



# QUALYSGUARD®

## WEB APPLICATION SCANNING GETTING STARTED GUIDE

### VERSION 1.3

September 23, 2010



Copyright 2009-2010 by Qualys, Inc. All Rights Reserved.

Qualys, the Qualys logo and QualysGuard are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.  
1600 Bridge Parkway  
Redwood Shores, CA 94065  
1 (650) 801 6100



# Table of Contents

<b>Introducing Web Application Scanning .....</b>	<b>4</b>
Web Application Scanning Workflow .....	4
Users and Web Application Scanning.....	6
<b>First Steps .....</b>	<b>7</b>
Your Account Information.....	8
Managing Permissions for Sub-Accounts.....	9
<b>Web Applications .....</b>	<b>10</b>
Viewing Web Applications.....	10
About Web Applications and Permissions .....	11
Creating Web Applications .....	11
Editing Web Applications.....	12
Adding Web Authentication Records.....	15
Granting User Access to Web Applications .....	19
Removing Web Applications.....	20
<b>Web Application Scans.....</b>	<b>21</b>
About Web Application Scanning .....	21
Web Application Profiles .....	22
Web Application Profile Settings.....	23
Launching Web Application Scans.....	28
Web Application Scan Settings .....	29
Viewing Web Application Scan History .....	30
Scan Summary Notification.....	31
Web Application Discovery Scan Results.....	32
Web Application Vulnerability Scan Results.....	35
Scheduling Web Application Scans.....	38
Scan Troubleshooting .....	39
<b>Web Application Reports.....</b>	<b>40</b>
Scorecard Report .....	40
Interactive Report.....	43
<b>Web Application Vulnerabilities .....</b>	<b>45</b>
Viewing Web Application Vulnerabilities .....	45
Severity Levels.....	46
<b>User Permissions.....</b>	<b>47</b>
<b>Contact Support .....</b>	<b>48</b>



# Introducing Web Application Scanning

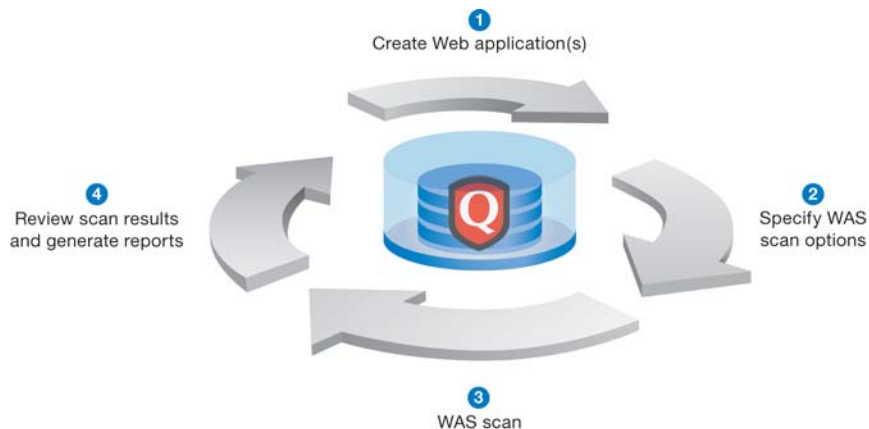
QualysGuard® Web Application Scanning (WAS) allows users to crawl web applications, detect cross-site scripting and SQL injection vulnerabilities, detect sensitive content in HTML based on user settings, and conduct authenticated and non-authenticated scanning to capture the perspective of both authorized and non-authorized users. The WAS solution automates techniques used to identify most web vulnerabilities and delivers a broad scope of coverage for testing web application vulnerabilities such as those in the OWASP Top 10 and WASC-TC, including SQL Injection and Cross-Site Scripting. The WAS scanning engine combines pattern recognition and observed behaviors to accurately identify and verify vulnerabilities.

Web Application Scanning is available in your account only when the WAS module is enabled for your QualysGuard subscription. If you would like us to enable the WAS module for your subscription, please contact Technical Support or your Technical Account Manager.

This getting started guide describes features and functionality included with the WAS module. Online help is always available. You can click the Help button anytime you are stepping through a workflow. For more assistance, view the online help (Help—>Online Help) and the user guides in the Resources section (Help—>Resources). If you are new to QualysGuard, we recommend the *QualysGuard Quick Tour* as a good way to get started.

## Web Application Scanning Workflow

The Web Application Scanning process is shown below.



### Create Web Applications

One web application may be selected as the target for a web application scan. A web application is defined as a virtual host (FQDN or IP address), starting port and starting URI, as well as other optional scan settings for black/white lists, authentication records, and business information for tracking. See [Creating Web Applications](#).

## Add Authentication Records to Web Application

Authentication to HTML forms is optional. Multiple authentication techniques are supported. To enable authentication, add authentication records to the web applications in your account. When enabled, the crawler attempts authentication the first time the web crawler encounters a login form. Upon success the crawler visits the form action link, gathers information for analysis and continues crawling. See [Adding Web Authentication Records](#).

## Run Web Application Scans

You can run web application scans in two modes: discovery and vulnerability.

**Discovery Scan.** The first time you scan a particular web application, it's recommended you launch a discovery scan. A discovery scan follows the links it encounters in your web application and gathers information about it, but does not perform vulnerability testing. A discovery scan is a good way to understand where the scan will go and whether there are URIs you should blacklist for vulnerability scans.

**Vulnerability Scan.** When running a vulnerability scan, the scanning engine performs vulnerability checks and information gathered checks. Vulnerability checks may include: cross-site vulnerability checks (persistent, reflected, header, browser-specific) and SQL injection vulnerabilities (regular and blind). Sensitive content checks may include: Social Security number (United States), credit card numbers and custom defined.

Web application scans analyze the security of your web applications.

**Launch web application scans.** You have the option to launch a web application scan on demand or schedule it to run at a later time. When scanner appliances are installed, select a Scanner Appliance to scan web applications on your internal network.

**View web application scan results.** You may view the scan results for a completed web application scan. The report summary includes scan settings, status and duration. The details section identifies detections for vulnerabilities, sensitive content, and information gathered based on your option profile settings. See [Web Application Scans](#).

## Run Web Application Reports

Web Application scan reports draw on data from the most recent scan of the web application.

### Interactive Report

The Web Application Interactive Report identifies vulnerabilities, sensitive content and information gathered detected by the most recent scan of a selected web application. You can keep changing the report settings to get different views of your web application scan data.

### Scorecard Report

The Web Application Scorecard Report allows you to report on web application scan data for different business groups and functions. This identifies the vulnerabilities, sensitive content and information gathered detected for one or more web applications.

See [Web Application Reports](#).

## **Users and Web Application Scanning**


The WAS module implements a two-level permissions system for managing user access to web application management features.

At the account level, Managers have full access rights for web application management. Managers have the ability to grant extended permissions for web application management to any user in the subscription. Unit Managers have the ability to grant extended permissions to any user in their business unit as long as the Unit Manager also has the permissions.

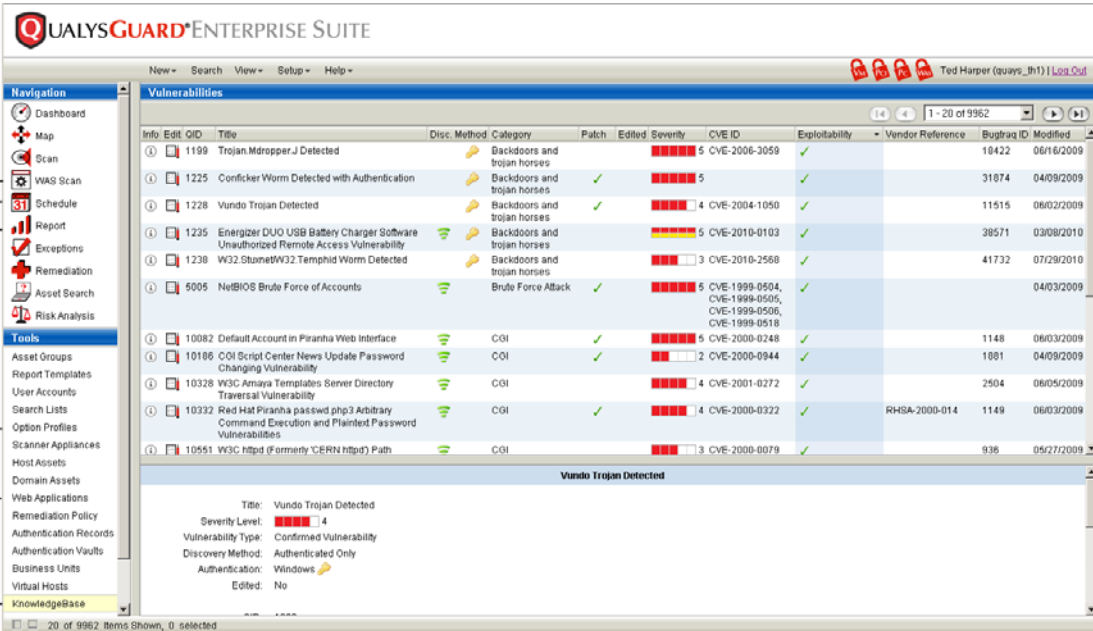
At the web application level, Managers have full access rights (Read, Write, and/or Execute) for all web applications. Each web application owner has full rights to their own web application. Users with full access rights to a specific web application may grant other users access rights to the web application. A user may view the web application (Read), edit the web application and run reports on it (Write), and scan the web application (Execute).



## First Steps

The Web Application Scanning (WAS) module is enabled for your subscription when  appears in the top menu bar.

When enabled, Managers are granted access to web application management features automatically. Sub-accounts (Readers, Scanners, Unit Managers) may be granted access to these features.



The screenshot displays the QualysGuard Enterprise Suite interface. The top navigation bar includes 'New', 'Search', 'View', 'Setup', and 'Help'. The user is logged in as 'Ted Harper (quays\_bh1)'. The main content area shows a table of vulnerabilities with columns for Info, Edit, QID, Title, Disc. Method, Category, Patch, Edited, Severity, CVE ID, Exploitability, Vendor Reference, Bugtraq ID, and Modified. A detailed view of a 'Vundo Trojan Detected' vulnerability is shown at the bottom, including its title, severity level (4), type (Confirmed Vulnerability), discovery method (Authenticated Only), and authentication (Windows).

Info	Edit	QID	Title	Disc. Method	Category	Patch	Edited	Severity	CVE ID	Exploitability	Vendor Reference	Bugtraq ID	Modified
①		1199	Trojan.Mdropper.J Detected		Backdoors and trojan horses			5	CVE-2006-3059	✓		18422	06/16/2009
①		1225	Conficker Worm Detected with Authentication		Backdoors and trojan horses	✓		5		✓		31874	04/09/2009
①		1228	Vundo Trojan Detected		Backdoors and trojan horses	✓		4	CVE-2004-1050	✓		11515	06/02/2009
①		1235	Energizer DUO USB Battery Charger Software Unauthorized Remote Access Vulnerability		Backdoors and trojan horses			5	CVE-2010-0103	✓		38571	03/08/2010
①		1238	W32.StunnetW32.Temphid Worm Detected		Backdoors and trojan horses			3	CVE-2010-2568	✓		41732	07/29/2010
①		5005	NetBIOS Brute Force of Accounts		Brute Force Attack	✓		5	CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-1999-0518	✓			04/03/2009
①		10082	Default Account in Piranha Web Interface		CGI	✓		5	CVE-2000-0248	✓		1148	06/03/2009
①		10186	CGI Script Center News Update Password Changing Vulnerability		CGI	✓		2	CVE-2000-0944	✓		1081	04/09/2009
①		10328	W3C Amaya Templates Server Directory Traversal Vulnerability		CGI			4	CVE-2001-0272	✓		2504	06/05/2009
①		10332	Red Hat Piranha password.php? Arbitrary Command Execution and PlainText Vulnerabilities		CGI	✓		4	CVE-2000-0322	✓	RHSA-2000-014	1149	06/03/2009
①		10551	W3C httpd (Formerly 'CERN httpd') Path		CGI			3	CVE-2000-0079	✓		936	05/27/2009

A. WAS Scan — Launch web application scans to analyze the security of your web applications and identify detected vulnerabilities, sensitive content, and information gathered.

B. Schedule — Schedule web application scans to run at some time in the future.

C. Report — Run reports with multiple views to review web application vulnerability status and verified solutions. Both scorecard reports and interactive reports for remediation and testing are provided.

D. Option Profiles — A web application profile with scan settings is applied to each web application scan. A user may configure settings for crawling, sensitive content search, and vulnerability detection.

## First Steps

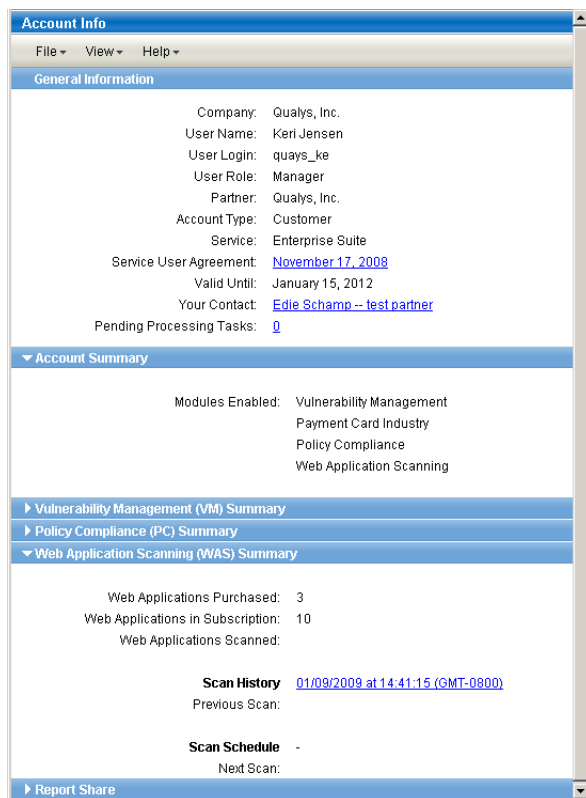
### Your Account Information

E. Web Applications — A web application is used as the target of a web application scan. It is defined by the location where crawling starts: virtual host (FQDN or IP address), port number, and starting URI (by default the web application root directory). User access is managed per web application by access rights: read (view), write (edit), and execute (launch a scan). Full rights are given to all Managers and the web application owner; other users may be granted rights.

F. Knowledgebase — The KnowledgeBase includes vulnerability checks performed for web application scans (all vulnerabilities in the Web Application category).

## Your Account Information

The Account Info page (Help—>Account Info) includes a section called Web Application (WAS) Summary. This section displays information about your web applications, scans and scheduled tasks. When Managers views this page, they see the total number of web applications purchased for the subscription and the total number of web applications currently in the subscription.



The screenshot shows the 'Account Info' window with the following sections:

- General Information:**
  - Company: Qualys, Inc.
  - User Name: Keri Jensen
  - User Login: quays\_ke
  - User Role: Manager
  - Partner: Qualys, Inc.
  - Account Type: Customer
  - Service: Enterprise Suite
  - Service User Agreement: [November 17, 2008](#)
  - Valid Until: January 15, 2012
  - Your Contact: [Edie Schamp -- test partner](#)
  - Pending Processing Tasks: 0
- Account Summary:**
  - Modules Enabled: Vulnerability Management, Payment Card Industry, Policy Compliance, Web Application Scanning
- Web Application Scanning (WAS) Summary:**
  - Web Applications Purchased: 3
  - Web Applications in Subscription: 10
  - Web Applications Scanned:
  - Scan History: [01/09/2009 at 14:41:15 \(GMT-0800\)](#)
  - Previous Scan:
  - Scan Schedule: -
  - Next Scan:

The Account Summary section identifies the modules that are enabled for your subscription: Vulnerability Management (VM), Payment Card Industry (PCI), Policy Compliance (PC), and Web Application Scanning (WAS). Only the modules that are enabled for your subscription appear in this section.


## Managing Permissions for Sub-Accounts

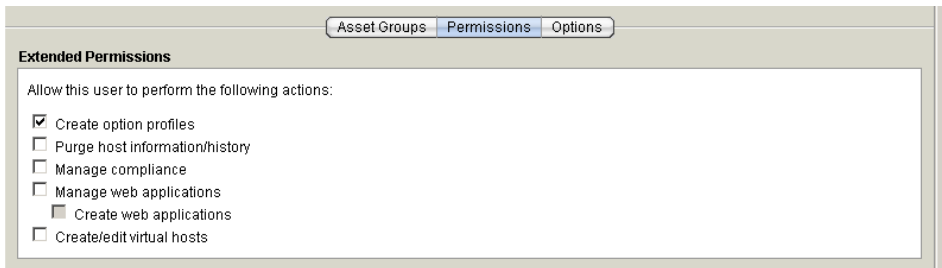
### Grant WAS permissions to sub-accounts

Role-based access controls allow multiple users access to QualysGuard with various privileges. Each user account is assigned a user role with certain privileges: Manager, Unit Manager, Scanner or Reader.

Managers should determine which sub-account users (Readers, Scanners and/or Unit Managers) will participate in web application management and edit accounts to grant access to WAS permissions. By default, the service does not assign WAS permissions to sub-accounts.

To grant WAS permissions to a sub-account:

- 1 Select User Accounts from the left menu. The user accounts list appears.
- 2 Click  next to the account you wish to edit. Managers have the ability to edit all sub-accounts in the subscription; Unit Managers have the ability to edit sub-accounts that belong to their own business unit.
- 3 Go the Permissions section for the account. Note the list of permissions varies based on the user role. For a Scanner, the permissions list looks like this:



- 4 Select WAS permissions appropriate for the user. The options are:

Option	Description
Manage web applications	Select this option to allow this user to perform web application management tasks based on the user's web application access permissions.
Create web applications	Select this option to give the user the ability to create web applications. This option is available only when "Manage web applications" is selected.

- 5 Click Save to save the user account with your changes.

### Grant User Access to Web Applications

Managers have full access rights for all web applications, when the web application scanning (WAS) module is enabled for the subscription. The web application owner has full rights for their own web application. Users with full access rights for a web application may grant access rights to other users.

Users may be granted various access rights (Read, Write, Execute) for each web application. We will describe how to grant users access to web applications in the next section.



# Web Applications

A web application is used as the target of a web application scan. Web applications are user-defined configurations and can be shared among users in the subscription. When the WAS module is first enabled, there are no web applications until users create them. User permissions for viewing, creating and running scans on web applications depends on user account level settings and web application level settings.

## Viewing Web Applications

View web applications in your account by selecting Web Applications from the left menu, under Tools. The Web Applications option is available when the web application management permission is enabled for your account. Only the web applications you have Read access rights to are included in the list.

Permissions — If you are a Manager, then this list includes all web applications in the subscription. If you have another user role (Reader, Scanner or Unit Manager), then the list consists of the web applications that you have Read access rights to.

The screenshot displays the QualysGuard Enterprise Suite interface. The top navigation bar includes 'New', 'Search', 'View', 'Setup', and 'Help'. The user is identified as 'Keri Jensen (quays\_ke)' with a 'Log Out' link. The left sidebar contains a 'Navigation' menu with options like Dashboard, Map, Scan, WAS Scan, Schedule, Report, Exceptions, Remediation, Asset Search, and Risk Analysis. Below this is a 'Tools' menu with options like Asset Groups, Report Templates, User Accounts, Search Lists, Option Profiles, Host Assets, Domain Assets, Web Applications (highlighted), and Remediation Policy. The main content area is titled 'Web Applications' and shows a table with the following data:

Info	Edit	Title	Virtual Host	Port	Starting URI	User	Created	Modified
		Demo Web Application	10.10.26.238	80	/	Keri Jensen	12/09/2008	02/23/2009
		phpBB 1.4.0	10.10.25.116	80	/phpBB/1.4.0	George Franks	12/08/2008	01/07/2009
		phpBB HTTP Basic	10.10.26.200	80	/phpBB/1.4.4_basic	Keri Jensen	12/08/2008	12/08/2008

Below the table, a detailed view for the 'Demo Web Application' is shown:

**Demo Web Application**

Title: Demo Web Application  
Virtual Host: 10.10.26.238  
Port: 80  
Starting URI: /

Owner: Keri Jensen (quays\_ke)  
Created: 12/09/2008 at 11:45:23 (GMT-0800)

At the bottom of the interface, it indicates '3 of 3 Items Shown, 0 selected'.

## About Web Applications and Permissions

Web application management features are available when the web application scanning (WAS) module is enabled for the subscription.

The WAS module implements a two-level permissions system for managing user access to web application management features. Managers have full access rights to all web application management features. Other users have assigned access rights based on user account and web application settings.

### User Account (Extended User Permissions)

Managers are automatically granted full permissions to manage web applications and create web applications. Managers may grant extended permissions to users, allowing them to use web application management features. The “Manage web applications” permission grants a user permissions to view web applications, edit web applications, and select them for scans and reports. The “Create web applications” permission grants a user permissions to create web applications. Unit Managers who are granted these permissions in their own account may grant the same user permissions to other users within their business unit.

### Web Application (User Access Rights per Web Application)

Managers have full access rights (Read, Write, and/or Execute) to all web applications. Each web application owner has full rights to their own web application. Users with full access rights to a specific web application may grant other users access rights to a web application. A user may view the web application (Read permission), edit the web application and run reports on it (Write permission), and scan the web application (Execute permission).

## Creating Web Applications

You can create a number of web applications up to the total number of web applications purchased.

Please note: It is your responsibility to verify that you have permission to scan all web applications that you specify as scan targets.

Permissions — The web application scanning (WAS) module must be enabled for the subscription. Users other than Managers must be granted permissions to create web applications.

### Steps for creating a web application

- 1 Select Web Applications from the left menu, under Tools.
- 2 Go to New—>Web Application on the top menu bar. The New Web Application page appears.
- 3 Enter web application settings on these tabs:
  - Application Info — Define the web application by providing the target virtual host (IP address or host name), port and starting URI where the web crawling will start from. You have the option to select a default web application profile that will be applied automatically when users launch or schedule a scan on the web application. See [Adding Application Information](#).

- Authentication — Add, edit and delete web application authentication records that can be selected by users for scanning the web application. Each record identifies form authorization credentials and settings to be used for authentication when the web crawler encounters a login form. See [Adding Web Authentication Records](#).
- Black/White Lists — Setup a black list and/or white list for the web application. The black/white lists provide a way to ensure that only selected parts of the web application will be scanned. Important! Automated web application scanning has the potential of causing data loss. Use the black list feature to avoid data loss. See [Adding Black/White Lists](#).
- Business Info — Provide information that describes the web application in business terms for tracking.
- Advanced — Select advanced options (optional) for the web application to select crawling hints and advanced options.

About Crawling Hints: Robots.txt is a convention to prevent cooperating web spiders and other web robots from accessing all or part of a website which is otherwise publicly viewable. Select the Robots.txt option to adhere to a robots.txt file if present in the web application. Sitemap.xml is an XML file that lists URLs for a site to inform search engines about URLs that are available for crawling. Select the Sitemap.xml option to adhere to a sitemap.xml file if present in the web application.


- 4 Click Save.

## Editing Web Applications

Web applications in your account can be edited when you have permissions to edit the web application.

Permissions — The web application scanning (WAS) module must be enabled for the subscription. Users other than Managers and web application owners must be granted permissions in order to edit web applications.

### Steps for editing a web application

- 1 Select Web Applications from the left menu, under Tools.
- 2 Identify the web application you want to change and click . The Edit Web Application page appears.
- 3 Make changes to the web application settings.
- 4 Click Save.

## Adding Application Information

You add application information on the Application Info tab.

The screenshot shows the 'New Web Application' dialog box with the 'Application Information' tab selected. The 'General Information' section at the top has 'Title' set to 'Demo Web Application' and 'Owner' set to 'Keri Jensen (Manager: queys\_ke)'. The 'Application Information' section contains the following fields and options:

- Application Definition:** Use the following fields to define the web application.
  - Virtual Host:** 10.10.26.238 (with a note: 'Use either an IP address or FQDN'). A callout box shows the URL 'http://www.example.com:80/your/application.html' with brackets identifying 'www.example.com' as the Site, '80' as the Port, and '/your/application.html' as the URI.
  - Starting Port:** 80
  - Starting URI:** /
  - Limit crawling to starting URI and its sub-directories
  - [Add Multi-Site Support](#)
- Option Profile:** Select a default option profile to use with this web application. The dropdown is set to 'None' with a 'View' link.

Buttons for 'Save', 'Cancel', and 'Help' are located at the bottom of the dialog.

### Virtual Host

The virtual host is the starting host from which to start web crawling. Enter an IP address or host name (FQDN) to start web crawling under. The web application can consist of a single physical host or multiple identical hosts behind a single load-balanced host.

### Starting Port

Enter the port number from which to start crawling.

### Starting URI

Enter the starting path from which to start crawling.

By default the crawling starts at the web application root directory. To start web crawling from a subdirectory, enter the path to the starting directory beginning with "/". This could be extracted from a correctly formed URL. For example:

```
/services/app1
```

### Limit crawling to starting URI and its sub-directories

Select this option to limit crawling to the starting URI and its sub-directories. When selected, the scanning engine scans the starting URI and any child directories it finds, but it will not scan any parent directories of the starting URI.

Sample Web Application:

Virtual Host	www.qualys.com
Port	80
Starting URI	/research/

Using the above web application, the scanning engine will start its scan at <http://www.qualys.com/research/>. From this page, links will be found to:

<http://www.qualys.com/research/exploits/>  
<http://www.qualys.com/research/top10/>  
<http://www.qualys.com/research/vulnlaws/>  
<http://www.qualys.com/research/knowledge/>  
<http://www.qualys.com/>  
[http://www.qualys.com/products/qg\\_suite/](http://www.qualys.com/products/qg_suite/)  
<http://www.qualys.com/customers/>  
etc...

From this list of links discovered, the scanning engine will NOT crawl:

<http://www.qualys.com/>  
[http://www.qualys.com/products/qg\\_suite/](http://www.qualys.com/products/qg_suite/)  
<http://www.qualys.com/customers/>

Notes:

<http://www.qualys.com/> will not be crawled because it is a parent directory of [/research/](http://www.qualys.com/research/).  
[http://www.qualys.com/products/qg\\_suite/](http://www.qualys.com/products/qg_suite/) and <http://www.qualys.com/customers/> will not be crawled because they are not child directories of [/research/](http://www.qualys.com/research/).

## Adding Web Authentication Records

Web application records appear on the Authentication tab. Each web authentication record identifies credentials for one or more authentication types — Form, HTTP Basic, NTLM and Digest — for the web application. To launch an authenticated web application scan, you select a target web application and optionally an authentication record.

To add an authentication record, click Add Record to the right of the records list. Provide authentication information and then click Save to add the record to the application.

The screenshot shows the 'New Web Application' dialog box with the 'Authentication' tab selected. The 'General Information' section contains a 'Title' field with 'Demo Web Application' and an 'Owner' dropdown menu showing 'Keri Jensen (Manager: quays\_ke)'. Below this is a tabbed interface with 'Authentication' selected. The 'Authentication' section contains a list of records with columns for 'Authentication', 'Type', and 'Add Record'. The list has one entry: 'My Record' with 'Form' as the type. There are 'Add Record' and 'Clear All' buttons to the right of the list. At the bottom of the dialog are 'Save', 'Cancel', and 'Help' buttons.

## Form Authentication

The screenshot shows the 'New Web Application Record' dialog box with the 'Form Authentication' tab selected. The 'General Information' section contains a 'Title' field with 'My Record'. Below this is a tabbed interface with 'Form Authentication' selected. The 'Form Authentication' section contains a text box with instructions: 'Enter the details for the login form. One of the easiest ways to find the form values is to view the source code and search for "-form" (without the quotes). Most browsers allow you to view the source either through the "View" menu or by right-clicking on the page.' Below this is the 'Form Details' section with a 'Type' dropdown menu set to 'Standard Login' and a checkbox for 'Send authentication over SSL only'. The 'Form Fields' section contains three input fields: 'User Name' with 'admin', 'Password' with masked characters, and 'Confirm Password' with masked characters. At the bottom of the dialog are 'Save', 'Cancel', and 'Help' buttons.

Enter one set of credentials for form authentication.

- Type — Select the form authentication type: Standard Login or Custom. The Custom type gives you additional fields for defining the form to authenticate to.

## Web Applications

### Adding Web Authentication Records

- Send authentication over SSL only — Select this option if you want the service to attempt authentication only when the form being authenticated to will be sent over SSL. When selected, authentication is attempted only when the form is submitted via a link that uses SSL (link URI https://...).
- Action — (Available when Custom type is selected). The form action as defined in its <FORM> tag. Your entry can have a maximum of 2048 characters.
- Form Fields — Enter form fields in the space provided.

### Form Authentication Type

When Standard Login is selected, enter form authentication fields for User Name and Password.

When Custom is selected, enter the login fields in the space provided. Login fields will commonly be User Name (or Login) and Password. There may be more fields and even hidden fields that do not show on the screen. If the form has fields that change depending on what you select we suggest you fill out the form entirely and then look at the source code of the page.

Each login field is defined on one line in the user interface. Initially the User Name and Password fields are defined. You can choose to rename these fields or add additional fields.

- Name — A form field name. Your entry can have a maximum of 128 characters.
- Value — A form field value. Your entry can have a maximum of 4096 characters. For a masked field, the value entered consists of mask characters.
- Confirm Value — (Available for masked field) A form field value. Your entry can have a maximum of 4096 characters. For a masked field, the value entered consists of mask characters.

Add more form fields as needed. Click Add Field to add a form field with the Name and Value elements. Click Add Masked Field to add a masked field with the Name, Value, and Confirm Value elements. For a masked form field, the characters you enter for Value and Confirm Value are masked.

### Defining Custom Form Fields

When defining custom form fields you have the option to rename the existing User Name and Password fields or to add more fields.

For an airline reservation site, you could define the fields: Ticket Number and Last Name.

For an online store, you could keep the User Name and Password fields and add these additional fields: Credit Card Number, CVV Code, and Billing Zip Code.

## Server Authentication

**New Web Application Record**

**General Information**

Title: \*

Form Authentication | **Server Authentication**

**Server Authentication**

Enter the basic authentication credentials into the following fields. You may have up to ten basic authentication credentials per web application record.

Send authentication over SSL only

Type:  [Remove](#)

Domain / Realm:

User Name:

Password:

Confirm Password:

[+ Add Another Set of Credentials](#)

Send authentication over SSL only — Select this option if you want the service to attempt authentication only when the form being authenticated to will be sent over SSL. When selected, authentication is attempted only when the form is submitted via a link that uses SSL (link URI <https://...>).

Enter one or more sets of credentials for server authentication. Click “Add Another Set of Credentials” to add a set of login credentials. Select an authentication type (HTTP Basic, NTLM or Digest) and enter login credentials in the fields provided. Click Add Another Set of Credentials to add another set of credentials for an authentication type.

Domain/Realm — For NTLM server authentication, enter the Windows domain name containing the credentials supplied in User Name/Password. For HTTP Basic server authentication, enter the protected realm name.

## Adding Black/White Lists

The screenshot shows a 'New Web Application' dialog box with the following details:

- General Information:**
  - Title: \* Demo Web Application
  - Owner: \* Keri Jensen (Manager: quays\_ke)
- Black/White Lists:**
  - Black List:** Set up a black list to prevent those URLs or their sub-directories from being scanned. Any link that matches a black list entry will not be scanned unless it also matches a white list entry.
    - URLs: Enter the URLs that should be ignored when a scan is run on this application. Text area contains: /test\_platform/. \*
    - Regular Expressions
  - White List:** Set up a white list to include those URLs or their sub-directories in the scan.
    - URLs
    - Regular Expressions

Buttons at the bottom: Save, Cancel, Help.

A black list identifies the links (URLs) in the web application that you do not want to be scanned. For each string specified, the crawler performs a string match against each link it encounters. When a match is found, the crawler does not submit a request for the link unless it also matches a white list entry.

A white list identifies the links (URLs) in the web application that you want to be scanned. Specifying a white list implies that only the links that match the list will be requested/crawled. For each string specified, the crawler performs a string match against each link it encounters. When a match is found, the crawler submits a request for the link.

The black/white list can consist of URLs and/or regular expressions.

**URLs** — Select to enter URLs for the list. Enter each URL on a new line. Each URL can have a maximum of 2048 characters. For example, specify corp for all URLs containing the string “corp”.

**Regular Expressions** — Select to enter regular expressions for the list. Enter each regular expression on a new line. Each regular expression can have a maximum of 2048 characters. For example, specify /my/path/. \* for all URLs under the /my/path/ directory.

You have the option to add a black list, a white list, or both.

**Black List Only.** When the web application has a black list only (no white list), any link that matches a black list entry will not be crawled.

**Black List and White List.** When the web application has both a black list and a white list, the white list entries are treated as exceptions to the black list. Any link that matches a black list entry will not be crawled unless it also matches a white list entry. Links that only match a black list entry will not be crawled. All other links including matches for white list entries will be crawled.

White List Only. When the web application has a white list only (no black list), no links will be crawled unless they match a white list entry.


Customers often wish to disallow the crawling of root sub-directories. An easy way to do this is to select the option “Limit crawling to starting URI and its sub-directories” in the web application profile for the scan. See [Web Application Profiles](#).

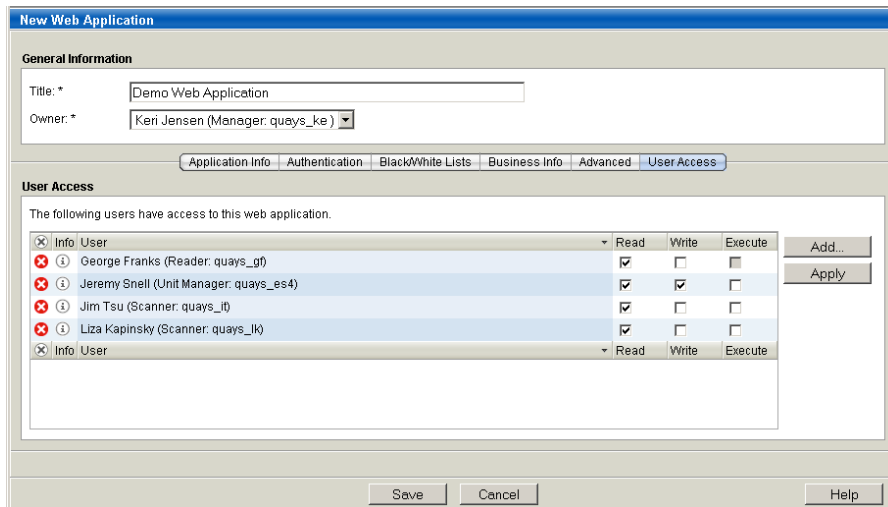
## Granting User Access to Web Applications

Managers have full access rights for all web applications, when the web application scanning (WAS) module is enabled for the subscription. The web application owner has full rights for their own web application. Users with full access rights for the web application may grant access rights to other users.

Other users may be granted various access rights (Read, Write, Execute) for web applications when the Manage web applications user permission is granted in their account. User access rights are granted for each web application, so a user may have more access rights for one web application than another.

### To grant a user access to a web application:

- 1 Select Web Applications from the left menu, under Tools.
- 2 Identify the web application you want to change and click . The Edit Web Application page appears.
- 3 Select the User Access tab to show the users who have been granted access. The access rights (Read, Write and Execute) for each user are displayed. (The user list does not include Manager users and the web application owner since these users are granted full access to the web application automatically.)



- 4 Click Add if you wish to add one or more users to the list. In the Select Users pop up select each user you want to add to the list, and then click Add.

- 5 For each user, assign access rights using the check boxes provided:
  - Read. Select to allow the user to view the web application and run reports on it. Read access is required if you also want to grant additional access (Write and/or Execute).
  - Write. Select to allow the user to edit the web application.
  - Execute. Allow the user to scan the web application (for Scanner or Unit Manager).
- 6 Click Apply to save your changes to the user access list. (Note that if you do not click Apply, your changes to the user access list will not be saved, even if you click Save to save the web application.)

## Removing Web Applications

Users cannot remove web applications from their subscription. If you wish to remove one or more web applications, please contact your account administrator or Technical Support. After a web application is removed, users will no longer be able to launch new scans on the web application.

To contact support, go to Help—>Contact Support.

To submit an email, enter your request in the Email section.

For phone support, see the phone numbers provided in the Phone section.



# Web Application Scans

Launch web application scans to analyze the security of your web applications and view reports identifying the detected vulnerabilities, sensitive content, and information gathered.

External scanning at the network perimeter is available to all users (with scanning privileges) using the perimeter scanners provided by the service. Internal scanning of private use internal IPs is supported using scanner appliances installed inside the corporate network. We recommend placing scanner appliances in your network topology in a way that avoids scanning through a firewall from the inside out.

You can run web application scans in two modes: discovery and vulnerability.

**Discovery Scan.** A discovery scan provides information that can help you define your web application settings for black/white lists. Discovery scans do not perform vulnerability assessment. Use them to learn what will be scanned in a vulnerability scan, including URLs and domains (FQDNs).

**Vulnerability Scan.** The vulnerability checks (QIDs) performed by the scanning engine for a vulnerability scan allow you to examine web applications for common vulnerability types. WAS vulnerability checks are performed for web application vulnerability scans only. These include: cross-site vulnerability checks (persistent, reflected, header, browser-specific) and SQL injection vulnerabilities (regular and blind). Additional checks identify information gathered about the web application, such as the links crawled, external links discovered, external form actions discovered, information about the host, and scan diagnostics.

## About Web Application Scanning

### Scanning Process

There are several events that take place during the web application scanning process. The service requests links and forms, parses HTML for parameter analysis and form values, and interacts with the web application.

### Web Crawling and Link Discovery

The web crawler crawls a web application under a single host name or IP address. The web application can consist of a single physical host or multiple identical hosts behind a single load-balanced host. When multi-site support is defined for a web application, the web crawler follows links to the selected domains. The web crawler parses HTML and extracts static links. It also extracts some JavaScript based links and has the capability to find custom links.

The web crawler automatically balances the web site crawling to follow links down the web site branch (number of clicks) and across the branch (links at the same level), and tracks unique links that have already been crawled. This enables the crawler to obtain a high degree of site coverage while avoiding the re-scanning of redundant and recursive links. The list of links crawled is identified by QID 150009 Links Crawled.

The web crawler crawls up to 5,000 links per web application. The number of links include form submission, links requested as an anonymous user and links requested as an authenticated user. The user may configure this setting.

Any external links and external form actions that are found to be present are not crawled. In this case, the term “external” refers to links discovered on a host (FQDN or IP address) which is not the virtual host (starting host) or domain added for multi-site support. External links not crawled are identified as information gathered by QID 150010 External Links Discovered and QID 150014 External Form Actions Discovered.

**Important!** Automated web application vulnerability scanning has the potential of causing data loss. The black list feature allows you to prevent the web crawler from making certain requests for certain links in your web application.

## **Data Analysis**

The service performs static, off-line analysis of HTTP headers, HTML content and other responses from the web application. For a web application vulnerability scan, the service performs dynamic, on-line analysis of the web application. Vulnerability testing is not performed for discovery scans.

## **Automated Scan Performance Monitoring**

During a web application scan, the scanning engine monitors the target web application server's average response time. This occurs during the entire web application scan, including web crawling and link discovery, and vulnerability testing. If the scanning engine detects a trend showing the average response time from the target web application is becoming slower (scan time is increasing), then the scanning engine automatically inserts a delay until the trend is normal.

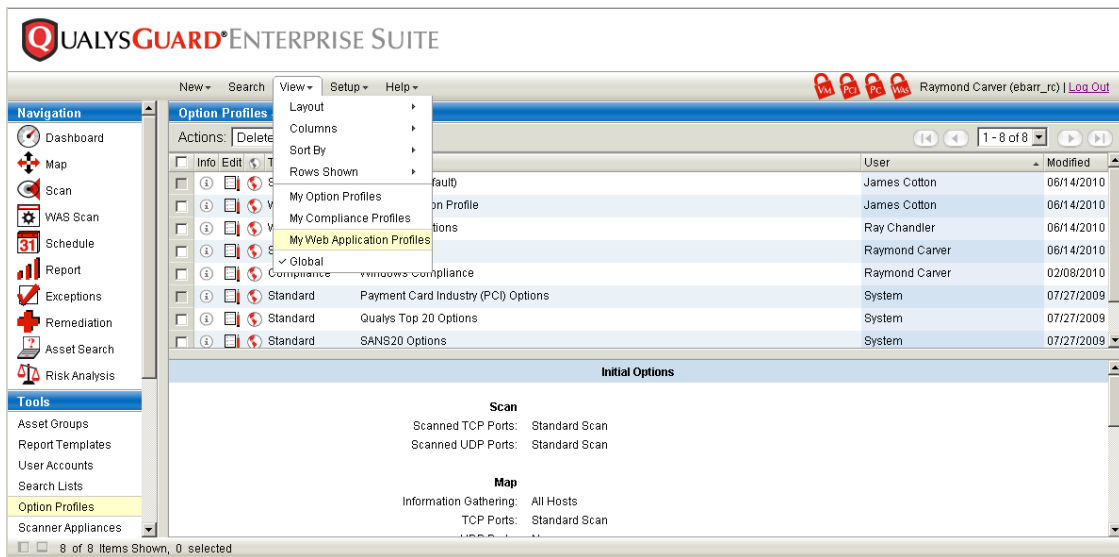
## **Web Application Profiles**

Before you can launch a web application scan, a web application profile, a profile with web application scan settings, must be available on the option profiles list in your account.

Permissions — The web application scanning (WAS) module must be enabled for the subscription. Users other than Managers must be granted permissions in order to create and edit web application profiles.

## **Viewing Web Application Profiles**


Web application profiles are listed with your option profiles. To view your option profiles, select Option Profiles from the left menu, under Tools. You may choose to filter the list to include only web application profiles. To do this, select “My Web Application Profiles” from the View menu.



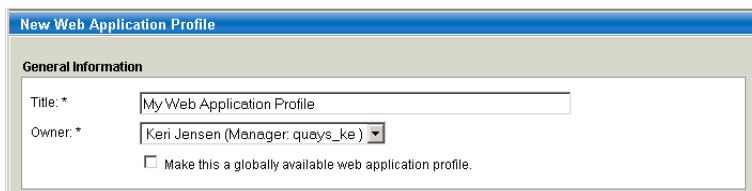
### Initial WAS Options

The profile “Initial WAS Options” is provided by the service to help you get started. You can edit this profile and save it with another name. Or you can define a new profile: select Option Profiles and then go to New—>Web Application Profile.

## Web Application Profile Settings

Web application profile settings are described in the sections below. To create a web application profile, go to New—>Web Application Profile on the top menu bar. To edit an existing profile, go to the Option Profiles list and click  next to the profile you’re interested in.

### General Information

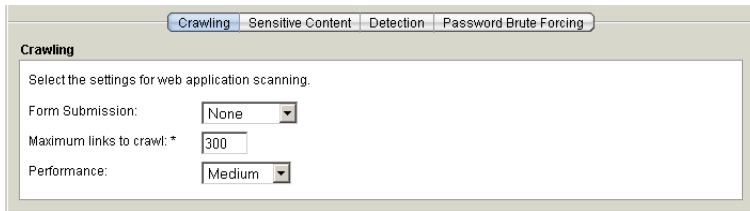


Title — Enter a title for the web application profile.

Owner — Initially, the user who creates the profile is the owner by default.

Make this a globally available profile — (Manager and Unit Manager only) Specify whether the profile should be globally available. When set by a Manager, the profile will be available to all subscription users. When set by a Unit Manager, the profile will be available to users in the Unit Manager's same business unit.

## Crawling



The screenshot shows a configuration window with four tabs: 'Crawling', 'Sensitive Content', 'Detection', and 'Password Brute Forcing'. The 'Crawling' tab is active. Below the tabs, the text reads 'Select the settings for web application scanning.' There are three settings: 'Form Submission' with a dropdown menu set to 'None', 'Maximum links to crawl.\*' with a text input field containing '300', and 'Performance' with a dropdown menu set to 'Medium'.

In the Crawling section select settings for crawling behavior and overall scan performance during the web application scan. The crawling options apply to both vulnerability scans and discovery scans.

### Form Submission

Select the method to be used by the web crawler to submit requests to forms. The web crawler follows links to form actions that it encounters when the form “method” attribute, as defined in each target form, matches the Form Submission setting you select.

This configuration does not apply to authentication. If an authentication record is selected for the scan, the scanning engine will attempt to authenticate no matter which Form Submission setting you select.

Your options are:

- None (Default) — No requests to forms will be submitted unless application authentication is requested, in which case only the login form will be tested.
- Post — Limits web crawling to POST forms.
- Get — Limits web crawling to GET forms.
- Post & Get — The web crawler submits requests to all forms. When authentication is desired, this option is recommended best practice to ensure maximum vulnerability analysis and the most comprehensive scan results.

### Maximum links to crawl

The maximum links to crawl during the scan. The default is 300 links. The maximum is 5,000 links.

### Performance

Select an overall performance level for the web application scan. It's recommended that you keep the default performance level of Medium to get started. Your options are: Maximum, High, Medium (default), Low, and Lowest. Each option represents several scan performance settings. Please see the online help for details on the various performance levels.

## Sensitive Content

The scanning engine has the ability to check for sensitive content in the web application pages it crawls based on known patterns (such as credit card numbers, social security numbers) or based on custom patterns you enter. Sensitive content checking will be performed only when you scan for QID 150016. Sensitive content checks apply to both vulnerability scans and discovery scans.

Please Note: The expression search mechanism is designed to search for credit card numbers and social security numbers (United States only) while reducing false positives. The service does not collect credit card information or social security information.

You options are:

- Credit Card Numbers — When selected, the scan checks for sensitive content based on credit card numbers.
- Social Security Card Numbers (United States Only) — When selected, the scan checks for sensitive content based on United States social security numbers.
- Custom — Select if you want the scan to check for sensitive content based on custom patterns you specify. Enter custom patterns as strings and regular expressions (up to 10) in the field provided. Each custom pattern entry must be entered on a separate line, and can have 5 to 100 characters.

Important: If you select Custom in the Vulnerability Detection section, you must add a search list which includes QID 150016.

## Detection

You may include any number of any of the web application vulnerabilities (QIDs) in the Knowledgebase. For discovery scans, the service will include information gathered QIDs only (any other QIDs included in the profile will be ignored).

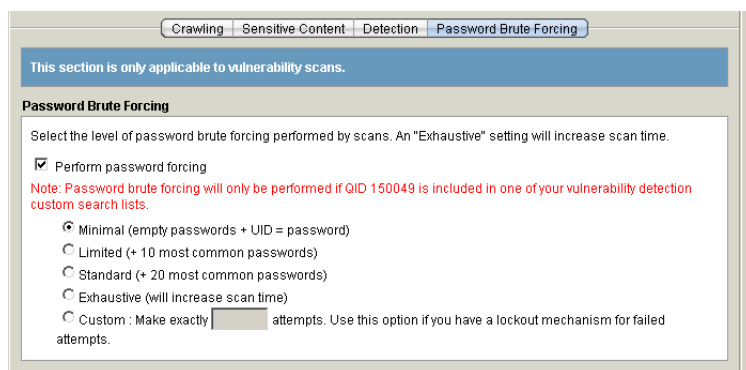
Your options are:

**Complete** — A scan of the complete list of web application vulnerabilities (QIDs) in the Vulnerability KnowledgeBase. When selected, the service will scan for all web application vulnerabilities.

**Custom** — A scan for custom list of web application vulnerabilities (QIDs) as defined in vulnerability search lists. First, create search lists containing some or all of the web application QIDs (go to Search Lists on the left menu). Then select Custom in the web application profile and click Add Lists to add search lists (up to 10). It's recommended you add search lists with all web application information gathered QIDs, since these QIDs return important scan information. When selected, only the QIDs defined in the search lists will be scanned for.

## Password Brute Forcing

The password brute forcing setting applies to vulnerability scans only.



The scanning engine has the ability to perform password brute forcing to test password security. Password brute forcing will be performed only when you scan for QID 150049. When performed, the scanning engine uses an internal list of common user names and an internal list of common passwords. The passwords list ranks passwords from most common to least common, and you have the option to select some number of the most common passwords to be tested. Email addresses are collected during the scan and tested as user names when you scan for QID 150054, where the part of the email address before the @ sign is tested as a user name.

**Warning!** The password brute forcing behavior may trigger lockouts depending on lockout policies you have in place. Please select a level of password brute forcing that is appropriate for your security policies.

To enable this feature, select Perform password brute forcing and a level of password brute forcing. Your options for the level are:

- **Minimal (empty passwords + UID = password)** — For each user name, test the empty password and the user name as a password. For example for the user name "jsmith" test the password "jsmith" and the empty password.

- Limited (+ 10 most common passwords) — For each user name, test these passwords: the user name, the empty password, plus the 10 most common passwords from the internal common passwords list defined by the WAS module.
- Standard (+ 20 most common passwords) — For each user name, test these passwords: the user name, the empty password, plus the 20 most common passwords from the internal common passwords list defined by the WAS module
- Exhaustive (will increase scan time) — For each user name, test these passwords: the user name, the empty password, plus all passwords in the internal common passwords list defined by the WAS module.
- Custom: [ ] attempts — Use this option if you have a lockout mechanism for a number of failed attempts.

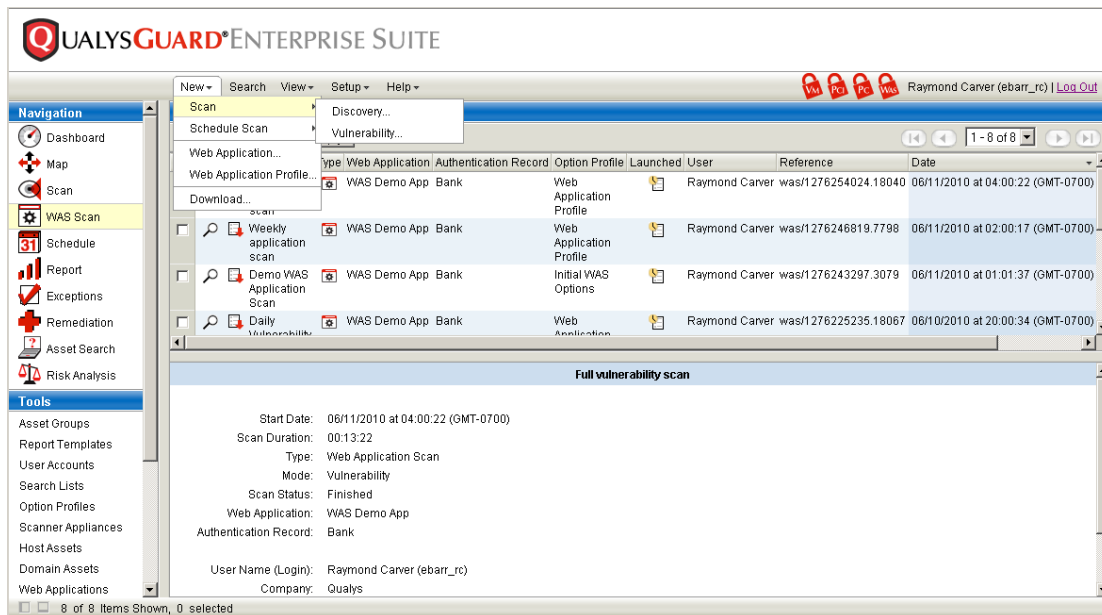
In the field provided, enter the exact number of attempts to be performed (a number greater than 0). If you have a lockout mechanism, enter the maximum number of guesses allowed.

The passwords tested will include the user name, the empty password, plus common passwords from the internal passwords list defined by the WAS module. For example if you enter 10, the following passwords will be tested: the empty password, the user name, plus the 8 most common passwords in the internal common passwords list defined by the WAS module. If you enter 1, this one password will be tested: the user name. If you enter 2, these two passwords will be tested: the user name and the empty password.

**Important:** If you select Custom in the Detection section, you must add a search list which includes QID 150049. Also if you want to use email addresses found in the web application HTML for password brute forcing you must add a search list which includes QID 150054.

## Launching Web Application Scans

Web Application scans can be launched on demand and scheduled to run at a future date and time. To launch an on-demand scan, select  WAS Scan from the left menu. The scan history list appears.

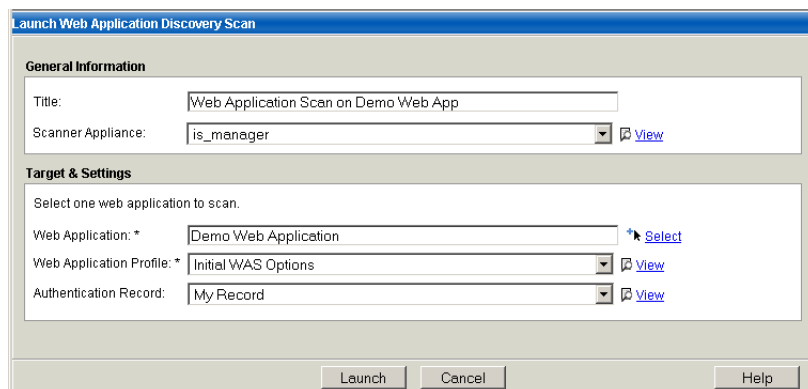


Go to New—>Scan and select Discovery or Vulnerability to display the launch page.

### Discovery Scan is Recommended

It's recommended that you run a discovery scan the first time you scan a particular web application.

The Launch Web Application (Discovery or Vulnerability) Scan page appears.



## Web Application Scan Settings

The settings for a web application scan are described below.

### General Information

**Title** — Enter a title to identify the scan. The title you enter appears in the scan summary email and the scan results report.

**Scanner Appliance** — When your account has scanner appliances, select a scanner option from the menu: “External” for the external scanners, or a scanner appliance name.

### Web Application

Select the web application that you want to scan from the menu provided. The web applications that you have access to are listed.

### Web Application Profile

Select a web application profile to apply to the task from the menu. The profile identifies scan settings. The profile “Initial WAS Options” is provided to get you started. You can use this profile as it is, edit it, or create a new one using the Save As function.

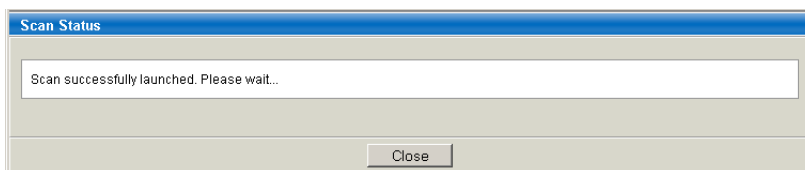
You have the option to select “Default” or a web application profile that is available in your account. If you leave this setting as “Default” then the service will use the default web application profile as it is defined for the web application.

### Authentication Record

Authentication to HTML forms is optional for a web application scan. Select an authentication record to apply to the scan if authentication is desired. The menu displays all authentication records defined for the selected web application. By default, no authentication record is selected.

### Scan Status

After you click the Launch button, the Scan Status page will appear with a message like this:



Click Close to close the window. Your scan will continue to run in the background.

## Viewing Web Application Scan History


The WAS scan history list shows all scan types by default. The Status column indicates whether the scan is Running or Finished. (Note it's not possible to pause and resume web application scans.)

The screenshot displays the QualysGuard Enterprise Suite interface. The main window shows a table of scan history with the following columns: View, Title, Type, Web Application, Authentication Record, Option Profile, Launched, User, Reference, Date, and Status. The table lists several scans, all of which are 'Finished'. Below the table, a detailed view of an 'Initial Discovery' scan is shown, including the following information:

- Start Date: 06/12/2010 at 11:00:28 (GMT-0700)
- Scan Duration: 00:11:38
- Type: Web Application Scan
- Mode: Discovery
- Scan Status: Finished
- Web Application: WAS Demo App
- Authentication Record: Bank

### Scan Status

The scan status is Running when the scan is in progress. The status is Finished when the scan has completed.

A warning indicator  may appear next to the status code to indicate that more information is available. Place your cursor over the icon to view the message. (When viewing the web application scan results, the message appears in parentheses after the status code.) If the status message is unexpected, you can look at your scan results to troubleshoot the issue. Please contact Support for help with troubleshooting your scan.


### For Running Scan

Cancel Scan — Click  to cancel a scan.

It's not possible to pause and resume web application scans.

### For Finished Scan

View — Click  to view web application scan results.

Download Scan Results — Click  to download web application scan results in one of these file formats: PDF, HTML, MHT, XML, or CSV.

## Scan Summary Notification

A scan email notification is sent at the completion of web application scans when the Scan Notification option is enabled in your account. This setting applies to both on-demand and scheduled scans. Any user can edit their own account to enable/disable this setting.

The image below shows the Notification Options section as it appears in a Manager account.

**Notification Options**

The following selections will configure when this user will receive notifications from QualysGuard and what they will receive them for.

Latest Vulnerabilities:	Scan Notification:	Map Notification:	Report Notification:	Exception Notification:	Other Notifications:
<input checked="" type="radio"/> Weekly <input type="radio"/> Daily <input type="radio"/> None	<input checked="" type="radio"/> All scans <input type="radio"/> No notification	<input checked="" type="radio"/> All maps <input type="radio"/> No notification	<input type="radio"/> All reports <input type="radio"/> My reports <input checked="" type="radio"/> No notification	<input type="radio"/> My exceptions <input checked="" type="radio"/> No notification	<input type="checkbox"/> Daily trouble tickets updates

A sample notification for a web application scan is below.

From: Qualys  
Sent: Friday, June 11, 2010 4:28 PM  
To: Keri Jensen  
Subject: QualysGuard: Web Application Scan Results

Email scan summary by QualysGuard

Scan Title : Web Application Scan  
Start Date : 06/11/2010 at 04:16:07 (GMT-0700)  
Duration : 00:11:33

Target : WAS Demo App: Bank  
Active Hosts : 1

Web Application Profile: Web Application Profi

Launched By : Raymond Carver (ebarr\_rc)  
Company : Qualys, Inc.  
Launch Type : On demand

Scan Status : Finished  
Next Action : None

---

Click here to view your web application scan results:

[https://qualysguard.qualys.com/fo/report/webapp/webapp\\_scan\\_result.php?authfirst=true&em=1&id=nnnnnnn](https://qualysguard.qualys.com/fo/report/webapp/webapp_scan_result.php?authfirst=true&em=1&id=nnnnnnn)

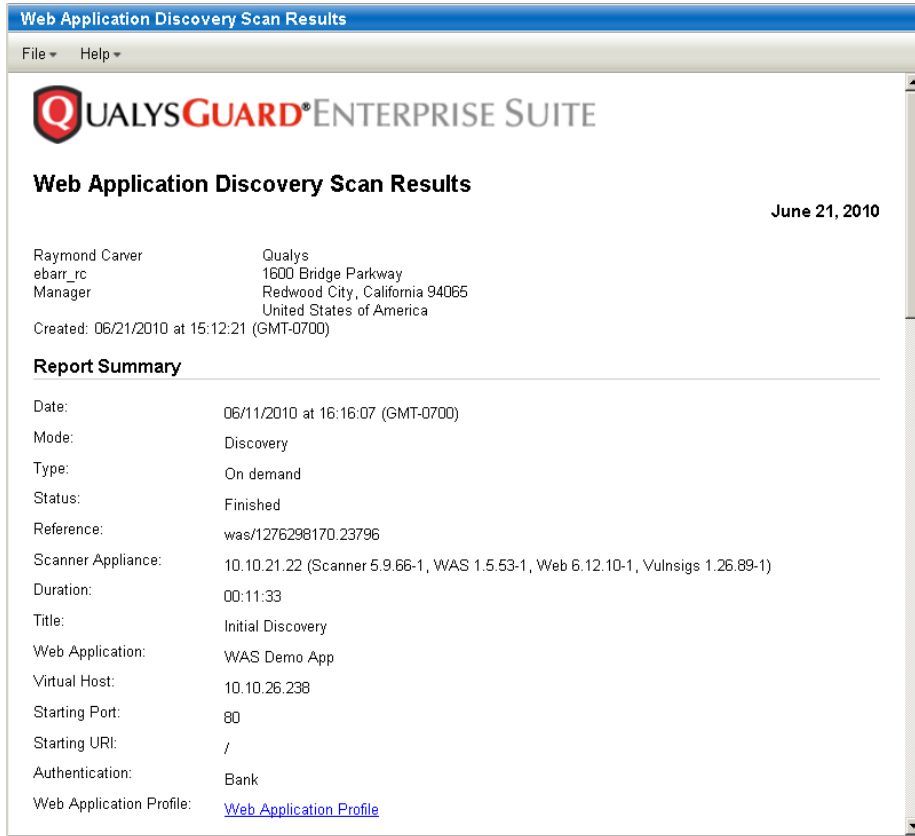
For more information, please email your primary contact:  
<mailto:manager@qualys.com>

---

(c) Copyright 1999-2010 Qualys, Inc. All rights reserved.

## Web Application Discovery Scan Results

Sample discovery scan results are below. The Report Summary provides information about the scan such as the date and time of the scan, mode (in this case Discovery), the web application name and the virtual host.



For discovery scans, results are organized by sensitive content and information gathered.

Sensitive content detections do not appear in scan results unless at least one sensitive content option is selected in the web application profile for the scan. See [Web Application Profile Settings](#) for more information.

## Sensitive Content

**Summary of Sensitive Content**

Group	Total
CC	1
CUSTOM	1
SSN-US	2
Total	4

▼ **Sensitive Content (4)** [grid] [list]

▼ **CC (1)** [grid] [list]

▼ **3 Credit Card Number Pattern Identified in HTML (1)**

**QID:** 150033  
**Category:** Web Application  
**CVE ID:** -  
**Vendor Reference:** -  
**Bugtraq ID:** -  
**Service Modified:** 06/29/2009  
**User Modified:** -  
**Edited:** No

**THREAT:**  
Sensitive content was discovered within the server's response. This content matches the pattern used by credit card numbers and the number has a correct checksum.

**IMPACT:**  
Disclosure of this content may affect confidentiality of information.

**SOLUTION:**  
The content should be reviewed to determine whether it could be masked or removed.

▼ **http://10.10.26.238/?ID=1&account=credit** 10.10.26.238: 80

Result: 6011-6011-6011-xxxx

The sensitive content detections are sorted by group: credit card number (CC), custom sensitive content (Custom) and social security number - US only (SSN-US).

For each custom detection, the payload appears next to the QID title. For other sensitive content detections, no payload is displayed. The scan results identify the URI where detected and the scan test result that confirms the presence of the QID.

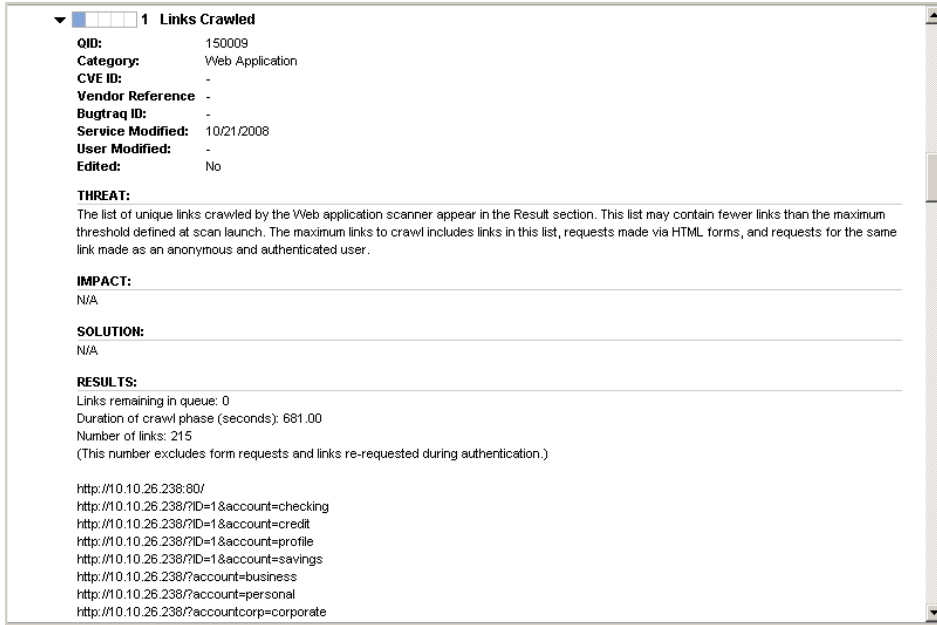
## Information Gathered

▼ **Information Gathered (18)** [grid] [list]

- ▶ **3 Session Cookie Does Not Contain the "secure" Attribute**
- ▶ **3 Server Returns HTTP 500 Message for Request**
- ▶ **3 Login Form Is Not Submitted Via HTTPS**
- ▶ **3 Session Cookie Does Not Contain the "HTTPOnly" Attribute**
- ▶ **2 Connection Error Occurred During Web Application Scan**
- ▶ **1 DNS Host Name**
- ▶ **1 Host Scan Time**
- ▶ **1 ICMP Replies Received**
- ▶ **1 Web Application Authentication Method**
- ▶ **1 Links Crawled**
- ▶ **1 External Links Discovered**
- ▶ **1 External Form Actions Discovered**
- ▶ **1 Links Rejected By Scan Permissions**
- ▶ **1 Scan Diagnostics**
- ▶ **1 Cookies Collected**

Information gathered for a web application scan are not associated with groups. The report displays information gathered QID details sorted by severity level and QID.

The QID details section provides a description as well as information detected by the scan. The details for QID 150009 Links Crawled is shown below. The Results section indicates the total number of links crawled and a list of those links.



▼ 1 Links Crawled

**QID:** 150009  
**Category:** Web Application  
**CVE ID:** -  
**Vendor Reference:** -  
**Bugtraq ID:** -  
**Service Modified:** 10/21/2008  
**User Modified:** -  
**Edited:** No

**THREAT:**  
The list of unique links crawled by the Web application scanner appear in the Result section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

**IMPACT:**  
N/A

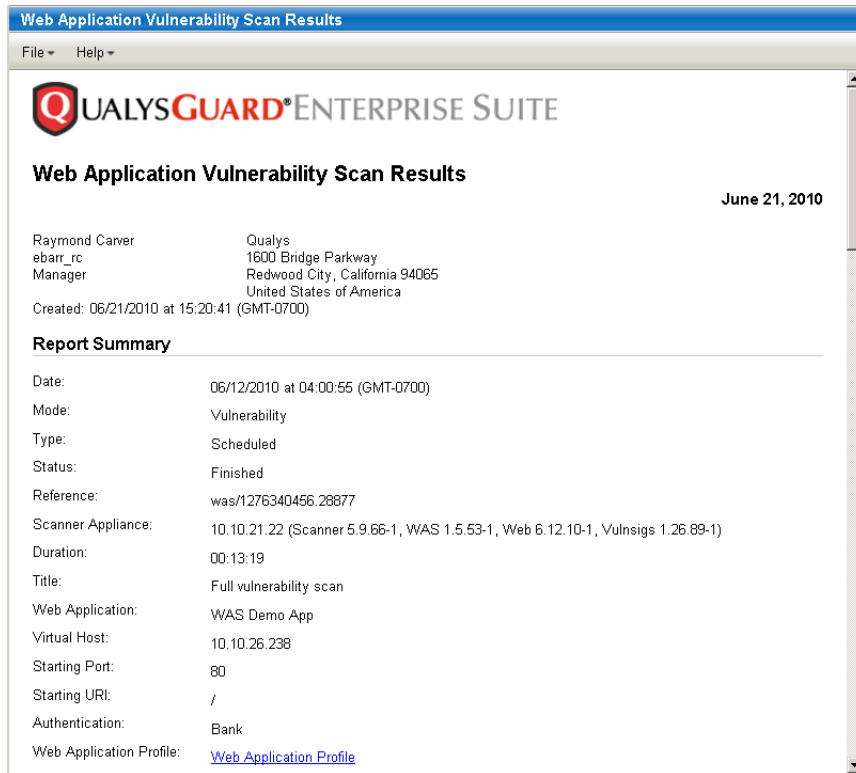
**SOLUTION:**  
N/A

**RESULTS:**  
Links remaining in queue: 0  
Duration of crawl phase (seconds): 681.00  
Number of links: 215  
(This number excludes form requests and links re-requested during authentication.)

http://10.10.26.238:80/  
http://10.10.26.238/?ID=1&account=checking  
http://10.10.26.238/?ID=1&account=credit  
http://10.10.26.238/?ID=1&account=profile  
http://10.10.26.238/?ID=1&account=savings  
http://10.10.26.238/?account=business  
http://10.10.26.238/?account=personal  
http://10.10.26.238/?accountcorp=corporate

## Web Application Vulnerability Scan Results

Sample vulnerability scan results are below. The Report Summary provides information about the scan such as the date and time of the scan, mode (in this case Vulnerability), the web application name and the virtual host.



For vulnerability scans, assessment results are organized by detection group for vulnerabilities, information gathered, and sensitive content.

## Vulnerabilities

Summary of Vulnerabilities							Summary of Sensitive Content	
Group	Severity						Group	Total
Name	5	4	3	2	1	Total		
XSS	2	0	0	0	0	2	CC	0
SQL	3	0	0	0	0	3	CUSTOM	0
PATH	0	0	0	13	0	13	SSN-US	0
INFO	0	1	4	0	0	5	Total	0
Total	5	1	4	13	0	23		

▼ **Vulnerabilities (23)** [ ] [ ]

▼ **XSS (2)** [ ] [ ]

- ▶ [ ] [ ] [ ] [ ] [ ] [ ] **5 Reflected Cross-Site Scripting (XSS) Vulnerabilities (2)**

▼ **SQL (3)** [ ] [ ] [ ]

- ▶ [ ] [ ] [ ] [ ] [ ] [ ] **5 SQL Injection (1)**
- ▶ [ ] [ ] [ ] [ ] [ ] [ ] **5 Blind SQL Injection (2)**

▼ **PATH (13)** [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

- ▶ [ ] [ ] [ ] [ ] [ ] [ ] **2 Path-based Vulnerability (1)**
- ▶ [ ] [ ] [ ] [ ] [ ] [ ] **2 Directory Listing (12)**

▼ **INFO (5)** [ ] [ ] [ ] [ ] [ ]

- ▶ [ ] [ ] [ ] [ ] [ ] [ ] **4 Login Brute Force Vulnerability (1)**

The vulnerabilities found are sorted by group: cross-site scripting (XSS), SQL injection (SQL), path-based vulnerability (PATH), and other vulnerability information (INFO).

For each vulnerability, scan results identify the URI where the vulnerability was detected, the payload, and scan test result that confirms the presence of the vulnerability.

▼ [ ] [ ] [ ] [ ] [ ] [ ] **5 Reflected Cross-Site Scripting (XSS) Vulnerabilities (2)**

QID: 150001  
Category: Web Application  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Modified: 05/26/2009  
Edited: No

**THREAT:**  
XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

**IMPACT:**  
XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used to as a part of a compromise.

**SOLUTION:**  
Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.  
Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

▼ **http://10.10.26.238:80/** **10.10.26.238:80**

Params: login

Payload: action=login&password=password&login=%22%3e%3cqqss%3e&submit>Login

Result: </div> <div id="content"> Unknown User. "><qqss> </div> </body> </html>

## Sensitive Content

The screenshot displays a section titled 'CUSTOM (2)' with a sub-section 'Sensitive Content in HTML:password (2)'. It lists two detections with the following details:

- QID:** 150016
- Category:** Web Application
- CVE ID:** -
- Vendor Reference:** -
- Bugtraq ID:** -
- Modified:** 01/22/2009
- Edited:** No

**THREAT:** Sensitive content was discovered within the server's response.

**IMPACT:** Disclosure of this content may affect confidentiality of information.

**SOLUTION:** The content should be reviewed to determine whether it could be masked or removed.

**COMPLIANCE:** Not Applicable

The first detection is for the URI `http://10.10.26.238:80/` with the result: `'text' name='user_login'><br> Password: <input type='password' name='password'><br>`. The second detection is for the URI `http://10.10.26.238:80/index.php` with the same result.

The sensitive content detections are sorted by group: credit card number (CC), custom sensitive content (Custom) and social security number - US only (SSN-US).

For each custom detection, the payload appears next to the QID title. For other sensitive content detections, no payload is displayed. The scan results identify the URI where detected and the scan test result that confirms the presence of the QID.

## Information Gathered

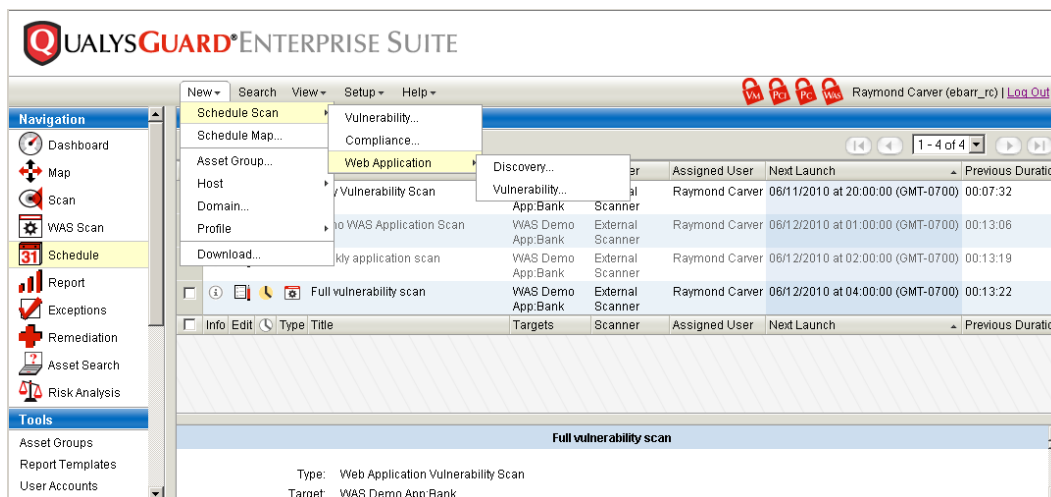
The screenshot displays a section titled 'Information Gathered (18)'. It lists 18 detections with the following details:

- 3 Session Cookie Does Not Contain the "secure" Attribute
- 3 Server Returns HTTP 500 Message for Request
- 3 Login Form Is Not Submitted Via HTTPS
- 3 Session Cookie Does Not Contain the "HTTPOnly" Attribute
- 2 Connection Error Occurred During Web Application Scan
- 1 DNS Host Name
- 1 Host Scan Time
- 1 ICMP Replies Received
- 1 Web Application Authentication Method
- 1 Links Crawled
- 1 External Links Discovered
- 1 External Form Actions Discovered
- 1 Links Rejected By Scan Permissions
- 1 Scan Diagnostics
- 1 Cookies Collected

Information gathered for a web application scan is not associated with groups. The report displays information gathered QID details sorted by severity level and QID.

## Scheduling Web Application Scans

You can schedule web application discovery and vulnerability scans to run at a later date or on a recurring schedule. To define a schedule, select **31** Schedule from the left menu. The Schedules section appears.

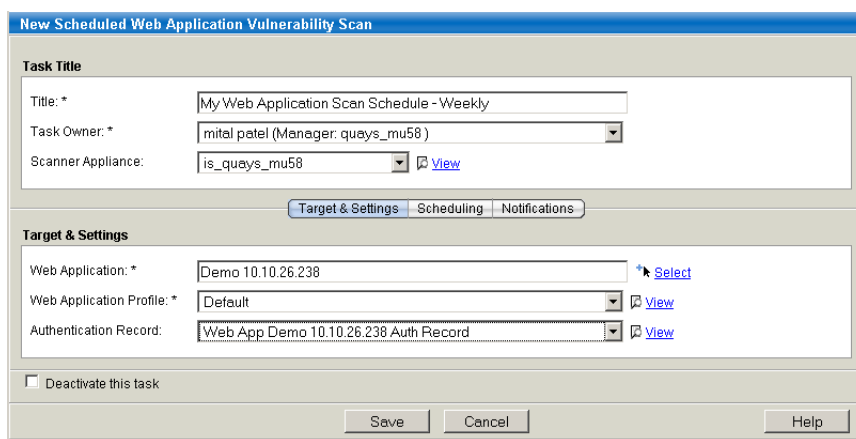


Go to New—>Schedule Scan—>Web Application on the top menu bar and select either Discovery or Vulnerability.

### Discovery Scan is Recommended

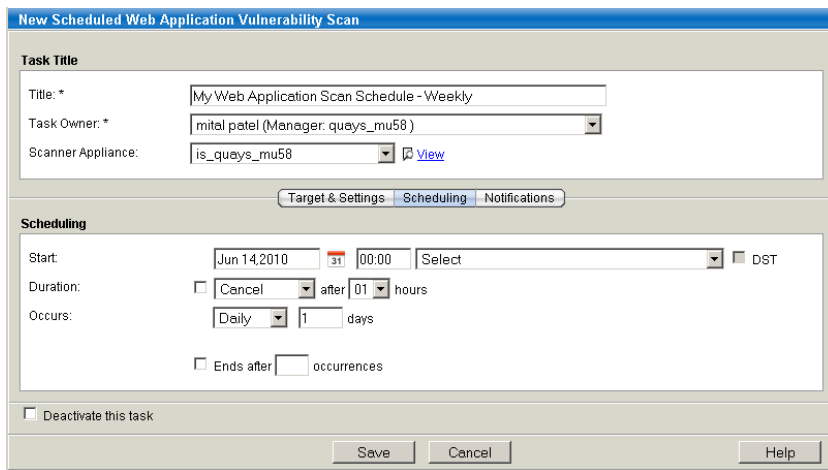
It's recommended that you run a discovery scan the first time you scan a particular web application.

The New Scheduled Web Application (Discovery or Vulnerability) Scan page appears.



Enter the title and target settings information as you would for an on demand scan, then click the Scheduling tab to define a schedule for the task. See [Web Application Scan Settings](#) for details.

You'll notice the scheduling settings for web application scans are similar to those for vulnerability management scans.



## Scan Troubleshooting

There are some common issues that users may encounter when getting started with web application scans. For your convenience, detailed assistance on these topics is provided in the online help. To access this information Go to Help—>Online Help on the top menu bar. The help window appears.

In the Contents section (on the left), go to Web Application Scanning—>WAS Troubleshooting.

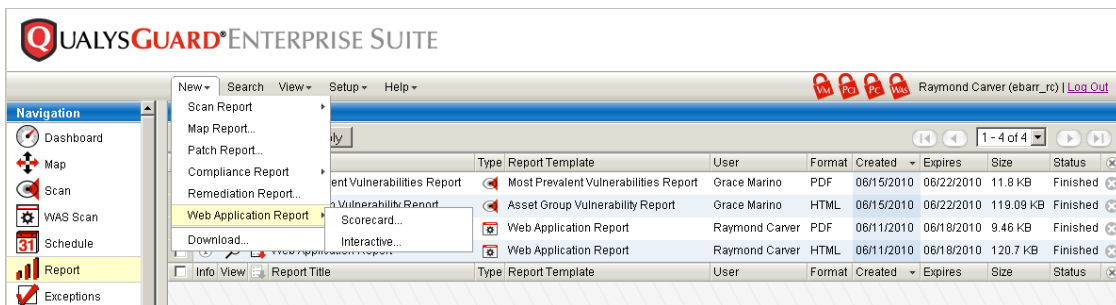




# Web Application Reports

Web application scan reports draw on data returned from the most recent complete vulnerability scan of each target web application, including vulnerability and sensitive content detection data. These types of scan reports are available: Scorecard and Interactive.

Note: The web application reports do not draw on any data from discovery scans.




Permissions — The web application scanning (WAS) module must be enabled for the subscription. Users other than Managers and web application owners must be granted permissions in order to run web application reports.

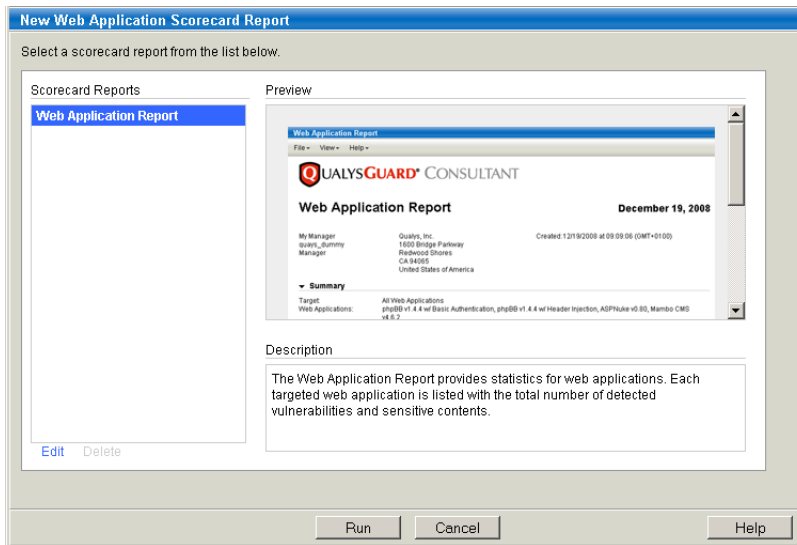
## Scorecard Report

The Web Application Scorecard Report is provided by the service for reporting on web application scan data for different business groups and functions. You may run this scorecard report with its predefined report settings and/or user-defined scorecard reports with customized settings.

A web application scorecard report identifies the vulnerabilities and sensitive contents detected for one or more target web applications in your account. The scorecard reports include the most recent scan data for the target web applications.

### Running the scorecard report

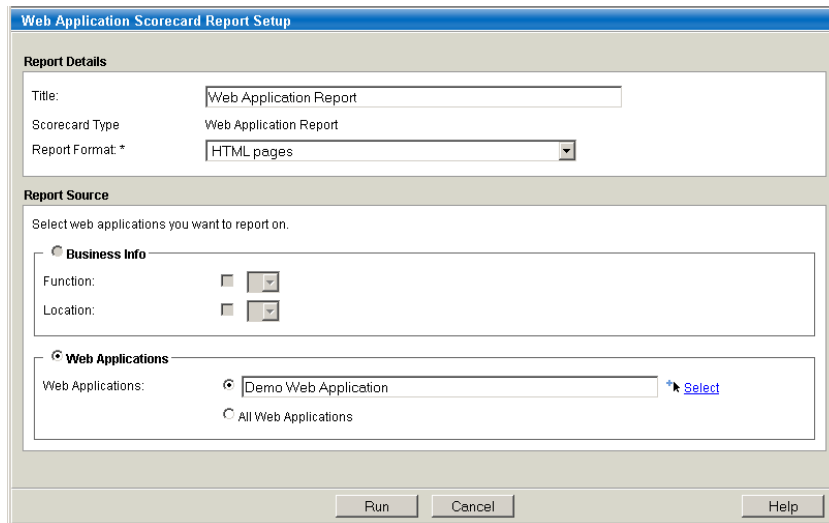
- 1 Select  Report from the left menu.
- 2 Go to New—>Web Application—>Scorecard.
- 3 Select the scorecard title in the left pane. You will notice the report preview and description on the right. (Click Edit if you wish to create another scorecard report with custom settings).



4 Click Run.

5 In the report setup window enter report settings:

- Report Details: Enter the report title, report format (PDF, HTML pages (ZIP), MHT, XML, or CSV) and add secure PDF distribution.
- Report Source: Select the report source. Select Business Info and enter business information tags in the fields provided (one tag per field), or select Web Applications and enter one or more target web applications.



6 Click Run.

When Report Share is enabled in your subscription, the report is saved to Report Share in the selected format, and it is published in the report history list for users to access.

## Scorecard Report sample

Web Application Report

File View Help

QUALYS GUARD ENTERPRISE SUITE

May 26, 2009

Web Application Report

Keri Jensen  
quays\_ke  
Manager

Qualys, Inc.  
1600 Bridge Parkway  
Redwood City, California 94065  
United States of America

Created: 05/26/2009 at 15:20:57 (GMT-0700)

▼ Summary

Target: Web Applications  
Web Applications: Demo Web Application

▼ Results

Web Application				Statistics		# Vulns				# Sensitive Content			
Title	Authentication	Port	Owner	# Links	Scan Time	XSS	SQL	INFO	PATH	CC	SSN	CUSTOM	Total
Demo Web Application	None	80	Keri Jensen	27	00:20:13	1	5	0	2	0	0	0	8
Demo Web Application	Bank	80	Keri Jensen	58	00:30:06	2	6	0	4	0	0	0	12
Title	Authentication	Port	Owner	# Links	Scan Time	XSS	SQL	INFO	PATH	CC	SSN	CUSTOM	Total
Web Application				Statistics		# Vulns				# Sensitive Content			

Each row in the report results section identifies one web application with scan statistics and results for a particular scan.

**Web Application** — Information about the target web application, including the web application title, the web authentication record applied to the scan, the web application port and owner.

**Statistics** — The number of links crawled and the overall scan time.

**# Vulns** — The number of vulnerabilities found for each of the various groups for a particular scan. The vulnerability groups are: cross-site scripting (XSS), SQL injection (SQL), path-based vulnerability (PATH), and other vulnerability information (INFO).


**# Sensitive Content** — The number of sensitive content detections for a particular scan. The scanning engine checks for sensitive content when sensitive content search options are selected in the web application profile that is applied to a scan. The sensitive content groups are: custom sensitive content (CUSTOM), credit card number (CC), and social security number - United States only (SSN-US).

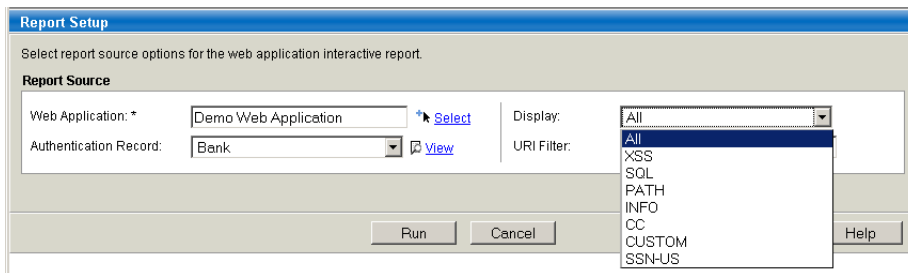
**Total** — The total number of vulnerabilities found and sensitive content detections for a particular scan.

## Interactive Report

The Web Application Interactive Report identifies vulnerabilities and sensitive content detected by the most recent scan of a selected web application. The interactive report allows you to keep changing the report settings to get different views of your web application scan data. Note that interactive report results are not saved to Report Share so you should download or print the report from the File menu if you wish to save it.

### Running an interactive report

- 1 Select  Report from the left menu.
- 2 Go to New—>Web Application Report—>Interactive. The Report Setup page appears.
- 3 Select report source options: a web application that has been scanned, the authentication record used for the scan, the detection groups to display and URI filter.



- 4 Click Run.

The report results appear in the same window in the interactive report pane.

### Interactive Report sample

Group	QID	Title	URI
PATH	150004	Path-based Vulnerability	http://10.10.26.238/authenticated/index.bak
PATH	150004	Path-based Vulnerability	http://10.10.26.238/backup/
PATH	150004	Path-based Vulnerability	http://10.10.26.238.80/backup/
PATH	150004	Path-based Vulnerability	http://10.10.26.238.80/index.bak
SQL	150003	SQL Injection	http://10.10.26.238/authenticated/index.php
SQL	150012	Blind SQL Injection	http://10.10.26.238/authenticated/index.php
SQL	150012	Blind SQL Injection	http://10.10.26.238/aux/ParseAction

**Path-based Vulnerability**

**QID:** 150004  
**Category:** Web Application  
**CVE ID:** -  
**Vendor Reference:** -

The report results includes these sections:

Unique URIs — The unique number of URIs detected.

Vulnerabilities Found — The vulnerabilities and sensitive content found are sorted by group. Some or all of the groups may appear in your report.

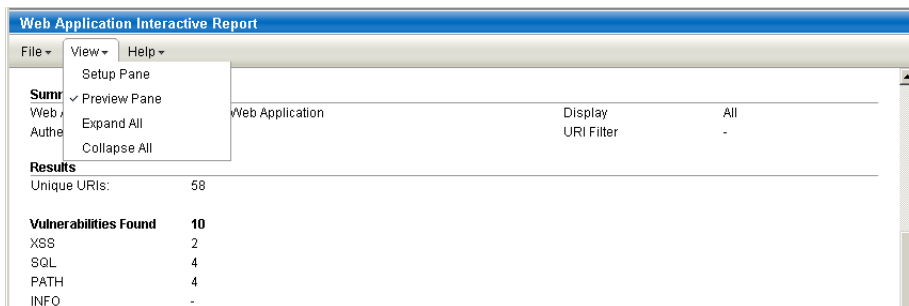
The vulnerability groups are: cross-site scripting (XSS), SQL injection (SQL), path-based vulnerability (PATH), and other vulnerability information (INFO).

The sensitive content groups are: custom sensitive content (CUSTOM), credit card number (CC), and social security number - United States only (SSN-US).

Details List — The results list identifies all detected vulnerabilities and sensitive content issues. For each item in the list, the report shows the group, the vulnerability ID (QID) and title associated with the vulnerability/sensitive content, and the URI on which the vulnerability/sensitive content was detected. Click on a result in the list to view its details in the preview pane (below the list area).

### Changing report source settings

You can easily make changes to your report source by returning to Report Setup. Go to the View menu and select the Setup Pane option to view the current report source settings.



The Report Setup will appear at the top of your report window in a separate pane, showing the current report source settings. Modify your report settings and click Run to update the report based on your new settings. In this way you can change the settings as often as you like.



# Web Application Vulnerabilities

The vulnerability checks (QIDs) performed by the scanning engine for a web application scan allow the user to examine web applications with an eye toward discovering common vulnerability types. Web application vulnerability checks are performed for web application scans only (not vulnerability scans or compliance scans). These include:

Cross-site Scripting Vulnerabilities: Persistent, Reflected, Header, Browser-specific

SQL Injection Vulnerabilities: Regular and Blind

Additional web application vulnerabilities identify information gathered about the web application during the scan process, such as links crawled, the external links discovered, external form actions discovered, host information, and scan diagnostics.

## Viewing Web Application Vulnerabilities

- 1 Select KnowledgeBase from the left menu, under Tools.
- 2 Click Search on the top menu bar. The Search pop-up window appears.
- 3 From the Category menu, select Web Application.

The image shows a 'Search' dialog box with the following fields and options:

- QID: [Text input]
- Vulnerability Title: [Text input]
- Discovery Method: [Dropdown menu: All (default)]
- Authentication Type:  Windows  Unix  Oracle  SNMP
- User Configuration:  Disabled  Edited
- Category: [Dropdown menu: Web Application] (highlighted with a red box)
- Patch Available:  Yes  No
- CVE ID: [Text input]
- Exploitability:  Core Security  Immunity  Immunity - Agora  Immunity - Dsquare






Buttons: Search, Close

- 4 Click Search.

## Severity Levels




### Vulnerabilities

Vulnerabilities are design flaws, programming errors, or mis-configurations that make your web application and web application platform susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information to a complete compromise of the web application and/or the web application platform. Even if the web application isn't fully compromised, an exploited vulnerability could still lead to the web application being used to launch attacks against users of the site.

Severity icon	Severity level	Description
	5 - Urgent	Intruders can exploit the vulnerability to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture.
	4 - Critical	Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the web application. Examples include certain types of cross-site scripting and SQL injection attacks.
	3 - Serious	Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non-encrypted channels.
	2 - Medium	Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.
	1 - Minimal	Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.

### Information Gathered

Information Gathered includes visible information about the web application's platform, code, or architecture. It may also include information about users of the web application.

Severity icon	Severity level	Description
	3 - Serious	Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the web application.
	2 - Medium	Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the web application.
	1 - Minimal	Intruders may be able to retrieve sensitive information related to the web application platform.



# User Permissions

Web application scanning features are available to users when the WAS module is enabled for the subscription, and users have WAS permissions as shown below. A filled circle (●) means permission is granted to the user automatically. “N/A” means the permission is not applicable.

Features	Manager	Web Application Owner	Other User (Reader, Scanner, Unit Manager)
<b>Web Application Reporting</b>			
Run web application reports	●	●	User must be granted: <b>Manage web applications</b> permission AND <b>Read</b> access for target web application(s)
View web application scorecard reports from Report Share	●	User Role Permissions	User must be granted: <b>Manage web applications</b> permission  User role permissions for Report Share access apply (see below). User access to individual reports may be granted by Manager or Unit Manager.
<b>Web Application Scanning</b>			
View web application scan results	●	●	User must be granted: <b>Manage web applications</b> permission AND <b>Read</b> access for target web application
Manage web application scans - Launch scan - Schedule scan - Cancel scan	●	●	User (Scanner or Unit Manager) must be granted: <b>Manage web applications</b> user permission, AND <b>Execute</b> access permission for the web application <b>Create option profiles</b> user permission is recommended  If not granted this permission, the user must launch scans using the service-provided option profile or a global option profile created by another user.  Reader does not have Execute permission and cannot be assigned Execute permission even if the Reader is the web application owner.

Features	Manager	Web Application Owner	Other User (Reader, Scanner, Unit Manager)
Manage web application profiles	●	User Role Permissions	User (Scanner or Unit Manager) must be granted: <b>Manage web applications</b> permission AND <b>Create option profiles</b> permission  User role permissions for option profiles apply (see below).
<b>Web Application Management</b>			
View web applications	●	●	User must be granted: <b>Manage web applications</b> permission AND <b>Read</b> access for web application
Edit web applications	●	●	User must be granted: <b>Manage web applications</b> permission AND <b>Write</b> access for web application
Create web applications	●	N/A	User must be granted: <b>Manage web applications</b> permission AND <b>Create web applications</b> permission

### User Role Permissions for Report Share Access

A Reader or Scanner automatically views reports launched by their own account. For a custom business unit, a Unit Manager automatically views all reports launched by users in the same business unit.

### User Role Permissions for Option Profiles

A Scanner or Unit Manager may create/edit their own option profiles, called web application profiles, for web application scans provided the option to do so is set in their user account. A Unit Manager may create/edit global profiles, which are available to users in the same business unit.

## Contact Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at [www.qualys.com/support/](http://www.qualys.com/support/).