Tenable.io Web Application Scanning

Last Updated: January 23, 2018

Table of Contents

Getting Started with Tenable.io Web Application Scanning

Tenable.io Web Application Scanning offers significant improvements over the existing **Web Application Tests** policy template provided by the Nessus scanner, which is incompatible with modern web applications that rely on Javascript and are built on HTML5. This leaves you with an incomplete understanding of your web application security posture.

Tenable.io Web Application Scanning provides comprehensive vulnerability scanning for modern web applications. Tenable.io Web Application Scanning's accurate vulnerability coverage minimizes false positives and false negatives, ensuring that security teams understand the true security risks in their web applications. The product offers safe external scanning that ensures production web applications are not disrupted or delayed, including those built using HTML5 and AJAX frameworks.

If you are using Tenable.io Web Application Scanning for the first time, see the workflow to get started.

Click here to download Tenable CoreOS to use Tenable.io Web Application Scanning with internal scanning.

Other Tenable.io Products

Tenable.io Vulnerability Management

See the User Guide

Tenable.io Vulnerability Management allows security and audit teams to share multiple Nessus scanners, scan schedules, scan policies, and scan results with an unlimited set of users or groups.

By making multiple resources available for sharing among users and groups, Tenable.io Vulnerability Management provides endless possibilities for creating customized workflows for vulnerability management programs, while accommodating the numerous regulatory or compliance drivers that demand you keep your business secure.

Tenable.io Vulnerability Management can schedule scans, push policies, view scan findings, and control multiple Nessus scanners from the cloud. This enables the deployment of Nessus scanners throughout networks to both public clouds, private clouds, and physical locations.

Tenable.io Container Security

See the User Guide

Tenable.io Container Security stores and scans container images as the images are built, before production. It provides vulnerability and malware detection, along with continuous monitoring of container images. By integrating with the continuous integration and continuous deployment (CI/CD)

systems that build container images, Tenable.io Container Security ensures every container reaching production is secure and compliant with enterprise policy.

Tenable.io Web Application Scanning Workflow

Register for Tenable.io Web Application Scanning with an Existing Tenable.io License

1. In a browser, access https://cloud.tenable.com/app.html.

   The Tenable.io login page appears.

2. In the **Username** box, type your Tenable.io username.

3. In the **Password** box, type your Tenable.io password.

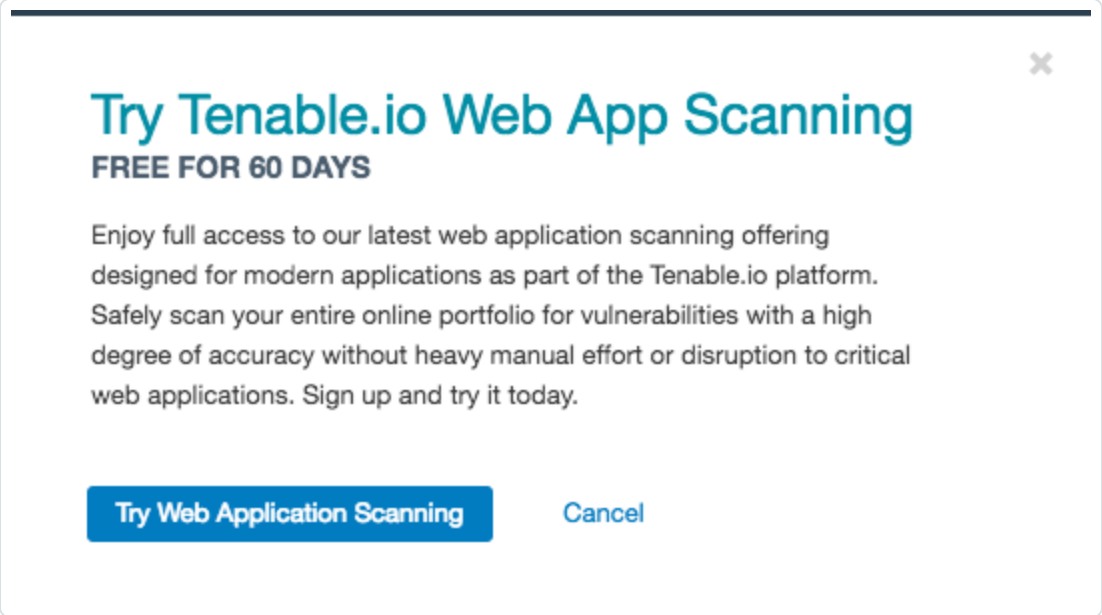
4. To remain logged in until you click **Log Out** or close the browser, select the **Remember Me** check box. Otherwise, you are logged out after a period of inactivity.

5. Click **Sign In**.

   The Tenable.io Vulnerability Management **Dashboard** page appears.

6. In the top navigation bar, click the **Vulnerability Management** drop-down box, and click **Web Applications**.

   The **Try Tenable.io Web App Scanning** box appears.



7. To start a free 60-day trial, click the **Try Web App Scanning** button.

Your trial begins and the **Web Applications** workbench appears. Additionally, the Web Applications scan templates are available.

> **Note:** To purchase a license for Tenable.io Web Application Scanning, contact support@tenable.com.

Register for Tenable.io Web Application Scanning without an Existing Tenable.io License

1. In a browser, access http://www.tenable.com/products/tenable-io.
2. In the **Applications** section, under **Web Application Scanning**, click the **Free Trial** button.

   The **Try Tenable.io Web Application Scanning** page appears.
3. In the **First Name** box, type your first name.
4. In the **Last Name** box, type your last name.
5. In the **Business Email** box, type your business email.
6. In the **Phone** box, type your business phone number.
7. In the **Company Name** box, type your company name.
8. If you want to also start a free 60-day trial of Tenable.io Vulnerability Management and/or Tenable.io Container Security, select the **I'd also like to try additional applications** check box.

   The **Which additional applications would you like to try?** section appears.
9. Select the check boxes for the products you want to try.
10. Click the **Get Started** button.

    Your trial begins and you will receive an email with a link to Tenable.io.

    When you log in to Tenable.io, the **Web Applications** workbench appears, and the Web Applications scan templates are available.

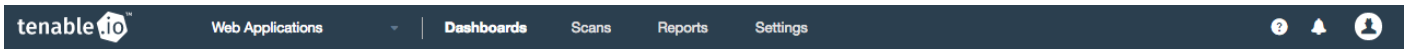
> **Note:** To purchase a license for Tenable.io Web Application Scanning, contact support@tenable.com.

Collect Data Using Tenable.io Web Application Scanning

1. Create a scan using a Web Application scan template.
2. Configure the scan settings and permissions.
3. Run the scan to collect data.
4. View the data on the Web Applications workbench.

Navigate Tenable.io Web Application Scanning

The top navigation bar displays a toggle to switch between the Tenable.io products (Vulnerability Management, Container Security, and Web Applications), as well as links to the four main pages: **Dashboards**, **Scans**, **Reports**, and **Settings**.You can perform all Tenable.io primary tasks using these four pages. Click a page name to open the corresponding page.



On the right side of the top navigation bar, you can find the following options:

Element	Description
	Toggles the **Need Help?** box, which displays a list of common Tenable.io tasks. Click a link to begin a walkthrough guide.
	Toggles the **Notifications** box, which displays a list of notifications, successful or unsuccessful login attempts, errors, and system information generated by Tenable.io. **Note:** Notifications are not preserved after a session expires.
Username	Displays a drop-down menu with the following options: **My Account**, **What's New**, **Documentation**, and **Sign Out**.

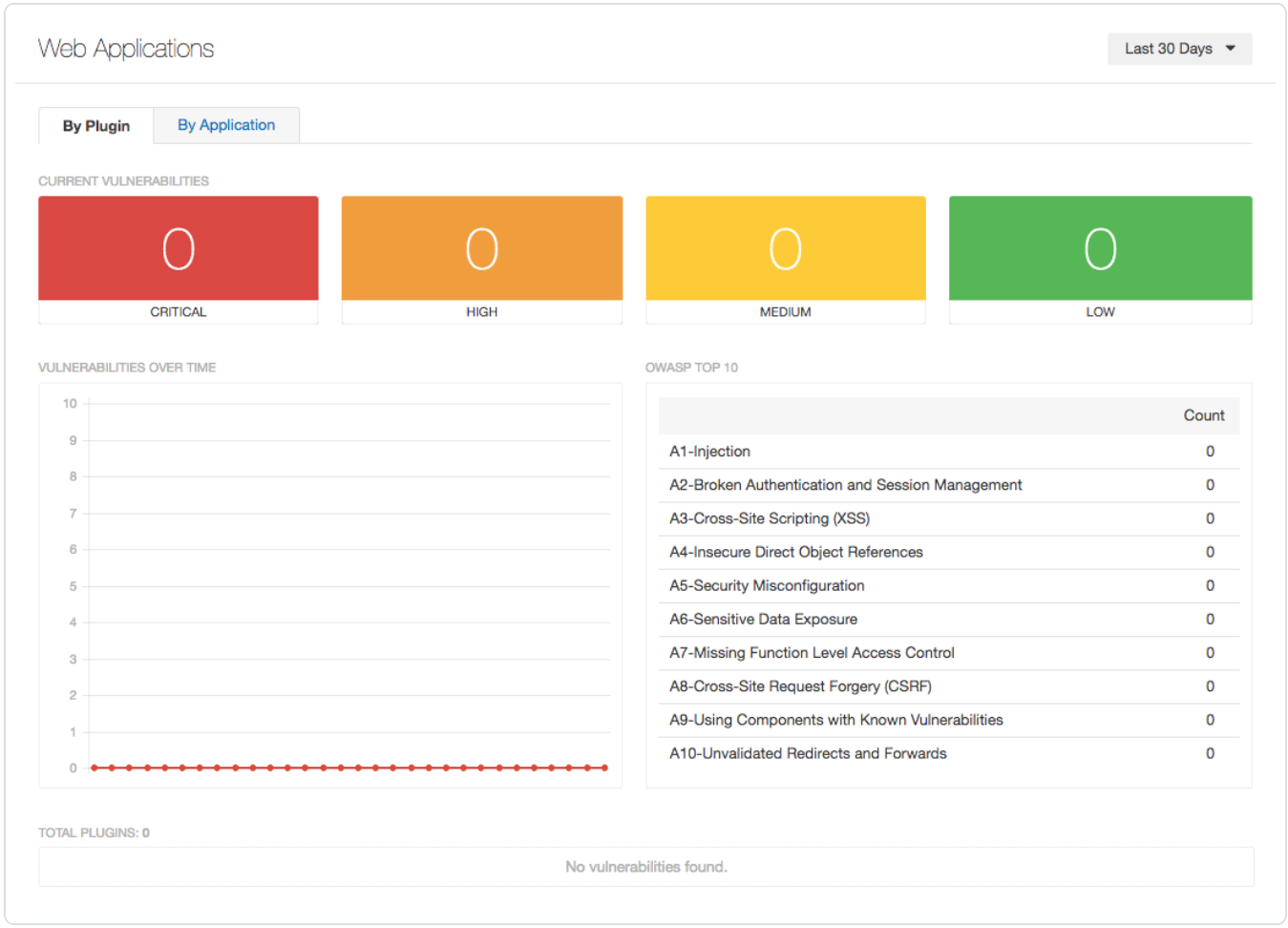
Access the Tenable.io Web Application Scanning Workbench

1. In Tenable.io, in the top navigation bar, click **Dashboards**.

   The **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Web Applications**.

The **Web Applications** workbench appears.



Access the Tenable.io Web Application Scanning Scan Templates

1. In Tenable.io, in the top navigation bar, click **Scans**.

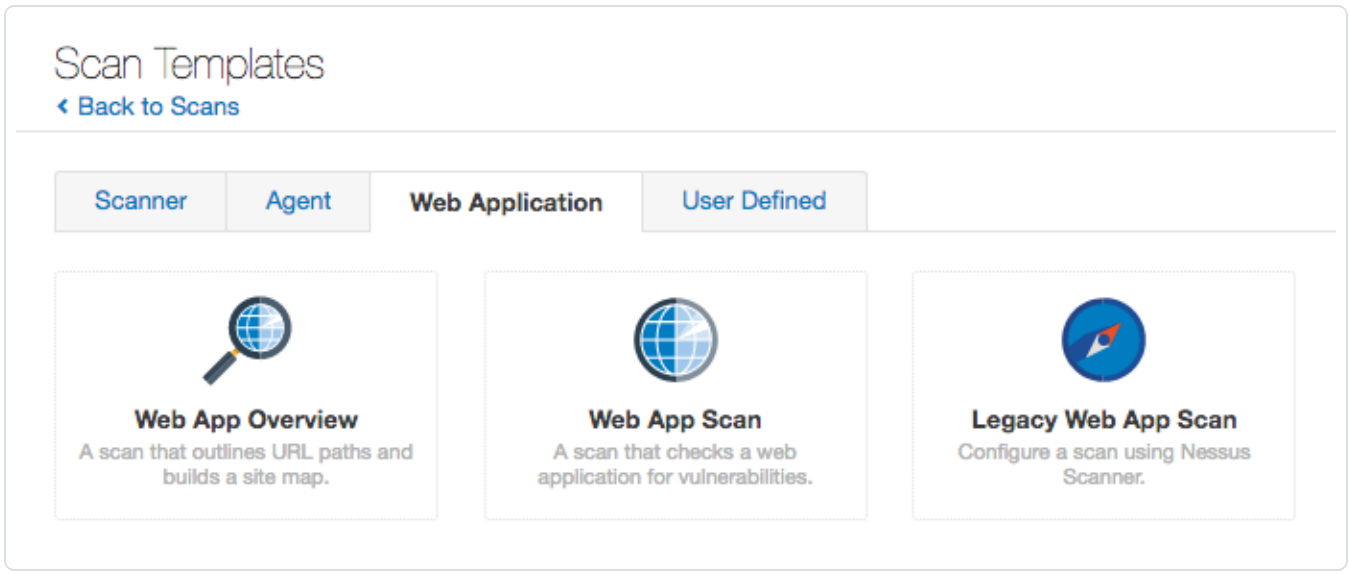
   The **My Scans** page appears.

2. In the upper right corner, click the **New Scan** button.

   The **Scan Templates** page appears.

3. Click the **Web Application** tab.

The Web Application scan templates appear.



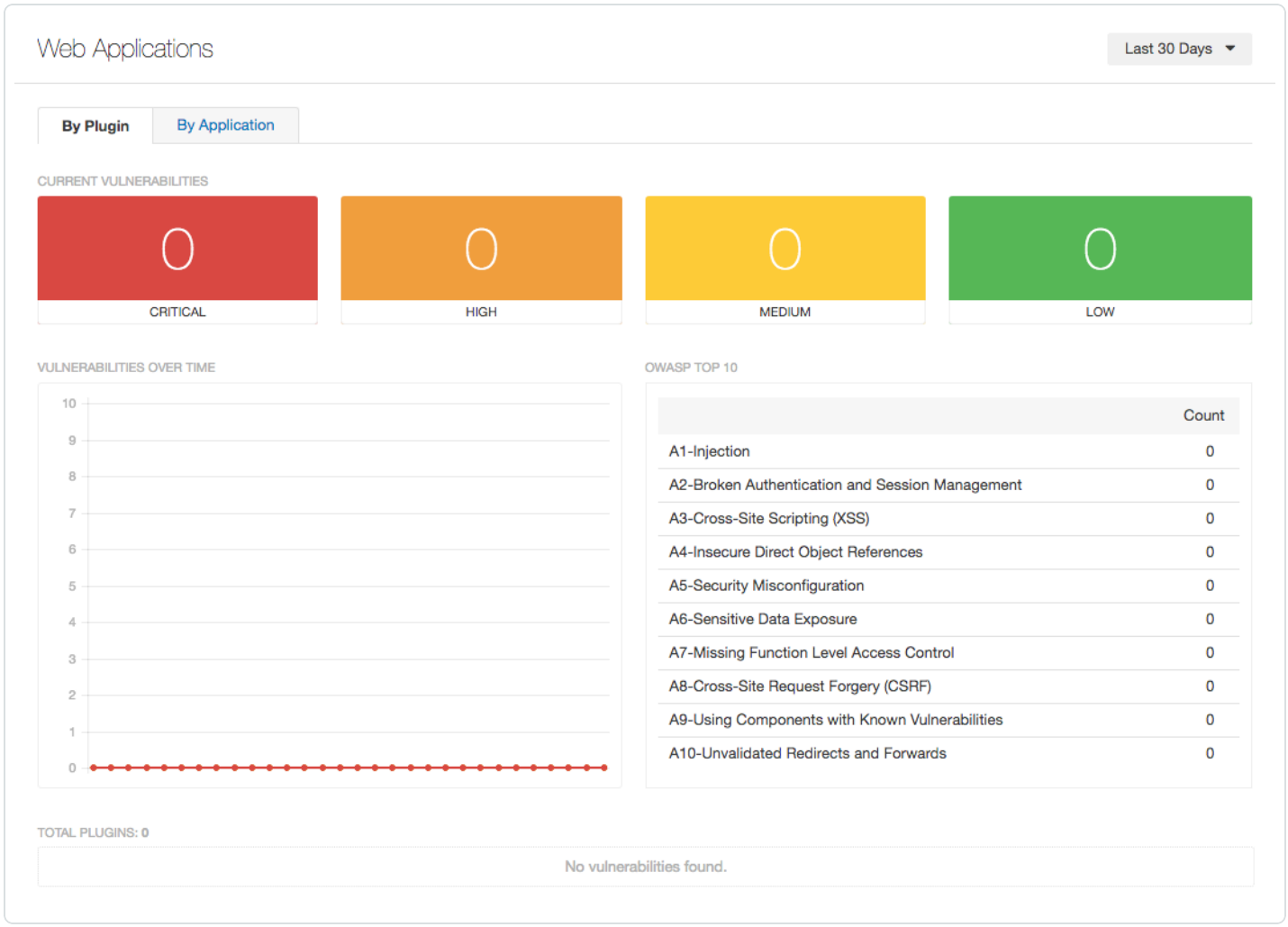
Tenable.io Web Application Scanning Features

This section describes the following features available with Tenable.io Web Application Scanning:

- Web Applications Workbench
- Web Application Scan Templates
- Plugin Information

Web Applications Workbench

The **Web Applications** workbench displays data collected by Web Application scans.



The table below describes the charts available on the **Web Applications** workbench. You can view details about the data in a chart by clicking the chart.

Chart	Description
Web Applications: By Plugin	
Current Vulnerabilities	Each number (**Critical**, **High**, **Medium**, and **Low**) represents the vulnerabilities discovered by Web Application scans within the selected time interval and sorted by severity.
Vulnerabilities	Vulnerabilities discovered over time by Web Application scans. Each data point

Chart	Description
Over Time	on the line graph represents the number of unique vulnerabilities found on a particular day.
OWASP Top 10	A list of the vulnerabilities discovered by Web Application scans that appear in the Open Web Application Security Project (OWASP) Top 10 Most Critical Web Application Security Risks document.
Total Plugins	A list of all the plugins that detected the vulnerabilities that appear on the Web Applications workbench.
Web Applications: By Application	
Apps Over Time	Applications scanned over time. Each data point on the line graph represents the number of unique applications scanned on a particular day.

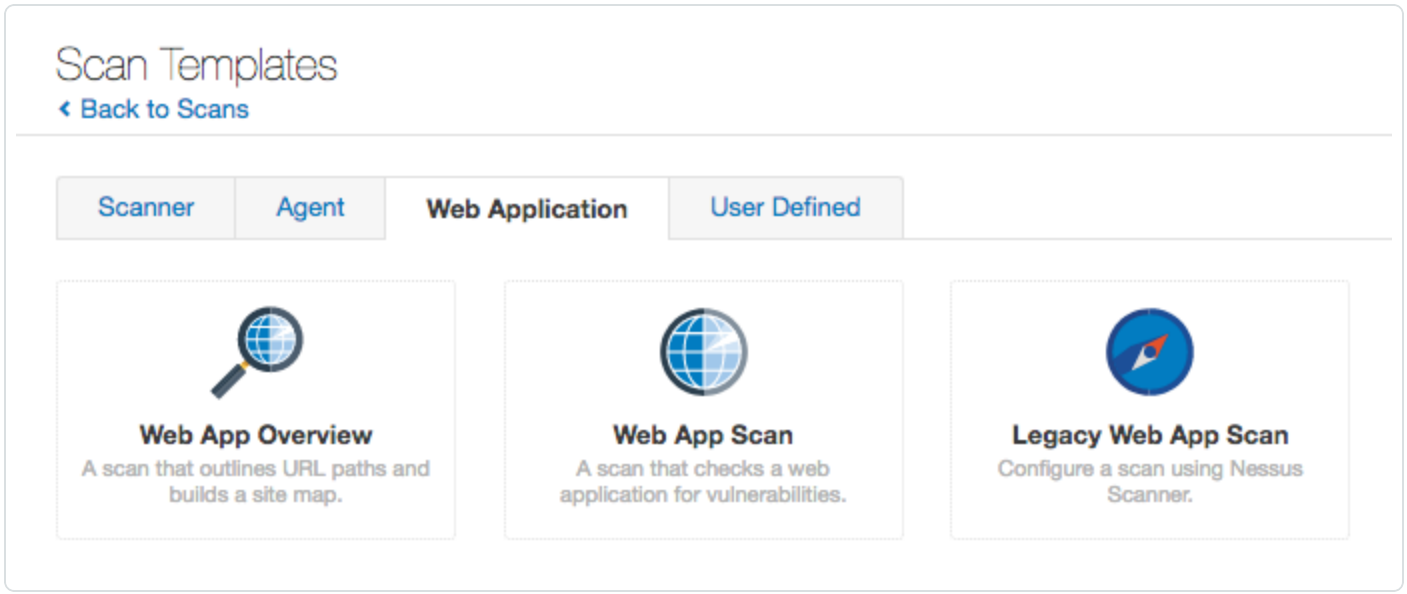
Web Application Scans

This section includes the following information you need to know about new features and caveats with regards to Web Application scan templates:

- Web Application Scan Templates
- Cloud Scanners

Web Application Scan Templates

On the **Scans** page, the **Web Application** tab appears, which hosts Web Application scan templates. You can use these templates to launch scans, or you can create templates using your own Web Application Scanning policies.



The **Web Application** tab displays the following templates for the Tenable.io Web Application Scanning engine:

- Web App Overview
- Web App Scan
- Legacy Web App Scan

Web App Overview Scan Settings

Basic Settings

General

Setting	Default Value	Description
Name	None	The name of the scan or policy. This value appears in the Tenable.io

Setting	Default Value	Description
		interface.
Description	None	A description of the scan or policy.
Folder	My Scans	The folder where the scan appears after saving.
Scanner	Varies	The scanner that performs the scan. The default scanner varies based on the organization and user.
Target	None	The target to be scanned.

Schedule

Setting	Default Value	Description
Enabled	Off	The toggle that specifies whether the scan is scheduled. By default, scans are not scheduled. To modify the following **Schedule** settings, click the **Off** button.
Frequency	Once	How often the scan launches. • **Once**: Schedule the scan at a specific time. • **Daily**: Schedule the scan to occur on a daily basis, at a specific time, for up to 20 days. • **Weekly**: Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks. • **Monthly**: Schedule the scan to occur every month, by time and day of month or week of month, for up to 20 months. • **Yearly**: Schedule the scan to occur every year, by time and day, for up to 20 years.
Starts	Varies	The exact date and time when a scan launches. The starting date defaults to the date when you create the scan. The starting time is the nearest next half-hour interval. For example, if you

Setting	Default Value	Description
		create your scan on 10/31/2016 at 9:12 AM, the default starting date and time is *10/31/2016* and *09:30*.
Timezone	Zulu	The timezone of the value set for **Starts**.
Summary	Not applicable	A summary of the schedule for your scan based on the values you have specified for the available settings.

Notifications

Setting	Default Value	Description
Email Recipient(s)	None	The email addresses that are alerted when a scan completes and the results are available.
Result Filters	None	The type of information to be emailed.

Permissions

Using settings in the **Permissions** section, you can assign various permissions to groups and individual users. When you assign a permission to a group, that permission applies to all users within the group. The following rows describe the permissions that can be assigned.

Setting	Description
Add users or groups	The users or groups to which you want to apply permissions. **Note:** When you apply a permission to a group, the permission applies to all users within the group. The following rows describe the permissions that you can assign.
No access	Groups and users set to **No access** cannot interact with the scan in any way. When you create a scan or policy, no other users or groups have access to it by default.
Can view	Groups and users set to **Can view** can view the results of the scan.
Can control	Groups and users set to **Can control** can launch, pause, and stop a scan, as well as view its results.

Setting	Description
Can configure	Groups and users set to **Can configure** can modify the configuration of the scan in addition to all other permissions.

Scope Settings

The **Scope** settings specify URLs and file types that you want to exclude from your scan.

Setting	Default Value	Description
URL Exclusion Patterns	logout	A text box in which you can type URLs to exclude from the scan.
Exclude URLs per file extension	None	A text box in which you can type file types to exclude from the scan.

Discovery Settings

The **Discovery** settings include configurable settings that allow the scan to discover new URLs other than the ones discovered during crawling. If you select **Custom** in the **Scan Type** drop-down box, the **Path Discovery** and **Common Paths** sections appear.

Path Discovery

Setting	Default Value	Description
URL Parameter Manipulation	Cleared	Whether the scanner will change values found in a query string, and resubmits the URL to discover new pages.
Maximum Manipulation Attempts	10	The maximum number of times the scanner will attempt to manipulate query string values.

Common Paths

Setting	Default Value	Description
Administration	Selected	Whether the scanner will attempt to append different paths to the

Setting	Default Value	Description
Interfaces		URL to access well-known web administration interfaces.
Common Files	Selected	Whether the scanner will attempt to append different paths or text to the URL to access common files.
Common Directories	Selected	Whether the scanner will attempt to append different paths or text to the URL to access common directories.

Advanced Settings

The **Advanced** settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enable plugin debugging.

General

Setting	Default Value	Description
Scan Settings		
Overall Scan max time (HH:MM:SS)	08:00:00	The maximum duration the scan runs before it stops automatically. **Note:** The maximum scan time differs slightly from the time you type in the **Overall Scan Max Time** box, because the scanner takes time to stop. The length of the scan impacts how long the scanner takes to stop.
Limits		
Number of URLs to Crawl and Browse	10000	The maximum number of URLs the scanner attempts to crawl and therefore audit.
Path Directory Depth	10	The maximum number of sub-directories the scanner crawls. For example, `http://www.tenable.com/products/tenable-io` has two sub-directories.
Page DOM	5	The maximum depth of HTML nested elements the scanner crawls.

Setting	Default Value	Description
Element Depth		
Maximum Response Size	500000	The maximum load size of a page in order to be audited. If the scanner crawls a URL and the response exceeds the limit, then it is not audited and no vulnerability assessment is performed.
Request Redirect Limit	1	The number of redirects the scan follows before it stops trying to crawl the page.

Discovery

Setting	Default Value	Description
Crawl Settings		
User Agent	Nessus WAS/%v	The user-agent header used by the scanner when sending an HTTP request. **Note:** The %v placeholder indicates the version of the scan engine.
Custom Headers	None	A list of custom headers you want to inject into each HTTP request. **Note:** If you specify the user-agent value in this list, that value will override the value entered in the **User Agent** box.
Screen Settings - settings of the virtual browser instance spun up by the scanner		
Screen Width	1600	The screen width, in pixels, of the browser embedded into the scanner.
Screen Height	1200	The screen height, in pixels, of the browser embedded into the scanner.

Setting	Default Value	Description
Ignore Images	Selected	Whether images on web pages should be crawled or ignored by the browser embedded into the scanner.

Performance

Setting	Default Value	Description
Max number of concurrent HTTP connections	10	The maximum number of established HTTP sessions for a single host.
Max number of HTTP requests per second	25	The maximum number of HTTP requests for the entire scan for a single host.
Slow down the scan when network congestion is detected	Selected	Whether the scan is throttled when it detects network congestion.
Network timeout (in seconds)	5	The time that the scanner waits for a response from a host, unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a higher number of seconds.
Browser timeout (in seconds)	10	The time that the scanner waits for a response from a browser, unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a higher number of seconds.

Credentials

When you click **General**, there are two options for the **Authentication Method** box: **Basic Authentication** and **Login Form**. Depending on which option you select, different options appear.

Setting	Default Value	Description
Authentication Method	Basic Authentication	A box where you can specify one of two options: **Basic Authentication** or **Login Form**. Depending on which option you select, the following options will appear: **Basic Authentication** authenticates toward the server. • Username • Password **Login Form** authenticates toward the application. • Login Page • Regex to verify successful auth • Credentials **Cookie Authentication** authenticates toward the session. • Cookies • Page to verify active session • Regex to verify active session • Session Cookies **Note:** If the scan fails to authenticate, it aborts immediately with a message explaining that it could not authenticate.
Username	None	The user name of the authorized user. For example, the user name of one of the users listed in the `htpasswd` file on an Apache server.
Password	None	The password of the authorized user.

Setting	Default Value	Description
Login Page	None	The URL that is specified in the `form action` attribute and used to submit the form authentication. This may not be the URL for the login form. **Note:** This parameter accepts relative or absolute URLs.
Regex to verify successful auth	None	The regular expression to be matched against the form submission response to verify that the login was successful.
Credentials	None	One or more key value pairs to perform authentication. The pairs are concatenated upon submission to create the list of parameters required by the form. For instructions on how to retrieve the key value pairs, see Configure Login Form Authentication. **Note:** The form may require more than just the user name and password parameters, so you must provide all parameters required by the form to ensure proper authentication.
Cookies	None	The session cookies to pass to the scanner
Page to verify active session	None	The URL used to verify if the scan is authenticated.
Regex to verify active session	None	The regular expression to be matched against the contents of the URL specified by the **Page to verify active session** parameter to verify if the scan is authenticated.
Session Cookies	None	One or more key value pairs to perform authentication. The pairs are concatenated upon submission to create the list of parameters required by the form.

Setting	Default Value	Description
		For instructions on how to retrieve the key value pairs, see Configure Login Form Authentication. **Note:** The form may require more than just the user name and password parameters, so you must provide all parameters required by the form to ensure proper authentication.
Global Credential Settings		
Check Authentication on page	None	The URL used to verify if the scanner is still authenticated for the full duration of the scan.
Regex to verify successful auth	None	The regular expression to be matched against the contents of the URL specified by the **Check Authentication on page** parameter to verify the scanner is still authenticated for the full duration of the scan.

Web App Scan Settings

Basic Settings

General

Setting	Default Value	Description
Name	None	The name of the scan or policy. This value appears in the Tenable.io interface.
Description	None	A description of the scan or policy.
Folder	My Scans	The folder where the scan appears after saving.
Scanner	Varies	The scanner that performs the scan. The default scanner varies based on the organization and user.
Target	None	The target to be scanned.

Schedule

Setting	Default Value	Description
Enabled	Off	The toggle that specifies whether the scan is scheduled. By default, scans are not scheduled. To modify the following **Schedule** settings, click the **Off** button.
Frequency	Once	How often the scan launches. • **Once**: Schedule the scan at a specific time. • **Daily**: Schedule the scan to occur on a daily basis, at a specific time, for up to 20 days. • **Weekly**: Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks. • **Monthly**: Schedule the scan to occur every month, by time and day of month or week of month, for up to 20 months. • **Yearly**: Schedule the scan to occur every year, by time and day, for up to 20 years.
Starts	Varies	The exact date and time when a scan launches. The starting date defaults to the date when you create the scan. The starting time is the nearest next half-hour interval. For example, if you create your scan on 10/31/2016 at 9:12 AM, the default starting date and time is *10/31/2016* and *09:30*.
Timezone	Zulu	The timezone of the value set for **Starts**.
Summary	Not applic-able	A summary of the schedule for your scan based on the values you have specified for the available settings.

Notifications

Setting	Default Value	Description
Email Recipient(s)	None	The email addresses that are alerted when a scan completes and the results are available.
Result Filters	None	The type of information to be emailed.

Permissions

Using settings in the **Permissions** section, you can assign various permissions to groups and individual users. When you assign a permission to a group, that permission applies to all users within the group. The following rows describe the permissions that can be assigned.

Setting	Description
Add users or groups	The users or groups to which you want to apply permissions. **Note:** When you apply a permission to a group, the permission applies to all users within the group. The following rows describe the permissions that you can assign.
No access	Groups and users set to **No access** cannot interact with the scan in any way. When you create a scan or policy, no other users or groups have access to it by default.
Can view	Groups and users set to **Can view** can view the results of the scan.
Can control	Groups and users set to **Can control** can launch, pause, and stop a scan, as well as view its results.
Can configure	Groups and users set to **Can configure** can modify the configuration of the scan in addition to all other permissions.

Scope Settings

The **Scope** settings specify URLs and file types that you want to exclude from your scan.

Setting	Default Value	Description
URL Exclusion Patterns	logout	A text box in which you can type URLs to exclude from the scan.

Setting	Default Value	Description
Exclude URLs per file extension	None	A text box in which you can type file types to exclude from the scan.

Assessment Settings

The **Assessment** settings include configurable settings that allow the scan to audit elements other than the ones discovered during crawling. If you select **Custom** in the **Scan Type** drop-down box, the **General** section appears.

Note: When you select a check box for an option in the **Elements** section, the scanner will analyze that element type and test all instances of the element for security vulnerabilities (e.g., OWASP Top 10).

Setting	Default Value	Description
Elements		
Audit cookies	Selected	The scan checks for cookie-based vulnerabilities.
Audit forms	Selected	The scan checks for form-based vulnerabilities.
Audit headers	Selected	The scan inspects headers for vulnerabilities and insecure configurations (e.g., missing X-Frame-Options).
Audit links	Selected	The scan includes links and their parameters in vulnerability checks.
Audit parameter names	Cleared	The scan performs extensive fuzzing of parameter names.
Audit parameter values	Selected	The scan performs extensive fuzzing of parameter values.
Audit JSON	Cleared	The scan audits JSON request data.

Setting	Default Value	Description
Audit XML	Cleared	The scan audits XML request data.
Audit UI Forms	Selected	The scan checks input and button groups associated with JavaScript code.
Audit UI Inputs	Selected	The scan checks orphan input elements with associated DOM events.
Options		
URL for Remote File Inclusion	http://rfi.nessus.org/rfi.txt	During Remote File Inclusion (RFI) testing, this setting specifies a file on a remote host to use for tests. By default, Tenable.io uses a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, you can use an internally hosted file for more accurate RFI testing.

Advanced Settings

The **Advanced** settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enable plugin debugging.

General

Setting	Default Value	Description
Scan Settings		
Overall Scan max time (HH:MM:SS)	08:00:00	The maximum duration scan runs before it stops automatically. **Note:** The maximum scan time differs slightly from the time you type in the **Overall Scan Max Time** box, because the scanner takes time to stop. The length of the scan determines how long the scanner takes to stop.
Limits		
Number of URLs to Crawl and	10000	The maximum number of URLs the scanner attempts to crawl and therefore audit.

Setting	Default Value	Description
Browse		
Path Directory Depth	10	The maximum number of sub-directories the scanner crawls. For example, `http://www.tenable.com/products/tenable-io` has two sub-directories.
Page DOM Element Depth	5	The maximum depth of HTML nested elements the scanner crawls.
Maximum Response Size	500000	The maximum load size of a page in order to be audited. If the scanner crawls a URL and the response exceeds the limit, then it is not audited and no vulnerability assessment is performed.
Request Redirect Limit	1	The number of redirects the scan follows before it stops trying to crawl the page.

Discovery

Setting	Default Value	Description
Crawl Settings		
User Agent	Nessus WAS/%v	The user-agent header used by the scanner when sending an HTTP request. **Note:** The %v placeholder indicates the version of the scan engine.
Custom Headers	None	A list of custom headers you want to inject into each HTTP request. **Note:** If you specify the user-agent value in this list, that value will override the value entered in the **User Agent** box.

Setting	Default Value	Description
Screen Settings - settings of the virtual browser instance spun up by the scanner		
Screen Width	1600	The screen width, in pixels, of the browser embedded into the scanner.
Screen Height	1200	The screen height, in pixels, of the browser embedded into the scanner.
Ignore Images	Selected	Whether images on web pages should be crawled or ignored by the browser embedded into the scanner.

Performance

Setting	Default Value	Description
Max number of concurrent HTTP connections	10	The maximum number of established HTTP sessions for a single host.
Max number of HTTP requests per second	25	The maximum number of HTTP requests for the entire scan for a single host.
Slow down the scan when network congestion is detected	Selected	Whether the scan will be throttled when network congestion is detected.
Network timeout (in seconds)	5	The time that the scanner waits for a response from a host, unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a higher number of seconds.
Browser timeout (in seconds)	10	The time that the scanner waits for a response from a browser, unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a higher number of seconds.

Credentials

When you click **General**, there are two options for the **Authentication Method** box: **Basic Authentication** and **Login Form**. Depending on which option you select, different options appear.

Setting	Default Value	Description
Authentication Method	Basic Authentication	A box where you can specify one of two options: **Basic Authentication** or **Login Form**. Depending on which option you select, the following options will appear: **Basic Authentication** authenticates toward the server. • Username • Password **Login Form** authenticates toward the application. • Login Page • Login Parameters • Regex to verify successful auth • Credentials **Cookie Authentication** authenticates toward the session. • Session Cookies • Page to verify active session • Regex to verify active session **Note:** If the scan fails to authenticate, it aborts immediately with a message explaining that it could not authenticate.
Username	None	The user name of the authorized user. For example, the user name of one of the users listed in the `htpasswd` file on an Apache server.
Password	None	The password of the authorized user.
Login Page	None	The URL that is specified in the `form action` attribute and used to submit the form authentication. This may not be the

Setting	Default Value	Description
		URL for the login form. **Note:** This parameter accepts relative or absolute URLs.
Regex to verify successful auth	None	The regular expression to be matched against the form submission response to verify that the login was successful.
Credentials	None	One or more key value pairs to perform authentication. The pairs are concatenated upon submission to create the list of parameters required by the form. For instructions on how to retrieve the key value pairs, see Configure Login Form Authentication. **Note:** The form may require more than just the user name and password parameters, so you must provide all parameters required by the form to ensure proper authentication.
Session Cookies	None	One or more key value pairs to perform authentication. The pairs are concatenated upon submission to create the list of parameters required by the form. For instructions on how to retrieve the key value pairs, see Configure Login Form Authentication. **Note:** The form may require more than just the user name and password parameters, so you must provide all parameters required by the form to ensure proper authentication.
Page to verify active session	None	The URL used to verify if the scan is authenticated.
Regex to verify active session	None	The regular expression to be matched against the contents of the URL specified by the **Page to verify active session** parameter to verify if the scan is authenticated.
Global Credential Settings		

Setting	Default Value	Description
Check Authentication on page	None	The URL used to verify if the scanner is still authenticated for the full duration of the scan.
Regex to verify successful auth	None	The regular expression to be matched against the contents of the URL specified by the **Check Authentication on page** parameter to verify the scanner is still authenticated for the full duration of the scan.

Legacy Web App Scan Settings

Basic Settings

General

Setting	Default Value	Description
Name	None	The name of the scan or policy. This value appears in the Tenable.io interface.
Description	None	A description of the scan or policy.
Folder	My Scans	The folder where the scan appears after being saved.
Scanner	Varies	The scanner that performs the scan. The default scanner varies based on the organization and user.
Target	None	The target to be scanned.
Upload Targets	None	A link to upload a text file that specifies targets. The targets file must be formatted in the following manner: • The file must be ASCII format. • Only one target per line. • No extra spaces should appear at the end of a line. • No extra lines should appear following the last target.

Setting	Default Value	Description
		Note: Unicode/UTF-8 encoding is not supported.

Schedule

Setting	Default Value	Description
Enabled	Off	The toggle that specifies whether the scan is scheduled. By default, scans are not scheduled. To modify the following **Schedule** settings, click the **Off** button.
Frequency	Once	How often the scan launches. • **Once**: Schedule the scan at a specific time. • **Daily**: Schedule the scan to occur on a daily basis, at a specific time, for up to 20 days. • **Weekly**: Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks. • **Monthly**: Schedule the scan to occur every month, by time and day of month or week of month, for up to 20 months. • **Yearly**: Schedule the scan to occur every year, by time and day, for up to 20 years.
Starts	Varies	The exact date and time when a scan launches. The starting date defaults to the date when you create the scan. The starting time is the nearest next half-hour interval. For example, if you create your scan on 10/31/2016 at 9:12 AM, the default starting date and time is *10/31/2016* and *09:30*.
Timezone	Zulu	The timezone of the value set for **Starts**.
Summary	Not applic-able	A summary of the schedule for your scan based on the values you have specified for the available settings.

Notifications

Setting	Default Value	Description
Email Recipient(s)	None	The email addresses that are alerted when a scan completes and the results are available.
Result Filters	None	The type of information to be emailed.

Permissions

Using settings in the **Permissions** section, you can assign various permissions to groups and individual users. When you assign a permission to a group, that permission applies to all users within the group. The following rows describe the permissions that can be assigned.

Setting	Description
Data Sharing	
Scan results	Specifies whether you want scan results to be private to your user account, or appear in the **Web Applications** workbench.
User Sharing	
Add users or groups	The users or groups to which you want to apply permissions. **Note:** When you apply a permission to a group, the permission applies to all users within the group. The following rows describe the permissions that you can assign.
No access	Groups and users set to **No access** cannot interact with the scan in any way. When you create a scan or policy, no other users or groups have access to it by default.
Can view	Groups and users set to **Can view** can view the results of the scan.
Can control	Groups and users set to **Can control** can launch, pause, and stop a scan, as well as view its results.
Can configure	Groups and users set to **Can configure** can modify the configuration of the scan in addition to all other permissions.

Discovery Settings

The **Discovery** settings include configurable settings that allow the scan to discover new URLs other

than the ones discovered during crawling. If you select **Custom** in the **Scan Type** drop-down box, the **Host Discovery**, **Port Scanning**, and **Service Discovery** sections appear.

Host Discovery

Setting	Default Value	Description
Ping the remote host	On	This option enables Tenable.io Web Application Scanning to ping remote hosts on multiple ports to determine if the hosts are alive. When set to *On*, **General Settings** and **Ping Methods** appear. **Note:** To scan VMware guest systems, **Ping the remote host** must be set to **Off**.
General Settings		
Use fast network discovery	Cleared	If a host responds to ping, Tenable.io Web Application Scanning attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. Selecting **Use fast network discovery** bypasses those additional tests.
Ping Methods		
ARP	Selected	Pings a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.
TCP	Selected	Pings a host using Transmission Control Protocol (TCP).
Destination ports (TCP)	built-in	Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that are checked via TCP ping.
ICMP	Selected	Pings a host using the Internet Control Message Protocol (ICMP).
Assume ICMP unreachable from the gateway means the host is down	Cleared	When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When you select **Assume ICMP unreachable from the gateway means the host is down**, when Tenable.io Web Application Scanning receives an ICMP Unreachable message, it considers the targeted host dead. This option helps speed up discovery on some networks.

		Note: Some firewalls and packet filters use this same behavior for hosts that are up, but connected to a port or protocol that is filtered. With this option enabled, this leads to the scan considering the host is down when it is indeed up.
Maximum number of retries	2	The number of attempts to retry pinging the remote host.
UDP	Cleared	Pings a host using the User Datagram Protocol (UDP). UDP is a stateless protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, these services and devices are not always remotely detectable.
Fragile Devices		
Scan Network Printers	Cleared	Instructs Tenable.io Web Application Scanning to scan network printers.
Scan Novell Netware hosts	Cleared	Instructs Tenable.io Web Application Scanning to scan Novell NetWare hosts.
Wake-on-LAN (Local Area Network) The Wake-on-LAN (WOL) menu identifies which hosts to which you want to send WOL magic packets prior to running a scan.		

List of MAC addresses	None	You can provide hosts that you want to start prior to scanning by uploading a text file that lists one MAC address per line.
		For example:
		`33:24:4C:03:CC:C7`
		`FF:5C:2C:71:57:79`

Boot time wait (in minutes)	5	The amount of time to wait for hosts to start before performing the scan.
Network Type		
Network Type	Mixed	Specifies if you are using publicly routable IPs, private non-Internet

	(use RFC 1918)	routable IPs, or a mix of these. This setting has three options: • **Mixed (use RFC 1918)** • **Private LAN** • **Public WAN (Internet)** The default value, **Mixed**, should be selected if you are using RFC 1918 addresses and have multiple routers within your network.

Port Scanning

Setting	Default Value	Description
Ports		
Consider unscanned ports as closed	Cleared	If a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), Tenable.io Web Application Scanning considers it closed.
Port scan range	default	Two keywords can be typed into the **Port scan range** box. • *default* instructs Tenable.io Web Application Scanning to scan approximately 4,790 commonly used ports. The list of ports can be found in the nessus-service file. • *all* instructs Tenable.io Web Application Scanning to scan all 65,536 ports, including port 0. Additionally, you can type a custom range of ports by using a comma-delimited list of ports or port ranges. For example, `21,23,25,80,110` or `1-1024,8080,9000-9200`. If you wanted to scan all ports excluding port 0, you would type `1-65535`. The custom range specified for a port scan is applied to the protocols you selected in the **Network Port Scanners** group of settings. If scanning both TCP and UDP, you can specify a split range specific to

Setting	Default Value	Description
		each protocol. For example, if you want to scan a different range of ports for TCP and UDP in the same policy, you would type `T:1-1024,U:300-500`. You can also specify a set of ports to scan for both protocols, as well as individual ranges for each separate protocol. For example, `1-1024,T:1024-65535,U:1025`.
Network Port Scanners		
TCP	Cleared	On some platforms (e.g., Windows and Mac OS X), enabling this scanner causes Tenable.io Web Application Scanning to use the SYN scanner to avoid serious performance issues native to those operating systems.
Override automatic firewall detection	Cleared	When enabled, this setting overrides automatic firewall detection. This setting has three options: • **Use soft detection** disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device. • **Use aggressive detection** attempts to run plugins even if the port appears to be closed. Tenable, Inc. does not recommend that you select this option on a production network. • **Disable detection** disables the firewall detection feature. This description also applies to the **Override automatic firewall detection** setting that is available following SYN.
SYN	Selected	Use the Tenable.io Web Application Scanning SYN scanner to identify open TCP ports on the target hosts. SYN scans are generally considered to be less intrusive than TCP scans depending on the security monitoring device, such as a firewall or Intrusion Detection System (IDS). The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and determines the port state based on a reply or lack of reply.
UDP	Cleared	This option enables the Tenable.io Web Application Scanning built-in

Setting	Default Value	Description
		UDP scanner to identify open UDP ports on the targets. Due to the nature of the protocol, it is generally not possible for a port scanner to tell the difference between open and filtered UDP ports. Enabling the UDP port scanner may dramatically increase the scan time and produce unreliable results. Consider using the netstat or SNMP port enumeration options instead.

Service Discovery

Setting	Default Value	Description
General Settings		
Probe all ports to find services	Selected	Attempts to map each open port with the service that is running on that port. **Caution:** In some rare cases, probing might disrupt some services and cause unforeseen side effects.
Search for SSL/TLS services	On	Controls how Tenable.io Web Application Scanning will test Secure Sockets Layer (SSL)- and Transport Layer Security (TLS)-based services. **Caution:** Testing for SSL capability on all ports may be disruptive for the tested host.
Search for SSL/TLS on	Known SSL/TLS ports	This setting has two options: • **Known SSL/TLS ports** • **All ports**
Identify certificates expiring within x days	60	Identifies SSL and TLS certificates that are within the specified number of days of expiring.

Setting	Default Value	Description
Enumerate all SSL/TLS ciphers	Selected	When enabled, Tenable.io Web Application Scanning ignores the list of ciphers advertised by SSL/TLS services and enumerates them by attempting to establish connections using all possible ciphers.
Enable CRL checking (connects to Internet)	Cleared	When enabled, Tenable.io Web Application Scanning checks that none of the identified certificates have been revoked.

Assessment Settings

General

Setting	Default Value	Description
Override normal accuracy	Cleared	In some cases, Tenable.io Web Application Scanning cannot remotely determine whether a flaw is present or not. • **Show potential false alarms**: A flaw will be reported every time, even when there is a doubt about the remote host being affected. • **Avoid potential false alarms**: Tenable.io Web Application Scanning will not report any flaw whenever there is a hint of uncertainty about the remote host.
Perform thorough tests (may disrupt your network or impact scan speed)	Cleared	When enabled, this option causes various plugins to work harder. For example, when looking through Server Message Block (SMB) file shares, a plugin can analyze 3 directory levels deep instead of 1. This could cause much more network traffic and analysis in some cases. By being more thorough, the scan is more intrusive and is more likely to disrupt the network, while potentially providing better audit results.

Web Applications

By default, web applications are not scanned. When you first access the **Web Application** section, the **Scan web applications** setting appears and is set to **Off**. To modify the Web Application settings listed on the following table, click the **Off** button. The rest of the settings appear.

Setting	Default Value	Description
General Settings		
Use a custom User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	Specifies which type of web browser Tenable.io Web Application Scanning impersonates while scanning.
Web Crawler		
Start crawling from	/	The URL of the first page that is tested. If multiple pages are required, use a colon delimiter to separate them (e.g., /:/php4:/base).
Excluded pages (regex)	/server_privileges\.php|logout	Specifies portions of the web site to exclude from being crawled. For example, to exclude the /manual directory and all Perl CGI, set this field to: (^/manual) **<>** (\.pl(\?.*)?$). Tenable.io Web Application Scanning supports POSIX regular expressions for string matching and handling, as well as Perl-Compatible Regular Expressions (PCRE).
Maximum pages to crawl	1000	The maximum number of pages to crawl.
Maximum depth to crawl	6	Limit the number of links Tenable.io Web Application Scanning follows for each start page.
Follow dynamically generated pages	Cleared	If selected, Tenable.io Web Application Scanning follows dynamic links and may exceed the parameters set in the **Web Crawler** section.

Setting	Default Value	Description
Application Test Settings		
Enable generic web application tests	Selected	Enables the options listed below.
Abort web application tests if HTTP login fails	Cleared	If Tenable.io Web Application Scanning cannot log in to the target via HTTP, then Tenable.io Web Application Scanning does not run any web application tests.
Try all HTTP methods	Cleared	This option instructs Tenable.io Web Application Scanning to also use POST requests for enhanced web form testing. By default, the web application tests only use GET requests, unless this option is enabled. Generally, more complex applications use the POST method when a user submits data to the application. This setting provides more thorough testing, but may considerably increase the time required. When selected, Tenable.io Web Application Scanning tests each script or variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.
Attempt HTTP Parameter Pollution	Cleared	When performing web application tests, attempt to bypass filtering mechanisms by injecting content into a variable while also supplying the same variable with valid content. For example, a normal SQL injecton test may look like /target.cgi?a='&b=2. With HTTP Parameter Pollution (HPP) enabled, the request may look like /target.cgi?a='&a=1&b=2.
Test embedded web servers	Cleared	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-

Setting	Default Value	Description
		responsive when scanned. Tenable recommends selecting this option to scan embedded web servers separately from other web servers.
Test more than one parameter at a time per form	Cleared	This setting manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying non-attack variations for additional parameters. For example, Tenable.io Web Application Scanning would attempt `/test.php?arg1=XSS&b=1&c=1`, where b and c allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. This setting has four options: • **Test random pairs of parameters**: This form of testing randomly checks a combination of random pairs of parameters. This is the fastest way to test multiple parameters. • **Test all pairs of parameters (slow)**: This form of testing is slightly slower but more efficient than the one value test. While testing multiple parameters, it tests an attack string, variations for a single variable and then uses the first value for all other variables. For example, Tenable.io Web Application Scanning would attempt /test.php?a=XSS&b=1&c=1&d=1 and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process), and any other variables are given the first value. In this case, Tenable.io Web Application Scanning would never test for /test.php?a=XSS&b=3&c=3&d=3

Setting	Default Value	Description
		when the first value of each variable is 1. • **Test random combinations of three or more parameters (slower)**: This form of testing randomly checks a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Increasing the amount of combinations by three or more increases the web application test time. • **Test all combinations of parameters (slowest)**: This method of testing checks all possible combinations of attack strings with valid input to variables. Where all-pairs testing seeks to create a smaller data set as a tradeoff for speed, all combinations makes no compromise on time and uses a complete data set of tests. This testing method may take a long time to complete.
Do not stop after first flaw is found per web page	Cleared	This setting determines when a new flaw is targeted. This applies at the script level. Finding an XSS flaw does not disable searching for SQL injection or header injection, but unless otherwise specified, there is at most one report for each type on a given port. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported if the flaws were caught by the same attack. This setting has three options: • **Stop after one flaw is found per web server (fastest)**: As soon as a flaw is found on a web server by a script, Tenable.io Web Application Scanning stops and switches to another web server on a different port. • **Stop after one flaw is found per para-**

Setting	Default Value	Description
		meter (slow): As soon as one type of flaw is found in a parameter of a CGI (e.g., XSS), Tenable.io Web Application Scanning switches to the next parameter of the same CGI, the next known CGI, or to the next port or server. • **Look for all flaws (slowest)**: Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.
URL for Remote File Inclusion	http://rfi.nessus.org/rfi.txt	During Remote File Inclusion (RFI) testing, this setting specifies a file on a remote host to use for tests. By default, Tenable.io Web Application Scanning uses a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, you can use an internally hosted file for more accurate RFI testing.
Maximum run time (minutes)	5	This option manages the amount of time, in minutes, spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given website. Scanning the local network for web sites with small applications typically completes in under an hour, however web sites with large applications may require a higher value.

Report Settings

Setting	Default Value	Description
Processing		
Override normal verbosity	Cleared	This setting has two options: • **I have limited disk space. Report as little information as possible**: Provides less information about plugin activity

Setting	Default Value	Description
		in the report to minimize impact on disk space. • **Report as much information as possible**: Provides more information about plugin activity in the report.
Show missing patches that have been superseded	Selected	If enabled, includes superseded patch information in the scan report.
Hide results from plugins initiated as a dependency	Selected	If enabled, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, disable this setting.
Output		
Allow users to edit scan results	Selected	When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.
Designate hosts by their DNS name	Cleared	Uses the host name rather than IP address for report output.
Display hosts that respond to ping	Cleared	Reports hosts that successfully respond to a ping.
Display unreachable hosts	Cleared	When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.

Advanced Settings

The **Advanced** settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enabled plugin debugging.

Setting	Default Value	Description
General Settings		
Enable safe checks	Selected	When enabled, disables all plugins that may have an adverse effect on the remote host.
Stop scanning hosts that become unresponsive during the scan	Cleared	When enabled, Tenable.io Web Application Scanning stops scanning if it detects that the host has become unresponsive. This may occur if users turn off their PCs during a scan, a host has stopped responding after a denial of service plugin, or a security mechanism (for example, an IDS) has started to block traffic to a server. Normally, continuing scans on these machines sends unnecessary traffic across the network and delays the scan.
Scan IP addresses in a random order	Cleared	By default, Tenable.io Web Application Scanning scans a list of IP addresses in sequential order. When enabled, Tenable.io Web Application Scanning scans the list of hosts in a random order across the entire target IP space. This is typically useful in helping to distribute the network traffic during large scans.
Create unique identifier on hosts scanned using credentials	Selected	A unique identifier for credentialed scans.
Performance Options		
Slow down the scan when network congestion is detected	Cleared	This enables Tenable.io Web Application Scanning to detect when it is sending too many packets and the network pipe is approaching capacity. If detected, Tenable.io Web Application Scanning throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Tenable.io Web Application Scanning automatically attempts to use the available space within the network pipe again.
Use Linux ker-	Cleared	This enables Tenable.io Web Application Scanning to use the Linux

Setting	Default Value	Description
nel congestion detection		kernel to detect when it is sending too many packets and the network pipe is approaching capacity. If detected, Tenable.io Web Application Scanning throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Tenable.io Web Application Scanning automatically attempts to use the available space within the network pipe again.
Network timeout (in seconds)	5	The time that Tenable.io Web Application Scanning waits for a response from a host unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a greater number of seconds.
Max simultaneous checks per host	5	The maximum number of checks a Tenable.io Web Application Scanning scanner performs against a single host at one time.
Max simultaneous hosts per scan	30	The maximum number of hosts that a Tenable.io Web Application Scanning scanner scans simultaneously.
Max number of concurrent TCP sessions per host	None	The maximum number of established TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner eventually sends (e.g., if this option is set to 15, the SYN scanner sends up to 1500 packets per second).
Max number of concurrent TCP sessions per scan	None	This setting limits the maximum number of established TCP sessions for the entire scan, regardless of the number of hosts being scanned. For scanners installed on any Windows host, this value must be set to 19 or less to get accurate results.
Debug Settings		
Enable plugin debugging	Disabled	This attaches available debug logs from plugins to the vulnerability output of this scan.

Credentials

Setting	Default Value	Description
Authentication method	HTTP login form	There are four types of HTTP Authentication methods: • **Automatic authentication**: Requires a username and password only. • **Basic/Digest authentication**: Requires a username and password only. • **HTTP login form**: Requires a user to specify settings to control where authenticated testing of a custom web-based application begins. • **HTTP cookies import**: Requires a user to upload an HTTP cookie file.
Username	None	Username of the specified user.
Password	None	Password of the specified user.
Login page	None	The absolute path to the login page of the application, e.g., /login.html.
Login submission page	None	The action parameter for the form method. For example, the login form for <form method="POST" name="auth_form" action="/login.php"> would be /login.php.
Login parameters	None	The authentication parameters (e.g., login=%USER%&password=%PASS%). If the keywords %USER% and %PASS% are used, the keywords will be substituted with values supplied on the Login configurations drop-down menu. This field can be used to provide more than two parameters if required (e.g., a group name or some other piece of information is required for the authentication process).
Check authentication on page	None	The absolute path of a protected web page that requires authentication, to better assist Tenable.io Web Application Scanning in determining authentication status (e.g., /admin.html).

Setting	Default Value	Description
Regex to verify successful authentication	None	A regex pattern to look for on the login page. Simply receiving a 200 response code is not always sufficient to determine session state. Tenable.io Web Application Scanning can attempt to match a given string (e.g., Authentication successful!)
Cookies file	None	This option appears only if you select **HTTP cookies import** in the **Authentication method** box. To facilitate web application testing, Tenable.io Web Application Scanning can import HTTP cookies from another piece of software (e.g., web browser, web proxy, etc.) with the HTTP cookies import settings. A cookie file can be uploaded so that Tenable.io Web Application Scanning uses the cookies when attempting to access a web application. The cookie file must be in Netscape format.
Global Credential Settings		
Login method	POST	The login action is performed via either a GET or POST request.
Re-authenticate delay (seconds)	0	The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.
Follow 30x redirections (# of levels)	0	If a 30x redirect code is received from a web server, this option directs Tenable.io Web Application Scanning to follow the redirect.
Invert authenticated regex	Cleared	A regex pattern to look for on the login page, that if found, tells Tenable.io Web Application Scanning authentication was not successful (e.g., Authentication failed!).
Use authenticated regex on HTTP headers	Cleared	Tenable.io Web Application Scanning can search the HTTP response headers (rather than the body) for a given regex pattern to better determine authentication state.
Case insensitive authenticated regex	Cleared	The regex searches are case sensitive by default. This instructs Tenable.io Web Application Scanning to ignore case.

Cloud Scanners

By default, Tenable.io is configured with region-specific Cloud Scanners. You can select these scanners when you create and launch scans.

The following table identifies each Tenable.io Scanner and, for whitelisting purposes, its IP address range. These IP ranges are exclusive to Tenable, Inc..

Scanner	IP Range	IPv6 Range
Amazon US-EAST (Ohio)	13.59.252.0/25	2600:1f16:8ca:e900::/56
Amazon US-EAST (Virginia)	54.175.125.192/26 34.201.223.128/25	2600:1f18:614c:8000::/56
Amazon US-WEST (California)	54.219.188.128/26 13.56.21.128/25	2600:1f1c:13e:9e00::/56
Amazon EU-CENTRAL (Frankfurt)	54.93.254.128/26 18.194.95.64/26	2a05:d014:532:b00::/56
Amazon EU-WEST (London)	35.177.219.0/26	2a05:d01c:da5:e800::/56
Amazon AP-SOUTHEAST (Singapore)	54.255.254.0/26	2406:da18:844:7100::/56
Amazon AP-SOUTHEAST (Sydney)	13.210.1.64/26	2406:da1c:20f:2f00::/56

Plugin Information

Plugin Families

Tenable.io Web Application Scanning includes the following new plugin families for categorization of web plugins:

Plugin Family	Description
Authentication & Session	Plugins related to authentication and session issues.
Code Execution	Plugins allowing code to be executed on the server and/or the application.
Cross Site Scripting	All types of XSS issues.
Cross Site Request Forgery	XSRF issues.
Data Exposure	Plugins allowing sensitive or relevant information to be collected.
File Inclusion	File can be uploaded using plugins of this family.
General	Plugins used to provide general information.
Injection	Any type of injection (e.g., SQL, noSQL, and Code).
Web Applications	Information and detection collected on the web application.
Web Servers	Information and detection collected on the web server running the web application.

Plugin IDs

The plugin range used by Tenable.io Web Application Scanning is 98000-98999. The following table lists the available plugins for use with Web Application scans.

Plugin ID	Plugin Name	Plugin Family
98000	"Scan Information" Detection	General

Plugin ID	Plugin Name	Plugin Family
98009	"Web Application Sitemap" Detection	General
98047	"Allowed HTTP methods" Detection	Web Applications
98048	"HTTP TRACE" Detection	Web Servers
98050	"Interesting response" Detection	Web Applications
98054	"Unvalidated redirect" Detection	Web Applications
98056	"Missing 'Strict-Transport-Security' header" Detection	Web Applications
98057	"Insecure 'Access-Control-Allow-Origin' header" Detection	Web Applications
98060	"Missing 'X-Frame-Options' header" Detection	Web Applications
98062	"Cookie set for parent domain" Detection	Web Applications
98063	"HttpOnly cookie" Detection	Web Applications
98064	"Insecure cookie" Detection	Web Applications
98065	"Insecure client-access policy" Detection	Web Applications
98067	"Insecure cross-domain policy (allow-access-from)" Detection	Web Applications
98068	Insecure cross-domain policy	Web Applications
98070	"Common administration interface" Detection	Web Applications
98071	"Common sensitive file" Detection	Web Applications
98072	"Common directory" Detection	Web Servers
98077	"Private IP address disclosure" Detection	Data Exposure
98078	"E-mail address disclosure" Detection	Data Exposure
98079	"CVS/SVN user disclosure" Detection	Data Exposure
98080	"Form-based File Upload" Detection	Web Applications
98081	"Password field with auto-complete" Detection	Authentication & Session

Plugin ID	Plugin Name	Plugin Family
98082	"Unencrypted password form" Detection	Authentication & Session
98083	"CAPTCHA protected form" Detection	Web Applications
98084	"Directory listing" Detection	Web Servers
98087	"WebDAV" Detection	Web Servers
98088	"Exposed localstart.asp page" Detection	Web Applications
98091	"Mixed Resource" Detection	Web Applications
98092	"HTML object" Detection	Web Applications
98095	"Misconfiguration in LIMIT directive of .htaccess file" Detection	Web Servers
98096	"Access restriction bypass via origin spoof" Detection	Authentication & Session
98097	"A backdoor file exists on the server" Detection	Backdoors
98098	"Source code disclosure" Detection	Data Exposure
98099	"Publicly writable directory" Detection	Web Servers
98100	"Path Traversal" Detection	Web Applications
98101	"Response Splitting" Detection	Cross Site Scripting
98102	"Session fixation" Detection	Authentication & Session
98103	"Unvalidated DOM redirect" Detection	Web Applications
98104	"Cross-Site Scripting (XSS)" Detection	Cross Site Scripting
98105	"Cross-Site Scripting (XSS) in HTML Tag" Detection	Cross Site Scripting
98106	"Cross-Site Scripting (XSS) in script context" Detection	Cross Site Scripting
98107	"Cross-Site Scripting (XSS) in path" Detection	Cross Site Scripting

Plugin ID	Plugin Name	Plugin Family
98108	"Cross-Site Scripting (XSS) in event tag of HTML element" Detection	Cross Site Scripting
98109	"DOM-based Cross-Site Scripting (XSS)" Detection	Cross Site Scripting
98110	"DOM-based Cross-Site Scripting (XSS) in script context" Detection	Cross Site Scripting
98112	"Cross-Site Request Forgery" Detection	Cross Site Request Forgery
98113	"XML External Entity" Detection	Injection
98114	"XPath Injection" Detection	Injection
98115	"SQL Injection" Detection	Injection
98116	"NoSQL Injection" Detection	Injection
98117	"Blind SQL Injection (differential analysis)" Detection	Injection
98118	"Blind SQL Injection (timing attack)" Detection	Injection
98119	"Blind NoSQL Injection (differential analysis)" Detection	Injection
98120	"Code injection" Detection	Code Execution
98121	"Code injection (php://input wrapper)" Detection	Code Execution
98122	"Code injection (timing attack)" Detection	Code Execution
98123	"Operating system command injection" Detection	Code Execution
98124	"Operating system command injection (timing attack)" Detection	Code Execution
98125	"File Inclusion" Detection	File Inclusion
98126	"Remote File Inclusion" Detection	File Inclusion
98127	"LDAP Injection" Detection	Injection

How To

This section contains the following tasks related to managing Tenable.io Web Application Scanning:

- Filter the Workbench
- Create a Scan
- Configure Scan Settings
- Set Scan Permissions
- Start or Stop a Scan
- View Scan Results
- Delete a Scan

Filter the Workbench

1. In the top navigation bar, click the **Dashboards** button.
2. In the left navigation bar, click **Web Applications**.

   The **Web Applications** workbench appears.
3. In the upper right corner, select the **Last 30 Days** drop-down box.
4. Select the interval of time by which you want to filter the data.

   The workbench updates based on your selected filter.

Create a Scan

Before You Begin

Refer to the scan templates documentation for descriptions, available settings, and credentials for each Web Application scan template.

Steps

This procedure can be performed by a standard user or administrator.

1. In the top navigation bar, click the **Scans** button.

   The **My Scans** page appears.

2. In the upper-right corner, click the **New Scan** button.

   The **Scan Templates** page appears.

3. Click the scan template that you want to use.

4. Configure the scan:

   a. In the **Name** box, type a name for the scan.

   b. In the **Targets** box, type an IP address, hostname, or range of IP addresses.

   c. Click the **Scanner** box, and then select the scanner or scanner group that you want to perform the scan.

   d. If desired, modify the scan's settings. The scan can be launched using the default settings.

   e. If you want to perform a credentialed scan, click the **Credentials** tab, and then specify the credentials that you want to use for the scan.

   f. If you want to use the scan to audit compliance, click the **Compliance** tab, and then specify which of the following platforms you want to audit. Tenable, Inc. provides best practice audits for each platform. Additionally, you can upload a custom audit file.

5. If you want to launch the scan later, click the **Save** button.

   The scan is saved.

   -or-

If you want to launch the scan immediately, click the button, and then click **Launch**.

The scan is saved and launched.

Create a Limited Plugin Scan

1. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.

2. In the upper right corner, click the **New Scan** button.

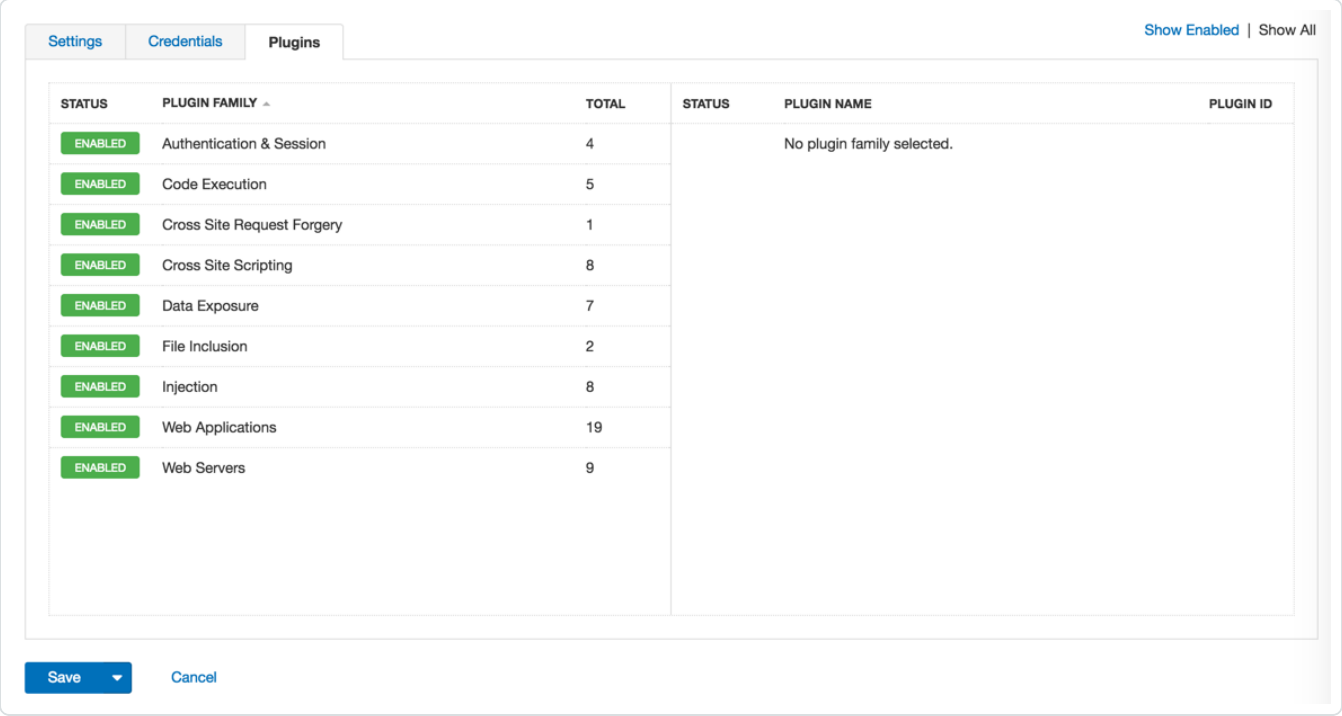
   The **Scan Templates** page appears.

3. Click the **Web Application** tab.

4. Depending on the template you want to use, click **Web App Overview** or **Web App Scan**.

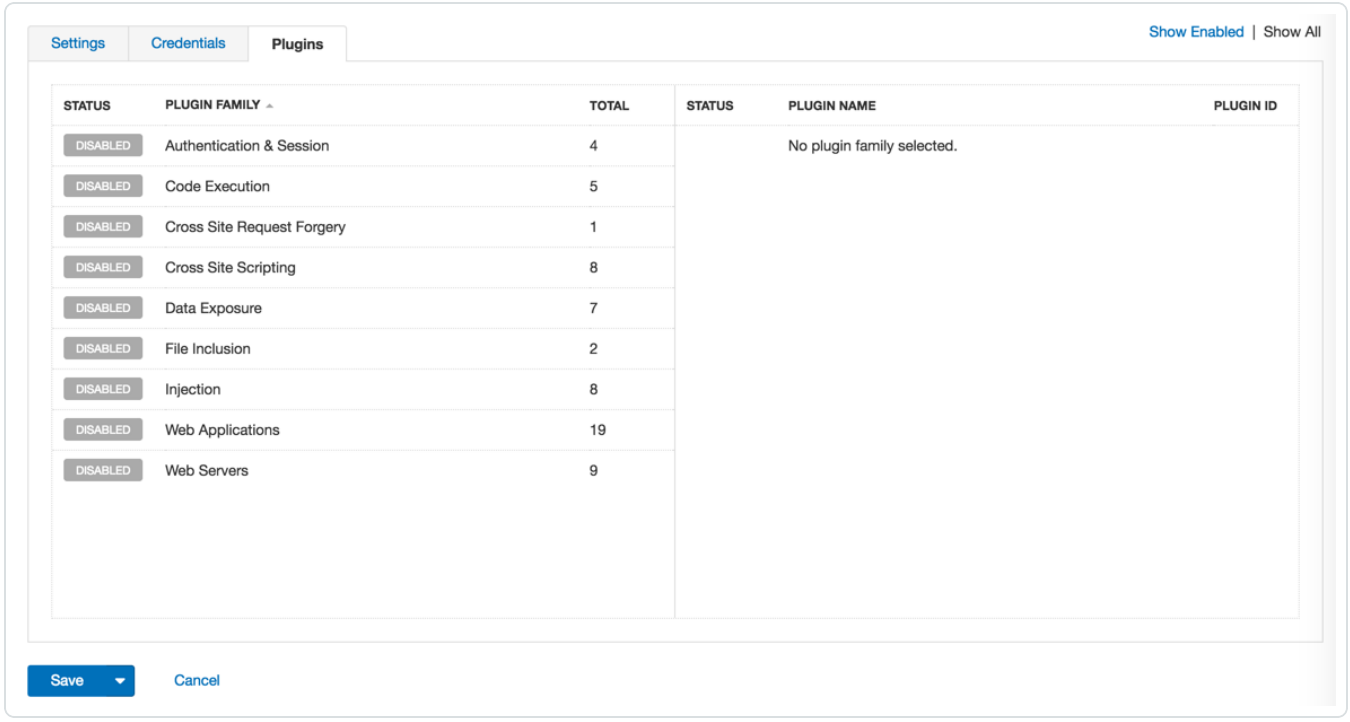
5. Click the **Plugins** tab.

   The list of plugin families appears, and by default, all of the plugin families are enabled.



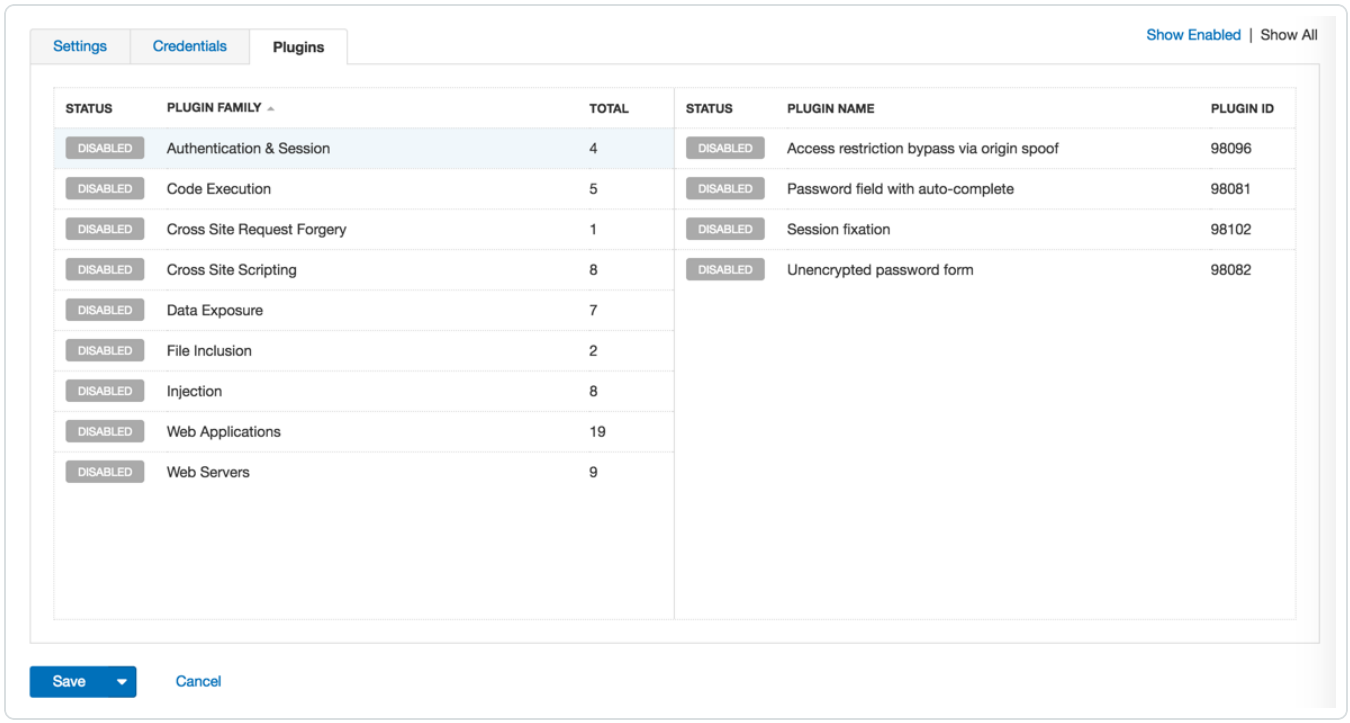
6. In the upper right corner, click the **Disable All** button.

   All the plugin families are disabled.



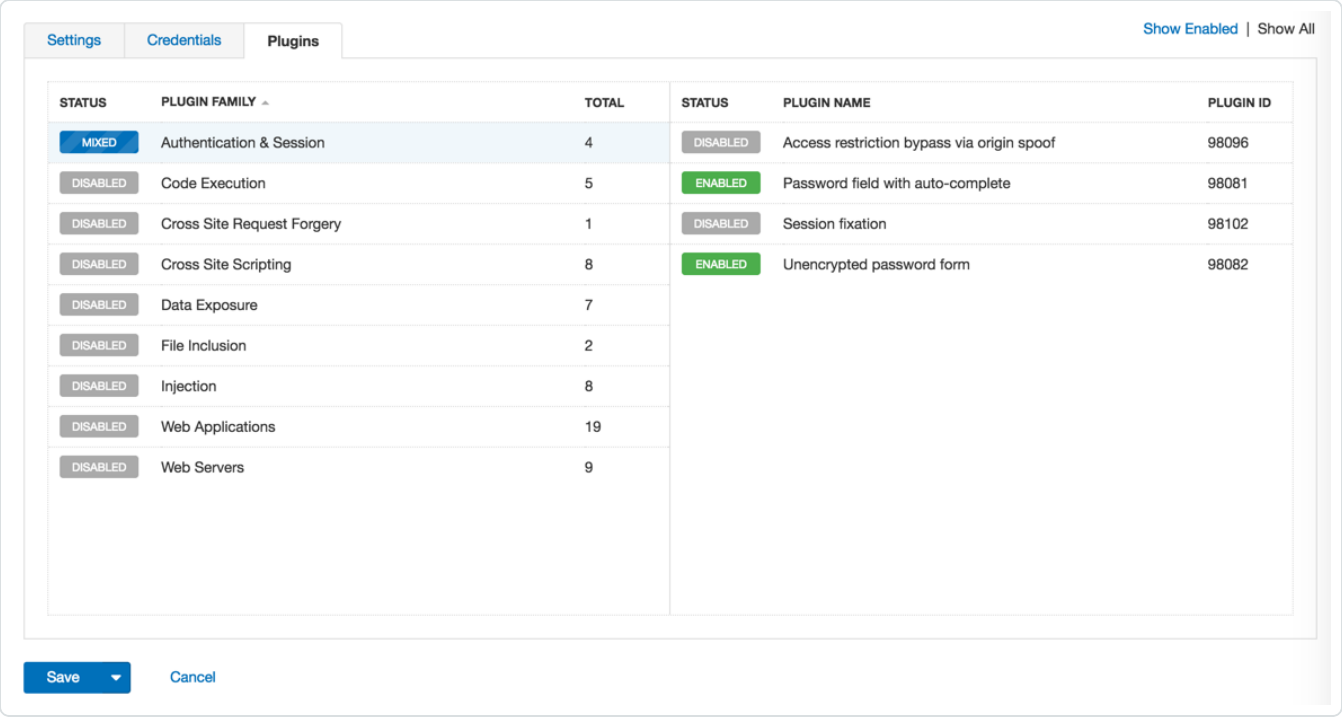
7. Click the plugin family that you want to include.

   The list of plugins appears in the right pane.



8. For each plugin that you want to enable, click the **Disabled** button.

Each plugin is enabled.



Tip: You can search for plugins and plugin families using the **Search Plugin Families** box in the upper right corner.

9. Click the **Save** button.

   The scan is saved.

Configure Scan Settings

This procedure can be performed by a standard user or administrator.

1. In the top navigation bar, click the **Scans** button.

   The **My Scans** page appears.

2. Optionally, on the left pane, click a different folder.

3. In the scans table, select the check box for the row corresponding to the scan that you want to configure.

   In the upper-right corner, the **More** button appears.

4. Click the **More** button.

5. Click **Configure**.

   The **Configuration** page for that scan appears.

6. Modify the settings.

7. Click the **Save** button.

   The changes save.

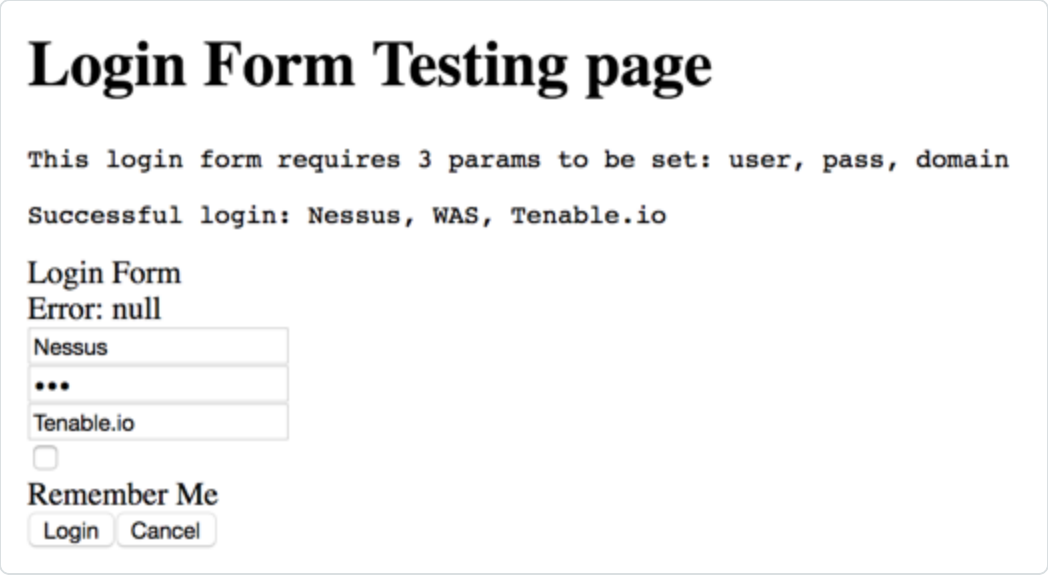
Configure Login Form Authentication

These steps describe how to check the authentication values for the **Login Form** authentication method in the **Credentials** settings for the **Web App Overview** and **Web App Scan** templates.

These steps assume that you already have a login form ready to test your credentials.

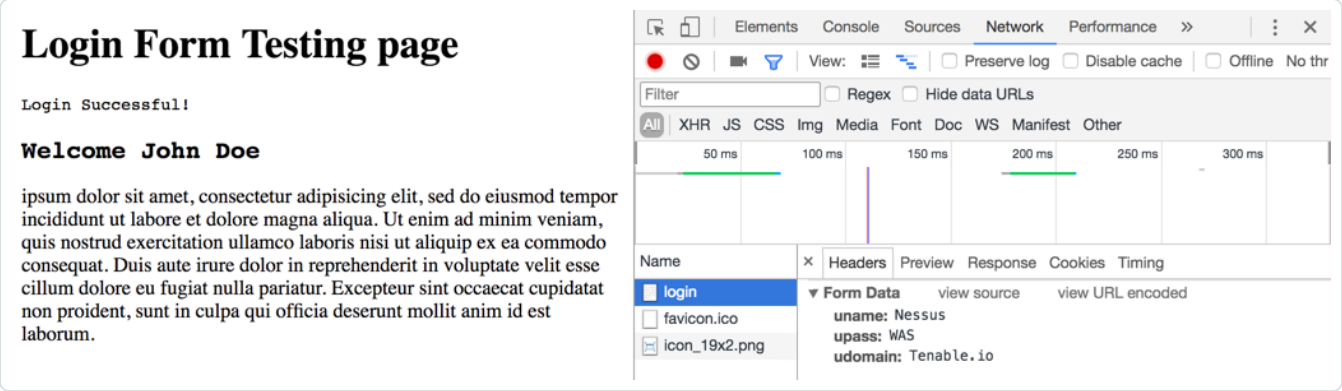
Steps

1. For the web application you want to scan, access the login page.
2. Type your credentials as necessary.



3. Upon successful authentication, in the browser console, locate the call that performs the authentication. In this example, the call is `login`.

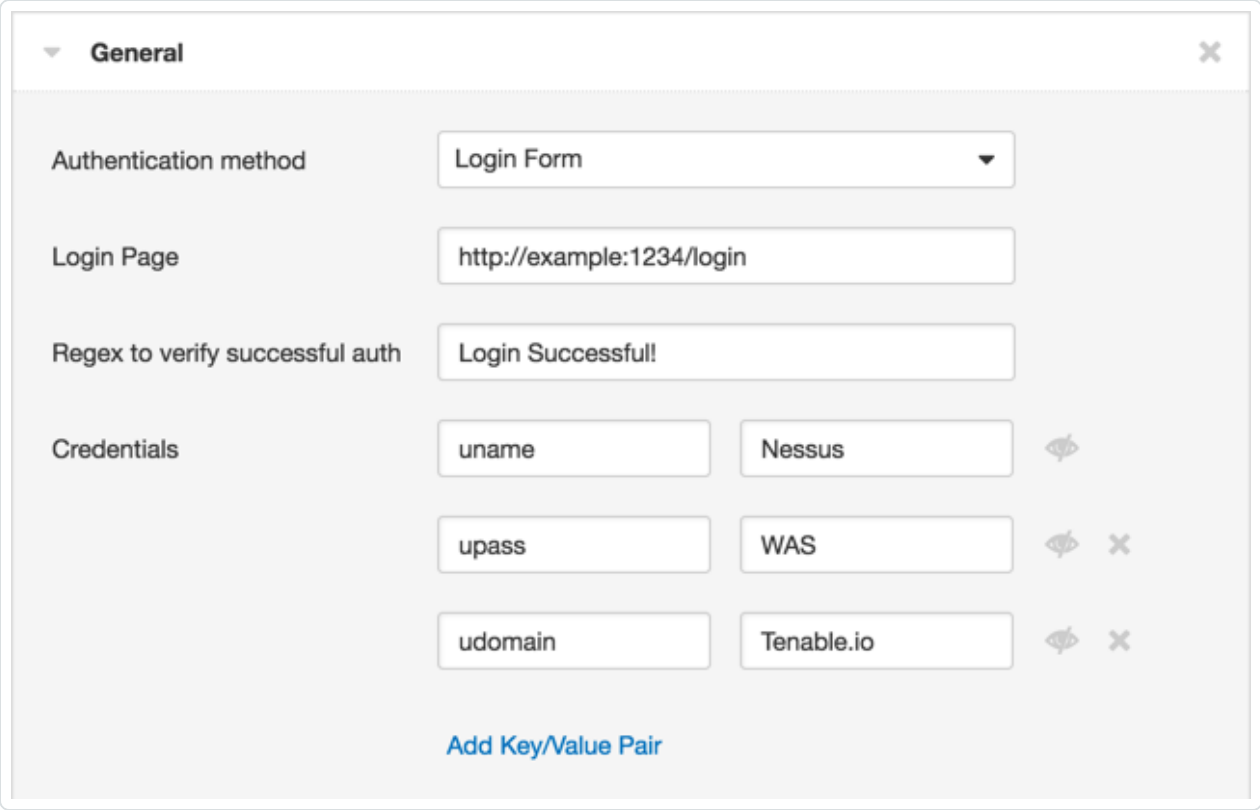
   The **Form Data** section displays the key/value pairs. In this example, the pairs are `uname: Nessus`, `upass: WAS`, and `udomain: Tenable.io`.



4. In Tenable.io Web Application Scanning, either create a new scan, or access the scan settings for which you want to add credentials.
5. In the scan settings, click the **Credentials** tab.
6. Click **General**.
    a. In the **Authentication Method** drop-down box, select **Login Form**.
    b. In the **Login Page** box, type the URL for your login form page.
    c. In the **Regex to verify successul auth** box, type the regex to match when the credentials are correct.

    > **Note:** In many cases, this is text that appears on the login page (e.g., `Login Successful!`)

d. In the **Credentials** boxes, type the key/value pairs that you retrieved in step 3.



7. Click the **Save** button.

Set Scan Permissions

This procedure can be performed by a standard user or administrator.

1. In the top navigation bar, click the **Scans** button.

   The **My Scans** page appears.

2. Optionally, on the left pane, click a different folder.

3. In the scans table, select the check box for the row corresponding to the scan that you want to configure.

   In the upper-right corner, the **More** button appears.

4. Click the **More** button.

5. Click **Permissions**.

   The **Update Permissions** window appears.

6. In the **Add users or groups box**, type the user name or group that you want to share the scan with. As you type, a filtered list of users and groups appears.

7. Click the **Update** button.

   The scan permissions update.

Start or Stop a Scan

Start a Scan

This procedure can be performed by a standard user or administrator.

1. In the top navigation bar, click the **Scans** button.

   The **My Scans** page appears.

2. Optionally, on the left pane, click a different folder.

3. In the scans table, on the row corresponding to the scan that you want to launch, click the ▶ button.

   The scan launches.

Stop a Scan

This procedure can be performed by a standard user or administrator.

1. In the top navigation bar, click the **Scans** button.

   The **My Scans** page appears.

2. Optionally, on the left pane, click a different folder.

3. In the scans table, on the row corresponding to the scan that you want to stop, click the ■ button.

   A dialog box appears, confirming your selection to stop the scan.

4. Click the **Stop** button.

   The scan stops.

View Scan Results

This procedure can be performed by a standard user or administrator.

1. In the top navigation bar, click the **Scans** button.

   The **My Scans** page appears.

2. Optionally, on the left pane, click a different folder.

3. In the scans table, click the name of the scan that you want to view results for.

   The results page for that scan appears.

Delete a Scan

This procedure can be performed by a standard user or administrator.

1. In the top navigation bar, click the **Scans** button.

   The **My Scans** page appears.

2. Optionally, on the left pane, click a different folder.

3. In the scans table, on the row corresponding to the scan that you want to delete, click the ✕ button.

   The scan moves to the **Trash** folder.

4. To permanently delete the scan, on the left pane, click the **Trash** folder.

   The **Trash** page appears.

5. On the **Trash** page, in the scans table, on the row corresponding to the scan that you want to delete, click the ✕ button.

   The **Delete Scan** dialog box appears.

6. Click the **Delete** button.

   The scan is deleted.

Tip: On the **Trash** page, in the upper-right corner, click the **Empty Trash** button to permanently delete all scans in the **Trash** folder.