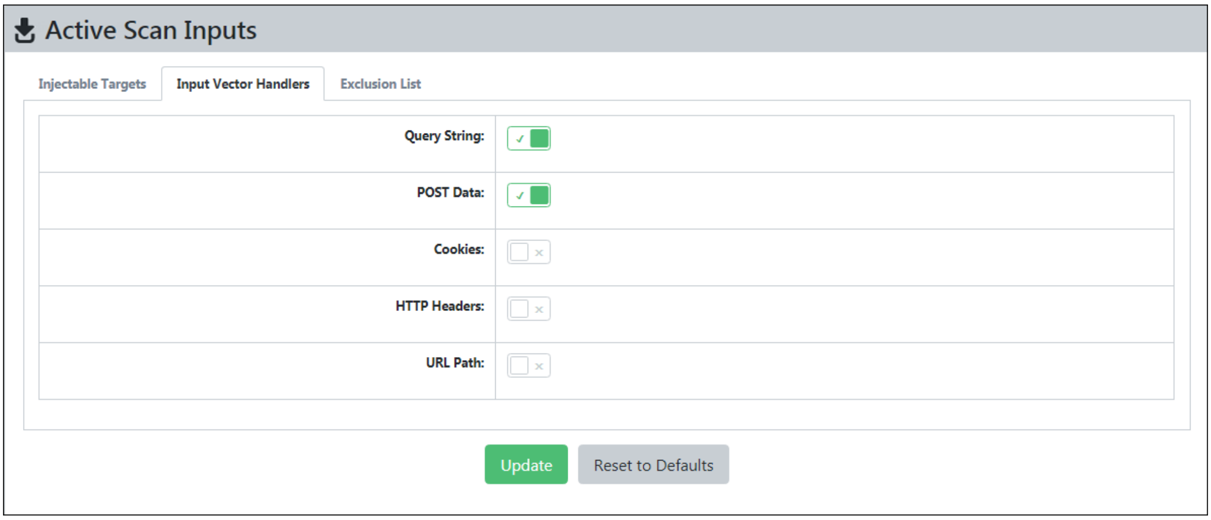
The data formats that the active scanner will target are as follows:

- **Multi-Part Form Data**: When a POST request is made, the active scanner will target multipart form data and scan it for vulnerabilities.
- **XML Tag/Attribute**: When a POST request is made, the active scanner will target XML tags or attributes and scan it for vulnerabilities.
- **JSON:** When a POST request is made, the active scanner will target JSON files and scans them for vulnerabilities.
- **Google Web Toolkit:** When a POST request is made, the active scanner will target JavaScript in the websites and scans them for vulnerabilities.
- **OData Filter:** When a POST request is made, the active scanner will target RESTful-based protocols in the websites and scans them for vulnerabilities.

- **Direct Web Remoting:** When a POST request is made, the active scanner will target Java code from the server and JavaScript in the websites and scans them for vulnerabilities.

Input Vector Handlers

This tab includes the request parameter that active scanner will target and you can enable or disable them according to your need.



Active Scan Inputs

Query String: ☑
POST Data: ☑
Cookies: ☐
HTTP Headers: ☐
URL Path: ☐

Query String

It will add a query parameter to GET requests that originally did not had one. This option is enabled by default.

POST Data

It is key-value pairs in the POST request data. This option is enabled by default.

Cookies

If this is enabled, it will target all the cookies present in the links of resources. It is disabled by default.

HTTP Headers

If this option is enabled, it will target all the HTTP Headers present in the links of resources. It is disabled by default.

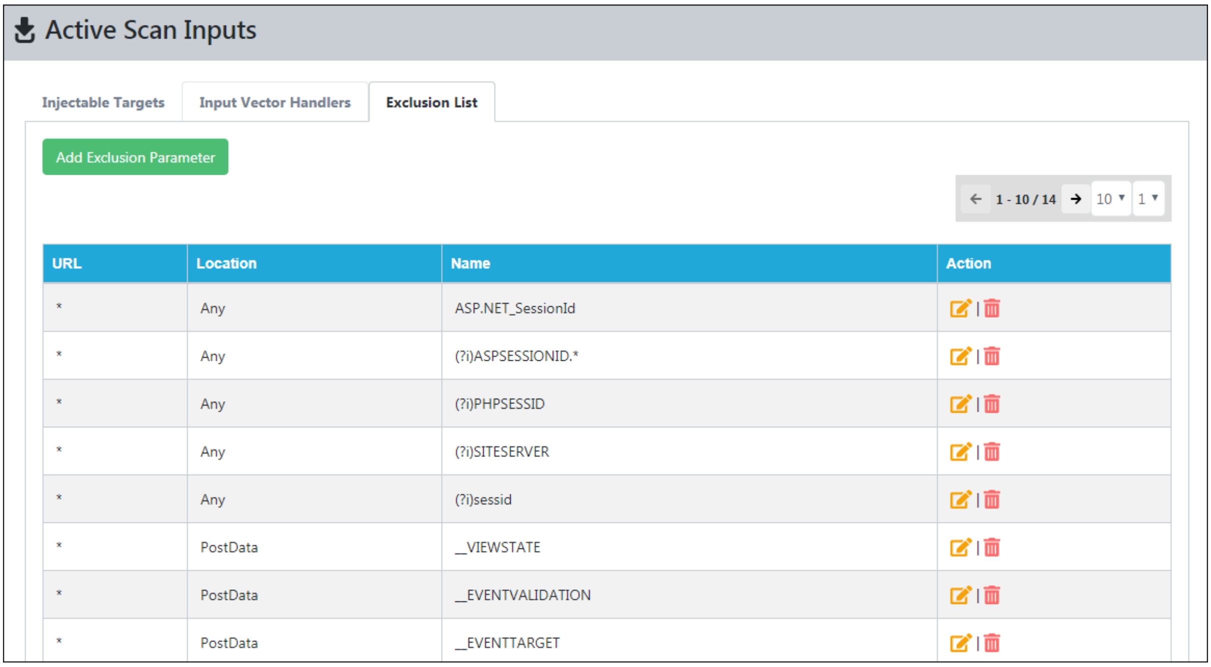
URL Path

If this option is enabled, it will target the entire path elements in the request URL, that is, elements separated by /. It is disabled by default.

Exclusion List

An Exclusion parameter is a part of URL that will be skipped by the active scanner. The Exclusion List contains a list of pre-defined parameters.

This tab allows you to add, edit, and delete the exclusion parameters.

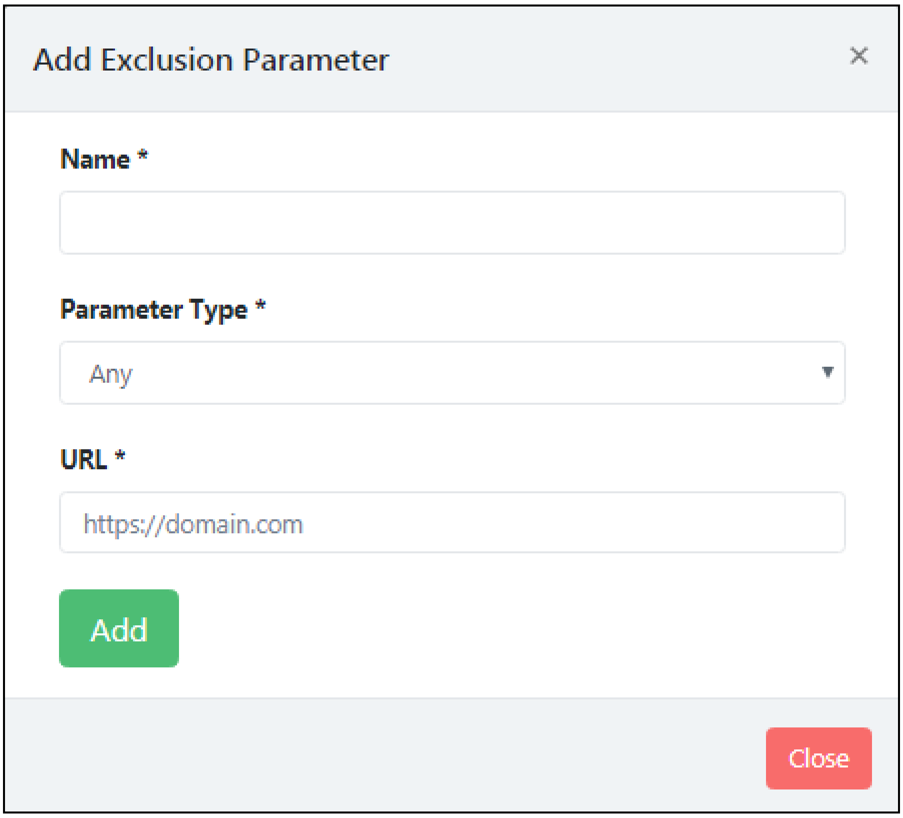


Active Scan Inputs

URL	Location	Name	Action
*	Any	ASP.NET_SessionId	✎ | 🗑
*	Any	(?i)ASPSESSIONID.*	✎ | 🗑
*	Any	(?i)PHPSESSID	✎ | 🗑
*	Any	(?i)SITESERVER	✎ | 🗑
*	Any	(?i)sessid	✎ | 🗑
*	PostData	__VIEWSTATE	✎ | 🗑
*	PostData	__EVENTVALIDATION	✎ | 🗑
*	PostData	__EVENTTARGET	✎ | 🗑

Adding an Exclusion Parameter

1. To add an exclusion parameter, click **Add Exclusion Parameter**.



Add Exclusion Parameter ×

Name *

Parameter Type *

Any

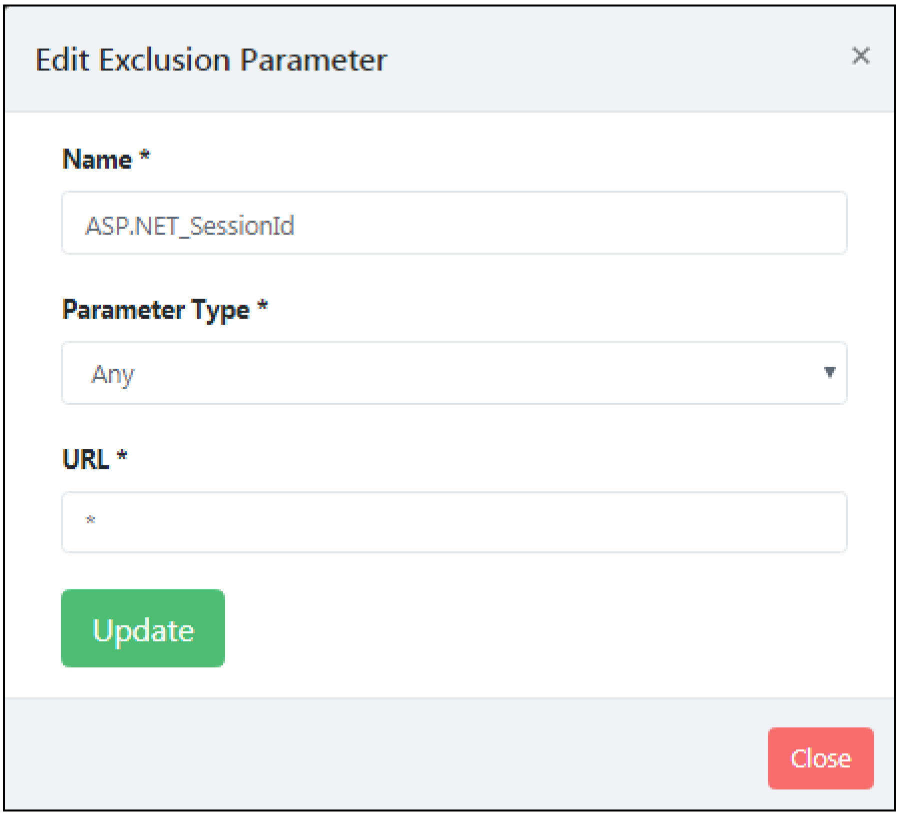
URL *

https://domain.com

2. Enter the **Name** of the parameter.
3. Click the **Parameter Type** drop-down and select a preferred type.
4. Enter the **URL**.
5. After you have entered all details click **Add**.
   The exclusion parameter will be added in the list.

Modifying an Exclusion Parameter

1. To modify an existing exclusion parameter click 📝.
   Edit Exclusion Parameter window appears.



Edit Exclusion Parameter

Name *

ASP.NET_SessionId

Parameter Type *

Any

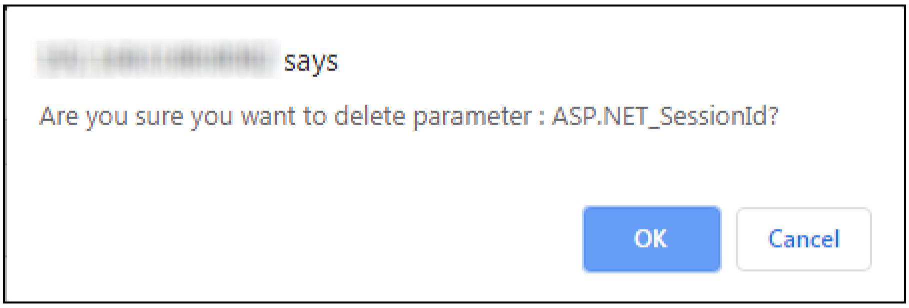
URL *

*

2. Modify the details and then click **Update**.
   The modified details will be updated.

Deleting an Exclusion Parameter

1. To delete an exclusion parameter, click 🗑.
   A delete confirmation prompt appears.



[redacted] says

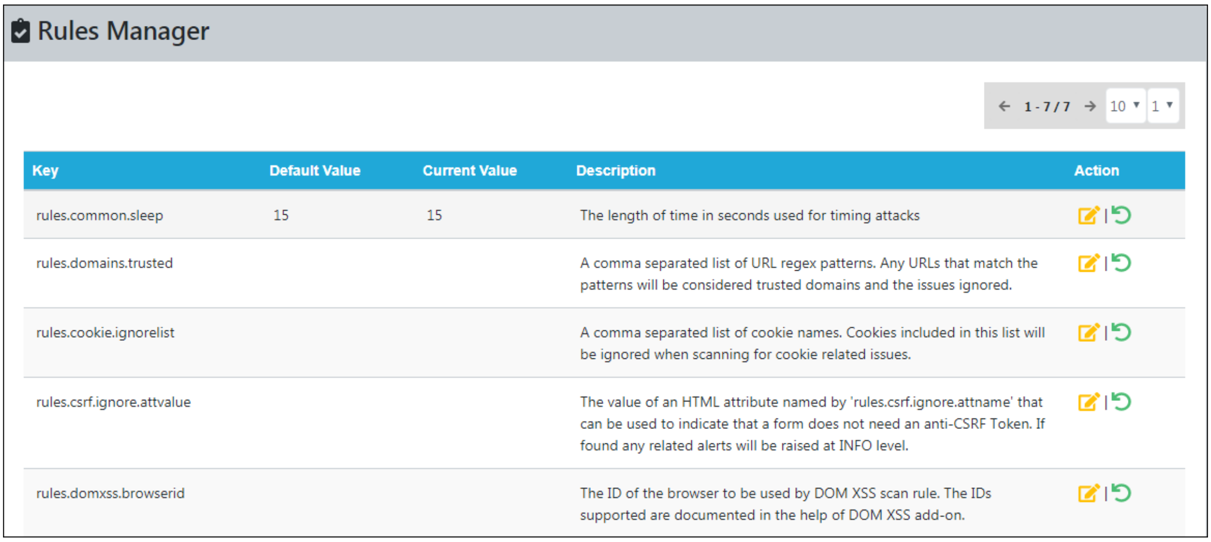
Are you sure you want to delete parameter : ASP.NET_SessionId?

2. Click **OK**. The parameter will be deleted.

Rules Manager

This submodule allows you to configure the behavior of an active and passive scan rules. It will display the following details of the replacement rule key (name), default value, change value (value), description, and actions.

These are the pre-defined rules by Nemasis.

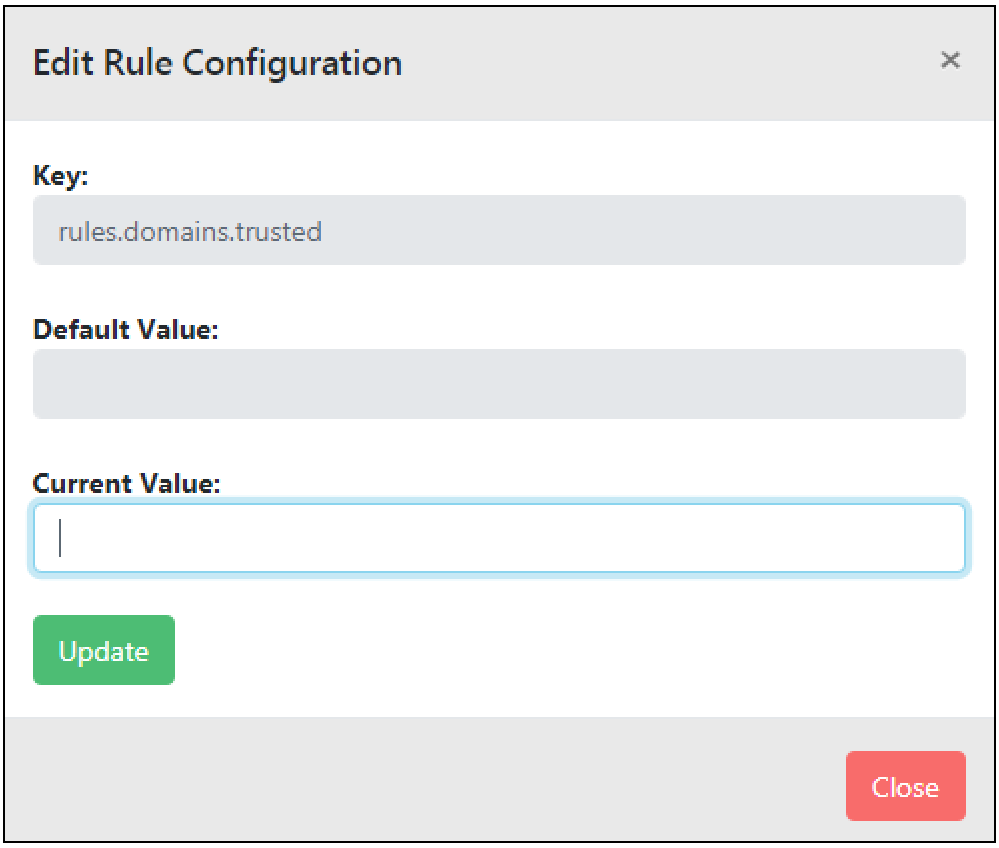


Rules Manager

Key	Default Value	Current Value	Description	Action
rules.common.sleep	15	15	The length of time in seconds used for timing attacks	✎ | ↺
rules.domains.trusted			A comma separated list of URL regex patterns. Any URLs that match the patterns will be considered trusted domains and the issues ignored.	✎ | ↺
rules.cookie.ignorelist			A comma separated list of cookie names. Cookies included in this list will be ignored when scanning for cookie related issues.	✎ | ↺
rules.csrf.ignore.attvalue			The value of an HTML attribute named by 'rules.csrf.ignore.attname' that can be used to indicate that a form does not need an anti-CSRF Token. If found any related alerts will be raised at INFO level.	✎ | ↺
rules.domxss.browserid			The ID of the browser to be used by DOM XSS scan rule. The IDs supported are documented in the help of DOM XSS add-on.	✎ | ↺

Editing the Rule Configuration

1. To edit the rule configuration, click ✎.
   Edit Rule Configuration window appears.



Edit Rule Configuration

Key: rules.domains.trusted

Default Value:

Current Value:

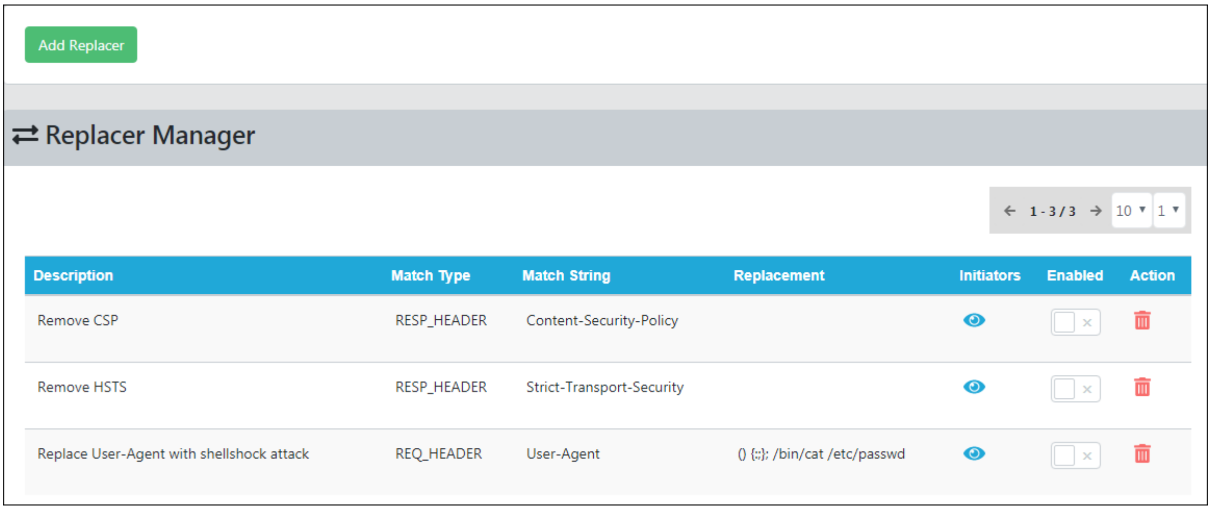
2. Enter the value in the **Current Value** field. Click **Update** to save the changes.

Resetting the pre-defined rules

To reset a rule, click ↺. The rule will reset to the default value.

Replacer Manager

This submodule is used in matching the string and then replacing it with the others for different initiators. It will display the following details of the replacement rule name, match type, match string, match regex, replacement, initiators, enabled, and action.



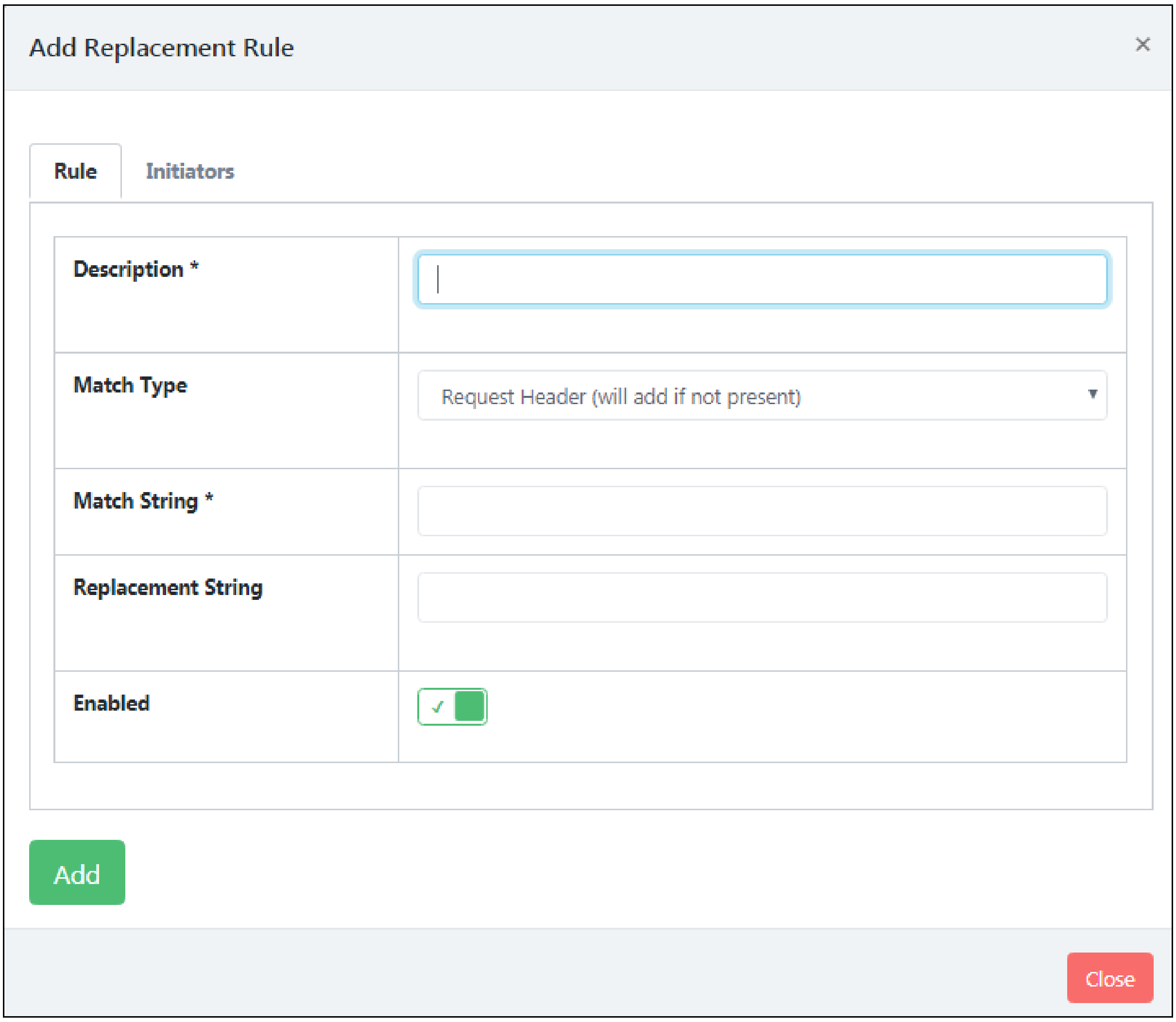
⇄ Replacer Manager

Description	Match Type	Match String	Replacement	Initiators	Enabled	Action
Remove CSP	RESP_HEADER	Content-Security-Policy		👁	□ ×	🗑
Remove HSTS	RESP_HEADER	Strict-Transport-Security		👁	□ ×	🗑
Replace User-Agent with shellshock attack	REQ_HEADER	User-Agent	() {:;}; /bin/cat /etc/passwd	👁	□ ×	🗑

Adding a Replacement Rule

To add a replacement rule, click **Add Replacer Rule**.
Add Replacement Rule window appears. It consists of following tabs:

- **Rule**
- **Initiators**



Add Replacement Rule ×

Description *	
Match Type	Request Header (will add if not present) ▾
Match String *	
Replacement String	
Enabled	✓

In **Rule** tab fill the details.

Description
Enter a name for the rule.

Match Type
Click the dropdown. Following options are available in the dropdown.

- **Request Header (will add if not present)**
  In this option, Match String will be a header name. If header is present then it will be replaced with the Replacement String. If header is empty and Replacement String is present then the header will be added. If Replacement String is empty then the header (if present) will be deleted.

- **Request Header String**
  In this option, Match String will be a string or regex expression. If it is present in the request header then it will be replaced with Replacement String.

- **Request Body String**
  In this option, Match String will be a string or regex expression. If it is present in the request body then it will be replaced with Replacement String.

- **Response Header (will add if not present)**
  In this option, Match String will be a header name. If header is present then it will be replaced with the Replacement String. If header is empty and Replacement String is present then the header will be added. If Replacement String is empty then the header (if present) will be deleted.

- **Response Header String**
  In this option, Match String will be a string or regex expression. If it is present in the response header then it will be replaced with Replacement String.

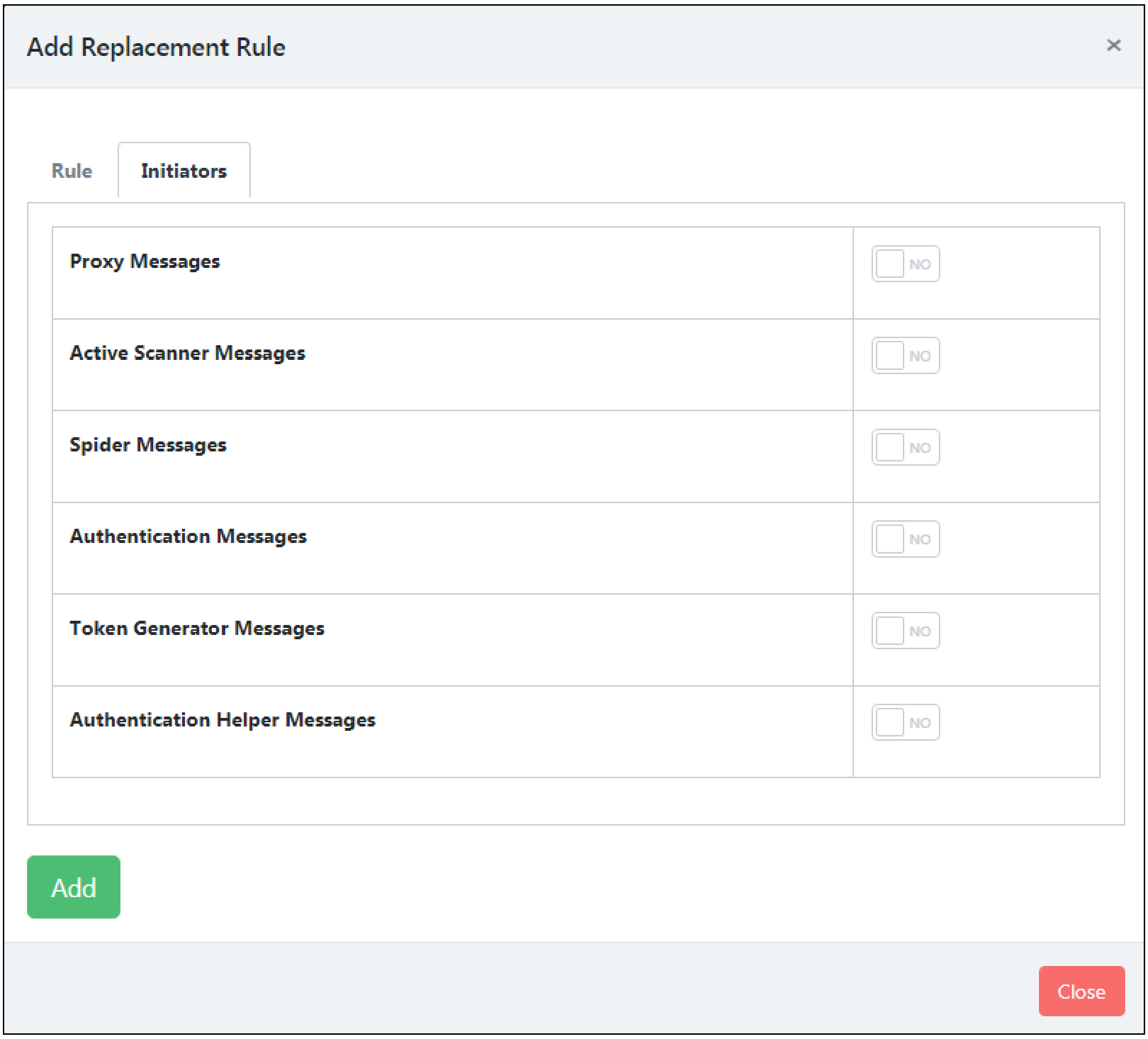
- **Response Body String**
  In this option, Match String will be a string or regex expression. If it is present in the response body then it will be replaced with Replacement String.

Match String
Add the string that has to be matched and replaced. To know more see **Match Type**.

Replacement String
Add the new string that will be used for replacement.

Enabled
If this option is not set then the rule will not apply.

Click the **Initiators** tab; toggle the rules on which the replacement rules have to be applied.
This gives you control over precisely when the rules that should be applied.



Add Replacement Rule

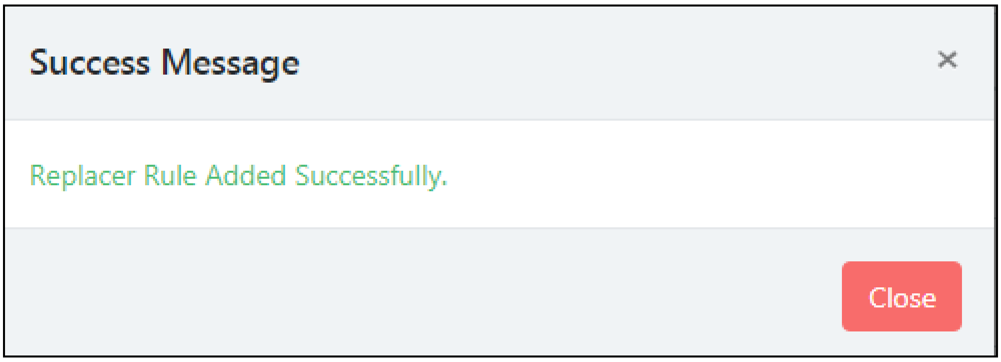
Proxy Messages	NO
Active Scanner Messages	NO
Spider Messages	NO
Authentication Messages	NO
Token Generator Messages	NO
Authentication Helper Messages	NO

Following options are available:

- **Proxy Messages**: When this initiator is enabled then the active scanner will replace request and response string from Proxy according to the **Match Type** set in the **Rule** tab.
- **Active Scanner Messages**: When this initiator is enabled then the active scanner will replace request and response string from Active Scanner according to the **Match Type** set in the **Rule** tab.
- **Spider Messages**: When this initiator is enabled then the active scanner will replace request and response from Spider according to the **Match Type** set in the **Rule** tab.
- **Authentication Messages**: When this initiator is enabled then the active scanner will replace request and response string while Authentication according to the **Match Type** set in the **Rule** tab.
- **Token Generator Messages**: When this initiator is enabled then the active scanner will replace request and response string when a token is generated according to the **Match Type** set in the **Rule** tab.

- **Authentication Helper Messages**: When this initiator is enabled then the active scanner will replace request and response string from Authentication Helper according to the **Match Type** set in the **Rule** tab.

After all the details are filled, click **Add**.
You will get the successful message.

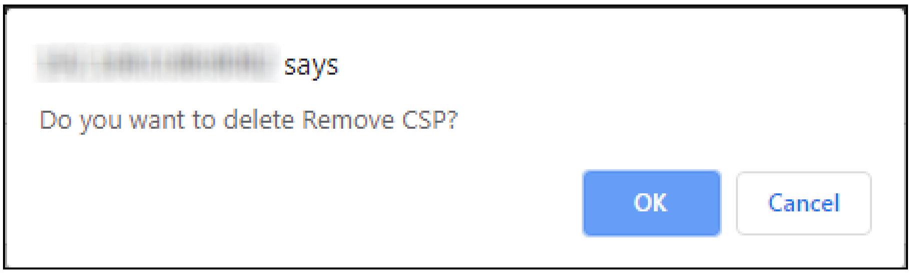


Success Message

Replacer Rule Added Successfully.

Deleting a Replacer Rule

1. To delete a Replacer rule, click 🗑.
   A delete confirmation prompt appears.



[redacted] says

Do you want to delete Remove CSP?

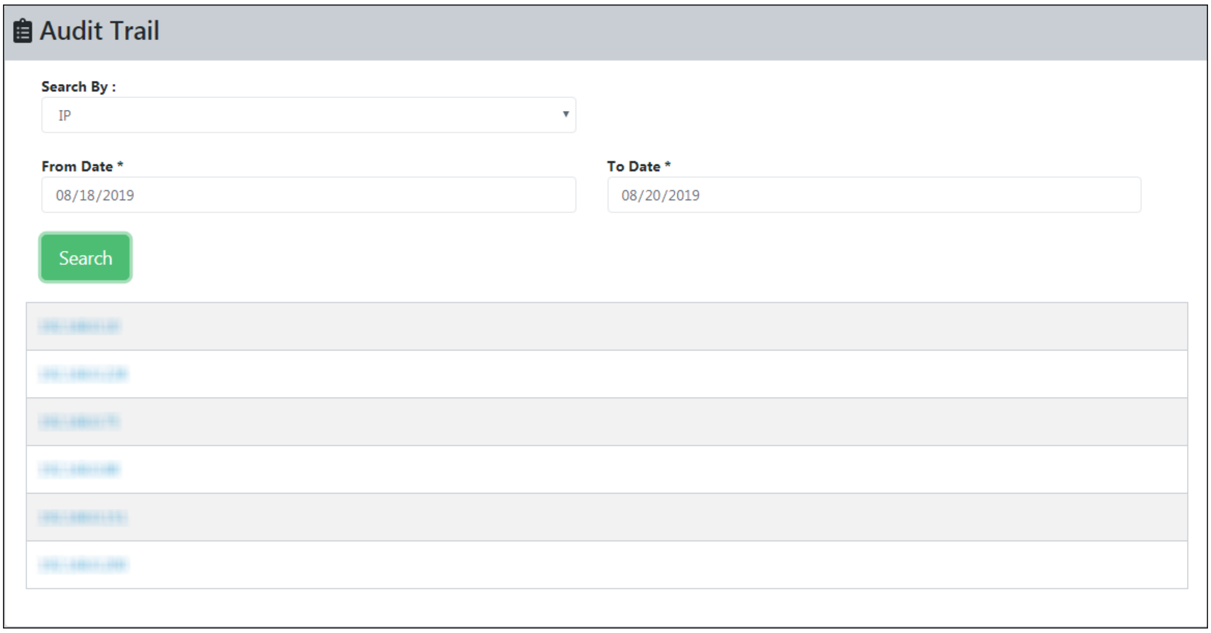
2. Click **OK**. The Replacement Rule will be deleted.

Audit Trail

You can view the audit by using the IP address of the system. You can also filter the audit based on the date and month on which audit was performed.

Search audit trail by IP address

1. Select the range date in the **From Date** and **To Date** fields.
2. Click **Search**. You will get the list of audit reports of different IPs.



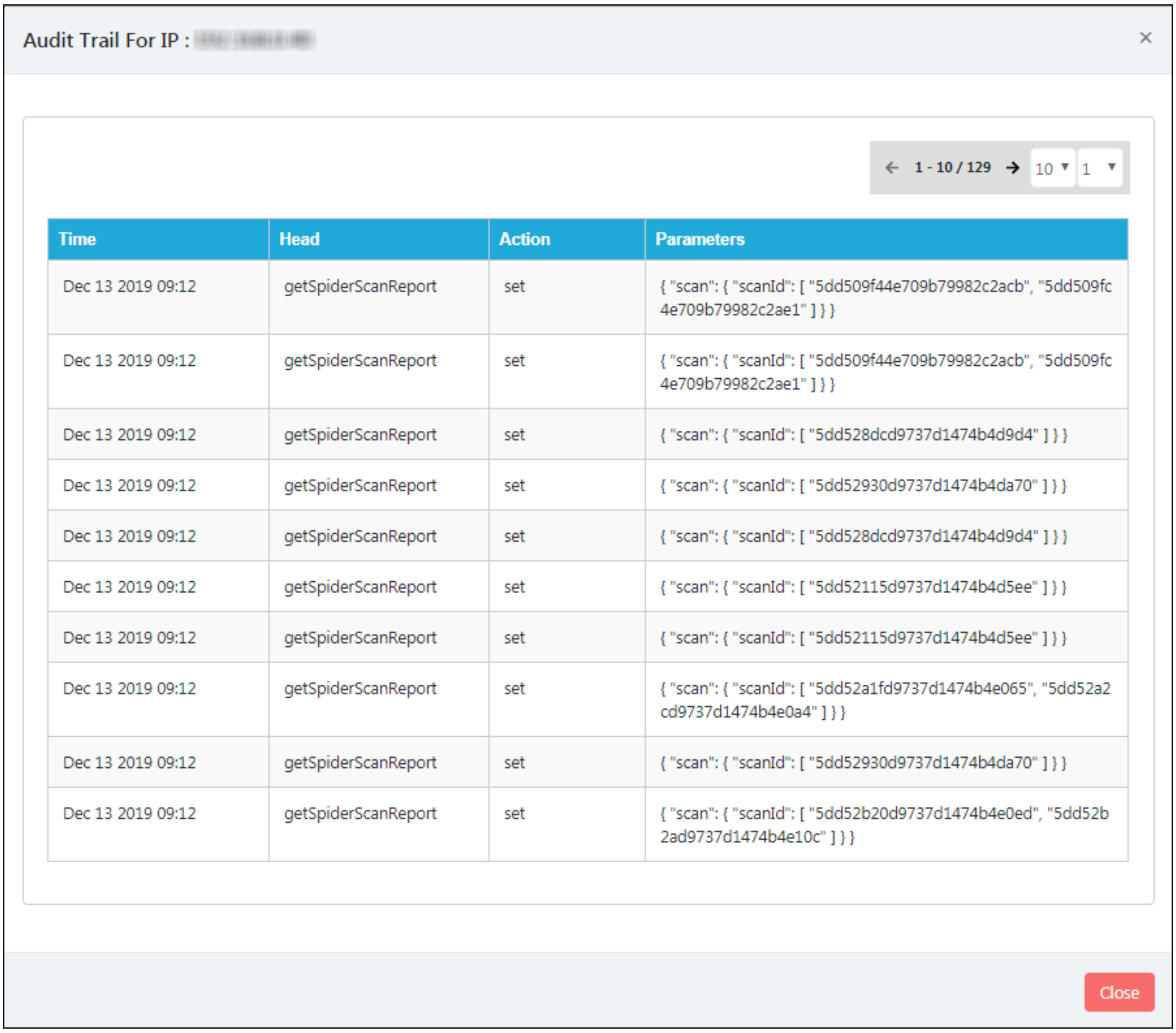
Audit Trail

Search By : IP

From Date * 08/18/2019

To Date * 08/20/2019

3. Click on the IP address for which you want to view the audit, you will get the detailed view of the audit.



Audit Trail For IP : [redacted]

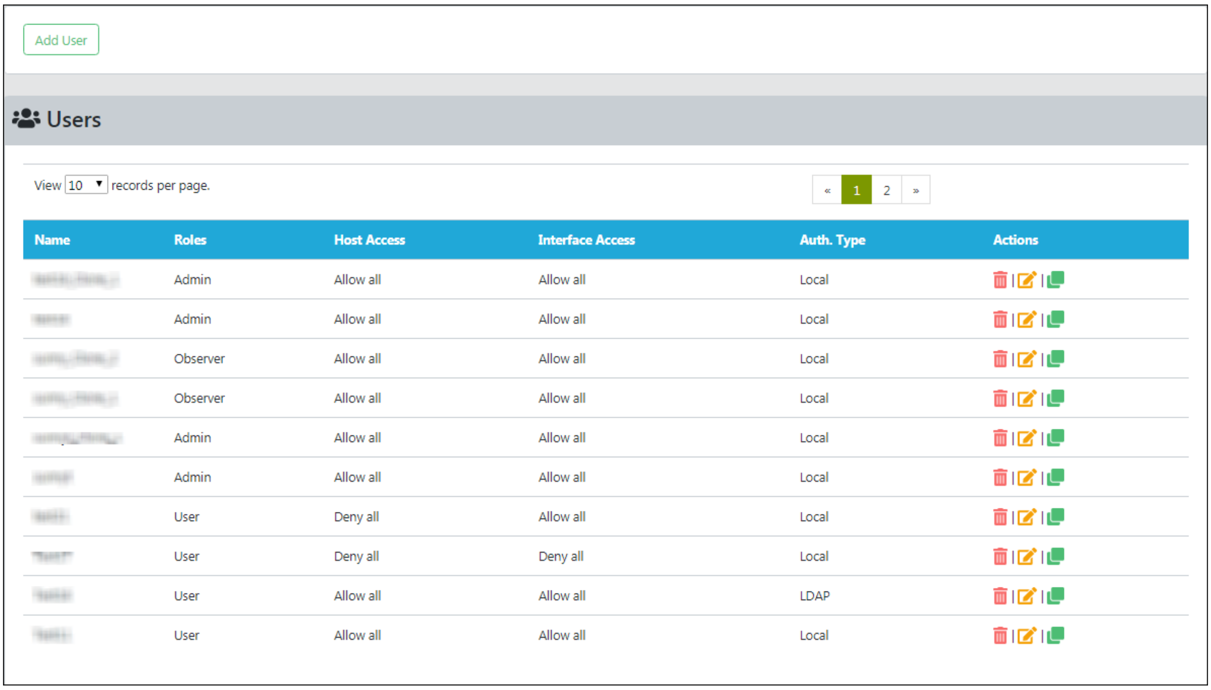
Time	Head	Action	Parameters
Dec 13 2019 09:12	getSpiderScanReport	set	{ "scan": { "scanId": ["5dd509f44e709b79982c2acb", "5dd509fc4e709b79982c2ae1"] } }
Dec 13 2019 09:12	getSpiderScanReport	set	{ "scan": { "scanId": ["5dd509f44e709b79982c2acb", "5dd509fc4e709b79982c2ae1"] } }
Dec 13 2019 09:12	getSpiderScanReport	set	{ "scan": { "scanId": ["5dd528dcd9737d1474b4d9d4"] } }
Dec 13 2019 09:12	getSpiderScanReport	set	{ "scan": { "scanId": ["5dd52930d9737d1474b4da70"] } }
Dec 13 2019 09:12	getSpiderScanReport	set	{ "scan": { "scanId": ["5dd528dcd9737d1474b4d9d4"] } }
Dec 13 2019 09:12	getSpiderScanReport	set	{ "scan": { "scanId": ["5dd52115d9737d1474b4d5ee"] } }
Dec 13 2019 09:12	getSpiderScanReport	set	{ "scan": { "scanId": ["5dd52115d9737d1474b4d5ee"] } }
Dec 13 2019 09:12	getSpiderScanReport	set	{ "scan": { "scanId": ["5dd52a1fd9737d1474b4e065", "5dd52a2cd9737d1474b4e0a4"] } }
Dec 13 2019 09:12	getSpiderScanReport	set	{ "scan": { "scanId": ["5dd52930d9737d1474b4da70"] } }
Dec 13 2019 09:12	getSpiderScanReport	set	{ "scan": { "scanId": ["5dd52b20d9737d1474b4e0ed", "5dd52b2ad9737d1474b4e10c"] } }

Administration

The Administration module lets you add new users, assign roles, define type of authentication and add LDAP, and add customize header to the reports. The Administration contains submodules which are **Users**, **Roles**, **Secure LDAP**, and **Customize Header**.

Users

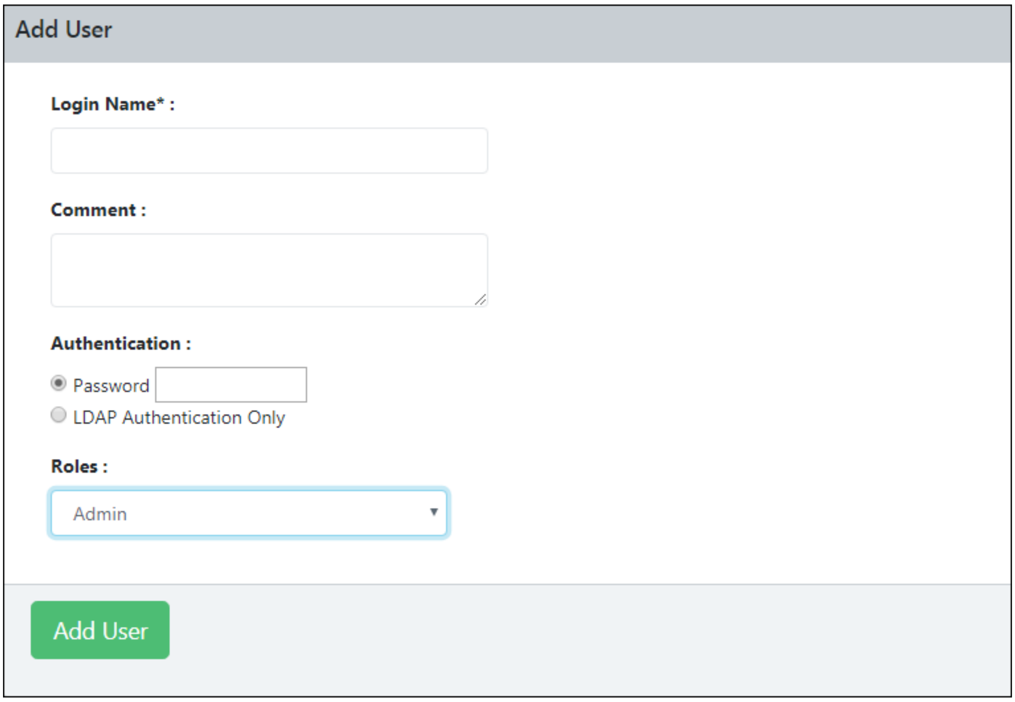
The **Users** submodule lets you add users, set authentication, and role for them.



Name	Roles	Host Access	Interface Access	Auth. Type	Actions
[redacted]	Admin	Allow all	Allow all	Local	🗑 | ✎ | ⧉
[redacted]	Admin	Allow all	Allow all	Local	🗑 | ✎ | ⧉
[redacted]	Observer	Allow all	Allow all	Local	🗑 | ✎ | ⧉
[redacted]	Observer	Allow all	Allow all	Local	🗑 | ✎ | ⧉
[redacted]	Admin	Allow all	Allow all	Local	🗑 | ✎ | ⧉
[redacted]	Admin	Allow all	Allow all	Local	🗑 | ✎ | ⧉
[redacted]	User	Deny all	Allow all	Local	🗑 | ✎ | ⧉
[redacted]	User	Deny all	Deny all	Local	🗑 | ✎ | ⧉
[redacted]	User	Allow all	Allow all	LDAP	🗑 | ✎ | ⧉
[redacted]	User	Allow all	Allow all	Local	🗑 | ✎ | ⧉

Adding a User

1. To add a User, click **Add User**.
   Add User form appears on the right pane.



Add User

Login Name* :

Comment :

Authentication :

● Password

○ LDAP Authentication Only

Roles : Admin

2. Enter a name for the User.
3. Enter a descriptive comment for the User.
4. Select the appropriate **Authentication** for the User login. There are two options available.
   - Password
   - LDAP Authentication Only

   If you are selecting the option **Password,** specify the password in the field next to it.

5. Click the dropdown and select the appropriate role for the User. The Roles and their accessible modules are mentioned below:
    - **Admin** – All modules
    - **Guest** – All modules
    - **Info** – Dashboard, Security Info, Passive Scanner, Help & Support
    - **Monitor** – Dashboard, Passive Scanner, Help & Support
    - **Observer** – Dashboard, Scan, Assets, Task Results, Reports, Security Info, Configurations, Passive Scanner, Help & Support
    - **User** – Dashboard, Scan, Assets, Task Results, Reports, Security Info, Configurations, Passive Scanner, Help & Support

6. After filling all the fields, click **Add User**. The new User will be added to the Users list.

Note	An individual User will have access to only their activities. Admin will be the superuser and have access to all users' activities.

Actions

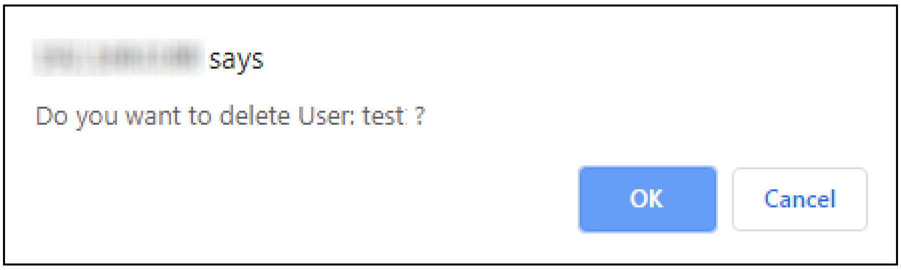
Clicking icons in the Actions column lets you take actions regarding a User.

- 🗑 Delete User
- ✎ Edit User
- ⧉ Clone User

Deleting a User

To delete a User, follow the steps given below:

1. In the Actions column, click 🗑.
   A delete confirmation prompt appears.



[redacted] says

Do you want to delete User: test ?

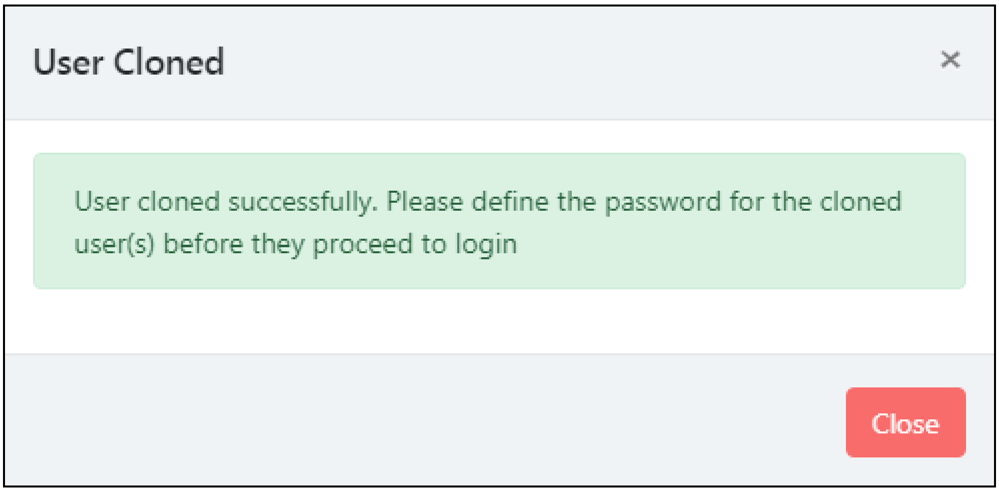
2. Click **OK**.
   The User will be deleted.

Note	A User will not be deleted if a scan task created by them is in progress.

Cloning a User

To clone a User, follow the steps given below:

1. In the Actions column, click 🟩.
   A success message appears.



User Cloned

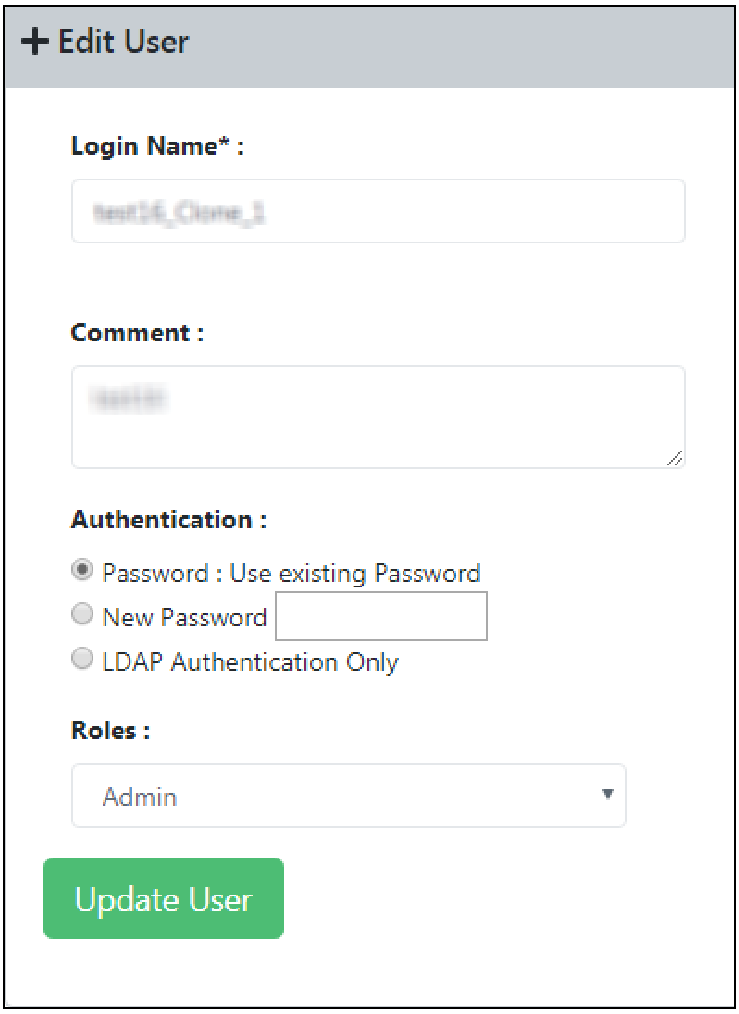
User cloned successfully. Please define the password for the cloned user(s) before they proceed to login

2. Close this message and then define the password for the Cloned User.

Editing a User

To edit a User’s details, follow the steps given below:

1. In the Actions column, click ✎.
   Edit User pop-up window appears.



+ Edit User

Login Name* : [redacted]

Comment : [redacted]

Authentication :

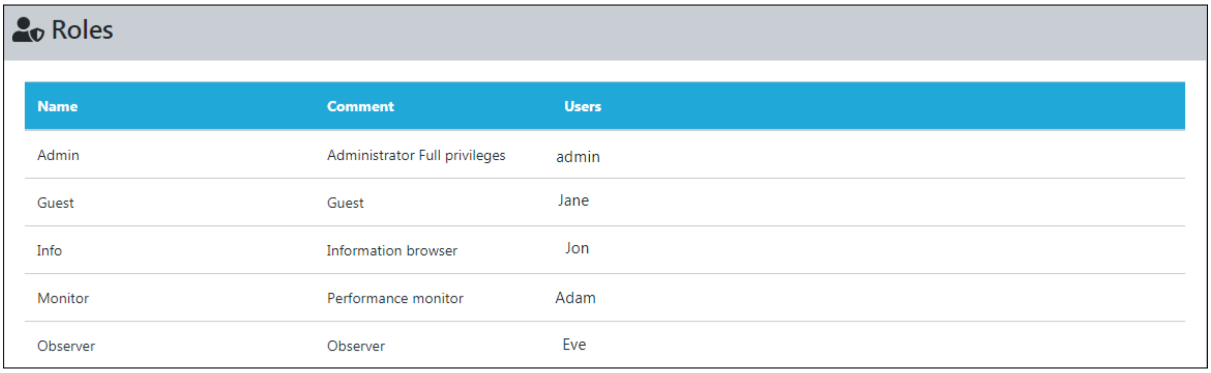
● Password : Use existing Password
○ New Password
○ LDAP Authentication Only

Roles : Admin

2. Make the necessary changes and then click **Update User**.
   The User details will be updated.

Roles

The Roles submodule displays the list of users and roles assigned to them.



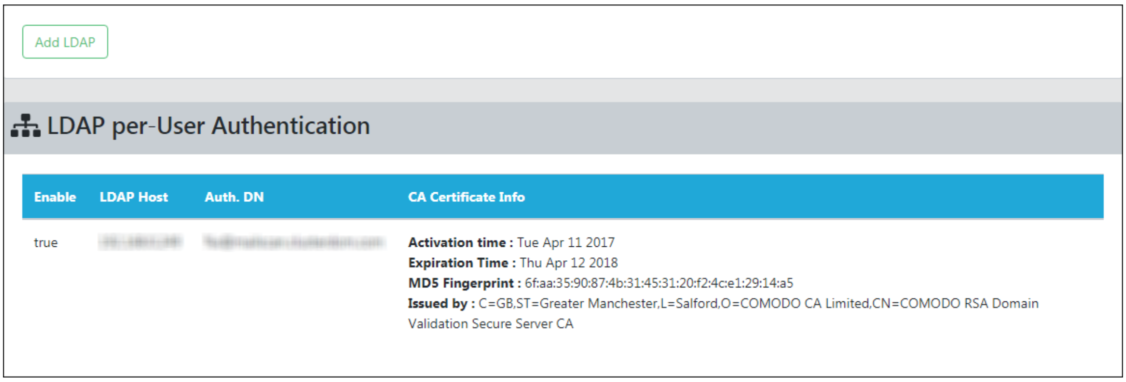
Roles

Name	Comment	Users
Admin	Administrator Full privileges	admin
Guest	Guest	Jane
Info	Information browser	Jon
Monitor	Performance monitor	Adam
Observer	Observer	Eve

Secure LDAP (LDAPS)

The Lightweight Directory Access Protocol (LDAP) is an industry standard application protocol for accessing and maintaining directory services across an organization. Nemasis uses a plain interface to add an LDAP. Normally the LDAP supporting systems search the LDAP tree for the matching object and after finding the object log in as the same (Search and Bind). The Nemasis utilizes a simple bind with a hard coded object path.

The Secure LDAP submodule displays added LDAPs and lets you add an LDAP.



LDAP per-User Authentication

Enable	LDAP Host	Auth. DN	CA Certificate Info
true	[redacted]	[redacted]	**Activation time :** Tue Apr 11 2017 **Expiration Time :** Thu Apr 12 2018 **MD5 Fingerprint :** 6f:aa:35:90:87:4b:31:45:31:20:f2:4c:e1:29:14:a5 **Issued by :** C=GB,ST=Greater Manchester,L=Salford,O=COMODO CA Limited,CN=COMODO RSA Domain Validation Secure Server CA

The DN (Distinguished Name) of an object can be defined in a distinctive manner. Thereby, the username is replaced by wildcard %s. Some examples for Auth. DN are mentioned below:

- cn=%s,ou=people,dc=domain,dc=de
- uid=%s,ou=people,dc=domain,dc=de
- %s@domain.de
- domain.de\%s

With correct attributes, the first two examples work for all LDAP servers. For an Active Directory, the third and fourth examples can be used.

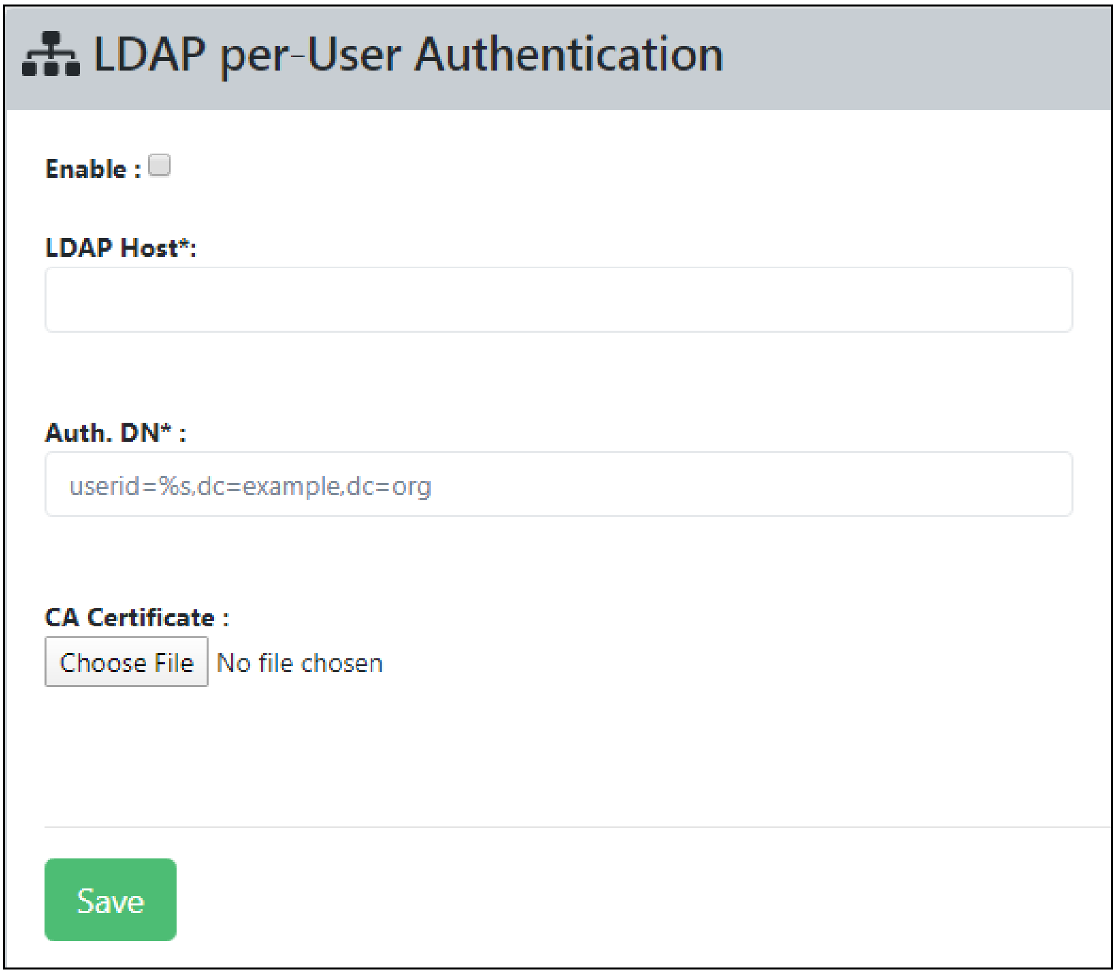
Hereby the exact location of the user object is irrelevant.
The first example is unable to support users in different recursive depths of an LDAP tree or different sub trees. It is necessary that every user that logs into Nemasis, must be in the same branch and level of an LDAP tree.

In second example,
uid = user is used as a filter
ou = people
dc = domain
dc = org

The above mentioned attributes are used as base objects to carry out a search and get the corresponding DN for authentication. As the **uid** attribute is important it should be typed first.

Adding an LDAP

1. To add an LDAP, click **Add LDAP**.
   LDAP per User authentication form appears on the right pane.



LDAP per-User Authentication

Enable : □

LDAP Host*:

Auth. DN* :

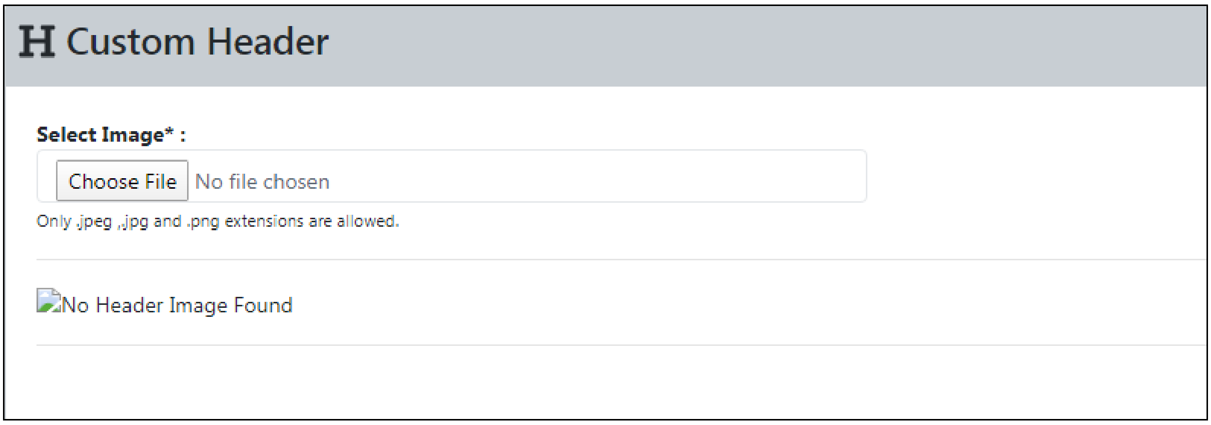
userid=%s,dc=example,dc=org

CA Certificate :

2. Select the **Enable** checkbox. Enter the IP address of the LDAP Host server. The Nemasis will access the LDAP host via SSL/TLS.
3. Enter the appropriate Distinguished Name.
4. Click **Choose File** and select the CA certificate. For verification of the LDAP Host, it is necessary that you upload its CA certificate to the Nemasis. Users should note that the Nemasis will refuse the LDAP authentication without the SSL/TLS. If the LDAP authentication fails, please check whether the LDAP Host entry matches the commonName of the certificate of the LDAP server. If the entries do not match, Nemasis will refuse the LDAP server use.
5. After filling all the details, click **Save**. The new LDAP will be added to Nemasis.

Customize Header

The Customize Header submodule helps you to customize the report header that appears on each page.



H Custom Header

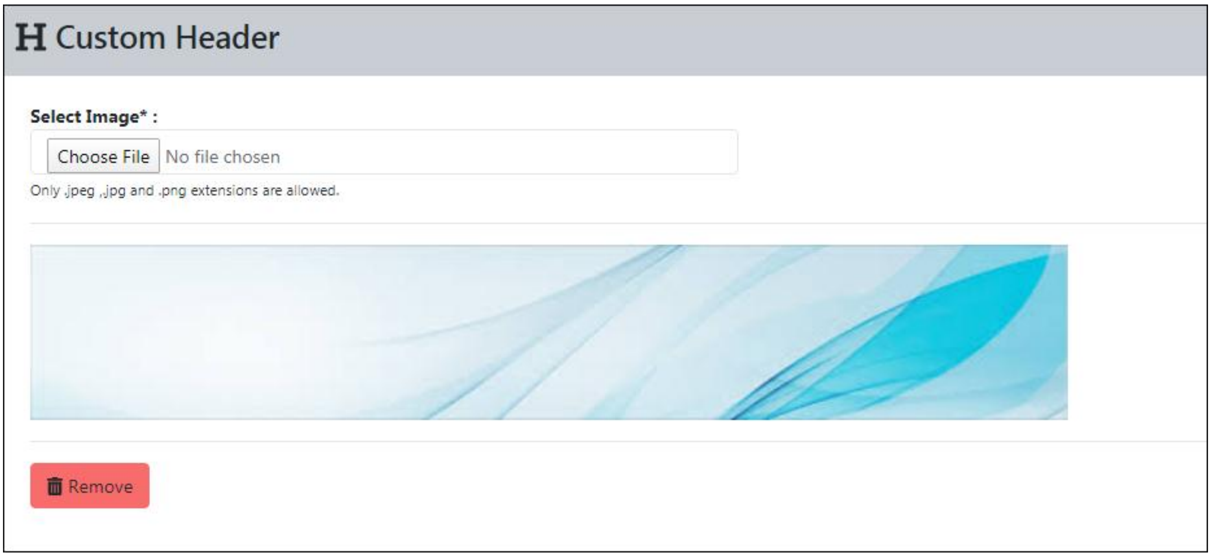
Select Image* :

Only .jpeg .jpg and .png extensions are allowed.

No Header Image Found

Adding a Custom Header

1. To add a custom header, click **Choose File.**
   File selection window appears.



H Custom Header

Select Image* :

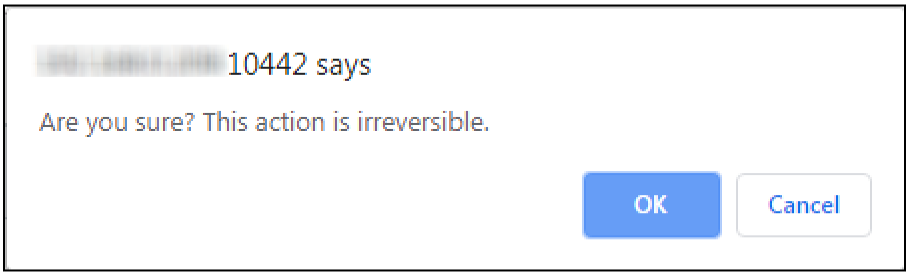
Only .jpeg .jpg and .png extensions are allowed.

2. After uploading the file, the custom header appears on all future reports.

Removing the Custom Header

To delete the Custom Header, follow the steps given below:

1. To remove the custom header, click **Remove**.
   A delete confirmation prompt appears.



[redacted]10442 says

Are you sure? This action is irreversible.

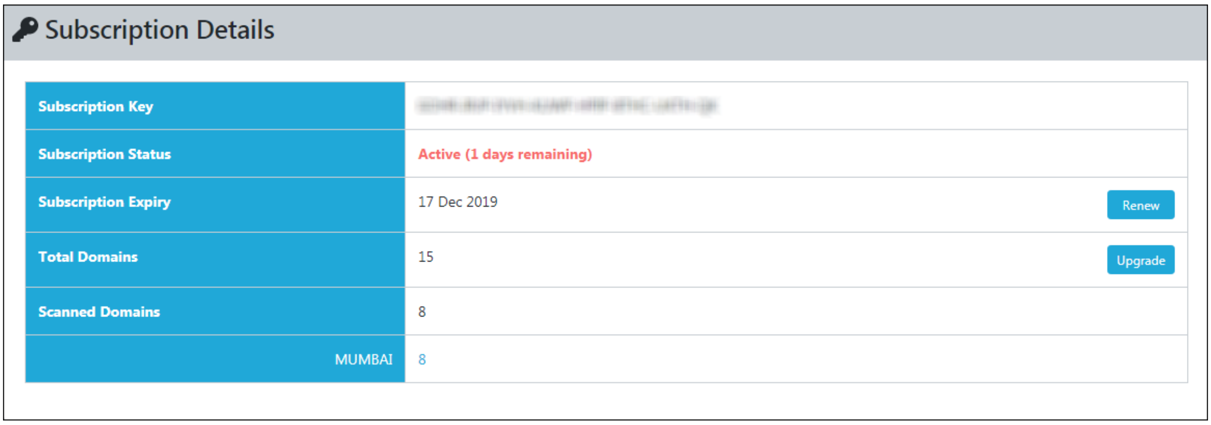
2. Click **OK**. The custom header will be deleted.

License

The License module has **Subscription Details** submodule, it consist of license information.

Subscription Details

The Subscription Details submodule shows your Subscription Key, Subscription Status, Subscription Expiry, Total Domains, and Scanned Domains. The module also lets you enter the subscription key and buy new license. You can also Upgrade and Renew your subscription.



Subscription Details

Subscription Key	[redacted]	
Subscription Status	Active (1 days remaining)	
Subscription Expiry	17 Dec 2019	Renew
Total Domains	15	Upgrade
Scanned Domains	8	
MUMBAI	8	

Subscription Status

It displays your subscription status (Trial, Active or Trial Expired).

Subscription Expiry

It displays your subscription expiry date.

Total Domain

It displays the total number of domain you are allowed to scan.

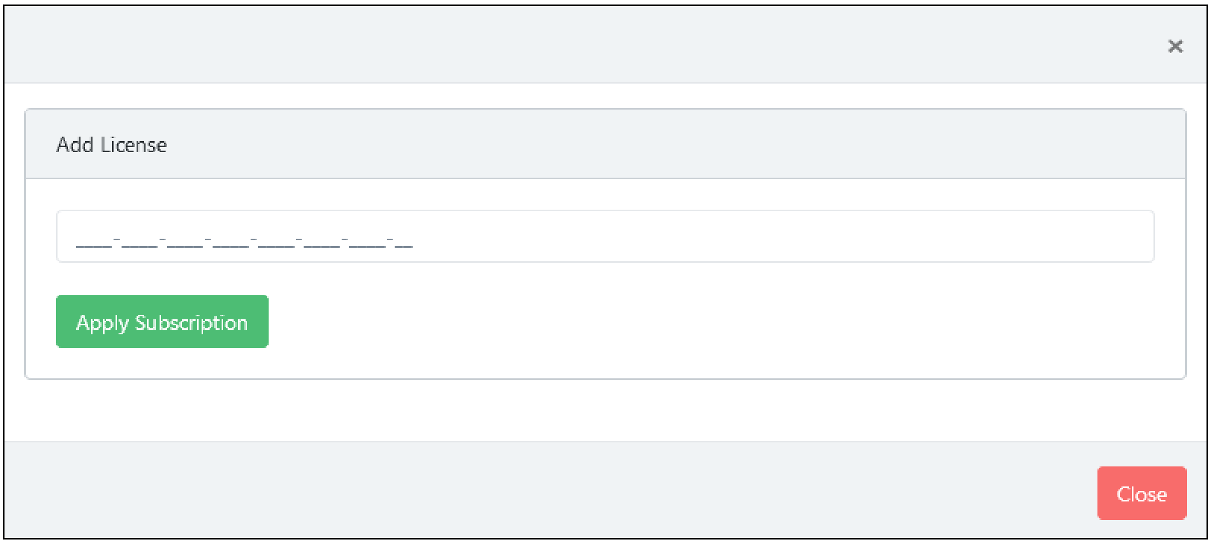
Scanned Domain

It displays the total number of domain you have scanned.

Enter Subscription Key

To enter the subscription key for Nemasis, click **Enter Subscription Key**.

Add License pop-up window appears.



Enter license key and then click **Apply Subscription**. A success message appears informing about successful registration.

Buy Now

The Trial version is valid for 7 **days** and lets you scan one domain with 2 levels (Depth of 2). If you have scanned domains with more than depth of 2, you will have to buy a new license. To buy a new license, click **Buy Now**.

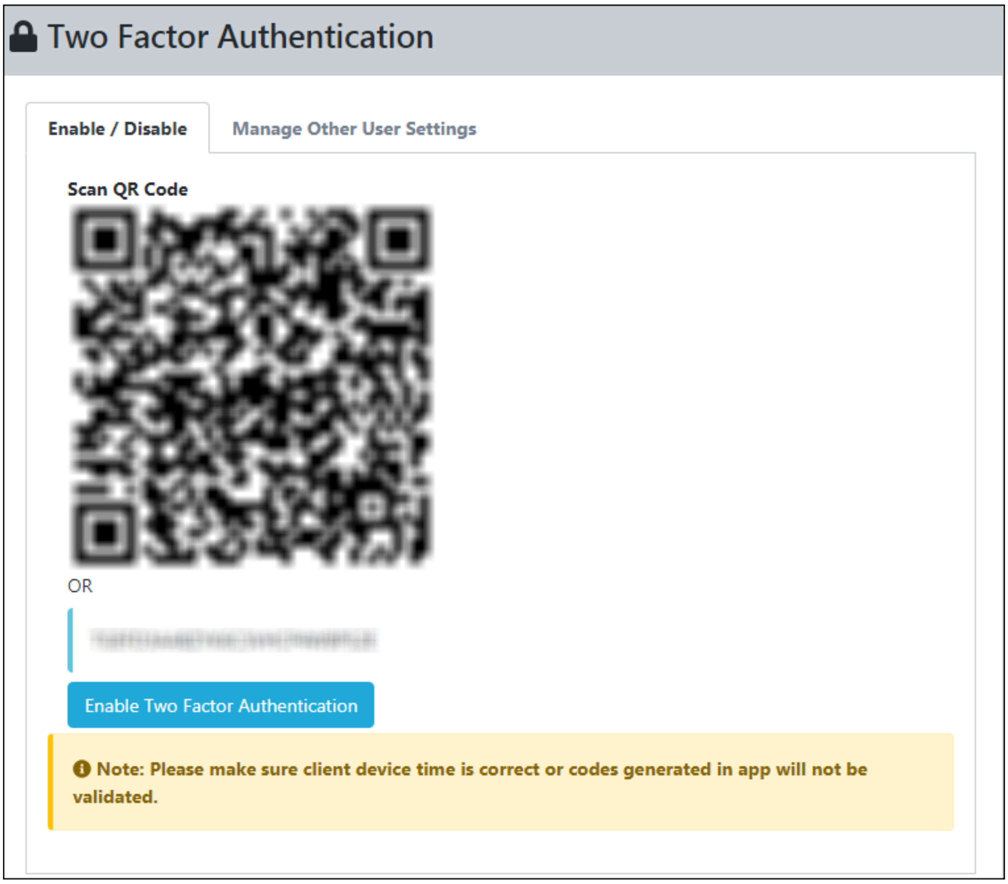
Manage Instance

The Manage Instance module lets you to import and export the Nemasis instance. It also has Two Factor Authentication along with lets user to get offline updates. The Manage Instance contains three submodules which are **Two Factor Auth. (2FA)**, **Import & Export**, and **Offline Update**.

Two Factor Auth. (2FA)

The 2FA submodule lets user to add an extra layer of protection to the Nemasis instance. This can be enabled by admin of the system, and then this feature can be enabled for the other users (roles) as well.

This module has two tabs, namely, **Enable / Disable** and **Manage Other User Setting**.

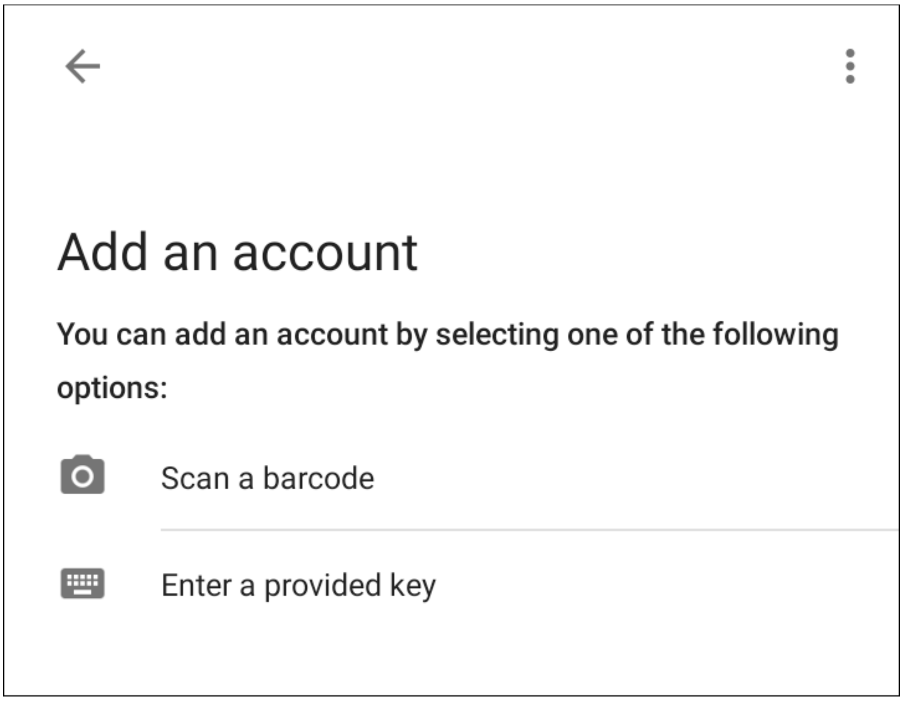

Two Factor Authentication
Enable / Disable
Manage Other User Settings
Scan QR Code
OR
Enable Two Factor Authentication

Note: Please make sure client device time is correct or codes generated in app will not be validated.

Enabling 2FA

To enable 2FA, follow the following steps:

1. In the 2FA screen, scan the QR code or insert the code provided on the Nemasis Console in the Authenticator app.



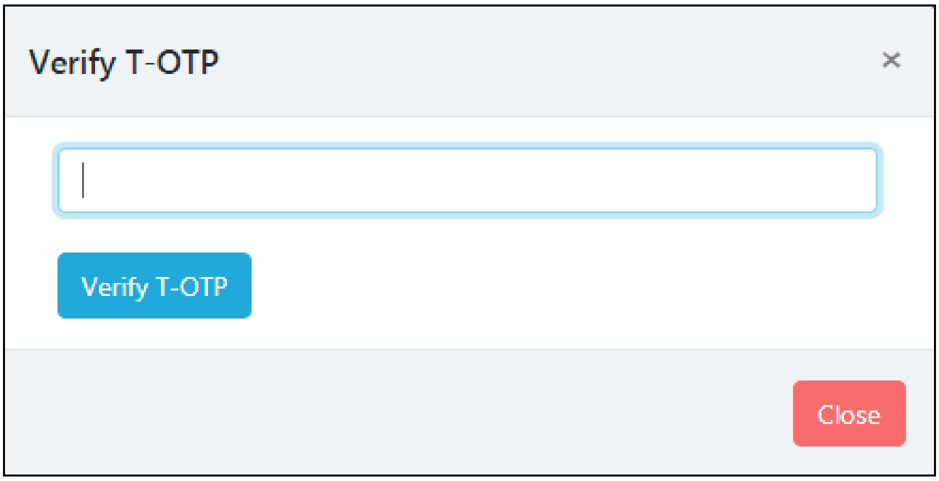
Add an account

You can add an account by selecting one of the following options:

Scan a barcode

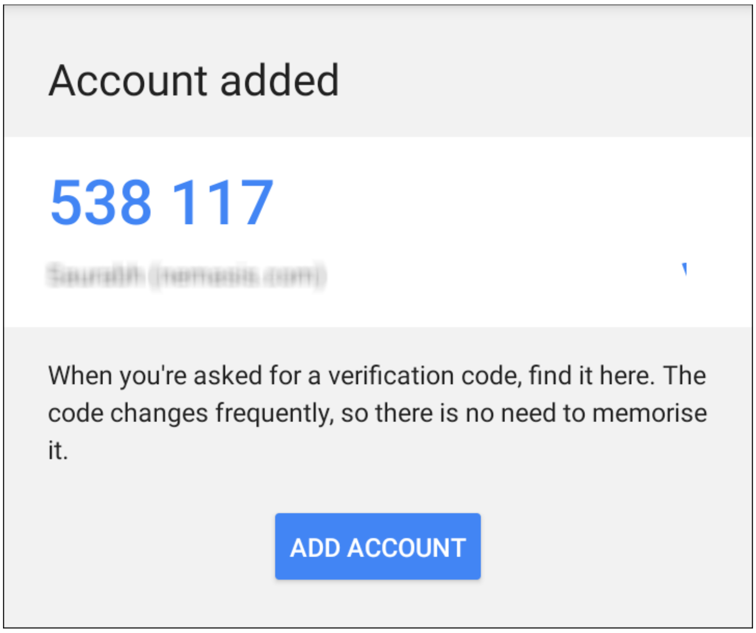
Enter a provided key

2. After scanning or entering the code, **Verify T-OTP** screen pops-up.



Verify T-OTP

3. Enter the OTP received on Authenticator app.



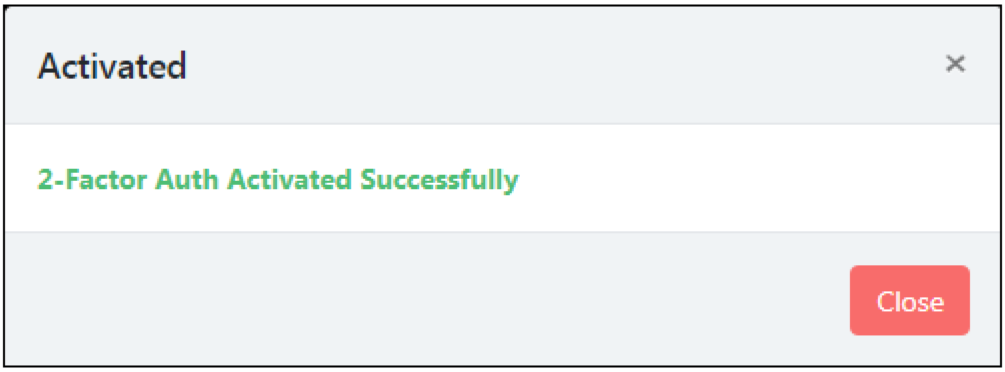
Account added

538 117

[redacted]

When you're asked for a verification code, find it here. The code changes frequently, so there is no need to memorise it.

4. After entering OTP, the 2FA feature will be enabled on the Nemasis Instance with a success message.



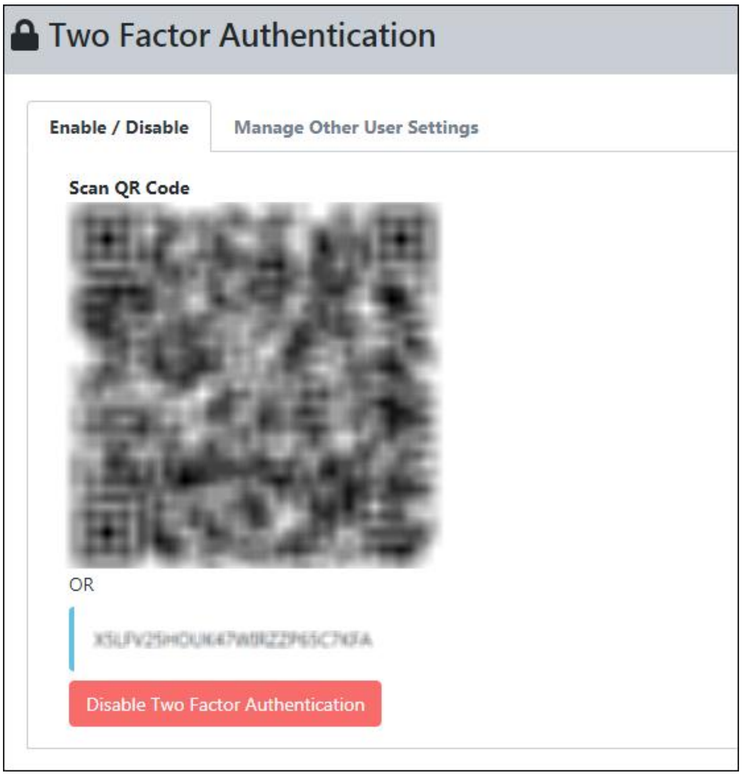
Activated

2-Factor Auth Activated Successfully

Disabling 2FA

To disable 2FA, follow the following steps:

1. Go to Two Factor Authentication page, click on **Disable Two Factor Authentication**.



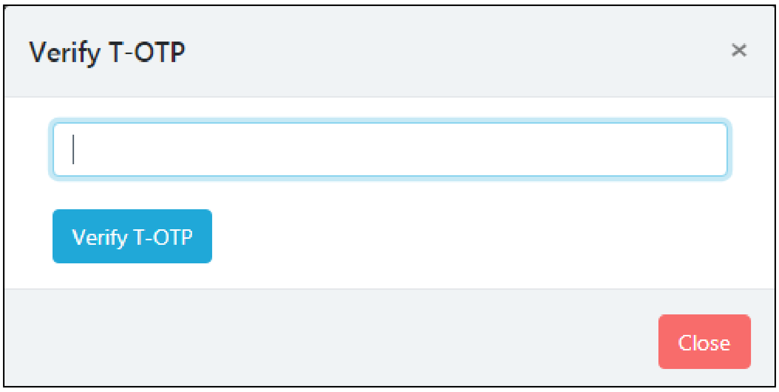
Two Factor Authentication

Scan QR Code

OR

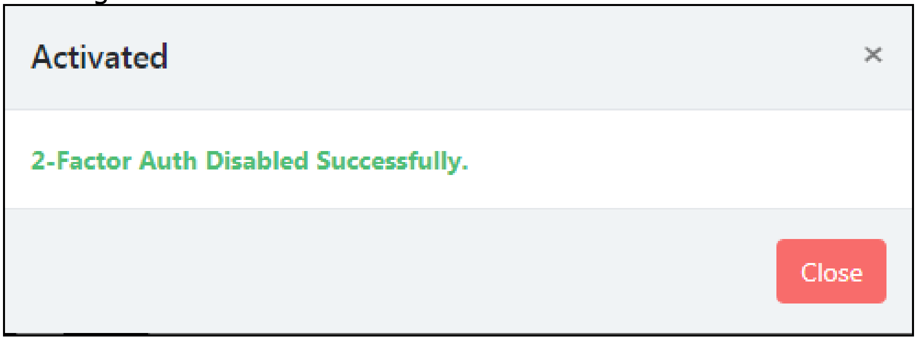
[illegible]

2. **Verify T-OTP** window pops-up.



Verify T-OTP

3. After entering the OTP received. Click **Verify T-OTP**, the 2FA will be disabled with success message.

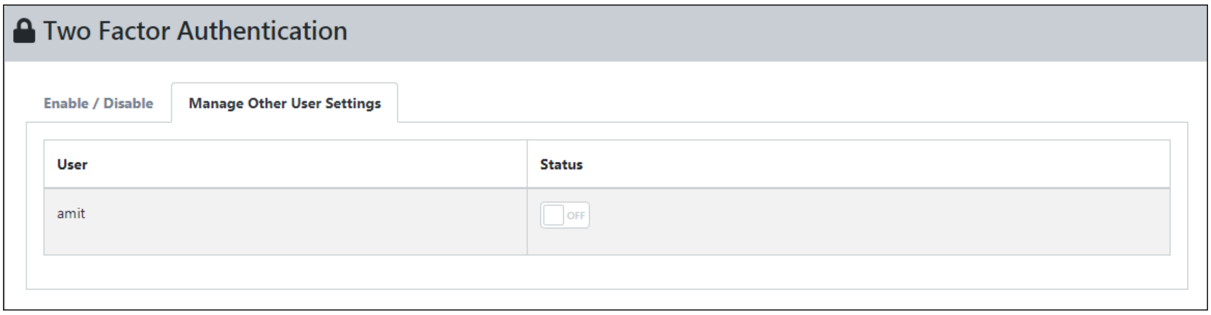


Activated

2-Factor Auth Disabled Successfully.

Managing Other User Settings

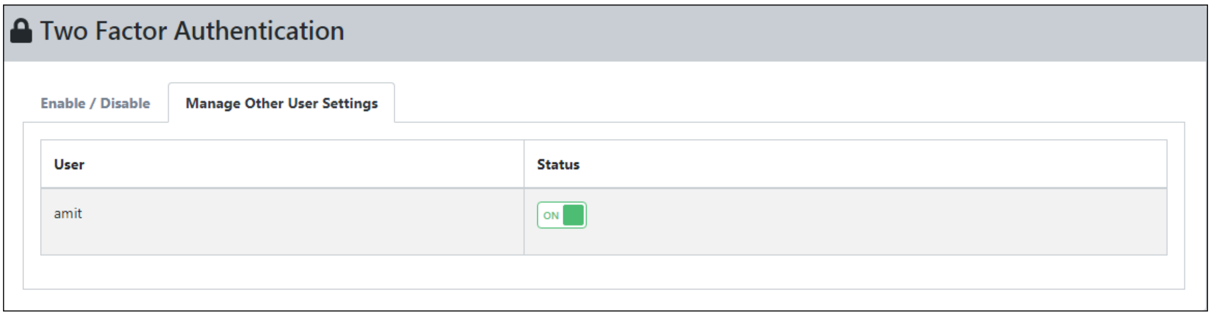
The **Managing Other User Setting** tab helps to enable 2FA feature for other users as well. This tab will have list of users added in the **User** submodule.
To know more, refer to **Adding a User**.



Two Factor Authentication

User	Status
amit	OFF

Enable the 2FA for other users by toggling the button under **Status** column.



Two Factor Authentication

User	Status
amit	ON

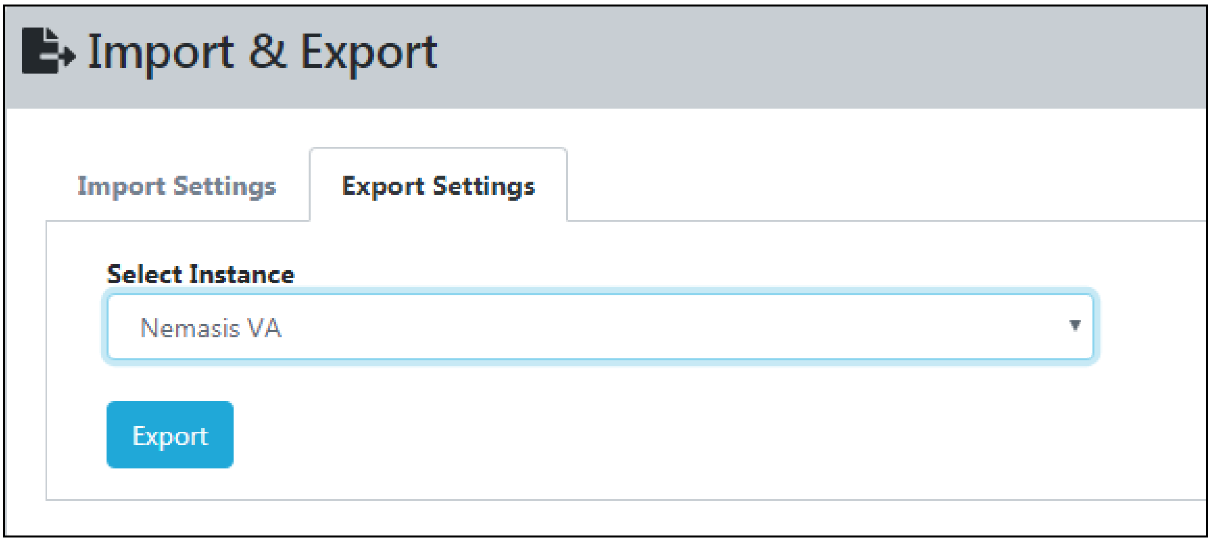
Import & Export

The Import & Export submodule lets user to import and export the Nemasis instance. This feature helps the organization to create a backup of the data of the instance and used in case of any disaster management or system failure.

Exporting a Instance

To export a Nemasis instance, follow the following steps:

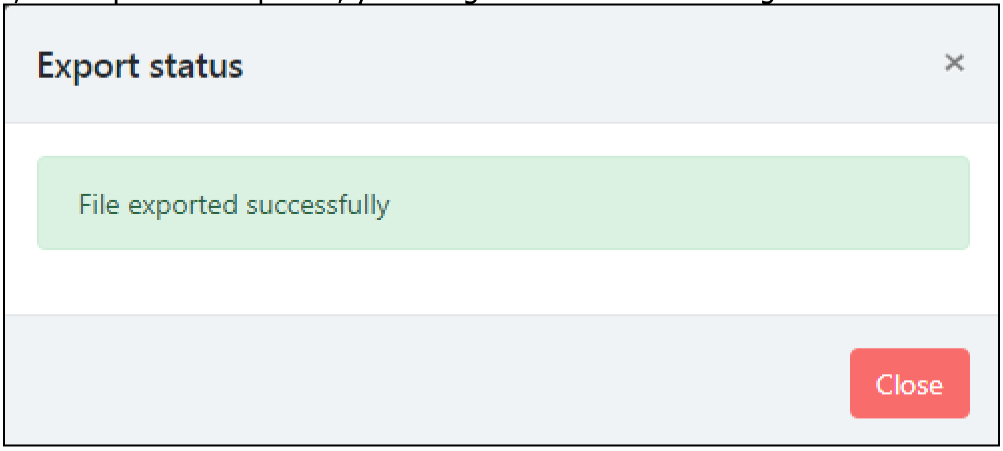
1. Select Instance, namely, Nemasis VA, Nemasis DA, and Nemasis VA & DA from the **Export Setting** tab.



Import & Export

Select Instance: Nemasis VA

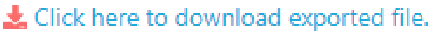
2. After selecting instance, click **Export**.
3. Once, the export is completed, you will get a successful message.



Export status

File exported successfully

4. After the file is exported is successfully, you can download the file by clicking

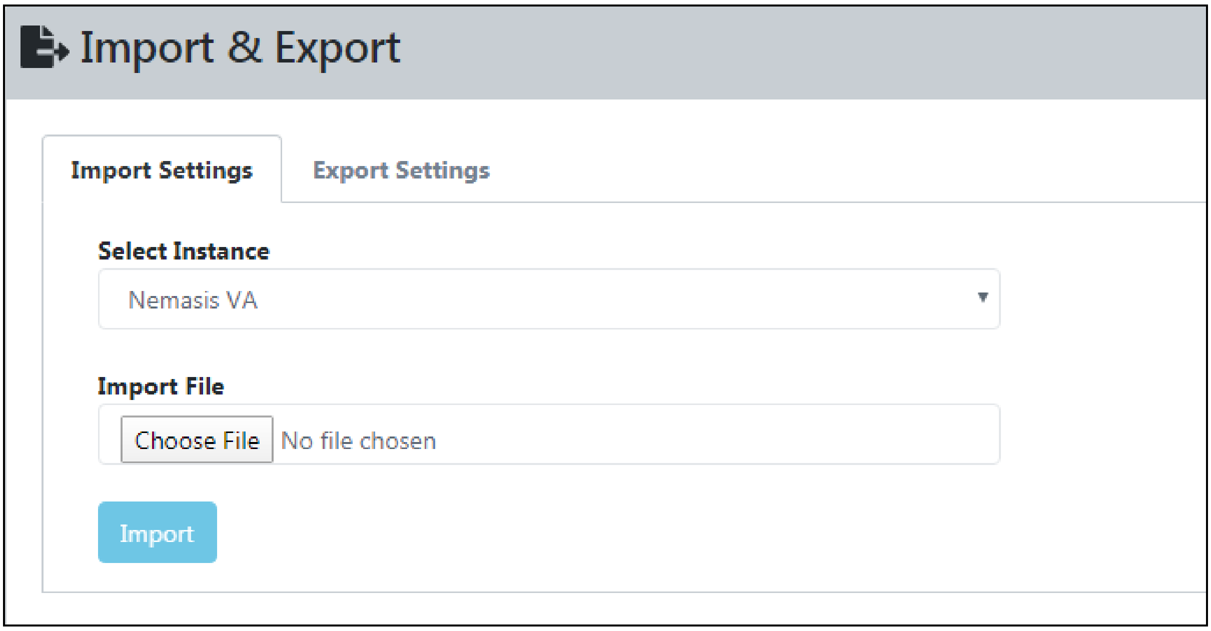


Click here to download exported file.

Importing a instance

To import a Nemasis instance, follow the following steps:

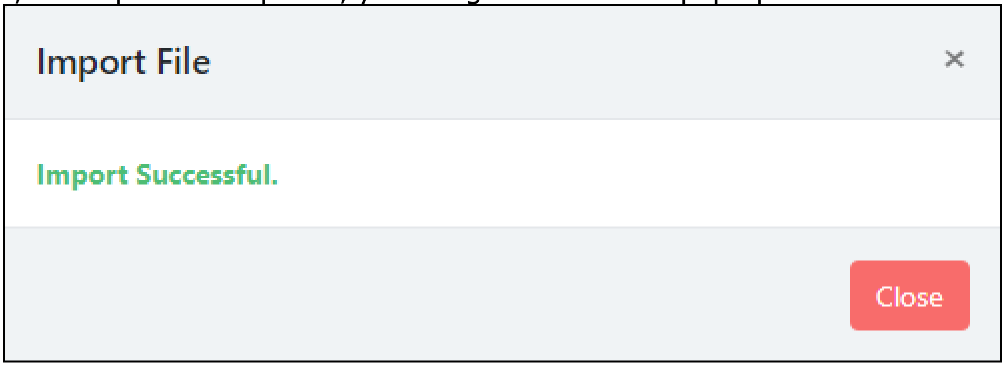
1. To import the instance, **Select Instance** from the dropdown menu. It has following options:
   - Nemasis VA
   - Nemasis DA
   - Nemasis VA & DA



Select Instance
Nemasis VA

Import File
Choose File No file chosen

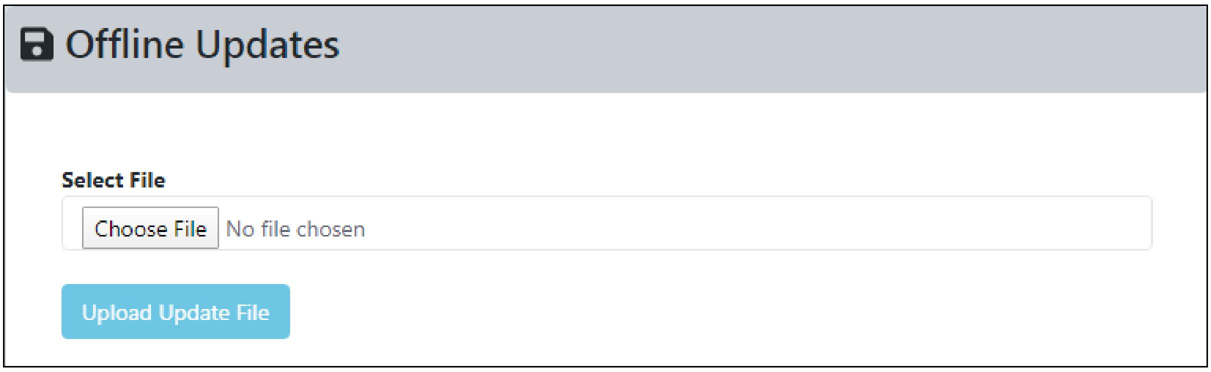
2. After selecting instance, choose file to import. Click **Import** button
3. Once, the import is completed, you will get a successful pop-up.



Import Successful.

Offline Updates

The **Offline Updates** submodule helps user to update Nemasis through offline mode for air-gapped system. User can download the patch from other system which is connected to the internet and can upload the patch to the Nemasis instance.
With Offline Updates, you can update/upgrade the Nemasis instance even if Nemasis trial period is over or license has expired.



Offline Updates

Select File

NOTE	Depending upon the component change, a running task may get interrupted.

Uploading Offline Updates

To upload the offline updates, perform the following steps:

1. Go to link provided below, and then download the available update patch (in ZIP format).
2. After downloading the patch, click on the **Upload Update File**. This will update the Nemasis instance through offline mode.

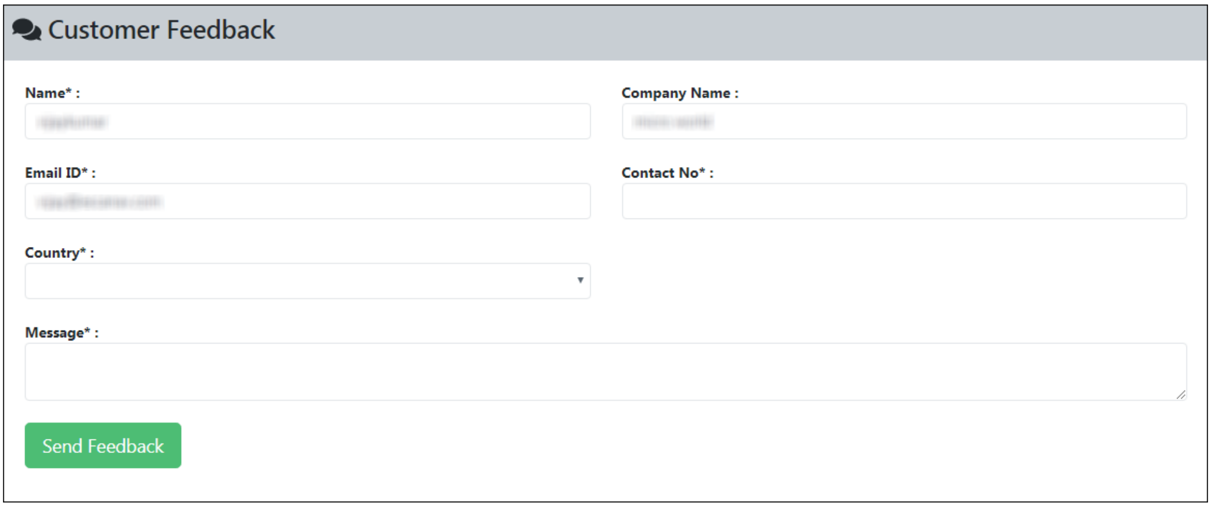
Note	Link for the Offline Update: https://download1.mwti.net/nemasis/nemasis_update.zip

Help & Support

The Help and Support module contains **Feedback** and **Support Request** submodules.

Feedback

The Feedback submodule lets you send a feedback about Nemasis DAST.



Customer Feedback

Name* : [illegible]

Company Name : [illegible]

Email ID* : [illegible]

Contact No* :

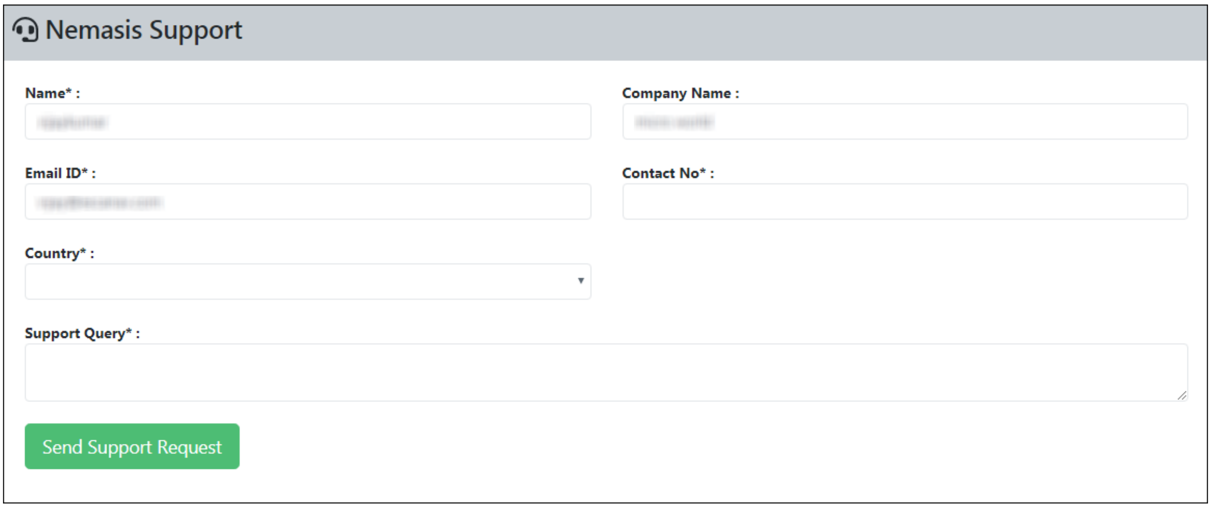
Country* :

Message* :

Your personal details are auto filled by Nemasis. Enter your feedback in the **Message** field and then click **Send Feedback**.

Support Request

The Support Request submodule lets you send a support request.



Nemasis Support

Name* : [illegible]

Company Name : [illegible]

Email ID* : [illegible]

Contact No* :

Country* :

Support Query* :