

# **HP WebInspect**

Software Version: 10.30

**WebInspect**

Document Release Date: September 2014  
Software Release Date: September 2014



## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notice

© Copyright 2001 - 2014 Hewlett-Packard Development Company, L.P.

### Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

### Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: <http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

### Support

Visit the HP Software Support Online web site at: <http://www.hp.com/go/hpsoftwaresupport>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)

**HP Software Solutions Now** accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is  
<http://h20230.www2.hp.com/sc/solutions/index.jsp>

## About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

# Contents

Introduction .....	19
Using Help .....	19
WebInspect Overview .....	20
User Interface .....	20
Starting WebInspect .....	20
Main Features of WebInspect .....	20
About WebInspect Enterprise .....	22
Preparing Your System for Audit .....	24
Effects to Consider .....	24
Helpful Hints .....	24
Quick Start .....	25
Update SecureBase™ .....	25
Prepare Your System for Audit .....	26
Start a Scan .....	26
Scanning Web Services at zero.webappsecurity.com .....	27
Conducting a Web Service Scan .....	27
User Interface Overview .....	31
The Activity Panel .....	31
Closing the Activity Panel .....	32
The Button Bar .....	32
Panes Associated with a Scan .....	33
Start Page .....	35
Home .....	35
Manage Scans .....	35
Manage Schedule .....	36
Menu Bar .....	36
File Menu .....	36
Edit Menu .....	37
View Menu .....	38
Tools Menu .....	39
Scan Menu .....	39
Enterprise Server Menu .....	40

Reports Menu .....	41
Help Menu .....	41
Toolbars .....	42
Buttons Available on the Scan Toolbar .....	42
Buttons Available on the Standard Toolbar .....	43
Buttons Available on the "Manage Scans" Toolbar .....	44
Navigation Pane .....	45
Site View .....	46
Excluded Hosts .....	47
Allowed Hosts Criteria .....	48
Sequence View .....	49
Search View .....	49
Step Mode View .....	50
Navigation Pane Icons .....	51
Navigation Pane Shortcut Menu .....	52
Information Pane .....	54
Scan Info Panel Overview .....	55
Dashboard .....	55
Traffic Monitor .....	56
Attachments .....	57
False Positives .....	57
Dashboard .....	58
Progress Bars .....	59
Progress Bar Descriptions .....	59
Progress Bar Colors .....	60
Activity Meters .....	60
Activity Meter Descriptions .....	61
Vulnerabilities Graphics .....	61
Statistics Panel - Scan .....	61
Statistics Panel - Crawl .....	63
Statistics Panel - Audit .....	63
Statistics Panel - Network .....	63
Traffic Monitor .....	64
Button Functionality .....	64
Attachments - Scan Info .....	65
False Positives .....	66
Importing False Positives .....	66
Inactive / Active False Positives Lists .....	66
Loading False Positives .....	66

Working with False Positives .....	66
Session Info Panel Overview .....	67
Options Available .....	68
Vulnerability .....	70
Web Browser .....	70
HTTP Request .....	70
HTTP Response .....	70
Stack Traces .....	71
Details .....	71
Steps .....	71
Links .....	71
Comments: Session Info .....	72
Text .....	72
Hiddens: Session Info .....	72
Forms: Session Info .....	72
E-Mail .....	73
Scripts - Session Info .....	73
Attachments - Session Info .....	73
Viewing an Attachment .....	73
Adding a Session Attachment .....	74
Editing an Attachment .....	74
Attack Info .....	75
Web Service Request .....	75
Web Service Response .....	75
XML Request .....	75
XML Response .....	75
Host Info Panel Overview .....	75
Options Available .....	76
P3P Info .....	77
P3P User Agents .....	77
AJAX .....	77
How AJAX Works .....	78
Certificates .....	79
Comments - Host Info .....	79
Cookies .....	79
E-Mails - Host Info .....	80
Forms - Host Info .....	80
Hiddens - Host Info .....	81
Scripts - Host Info .....	81
Broken Links .....	82

Offsite Links .....	82
Parameters .....	83
Summary Pane .....	84
Vulnerabilities Tab .....	84
Not Found Tab .....	88
Information Tab .....	88
Best Practices Tab .....	88
Scan Log Tab .....	89
Server Information Tab .....	89
Fortify Monitor .....	90
Guided Scan Overview .....	91
Predefined Templates .....	91
Mobile Templates .....	91
Running a Guided Scan .....	92
Predefined Template (Standard, Quick, or Thorough) .....	92
Mobile Scan Template .....	93
Native Scan Template .....	93
Using the Predefined Template .....	93
Launching a Guided Scan .....	93
About the Site Stage .....	94
Verifying Your Web Site .....	94
Choosing a Scan Type .....	96
About the Login Stage .....	97
Network Authentication Step .....	97
Configuring Network Authentication .....	97
Application Authentication Step .....	99
Selecting a Login Macro .....	99
About the Workflows Stage .....	99
To Add Burp Proxy results .....	100
About the Active Learning Stage .....	100
Using the Profiler .....	101
About the Settings Stage .....	103
Importing HP Unified Functional Testing (UFT) Files in a Guided Scan .....	104
Using the Mobile Scan Template .....	105
Launching a Mobile Scan .....	106
Creating a Custom User Agent Header .....	106
About the Site Stage .....	107
Verifying Your Web Site .....	107

Choosing a Scan Type .....	109
About the Login Stage .....	110
Network Authentication Step .....	110
Configuring Network Authentication .....	110
Application Authentication Step .....	112
Selecting a Login Macro .....	112
About the Workflows Stage .....	112
Adding Burp Proxy Results .....	113
Adding Burp Proxy Results .....	113
About the Active Learning Stage .....	114
Using the Profiler .....	114
About the Settings Stage .....	116
Importing HP Unified Functional Testing (UFT) Files in a Guided Scan .....	117
Using the Native Scan Template .....	119
Setting Up Your Mobile Device .....	119
Guided Scan Stages .....	119
Supported Devices .....	119
Supported Development Emulators .....	120
Launching a Native Scan .....	120
About the Native Mobile Stage .....	120
Choose Device/Emulator Type Step .....	121
Selecting a Profile .....	121
Setting the Mobile Device Proxy Address .....	121
Adding a Trusted Certificate .....	122
Choose Scan Type Step .....	123
About the Login Stage .....	124
Network Authentication Step .....	124
Configuring Network Authentication .....	124
Configuring a Client Certificate .....	126
Application Authentication Step .....	126
Selecting a Login Macro .....	126
Creating a Login Macro .....	127
Recording a Login Macro .....	127
Specifying a Logout Condition .....	127
About the Application Stage .....	127
Run Application Step .....	127
Finalizing Allowed Hosts and RESTful Endpoints .....	128
About the Settings Stage .....	128
Final Review Step .....	129

Validate Settings and Start Scan .....	129
Post Scan Steps .....	129
Running a Web Service Scan .....	130
Authentication and Connectivity .....	131
Detailed Scan Configuration .....	133
Congratulations .....	133
Running a Basic Scan .....	133
Basic Scan Options .....	134
Authentication and Connectivity .....	136
Coverage and Thoroughness .....	138
Detailed Scan Configuration .....	140
Profiler .....	140
Settings .....	141
Auto Fill Web Forms .....	141
Add Allowed Hosts .....	141
Reuse Identified False Positives .....	142
Sample Macro .....	142
Traffic Analysis .....	142
Message .....	142
Congratulations .....	143
Upload to WebInspect Enterprise Scan Template .....	143
Save Settings .....	143
Generate Reports .....	143
Running an Enterprise Scan .....	144
Edit the 'Hosts to Scan' List .....	147
Export a List .....	147
Start the Scan .....	147
Running a Manual Scan .....	148
Scan Status .....	150
Updates to Information in the Scan Manager .....	150
Opening a Saved Scan .....	151
Comparing Scans .....	151
Selecting Scans to Compare Scans .....	152
Reviewing the Scan Dashboard .....	153
Scan Descriptions .....	153
The Venn Diagram .....	154
Vulnerabilities Bar Chart .....	154

Effect of Scheme, Host, and Port Differences on Scan Comparison .....	154
Compare Modes .....	155
Session Filtering .....	155
Using the Session Info Panel .....	156
Using the Summary Pane to Review Vulnerability Details .....	156
Grouping and Sorting Vulnerabilities .....	157
Filtering Vulnerabilities .....	157
Working with Vulnerabilities .....	157
Manage Scans .....	158
Schedule a Scan .....	159
Configuring Time Interval for Scheduled Scan .....	160
Managing Scheduled Scans .....	161
Selecting a Report .....	163
Configuring Report Settings .....	164
Stopping a Scheduled Scan .....	165
Scheduled Scan Status .....	165
Exporting a Scan .....	166
Exporting Scan Details .....	168
Export Scan to Software Security Center .....	171
Exporting Protection Rules to HP TippingPoint .....	172
Exporting Protection Rules to Web Application Firewall .....	173
Importing a Scan .....	173
Importing False Positives .....	174
Importing Legacy Web Service Scans .....	174
Changing Import/Export Settings .....	175
Downloading a Scan from Enterprise Server .....	176
Uploading a Scan to Enterprise Server .....	176
Running a Scan in Enterprise Server .....	177
Transferring Settings to/from Enterprise Server .....	177
To Create a WebInspect Enterprise Scan Template .....	178
To Create a WebInspect Settings File .....	179
Publishing a Scan (WebInspect Enterprise Connected) .....	179
Integrating with WebInspect Enterprise .....	181
First scan .....	182
Second scan .....	182

Third scan .....	182
Fourth Scan .....	183
Using Macros .....	184
Recommendation .....	184
Unified Web Macro Recorder Overview .....	185
Traffic-Mode Web Macro Recorder of Previous WebInspect Versions (Obsolete) .....	185
Event-Based IE Compatible Web Macro Recorder of Previous WebInspect Versions (Hidden in user interface) .....	186
Using the Unified Web Macro Recorder .....	186
Upgrade Impacts .....	187
Traffic-Mode Web Macro Recorder of Previous WebInspect Versions (Obsolete) .....	187
Event-Based IE Compatible Web Macro Recorder of Previous WebInspect Versions (Hidden in user interface) .....	188
Server Profiler .....	188
Using the Server Profiler .....	188
Inspecting the Results .....	189
Basic Scan .....	190
Working with a Vulnerability .....	190
Working with a Group .....	191
Understanding the Severity .....	192
Working in the Navigation Pane .....	192
Web Services Scan .....	192
Search View .....	193
Using Filters and Groups in the Summary Pane .....	196
Using Filters .....	196
No Filters .....	196
Filtered by Method:Get .....	196
Specifying Multiple Filters .....	197
Filter Criteria .....	197
Using Groups .....	198
Auditing Web Services .....	199
Options Available from the Session Info Panel .....	200
Reviewing a Vulnerability .....	201
Adding/Viewing Vulnerability Screenshot .....	203
Viewing Screenshots for a Selected Session .....	204
Viewing Screenshots for All Sessions .....	204
Editing Vulnerabilities .....	204

Mark As False Positive .....	207
Mark As Vulnerability .....	207
Flag Session for Follow-Up .....	208
Viewing Flags for a Selected Session .....	208
Viewing Flags for All Sessions .....	208
Scan Note .....	208
Session Note .....	209
Viewing Notes for a Selected Session .....	209
Viewing Notes for All Sessions .....	210
Vulnerability Note .....	210
Viewing Notes for a Selected Session .....	210
Viewing Notes for All Sessions .....	210
Reviewing and Retesting .....	211
Review Individual Vulnerability .....	211
Retest Vulnerabilities .....	211
Rescan the Site .....	212
Compare Scans .....	213
Recovering Deleted Items .....	214
Sending Vulnerabilities to a Defect Tracking System .....	215
Additional Information Sent .....	215
Disabling Data Execution Prevention .....	216
For Microsoft Windows XP Service Pack 2 (or later) .....	216
For Windows Vista (32-bit) .....	216
Generating a Report .....	217
Saving a Report .....	218
Advanced Report Options .....	219
Standard Reports .....	219
Compliance Templates .....	221
Managing Settings .....	227
Creating a Settings File .....	227
Editing a Settings File .....	228
Deleting a Settings File .....	228
Importing a Settings File .....	228
Exporting a Settings File .....	228
Scanning with a Saved Settings File .....	229
SmartUpdate .....	229

Performing a SmartUpdate .....	230
Downloading Checks without Updating WebInspect .....	230
WebSphere Portal FAQ .....	230
Command Line Execution .....	232
Options .....	232
Examples .....	236
Hyphens in Command Line Arguments .....	237
WebInspect Policies .....	237
Best Practices .....	237
By Type .....	238
Custom .....	240
Hazardous .....	240
Regular Expressions .....	241
Regex Extensions .....	242
Regular Expression Tags .....	243
Regular Expression Operators .....	243
Examples .....	244
WebInspect API .....	244
About the WebInspect API .....	245
Configuring the WebInspect API .....	245
About Automating WebInspect .....	246
About the WebInspect API Service Providers .....	246
Proxy .....	246
Scanner .....	249
Example Proxy Automation Script Using cURL .....	258
Example Scanner Automation Script Using cURL .....	259
WebInspect API Server Logs .....	260
About the Burp API Extension .....	261
Benefits of Using the Burp API Extension .....	261
Supported Versions .....	261
Using the Burp API Extension .....	262
Loading the Burp Extension .....	262
Connecting to WebInspect .....	263
Refreshing the List of Scans .....	265
Working with a Scan in Burp .....	265
Sending Items from Burp to WebInspect .....	268
Add Page or Directory .....	270

Add Variation .....	271
Fortify Monitor: Configure Enterprise Server Sensor .....	272
After Configuring as a Sensor .....	272
Blackout Period .....	273
Create Exclusion .....	273
Example 1 .....	274
Example 2 .....	274
Example 3 .....	274
Example 4 .....	275
FilesToURLs Utility .....	275
Usage for FilesToURLs.exe .....	276
Usage for FilesToURLs.py .....	276
List-Driven Scan .....	277
Default Scan Settings .....	278
Scan Settings: Method .....	278
Scan Mode .....	278
Crawl and Audit Mode .....	279
Crawl and Audit Details .....	279
Navigation .....	280
SSL/TLS Protocols .....	281
Scan Settings: General .....	282
Scan Details .....	282
Crawl Details .....	283
Audit Details .....	286
Scan Settings: Content Analyzers .....	287
Flash .....	287
JavaScript/VBScript .....	287
Silverlight .....	289
Scan Settings: Requestor .....	289
Requestor Performance .....	289
Requestor Settings .....	290
Stop Scan if Loss of Connectivity Detected .....	291
Scan Settings: Session Storage .....	292
Log Rejected Session to Database .....	292
Session Storage .....	294
Scan Settings: Session Exclusions .....	294
Excluded or Rejected File Extensions .....	295

Excluded MIME Types .....	295
Other Exclusion/Rejection Criteria .....	295
Editing Criteria .....	296
Adding Criteria .....	296
Scan Settings: Allowed Hosts .....	298
Using the Allowed Host Setting .....	298
Adding Allowed Domains .....	299
Editing or Removing Domains .....	299
Scan Settings: HTTP Parsing .....	300
Options .....	300
CSRF .....	304
About CSRF .....	304
Using CSRF Tokens .....	304
Enabling CSRF Awareness in WebInspect .....	304
Scan Settings: Custom Parameters .....	305
URL Rewriting .....	305
Examples: .....	305
RESTful Services .....	306
Enable automatic seeding of rules that were not used during scan .....	307
Double Encode URL Parameters .....	307
Scan Settings: Filters .....	308
Options .....	308
Adding Rules for Finding and Replacing Keywords .....	309
Scan Settings: Cookies/Headers .....	310
Standard Header Parameters .....	310
Append Custom Headers .....	310
Adding a Custom Header .....	310
Append Custom Cookies .....	311
Adding a Custom Cookie .....	311
Scan Settings: Proxy .....	312
Options .....	312
Scan Settings: Authentication .....	315
Scan Requires Network Authentication .....	316
Authentication Method .....	316
Authentication Credentials .....	317
Client Certificates .....	317
Task 1: Find your certificate's serial number .....	318
Task 2: Create an entry in the SPI.Net.Proxy.Config file .....	318

Use a login macro for forms authentication .....	319
Login Macro Parameters .....	319
Use a startup macro .....	319
Scan Settings: File Not Found .....	320
Options .....	320
Scan Settings: Policy .....	322
Creating a Policy .....	322
Editing a Policy .....	322
Importing a Policy .....	322
Deleting a Policy .....	323
Crawl Settings .....	325
Crawl Settings: Link Parsing .....	325
Adding a Specialized Link Identifier .....	325
Crawl Settings: Session Exclusions .....	326
Excluded or Rejected File Extensions .....	326
Adding a File Extension to Exclude/Reject .....	326
Excluded MIME Types .....	326
Adding a MIME Type to Exclude .....	326
Other Exclusion/Rejection Criteria .....	327
Editing the Default Criteria .....	327
Adding Exclusion/Rejection Criteria .....	327
Audit Settings .....	330
Audit Settings: Session Exclusions .....	330
Excluded or Rejected File Extensions .....	330
Adding a File Extension to Exclude/Reject .....	330
Excluded MIME Types .....	331
Adding a MIME Type to Exclude .....	331
Other Exclusion/Rejection Criteria .....	331
Editing the Default Criteria .....	331
Adding Exclusion/Rejection Criteria .....	332
Audit Settings: Attack Exclusions .....	334
Excluded Parameters .....	334
Adding Parameters to Exclude .....	334
Excluded Cookies .....	334
Excluding Certain Cookies .....	334
Excluded Headers .....	335
Excluding Certain Headers .....	335
Audit Inputs Editor .....	336

Audit Settings: Attack Expressions .....	337
Additional Regular Expression Languages .....	337
Audit Settings: Vulnerability Filtering .....	337
Adding a Vulnerability Filter .....	338
Audit Settings: Smart Scan .....	339
Enable Smart Scan .....	339
Use regular expressions on HTTP responses .....	339
Use server analyzer fingerprinting and request sampling .....	339
Custom server/application type definitions .....	339
Application Settings: General .....	341
General .....	341
WebInspect Agent .....	343
Application Settings: Database .....	344
Connection Settings for Scan/Report Storage .....	345
Configuring SQL Server Standard Edition .....	345
Connection Settings for Scan Viewing .....	345
Application Settings: Directories .....	346
Changing Where WebInspect Files Are Saved .....	346
Application Settings: License .....	347
License Details .....	347
Direct Connection to HP .....	347
Connection to LIM .....	348
Application Settings: Server Profiler .....	349
Modules .....	349
Application Settings: Step Mode .....	351
Application Settings: Logging .....	352
Application Settings: Proxy .....	353
Not Using a Proxy Server .....	354
Using a Proxy Server .....	354
Configuring a Proxy .....	354
Application Settings: Reports .....	357
Options .....	357
Headers and Footers .....	358
Application Settings: Run as a Sensor .....	359
Sensor .....	359
Application Settings: Override SQL Database Settings .....	361
Override Database Settings .....	361

Configure SQL Database .....	361
Application Settings: Smart Update .....	362
Options .....	362
Application Settings: Support Channel .....	363
Opening the Support Channel .....	363
Application Settings: HP Quality Center .....	364
Running HP Quality Center and WebInspect on the Same Machine .....	365
Quality Center License Usage .....	365
Before You Begin .....	365
Creating a Profile .....	365
Application Settings: IBM Rational ClearQuest .....	366
Creating a Profile .....	367
Scan Log Messages .....	369
Contact Technical Support .....	390
E-Mail (Preferred Method) .....	390
Telephone .....	390
Online .....	391
Suggest Enhancement .....	391
Purchases and Renewals .....	391
New Purchases .....	391
Renew Your Product License .....	392
HTTP Status Codes .....	392
Uninstalling WebInspect .....	394
Options for Removing .....	395
About WebInspect .....	395
Send Documentation Feedback .....	396

# Introduction

Hewlett-Packard, the world's leading Internet application security provider, proudly introduces WebInspect™ 10.30.

WebInspect is the most accurate and comprehensive automated Web application and Web services vulnerability scan solution available today. With WebInspect, security professionals and compliance auditors can analyze the numerous Web applications and Web services in their environment quickly and easily.

WebInspect is the only product that is maintained and updated daily by the world's leading Web security experts. These solutions are specifically designed to assess potential security flaws and to provide all the information you need to fix them.

WebInspect delivers the latest evolution in scan technology, a Web application security product that adapts to any enterprise environment. As you initiate a scan, WebInspect assigns agents that dynamically catalog all areas of a Web application. These agents report their findings to a main security engine that analyzes the results. WebInspect then launches "Threat Agents" to evaluate the gathered information and apply attack algorithms to determine the existence and relative severity of vulnerabilities. With this smart approach, WebInspect continuously applies appropriate scan resources that adapt to your specific application environment.

## See Also

["Using Help" below](#)

["WebInspect Overview" on the next page](#)

# Using Help

This on-line Help file is context-sensitive.

When using WebInspect, press F1 to open a topic related to the area of the WebInspect user interface that currently has focus.

The left pane of the Help window contains the following tabs:

- **Contents:** The expandable table of contents presents a structured view of the available topics. Click a node to expand it. Click a topic to display it.
- **Search:** Use this tab to locate topics containing the word or phrase you specify. To locate a phrase, type quotation marks at the beginning and end of the phrase.
- **Favorites:** You can create a list of frequently accessed topics. To do so, navigate to a topic, click the **Favorites** tab, and then click **Add** (at the bottom of the left pane).

## See Also

["WebInspect Overview" on the next page](#)

## WebInspect Overview

Testing the security of your site can be an arduous, daunting, mind-numbing task. Who can inspect every aspect of a Web application, looking for vulnerabilities and security holes in your application and every other program you've installed on that server?

You can't. WebInspect can.

Using advanced artificial hacking intelligence, WebInspect probes your site's defenses to find the areas that require further attention. WebInspect lets you see what a hacker would see if he were attacking your site. Knowledge is the best defense.

## User Interface

For a description of the WebInspect user interface, see [Using WebInspect](#).

## Starting WebInspect

On the WebInspect **Start Page**, click one of the following selections:

- Start a [Guided Scan](#)
- Start a [Basic Scan](#)
- Start a [Web Service Scan](#)
- Start an [Enterprise Scan](#)
- Generate a [Report](#)
- Start [SmartUpdate](#)

## Main Features of WebInspect

The following is a brief overview of what you can do with WebInspect, and how it can benefit your organization.

**Crawling and Auditing** - WebInspect uses two basic modes for determining your security weaknesses.

- A crawl is the process by which WebInspect identifies the structure of the target Web site. In essence, a crawl runs until no more links on the URL can be followed.

- An audit is the actual vulnerability scan. A crawl and an audit, when combined into one function, is termed a scan.

**Reporting** - Use WebInspect reports to gain valuable, organized application information. You can customize report details, deciding what level of information to contain in each report, and gear the report for a specific audience. You can also save any customized report as a template, which you can then use to generate a report using the same reporting criteria, but with updated information. You can save reports in either PDF, HTML, Excel, Raw, RTF, or Text format, and you can also include graphic summaries of vulnerability data.

**Manual Hacking Control** - With WebInspect, you can see what's really happening on your site, and simulate a true attack environment. WebInspect functionality gives you the ability to view the code for any page that contains vulnerabilities, and make changes to server requests and resubmit them instantly.

**Summary and Fixes** - The information pane displays all summary and fix information for the vulnerability selected in either the [navigation pane](#) or the [summary pane](#). It also cites reference material and contains links to patches, instructions for prevention of future problems, and vulnerability solutions. As new attacks and exploits are formulated daily, we frequently update our summary and fix information database. Use [Smart Update](#) on the WebInspect toolbar to update your database with the latest vulnerability solution information, or check for updates automatically on startup (see [Application Settings: Smart Update](#)).

**Scanning Policies** - You can edit and customize scanning policies to suit the needs of your organization, reducing the amount of time it takes for WebInspect to complete a scan. For more information on configuring WebInspect policies, see [Policy Manager](#).

**Sortable and Customizable Views** - When conducting or viewing a scan, the navigation pane on the left side of the WebInspect window includes the Site, Sequence, Search, and Step Mode buttons, which determine the contents (or "view") presented in the navigation pane.

- Site view presents the hierarchical file structure of the scanned site, as determined by WebInspect. It also displays, for each resource, the HTTP status code returned by the server and the number of vulnerabilities detected.
- Sequence view displays server resources in the order they were encountered by WebInspect during an automated scan or a manual crawl (Step Mode).
- [Search view](#) allows you to locate sessions that fulfill the criteria you specify.
- [Step Mode](#) is used to navigate manually through the site, beginning with a session you select from either the site view or the sequence view.

**Enterprise-Wide Usage Capabilities** - Integrated scan provides a comprehensive overview of your Web presence from an overall enterprise perspective, enabling you to conduct application scans of all Web-enabled applications on the network.

**Web Services Scan Capabilities** - Provides a comprehensive scan of your Web services vulnerabilities. Enables you to assess applications containing Web services/SOAP objects.

**Export Wizard** - WebInspect's robust and configurable XML export tool enables users to export (in a standardized XML format) any and all information found during the scan. This includes comments,

hidden fields, JavaScript, cookies, Web forms, URLs, requests, and sessions. Users can specify the type of information to be exported.

**Web Service Test Designer** - Allows you to create a Web Service Test Design file (filename.wsd) containing the values that WebInspect should submit when conducting a Web service scan.

**Enhanced Third-Party Commercial Application Threat Agents** - WebInspect enables users to perform security scans for any Web application, including the industry-leading application platforms. Some standard commercial application threat agents with WebInspect include:

- IBM WebSphere
- Adobe ColdFusion
- Microsoft.NET
- Lotus Domino
- BEA Weblogic
- Macromedia JRun
- Oracle Application Server
- Jakarta Tomcat

#### See Also

["Contact Technical Support" on page 390](#)

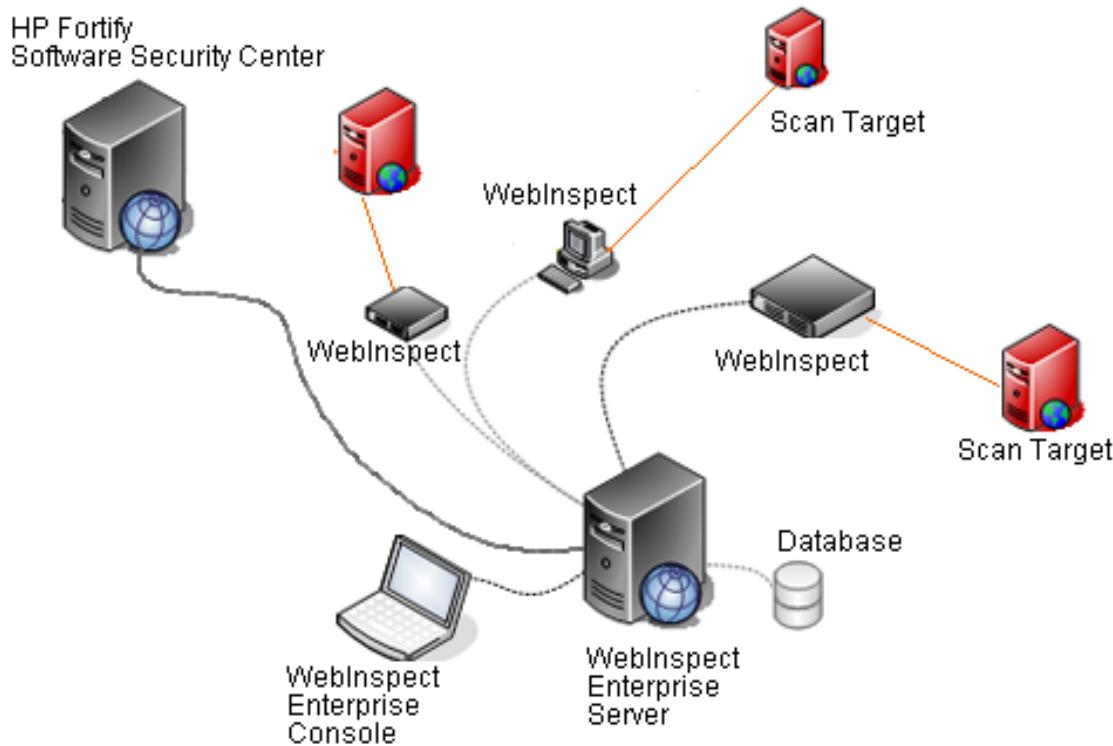
## About WebInspect Enterprise

WebInspect Enterprise is a centralized system for controlling a distributed network of WebInspect scanners and for publishing scan results and modifications to HP Fortify Software Security Center. This innovative architecture enables you to:

- Conduct a large number of automated security scans using any number of WebInspect sensors to scan Web applications and SOAP services.
- Manage large or small deployments of WebInspect across your organization controlling product updates, scan policies, scan permissions, tools usage and scan results all centrally from the WebInspect Enterprise console.
- Track, manage and detect your new and existing Web applications and monitor all activity associated with them.
- Integrate scan data into the HP Fortify Software Security Center.
- Independently schedule scans and **blackout periods**, manually launch scans, and update repository

information by using WebInspect or the WebInspect Enterprise console.

- Limit exposure to enterprise-sensitive components and data by using centrally defined roles for users.
- Obtain an accurate snapshot of the organization's risk and policy compliance through a centralized database of scan results, reporting, and trend analysis.
- Facilitate integration with third-party products and deployment of customized Web-based front ends using the Web Services application programming interface (API).



# Preparing Your System for Audit

WebInspect is an aggressive Web application analyzer that rigorously inspects your entire Web site for real and potential security vulnerabilities. This procedure is intrusive to varying degrees. Depending on which WebInspect policy you apply and the options you select, it can affect server and application throughput and efficiency. When using the most aggressive policies, you should perform this analysis in a controlled environment while monitoring your servers.

## Effects to Consider

During an audit of any type, WebInspect submits a large number of HTTP requests, many of which have "invalid" parameters. On slower systems, the volume of requests may degrade or deny access to the system by other users. Additionally, if you are using an intrusion detection system, it will identify numerous illegal access attempts.

To conduct a thorough scan, WebInspect attempts to identify every page, form, file, and folder that composes your application. If you select the option to submit forms during a crawl of your site, WebInspect will complete and submit all forms it encounters. Although this enables WebInspect to navigate seamlessly through your application, it may also produce the following consequences:

- If, when a user normally submits a form, the application creates and sends e-mails or bulletin board postings (to a product support or sales group, for example), WebInspect will also generate these messages as part of its probe.
- If normal form submission causes records to be added to a database, then forms submitted by WebInspect will create spurious records.

During the audit phase of a scan, WebInspect resubmits forms numerous times, manipulating every possible parameter to reveal problems in the applications. This will greatly increase the number of messages and database records created.

## Helpful Hints

- For systems that write records to a back-end server (database, LDAP, etc.) based on forms submitted by clients, some WebInspect users, before auditing their production system, create a backup copy of their database and then reinstall it after the audit is complete. If this is not feasible, you can query your servers after the audit, searching for and deleting records that contain one or more of the form values submitted by WebInspect. You can determine these values by opening the [Web Form Editor](#).
- If your system generates e-mail messages in response to user-submitted forms, consider disabling your mail server. Alternatively, you could redirect all e-mails to a queue and then, following the audit, manually review and delete those e-mails that were generated in response to forms submitted

by WebInspect.

- WebInspect can be configured to send up to 75 concurrent HTTP requests before waiting for an HTTP response to the first request. The default thread count setting is 5 for a crawl and 10 for an audit (if using separate requestors). In some environments, you may need to specify a lower number to avoid application or server failure. See [Scan Settings: Requestor](#) for more information.
- If for any reason you do not want WebInspect to crawl and attack certain directories, you must specify those directories using the Excluded URLs feature of WebInspect settings (see [Scan Settings: Session Exclusions](#)). You can also exclude specific file types and MIME types.
- By default, WebInspect is configured to ignore many binary files (images, documents, etc.) that are commonly found in Web applications. These documents cannot be crawled or attacked, so there is no value in auditing them. Bypassing these documents greatly increases the speed of the audit. If there are proprietary documents in use, try to ascertain the extensions of the documents and exclude them within WebInspect's default settings. If, during a crawl, WebInspect becomes extremely slow or even halts, there is a chance that it attempted to download a binary document.
- For form submission, WebInspect submits data extracted from a prepackaged file. If you require specific values (such as user names and passwords), you must create a file with HP's easy-to-use Web Form Editor and identify that file to WebInspect.
- Finally, WebInspect tests for certain vulnerabilities by attempting to upload files to your server. If your server allows this, WebInspect will record this susceptibility in its scan report and attempt to delete the file. Sometimes, however, the server will not allow a file to be deleted. For this reason, part of your post-scan maintenance should include searching for and deleting files whose name begins with "CreatedByHP."

#### See Also

["WebInspect Overview " on page 20](#)

["Quick Start " below](#)

## Quick Start

This topic provides information to help you get started with WebInspect. It includes links to more detailed information

## Update SecureBase™

To ensure that you have up-to-date information about the WebInspect catalog of vulnerabilities, use the following procedure to update your vulnerabilities database.

1. Start WebInspect.

**Note:** If WebInspect is installed as an interactive component of the Assessment Management Platform or WebInspect Enterprise, and if the enterprise server is currently using this WebInspect module to conduct a scan, then you cannot start WebInspect. The following message will be displayed: "Unable to start WebInspect. Permission denied."

2. On the **Start Page**, click **Start Smart Update**.

The Smart Update window appears, listing any updates that may be available.

3. Click **Update**.

**Note:** You should update the product each time you use it. In fact, you can select an [application setting](#) that will run Smart Update each time you start the program.

## Prepare Your System for Audit

Before performing an audit, you should understand the possible effects it will have on your Web site, as well as helpful hints to prepare for a successful audit. For more information, see "[Preparing Your System for Audit](#)" on page 24.

## Start a Scan

Once you have updated your database, you are ready to determine your Web application's security vulnerabilities.

On the WebInspect **Start Page**, click one of the following selections:

- Start a [Guided Scan](#)
- Start a [Basic Scan](#)
- Start a [Web Service Scan](#)
- Start an [Enterprise Scan](#)

### See Also

["Preparing Your System for Audit"](#) on page 24

["User Interface Overview"](#) on page 31

# Scanning Web Services at zero.webappsecurity.com

Web services are programs that communicate with other applications (rather than with users) and answer requests for information. Most Web services use Simple Object Access Protocol (SOAP) to send XML data between the Web service and the client Web application that initiated the information request.

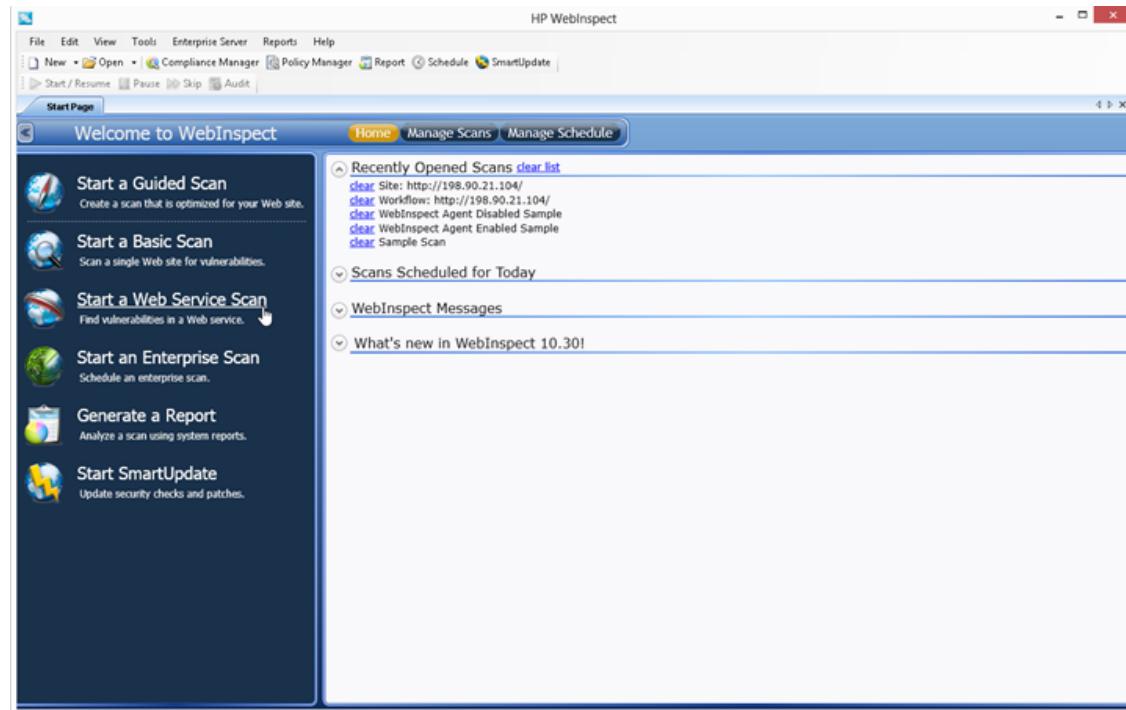
A client Web application that accesses a Web service receives a Web Services Definition Language (WSDL) document so that it can understand how to communicate with the service. The WSDL document describes the programmed procedures included in the Web service, the parameters those procedures expect, and the type of return information the client Web application will receive.

This tutorial illustrates how to conduct a Web service scan of zero.webappsecurity.com using a predefined Web service design (.wsd) file containing the values that WebInspect will submit when conducting the scan. For information on how to use the Web Service Test Designer to create a Web service design file (filename.wsd) for your site, refer to the Web Service Test Designer help.

## Conducting a Web Service Scan

1. Select **Start a Web Service Scan** from the WebInspect Start page.

WebInspect Start Page Image

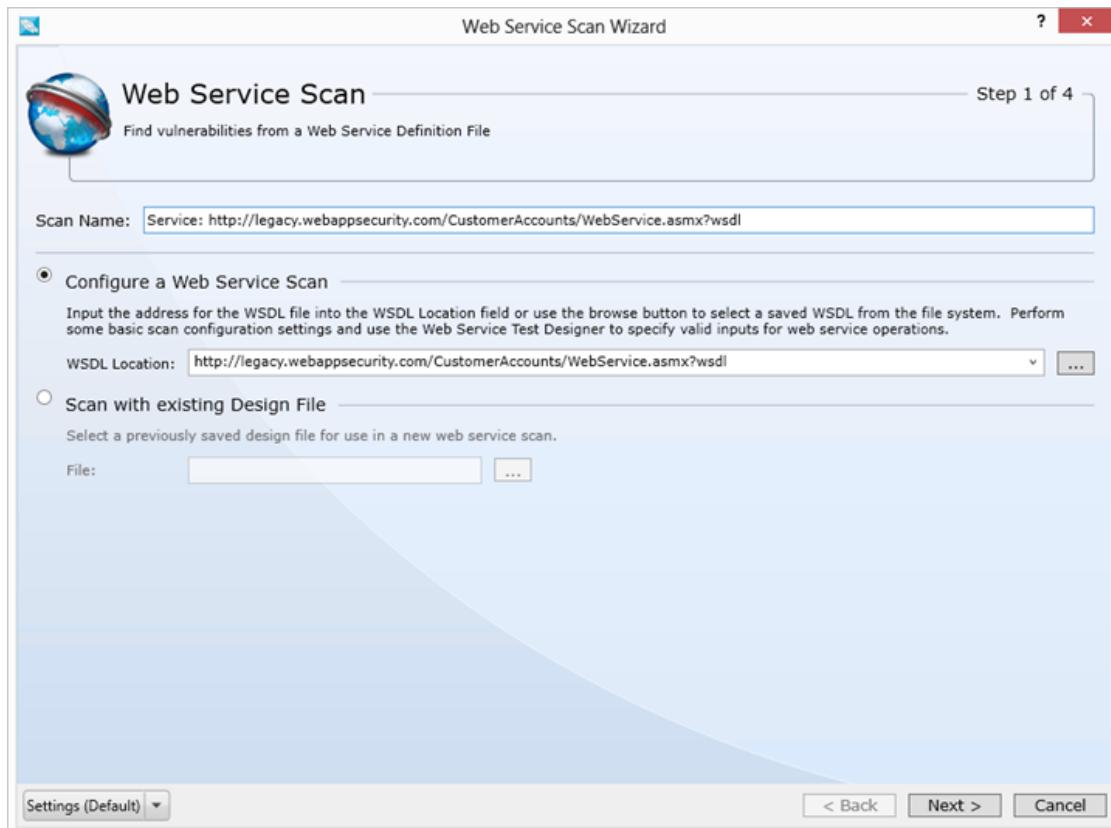


2. Accept the default name or enter a new **Scan Name** and select **Configure a Web Service Scan**.

**Note:** "Service:" is auto-filled at the start of the scan name.

**Tip:** If you were conducting a scan on your site, the Web Service Scan Wizard Step 3 of 4 would prompt you to open the Web Service Test Designer tool to create a .wsd file for your site. Then for subsequent scans of the same WSDL, you would re-use the .wsd file you created and select **Scan with existing Design File** on the Web Service Scan Wizard Step 1 of 4.

Web Service Scan Wizard Image Step 1 of 4

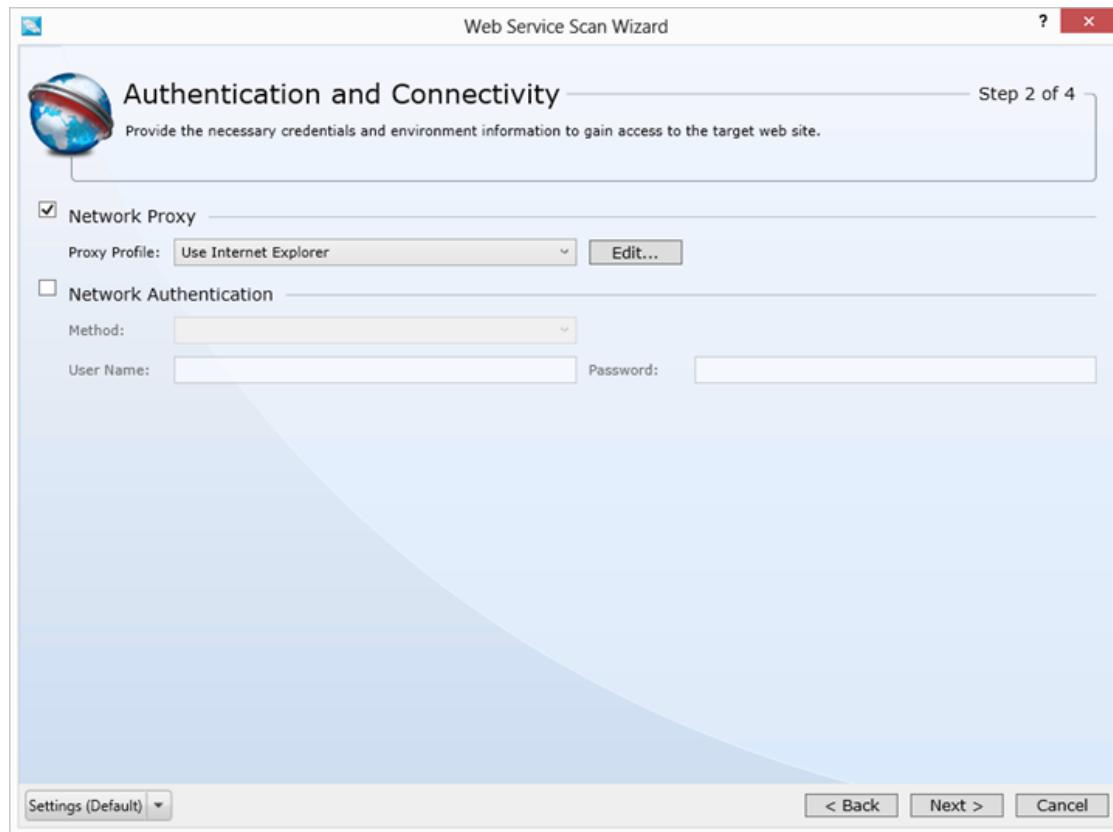


3. Accept the default URL for the **WSDL Location**.

**Tip:** If you were conducting a scan on your site, you would enter or select the fully qualified path to the WSDL file on your site.

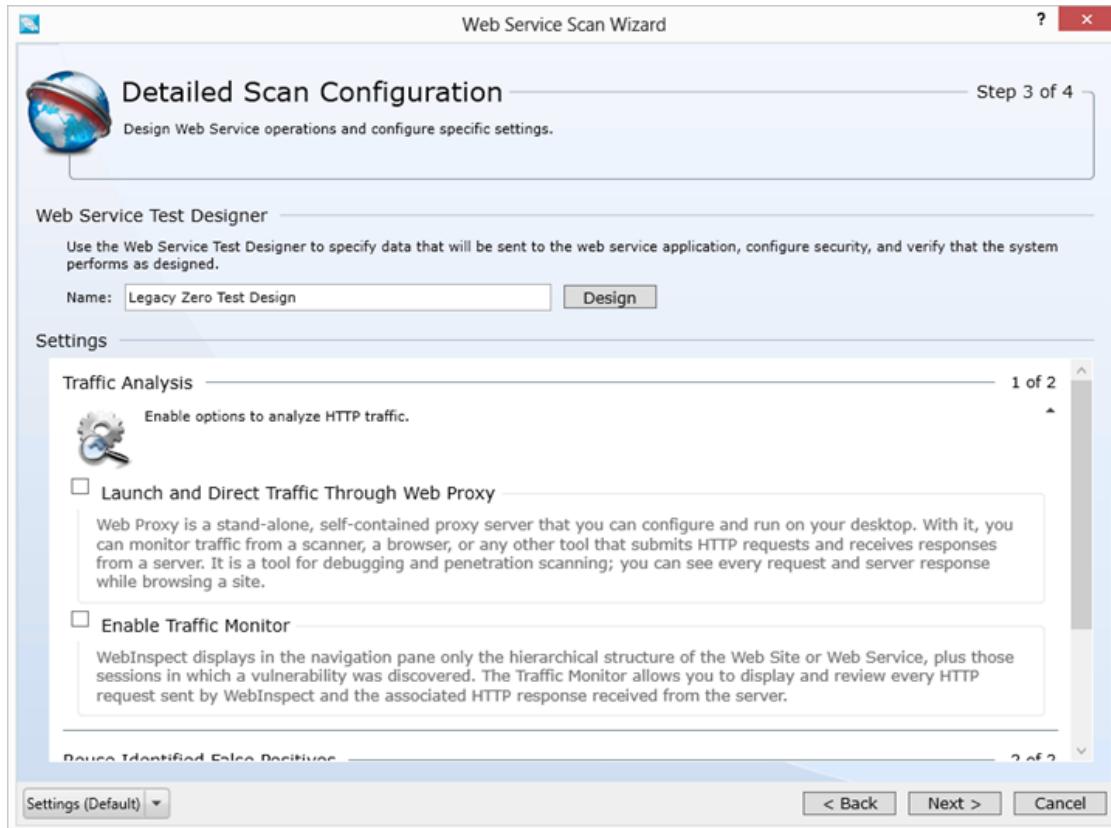
4. Click **Next**.

## Web Service Scan Wizard Image Step 2 of 4



5. If you need to access the target site through a proxy server, select **Network Proxy** and then choose an option from the **Proxy Profile** list.
6. If server authentication is required, select **Network Authentication** and then select an authentication method and enter your network credentials. For this exercise, accept the default.
7. Click **Next**.

## Web Service Scan Wizard Image Step 3 of 4



- Accept the defaults and click **Next**.

**Tip:** If you were conducting a scan on your site and had not created a .wsd file, the Web Service Scan Wizard Step 3 of 4 would prompt you to open the Web Service Test Designer tool to create a .wsd file for your site.

- Click **Scan**.

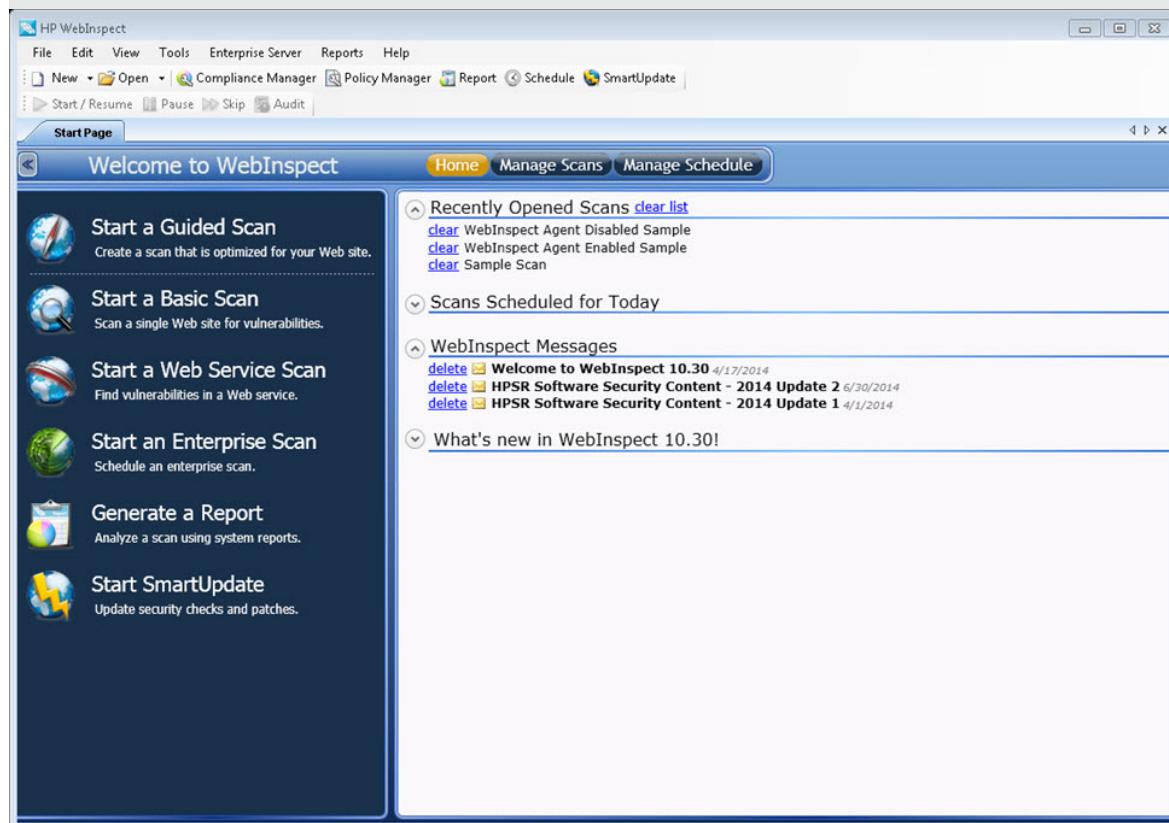
WebInspect conducts the Web Service scan.

# User Interface Overview

When you first start WebInspect, the application displays the **Start Page** in the client area, as illustrated below.

Start Page Image

**Note:** When WebInspect is connected to Enterprise Server, there is a button labeled "WebInspect Enterprise WebConsole" to the right of the SmartUpdate button. This button launches the Web Console.



## The Activity Panel

The left pane (the Activity Panel) displays hyperlinks to the following major functions:

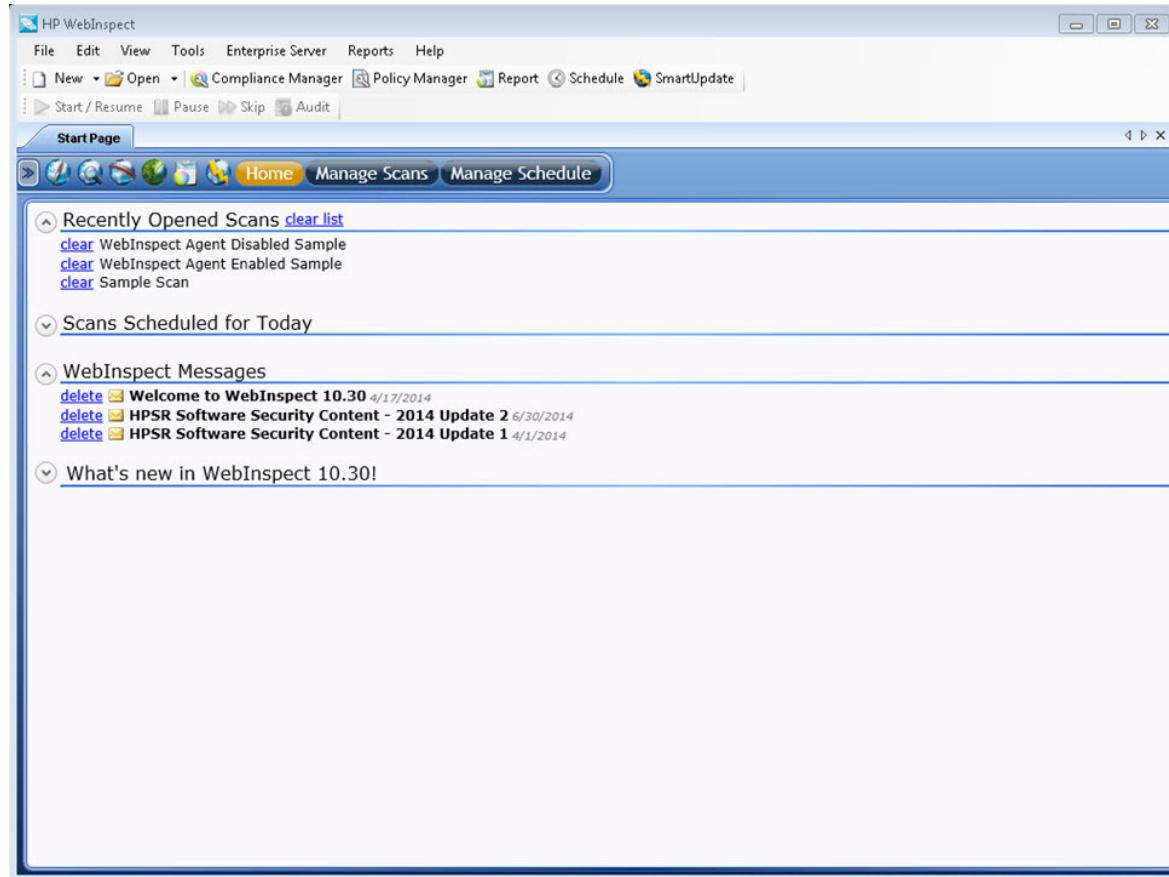
- [Start a Guided Scan](#)
- [Start a Basic Scan](#)
- [Start a Web Service Scan](#)

- Start an Enterprise Scan
- Generate a Report
- Start SmartUpdate

## Closing the Activity Panel

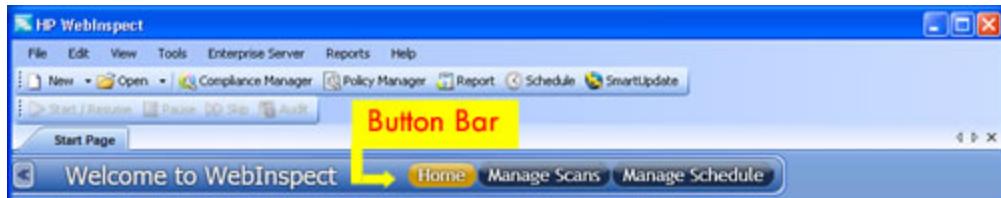
You can close the Activity Panel by clicking the Left Arrow  on the bar above the pane.

### Start Page with No Activity Panel Image



## The Button Bar

The contents of the right pane are determined by the button selected on the Button bar.

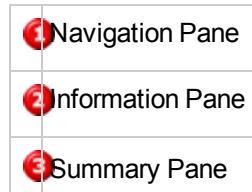
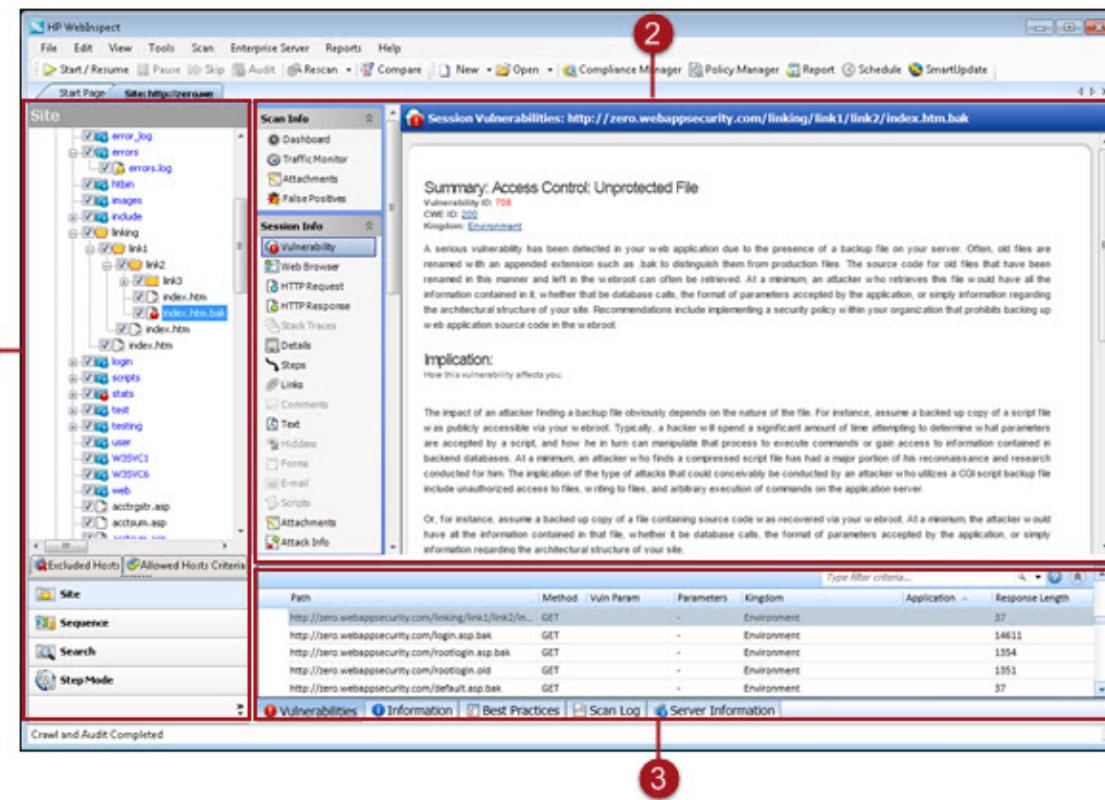


The choices are:

Button	Displayed List
Home	Displays a list of recently opened scans, as well as scans scheduled to be conducted today, recently generated reports, and messages downloaded from the HP server. If you hover the pointer over a scan name, WebInspect displays summary information about the scan. If you click the scan name, WebInspect opens the scan on a separate tab.
Manage Scans	Displays a list of previously conducted scans, which you can open, rename, or delete. Click <b>Connections</b> to choose a database: either Local (scans stored in a SQL Server Express Edition database on your machine) or Remote (scans stored in a SQL Server Standard Edition database configured on your machine or elsewhere on the network), or both.
Manage Schedule	Displays a list of scans that are scheduled to be performed. You can add a scan to the schedule, edit or delete a scheduled scan, or start the scan manually.

## Panes Associated with a Scan

Each time you open or conduct a scan, WebInspect opens a tab labeled with the name or description of the target site. This work area is divided into three regions, as depicted in the following illustration.



If you have a large number of scans open at the same time, and there is no room to display all tabs, you can scroll the tabs by clicking the arrows on the extreme right end of the tab bar. Click the **X** to close the selected tab.

## See Also

- "Menu Bar " on page 36
- "Toolbars " on page 42
- "Start Page " on the next page
- "Navigation Pane " on page 45
- "Summary Pane" on page 84
- "Information Pane " on page 54

## Start Page

The left-hand pane of the **Start Page** contains a list of activities related to the vulnerability scan of your Web site or Web service.

- [Start a Basic Scan](#)
- [Start a Web Service Scan](#)
- [Start an Enterprise Scan](#)
- [Generate a Report](#)
- [Start SmartUpdate](#)

The contents of the right-hand pane are controlled by the buttons on the Button bar.



## Home

When **Home** is selected (the default), WebInspect displays a list of:

- Recently opened scans.  
If you hover the pointer over a scan name, WebInspect displays summary information about the scan. If you click the scan name, WebInspect opens the scan on a separate tab.
- Scans scheduled to be conducted today
- Recently generated reports
- Messages downloaded from the HP server

## Manage Scans

When **Manage Scans** is selected, WebInspect displays a list of previously conducted scans, which you can open, rename, or delete. Click **Connections** to choose a database: either Local (scans stored in the SQL Server Express Edition database on your machine) or Remote (scans stored in the SQL Server database, if configured), or both.

## Manage Schedule

When **Manage Schedule** is selected, WebInspect displays a list of scheduled scans. You can add a scan to the schedule, edit or delete a scheduled scan, or start the scan manually.

### See Also

["User Interface Overview" on page 31](#)

["Using Help " on page 19](#)

## Menu Bar

Click any portion of the menu bar for more information.



Menu options are:

- [File](#)
- [Edit](#)
- [View](#)
- [Tools](#)
- [Scan](#)
- [Enterprise Server](#)
- [Reports](#)
- [Help](#)

## File Menu

The **File** menu contains the following commands:

Command	Description
<a href="#">New</a>	Allows you to select either Basic Scan or Web Service scan, and then launches the Scan Wizard, which steps you through the process of starting a scan.

Command	Description
<b>Open</b>	Allows you to open either a scan or a generated report.
<b>Schedule</b>	Opens the <i>Manage Scheduled Scans</i> window, which allows you to add, edit, or delete a scheduled scan.
<b>Import Scan</b>	Allows you to import a scan file.
<b>Export</b>	This command is available only when a tab containing a scan is selected. You may: <ul style="list-style-type: none"> <li>• Export a scan</li> <li>• Export scan details</li> <li>• Export a scan to Software Security Center</li> </ul>
<b>Close Tab</b>	When multiple tabs are open, closes the selected tab.
<b>Exit</b>	Closes the WebInspect program.

### See Also

["Edit Menu " below](#)

["View Menu " on the next page](#)

["Tools Menu " on page 39](#)

["Scan Menu " on page 39](#)

["Enterprise Server Menu" on page 40](#)

["Reports Menu " on page 41](#)

["Help Menu" on page 41](#)

## Edit Menu

The **Edit** menu contains the following commands:

Command	Description
<b>Default Scan Settings</b>	Displays the Default Settings window, allowing you to select or modify options used for scanning.
<b>Current Scan Settings</b>	Displays a settings window that allows you to select or modify options for the current scan. This command is available only when a tab containing a scan is selected.

Command	Description
<b>Manage Settings</b>	Opens a window that allows you to add, edit, or delete settings files.
<b>Application Settings</b>	Displays the <a href="#">Application Settings</a> window, allowing you to select or modify options controlling the operation of the WebInspect application.
<b>Copy URL</b>	Copies the selected URL to the Windows clipboard. This command is available only when a tab containing a scan is selected.
<b>Copy Scan Log</b>	Copies the log (for the scan on the selected tab) to the Windows clipboard. This command is available only when a tab containing a scan is selected.

#### See Also

- ["File Menu" on page 36](#)
- ["View Menu " below](#)
- ["Tools Menu " on the next page](#)
- ["Scan Menu " on the next page](#)
- ["Enterprise Server Menu" on page 40](#)
- ["Reports Menu " on page 41](#)
- ["Help Menu" on page 41](#)

## View Menu

The **View** menu contains the following commands.

Command	Description
<b>Word Wrap</b>	Inserts soft returns at the right-side margins of the display area when viewing HTTP requests and responses. This command is available only when a tab containing a scan is selected.
<b>Toolbars</b>	Allows you to select which <a href="#">toolbars</a> should be displayed.

#### See Also

- ["File Menu" on page 36](#)
- ["Edit Menu " on the previous page](#)
- ["Tools Menu " on the next page](#)
- ["Scan Menu " on the next page](#)
- ["Enterprise Server Menu" on page 40](#)

["Reports Menu " on page 41](#)

["Help Menu" on page 41](#)

## Tools Menu

The **Tools** menu contains commands to launch the tool applications.

### See Also

["File Menu" on page 36](#)

["Edit Menu " on page 37](#)

["View Menu " on the previous page](#)

["Scan Menu " below](#)

["Enterprise Server Menu" on the next page](#)

["Reports Menu " on page 41](#)

["Help Menu" on page 41](#)

## Scan Menu

The **Scan** menu appears on the menu bar only when a tab containing a scan has focus. It contains the following commands.

Command	Description
<b>Start/Resume</b>	Starts or resumes a scan after you paused the process.
<b>Pause</b>	Halts a crawl or audit. Click <b>Resume</b> to continue the scan.
<b>Skip</b>	If an audit is in progress, skips to the next audit methodology. If a crawl is in progress, skips to the audit.
<b>Audit</b>	Assesses the crawled site for vulnerabilities. Use the command after completing a crawl or exiting Step Mode.
<b>Rescan</b>	This command launches the Scan Wizard prepopulated with settings last used for the selected scan.

### See Also

["File Menu" on page 36](#)

["Edit Menu " on page 37](#)

["View Menu " on the previous page](#)

["Tools Menu " above](#)

["Enterprise Server Menu" below](#)

["Reports Menu " on the next page](#)

["Help Menu" on the next page](#)

## Enterprise Server Menu

The **Enterprise Server** menu contains the following commands:

Command	Description
<b>Connect to WebInspect Enterprise or Disconnect</b>	Establishes or breaks a connection to the WebInspect Enterprise server.
<b>Download Scan</b>	Allows you to select a scan for copying from the server to your hard drive.
<b>Publish Scan</b>	Displays a dialog allowing you to review vulnerabilities and transmit them to an enterprise server which, in turn, transmits them to an HP Fortify Software Security Center server. For more information, see <a href="#">Publish Scan (WebInspect Enterprise Connected)</a> .
<b>Upload Scan</b>	Allows you to select a scan for transferring data to the server. This is used most often when the application setting "auto upload scans" is not selected.
<b>Transfer Settings</b>	Allows you to select a WebInspect settings file and transfer it to the server, which will create a Scan Template based on those settings. Also allows you to select a Scan Template and transfer it to WebInspect, which will create a settings file based on the template. See <a href="#">Settings Transfer</a> for more information.
<b>WebConsole</b>	Launches the WebInspect Enterprise Web Console application.
<b>About Enterprise Server</b>	Displays information about WebInspect Enterprise.

**Note:** A WebInspect installation with a standalone license may connect to an enterprise server at any time, as long as the user is a member of a role in WebInspect Enterprise.

### See Also

["File Menu" on page 36](#)

["Edit Menu " on page 37](#)

["View Menu " on page 38](#)

["Tools Menu " on the previous page](#)

["Scan Menu " on page 39](#)

["Reports Menu " below](#)

["Help Menu" below](#)

## Reports Menu

The **Reports** menu contains the following commands.

Command	Description
<b>Generate Report</b>	Launches the Report Generator.
<b>Manage Reports</b>	Displays a list of standard and custom report types. You can rename, delete, or export custom-designed reports, and you may import a report definition file.
<b>Report Designer</b>	Launches the Report Designer, allowing you to define a custom report.

### See Also

["File Menu" on page 36](#)

["Edit Menu " on page 37](#)

["View Menu " on page 38](#)

["Tools Menu " on page 39](#)

["Scan Menu " on page 39](#)

["Enterprise Server Menu" on the previous page](#)

["Help Menu" below](#)

## Help Menu

The **Help** menu contains the following commands.

Command	Description
<b>WebInspect Help</b>	Opens this Help file.
<b>Index</b>	Opens this Help file, displaying the index in the left pane.
<b>Search</b>	Opens this Help file, displaying the search options in the left pane.

Command	Description
<b>Support</b>	<ul style="list-style-type: none"> <li>• <b>Request an Enhancement</b> - If the support channel is enabled (see <a href="#">Application Settings: Support Channel</a>), displays a window allowing you to submit enhancement requests to Hewlett-Packard.</li> <li>• <b>Support Tool</b> - Launches the HP Support tool, which allows you to upload files that may help HP support personnel analyze and resolve any problems you encounter.</li> <li>• <b>Technical Support</b> - Displays instructions for contacting HP Technical Support.</li> </ul>
<b>Tutorials</b>	Allows you to download tutorials and other WebInspect documentation.
<b>About WebInspect</b>	Displays information about the WebInspect application, including license information, allowed hosts, and attributes.

### See Also

["File Menu" on page 36](#)

["Edit Menu " on page 37](#)

["View Menu " on page 38](#)

["Tools Menu " on page 39](#)

["Scan Menu " on page 39](#)

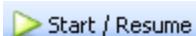
["Enterprise Server Menu" on page 40](#)

["Reports Menu " on the previous page](#)

## Toolbars

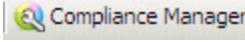
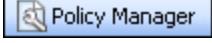
The WebInspect window contains two toolbars: Scan and Standard. You can display or hide either toolbar by selecting **Toolbars** from the **View** menu.

## Buttons Available on the Scan Toolbar

Button	Function
 Start / Resume	You can pause a scan and then resume scanning. Also, a completed scan may contain sessions that were not sent (because of timeouts or other errors); if you click <b>Start</b> , WebInspect will attempt to resend those sessions.
 Pause	Interrupts an ongoing scan. You can continue scanning by clicking the <b>Start/Resume</b> button.

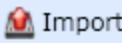
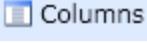
Button	Function
 Skip	When conducting a sequential crawl and audit, you can skip processing by whichever engine is running (if you selected <b>Test each engine type per session</b> ) or you can skip processing the session (if you selected <b>Test each session per engine type</b> ). See <a href="#">Scan Settings: Method</a> (sequential behavior) for more information.
 Audit	If you conduct a crawl-only scan or a <a href="#">Step Mode</a> scan, you can afterwards click this button to conduct an audit.
 Rescan ▾	This button appears only if you select a tab containing a scan. If you select <b>Scan Again</b> from the drop-down menu, it launches the Scan Wizard prepopulated with settings last used for the selected scan. If you select <b>Retest Vulnerabilities</b> , it starts a scan that examines only those portions of the target site in which vulnerabilities were detected during the original scan. For more information, see <a href="#">Review and Retest</a> .
 Compare	This button appears only if you select a tab containing a scan. It allows you to compare the vulnerabilities revealed by two different scans of the same target. For more information, see <a href="#">Comparing Scans</a> .
 Run in WebInspect Enterprise	This button appears only if WebInspect is connected to WebInspect Enterprise and a scan is open on the tab that has focus. It allows you to send the scan settings to WebInspect Enterprise, which creates a scan request and places it in the scan queue for the next available sensor. For detailed information, see <a href="#">"Running a Scan in Enterprise Server" on page 177</a> .
 Synchronize	This button appears only after connecting to WebInspect Enterprise. It allows you to specify a Software Security Center (SSC) project and version. WebInspect then downloads a list of vulnerabilities from SSC, compares the downloaded vulnerabilities to the vulnerabilities in the current scan, and assigns an appropriate status (New, Existing, Reintroduced, or Not Found) to the vulnerabilities in the current scan. For detailed information, see <a href="#">Integrating with WebInspect Enterprise</a> .
 Publish	This button appears only after connecting to WebInspect Enterprise and is enabled after you have synchronized WebInspect with Software Security Center. It uploads project version data through WebInspect Enterprise to Software Security Center.

## Buttons Available on the Standard Toolbar

Button	Function
 New ▾	Allows you to start a Basic Scan, a Web service scan, or an enterprise scan.
 Open ▾	Allows you to open a scan or a report.
 Compliance Manager	Starts the <a href="#">Compliance Manager</a> .
 Policy Manager	Starts the <a href="#">Policy Manager</a> .
 Report	Starts the <a href="#">Report Generator</a> .
 Schedule	Allows you to <a href="#">schedule a scan</a> to occur on a specific time and date.
 SmartUpdate	Contacts the central Hewlett-Packard database to determine if <a href="#">updates</a> are available for your system and, if updates exist, allows you to install them.
 WebInspect Enterprise WebConsole	Launches the WebInspect Enterprise Web Console application. This button appears only if you are connected to WebInspect Enterprise.

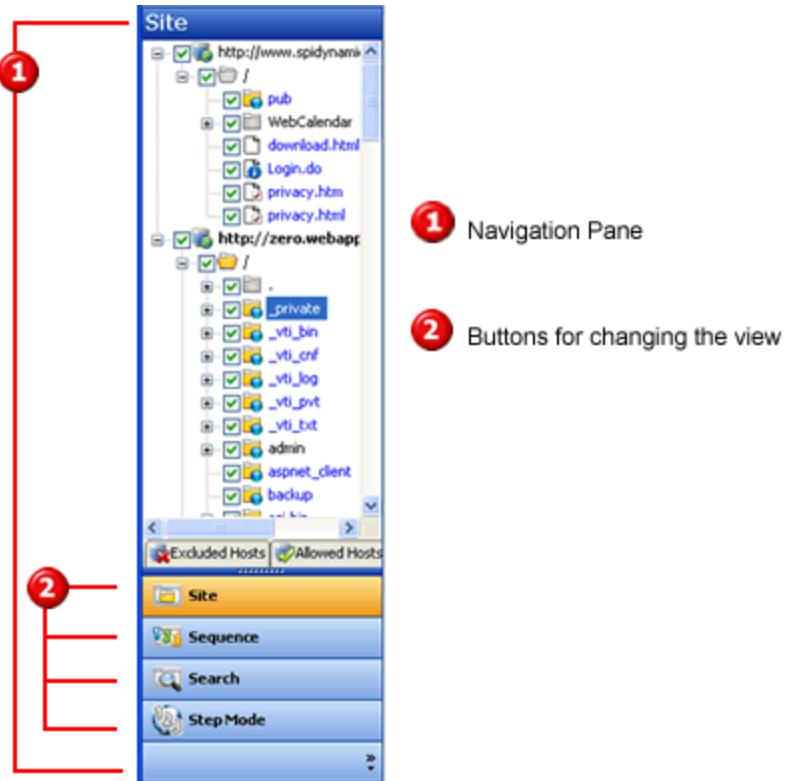
## Buttons Available on the "Manage Scans" Toolbar

Button	Function
 Open	To open scans, select one or more scans and click <b>Open</b> (or simply double-click an entry in the list). WebInspect loads the scan data and displays each scan on a separate tab.
 Rescan ▾	To launch the Scan Wizard prepopulated with settings last used for the selected scan, click <b>Rescan &gt; Scan Again</b> . To rescan only those sessions that contained vulnerabilities revealed during a previous scan, select a scan and click <b>Rescan &gt; Retest Vulnerabilities</b> . For more information, see <a href="#">Review and Retest</a> .
 Rename	To rename a selected scan, click <b>Rename</b> .
 Delete	To delete the selected scan(s), click <b>Delete</b> .

Button	Function
 Import	To import a scan, click <b>Import</b> .
 Export ▾	To export a scan, export scan details, or export a scan to Software Security Center, click the drop-down arrow on <b>Export</b> .
 Compare	To compare scans, select two scans (using Ctrl + click) and click <b>Compare</b> . For more information, see <a href="#">Comparing Scans</a> .
 Connections	By default, WebInspect lists all scans saved in the local SQL Server Express Edition and in a configured SQL Server Standard Edition. To select one or both databases, or to specify a SQL Server connection, click <b>Connections</b> .
 Refresh	When necessary, click <b>Refresh</b> to update the display.
 Columns	To select which columns should be displayed, click <b>Columns</b> . You can rearrange the order in which columns are displayed using the <b>Move Up</b> and <b>Move Down</b> buttons or, on the <b>Manage Scans</b> list, you can simply drag and drop the column headers.

## Navigation Pane

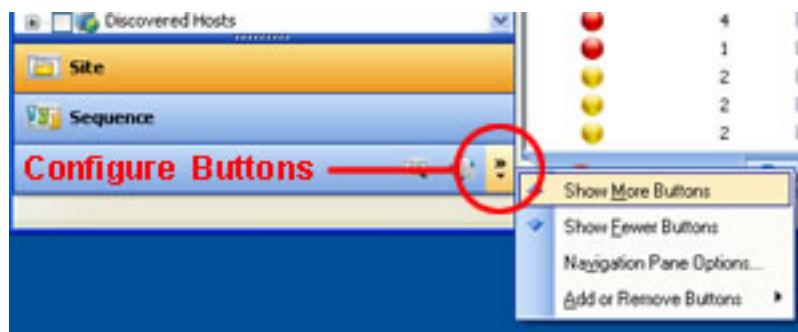
When conducting or viewing a scan, the navigation pane is on the left side of the *WebInspect* window. It includes the **Site**, **Sequence**, **Search**, and **Step Mode** buttons, which determine the contents (or "view") presented in the navigation pane.



① Navigation Pane

② Buttons for changing the view

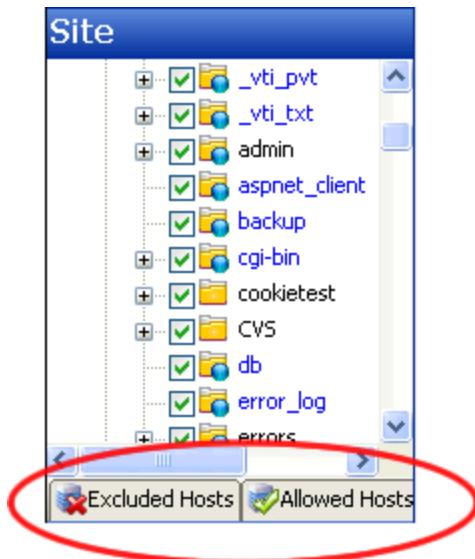
If all buttons are not displayed, click the drop-down arrow at the bottom of the button list and select **Show More Buttons**.



## Site View

WebInspect displays in the navigation pane only the hierarchical structure of the Web site or Web service, plus those sessions in which a vulnerability was discovered. During the crawl of the site, WebInspect selects the check box next to each session (by default) to indicate that the session will also be audited. When conducting a sequential crawl and audit (where the site is completely crawled and then audited), you can exclude a session from the audit by clearing its associated check box before the audit begins.

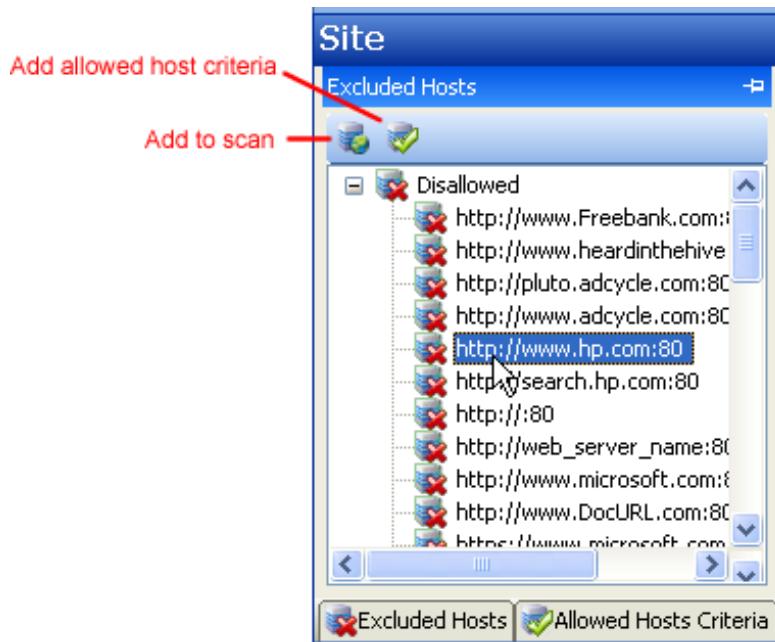
Site view also contains two pop-up tabs: **Excluded Hosts** and **Allowed Hosts Criteria**.



## Excluded Hosts

If you click the **Excluded Hosts** tab (or hover your pointer over it), the tab displays a list of all disallowed hosts. These are hosts that may be referenced anywhere within the target site, but cannot be scanned because they are not specified in the Allowed Hosts setting (Default/Current Scan Settings > Scan Settings > Allowed Hosts).

Using the **Excluded Hosts** tab, you can select an excluded host and click either **Add to scan** or **Add allowed host criteria**.



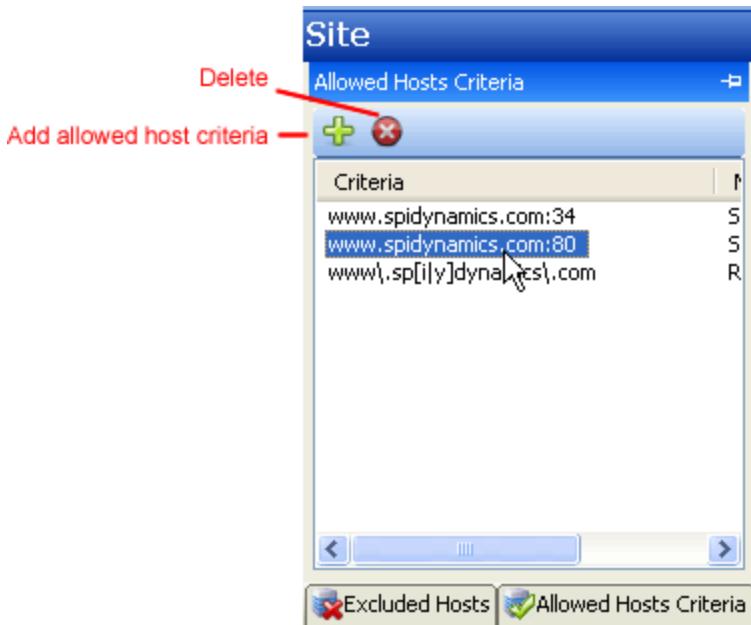
Adding a host to the scan creates a node in the site tree representing the host root directory. WebInspect will scan that session. If you have selected the option to log rejected sessions for invalid

hosts (Default/Current Scan Settings > Scan Settings > Session Storage), WebInspect will scan the entire host.

Adding a host to the allowed host criteria adds the URL to the list of allowed hosts in the Current Scan Settings. WebInspect will include in the scan any subsequent links to that host. However, if you add a host to the allowed host criteria after WebInspect has already scanned the only resource containing a link to that host, the added host will not be scanned.

## Allowed Hosts Criteria

If you click the **Allowed Hosts Criteria** tab (or hover your pointer over it), the tab displays the URLs (or regular expressions) specified in the WebInspect scan settings (under Allowed Hosts). If you click either **Delete** or **Add allowed host criteria**, WebInspect opens the *Current Settings* dialog, where you can add, edit, or delete allowed host criteria (a literal URL or a regular expression representing a URL).



If you add an entry, WebInspect will include in the scan any subsequent links it encounters to hosts that match the criteria. However, if you specify a host after WebInspect has already scanned the only resource containing a link to that host, the added host will not be scanned. Similarly, if you delete an entry from the allowed host list, the scan will still include any resources that WebInspect already encountered.

To save these settings for a future scan, select **Save settings as** (at the bottom of the left pane of the *Settings* window).

You must pause the scan before you can modify the excluded hosts or allowed hosts criteria. Furthermore, the scanning of added or deleted hosts may not occur as expected, depending on the point at which you paused the scan. For example, if you add an allowed host after WebInspect has already scanned the only resource containing a link to the added host, the added host will not be scanned.

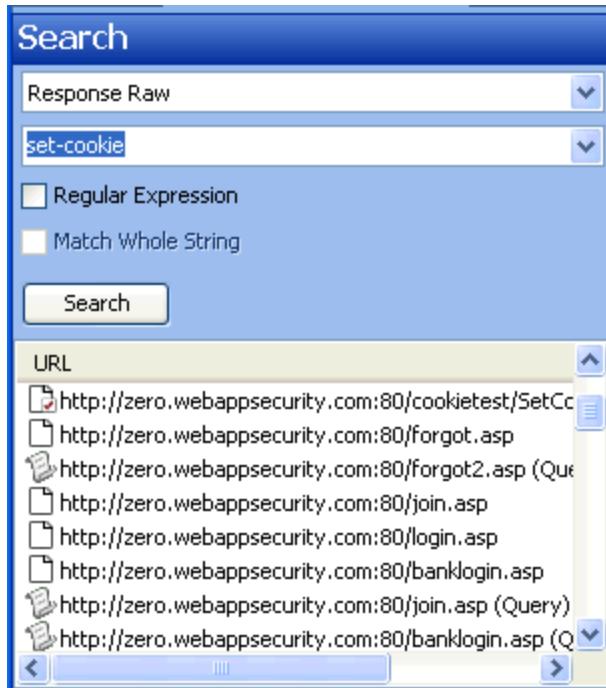
## Sequence View

Sequence view displays server resources in the order they were encountered by WebInspect during a scan.

**Note:** In both Site view and Sequence view, blue text denotes a directory or file that was "guessed" by WebInspect, rather than a resource that was discovered through a link. For example, WebInspect always submits the request "GET /backup/ HTTP/1.1" in an attempt to discover if the target Web site contains a directory named "backup."

## Search View

The Search view allows you to search across all sessions for various HTTP message components. For example, if you select **Response Raw** from the drop-down and specify **set-cookie** as the search string, WebInspect lists every session whose raw HTTP response includes the "set-cookie" command.



To use the Search view:

1. In the **navigation pane**, click **Search** (at the bottom of the pane).

If all buttons are not displayed, click the **Configure Buttons** drop-down at the bottom of the button list and select **Show More Buttons**.

2. From the top-most list, select an area to search.
3. In the combo box, type or select the string you want to locate.
4. If the string represents a [regular expression](#), select the **Regular Expression** check box.
5. To find an entire string in the HTTP message that exactly matches the search string, select the **Match Whole String** check box. The exact match is not case-sensitive.

**Note:** This option is not available for certain search targets.

6. Click **Search**.

## Step Mode View

Use Step Mode to navigate manually through the site, beginning with a session you select from either the site view or the sequence view.

Follow the steps below to step through the site:

1. In the site or sequence view, select a session.
2. Click the **Step Mode** button.  
If the button is not visible, click the **Configure Buttons** drop-down and select **Show More Buttons**.
3. When Step Mode appears in the navigation pane, select either **Audit as you browse** or **Manual Audit** from the **Audit Mode** list. Manual Audit is recommended.



4. Click **Record** .
5. Click **Browse**.  
A browser opens and displays the response associated with the selected session. Continue browsing to as many pages as you like.
6. When done, return to WebInspect and click **Finish**.

The new sessions are added to the navigation pane.

7. If you selected **Manual Audit** in step 3, click  Audit. WebInspect will audit all unaudited sessions, including those you added (or replaced) through Step Mode.

## Navigation Pane Icons

Use the following table to identify resources displayed in the navigation pane.

**Icons Used in the Navigation Pane**

Icon	Description
	Server/host: Represents the top level of your site's tree structure.
	Blue folder: A folder discovered by "guessing" and not by crawling.
	Yellow folder: A folder whose contents are available over your Web site.
	Grey folder: A folder indicating the discovery of an item via path truncation. Once the parent is found, the folder will display in either blue or yellow, depending on its properties.
	File.
	Query or post.
	DOM event.

**Icons superimposed on a folder or file indicate a discovered vulnerability**

Icon	Description
	A red dot with an exclamation point indicates the object contains a critical vulnerability. An attacker might have the ability to execute commands on the server or retrieve and modify private information.
	A red dot indicates the object contains a high vulnerability. Generally, the ability to view source code, files out of the Web root, and sensitive error messages.
	A gold dot indicates the object contains a medium vulnerability. These are generally non-HTML errors or issues that could be sensitive.
	A blue dot indicates the object contains a low vulnerability. These are generally interesting issues, or issues that could potentially become higher ones.

**Icons superimposed on a folder or file indicate a discovered vulnerability , continued**

Icon	Description
	An "i" in a blue circle indicates an informational item. These are interesting points in the site, or certain applications or Web servers.
	A red check mark indicates a "best practice" violation.

## Navigation Pane Shortcut Menu

If you right-click an item in the navigation pane while using the Site or Sequence view, a shortcut menu presents the following options:

- **Expand Children\*** - (Site View only) Expands branching nodes in the site tree.
- **Collapse Children\*** - (Site View only) Contracts branching nodes into the superior node.
- **Check All\*** - (Site View only) Marks the check box the parent node and all children.
- **Uncheck All\*** - (Site View only) Removes the check mark from the parent node and all children.
- **Generate Session Report\*** - (Site View only) Creates a report showing summary information, the attack request and attack response, links to and from the URL, comments, forms, e-mail addresses, and check descriptions for the selected session.
- **Export Site Tree\*** - (Site View only) Saves the site tree in XML format to a location you specify.
- **Copy URL** - Copies the URL to the Windows clipboard.
- **View in Browser** - Renders the HTTP response in a browser.
- **Links** - (Site View only) Lists all resources at the target site that contain links to the selected resource. The links may be rendered by HTML tags, scripts, or HTML forms. It also lists (under Linked To) all resources that are referenced by links within the HTTP response for the selected session. If you double-click a listed link, WebInspect shifts focus in the navigation pane to the referenced session. Alternatively, you can browse to the linked resource by viewing the session in the Web browser (click Web Browser).
- **Add** - Allows you to add locations discovered by means other than a WebInspect scan (manual inspection, other tools, etc) for information purposes. You can then add any discovered vulnerabilities to those locations so that a more complete picture of the site is archived for analysis.
  - **Page** - A distinct URL (resource).
  - **Directory** - A folder containing a collection of pages.

Choosing either **Page** or **Directory** invokes a dialog that allows you to name the directory or page and edit the HTTP request and response.

- **Variation** - A subnode of a location that lists particular attributes for that location. For example, the *login.asp* location might have the variation: “(Query)  
*Username=12345&Password=12345&Action=Login*”. Variations are like any other location in that they can have vulnerabilities attached to them, as well as subnodes.

Choosing **Variation** invokes the *Add Variation* dialog, allowing you to edit the variation attributes, specify Post or Query, and edit the HTTP request and response.

- **Vulnerability** - A specific security threat.

Choosing **Vulnerability** invokes the [Edit Vulnerabilities dialog](#), allowing you to edit the variation attributes, specify Post or Query, and edit the HTTP request and response.

- **Edit Vulnerabilities** - Allows you to edit a location that was added manually or [edit a vulnerability](#).
- **Remove Location** - Removes the selected session from the navigation pane (both Site and Sequence views) and also removes any associated vulnerabilities.

**Note:** You can recover removed locations (sessions) and their associated vulnerabilities. See [Recover Deleted Items](#) for details.

- **Review Vulnerability** - Allows you to retest the vulnerability, mark it as a false positive, or send it to HP Quality Center or IBM Rational ClearQuest. See [Vulnerability Review](#).
- **Mark as False Positive** - Flags the vulnerability as a false positive and allows you to add a note.
- **Send to** - Allows you convert the selected vulnerability to a defect and assign it to either HP Quality Center or IBM Rational ClearQuest, using the profile specified in the WebInspect application settings.
- **Remove Server** - Deletes the server from the navigation pane and does not include the server in any remaining scan activity. This command appears only when you right-click a server.
- **Crawl** - Recrawls the selected URL.
- **Attachments** - Allows you to create a note associated with the selected session, flag the session for follow-up, add a vulnerability note, or add a vulnerability snapshot.
- **Tools** - Presents a submenu of available tools.
- **Filter by Current Session** - Restricts the display of items in the Summary pane to those having the SummaryDataID of the selected session.

\* Command appears on shortcut menu only when the Navigation pane is using the Site view.

## See Also

"User Interface Overview" on page 31

"Search View" on page 193

"Inspecting the Results" on page 189

## Information Pane

When conducting or viewing a scan, the information pane contains three collapsible information panels and an information display area.

The screenshot shows the WebInspect interface with the Information Pane open. The pane is divided into four sections, each with a red circle containing a number:

- 1 Scan Info panel**: The top section, which is currently expanded, displays a list of vulnerabilities found during a session. It includes links to "Access Control: Unprotected File", "Privacy Violation: Autocomplete", "Credential Management: Insecure Transmission", and "Transport Layer Protection: Unencrypted Login Form".
- 2 Session Info panel**: The second section from the top, collapsed.
- 3 Host Info panel**: The third section from the top, collapsed.
- 4 Information display area**: The bottom section, which is also collapsed. It contains a "Fix" section with remediation instructions and sections for "For Security Operations" and "For Development".

Select the type of information to display by clicking on an item in one of these three information panels in the left column.

**Tip:** If you follow a link when viewing the vulnerability information, click the highlighted session in the navigation pane to return.

## See Also

["Summary Pane" on page 84](#)

["User Interface Overview" on page 31](#)

["Navigation Pane " on page 45](#)

["Scan Info Panel Overview " below](#)

["Session Info Panel Overview " on page 67](#)

["Host Info Panel Overview" on page 75](#)

## Scan Info Panel Overview

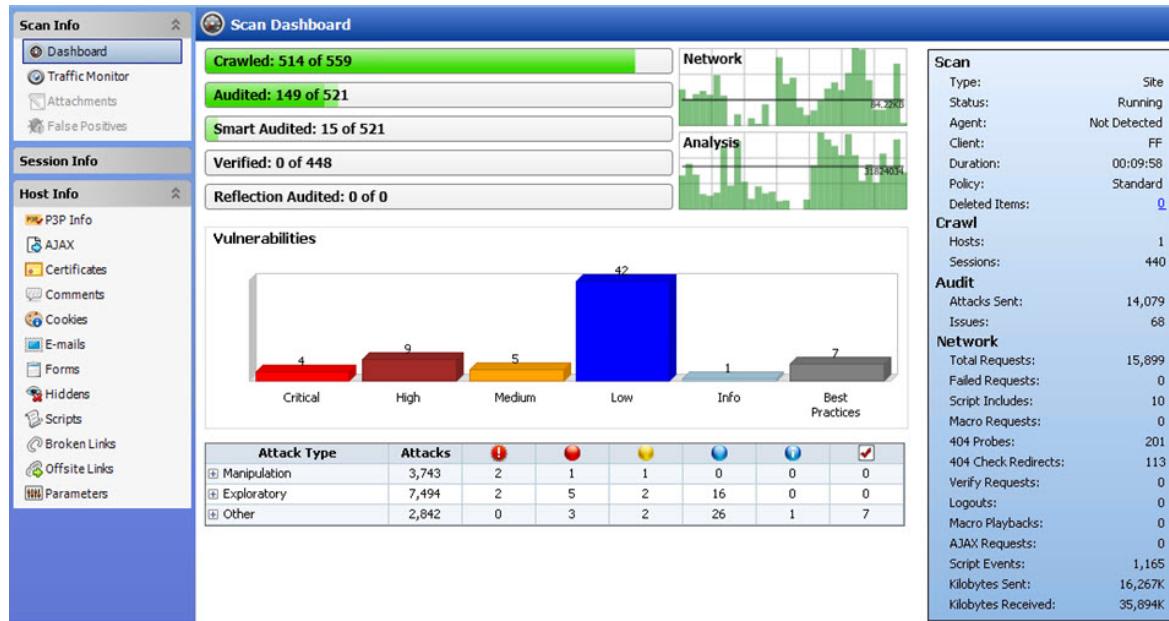
The **Scan Info** panel has the following choices:

- [Dashboard](#)
- [Traffic Monitor](#)
- [Attachments](#)
- [False Positives](#)

### Dashboard

The **Dashboard** selection displays a real-time summary of the scan results and a graphic representation of the scan progress. This section is displayed only if you select this option from the Default or Current settings. See [Dashboard](#) for additional information.

## Dashboard Image



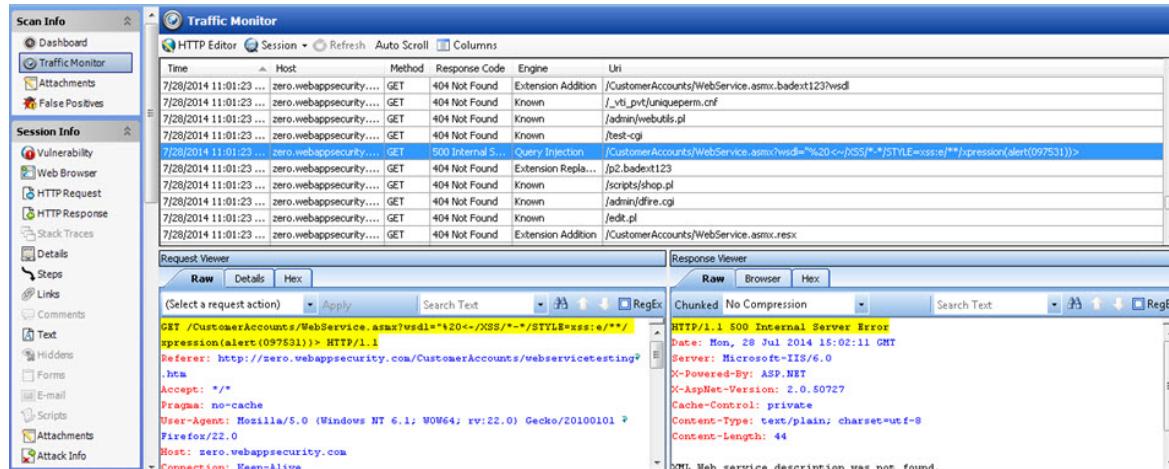
## Traffic Monitor

WebInspect displays in the **navigation pane** only the hierarchical structure of the Web site or Web service, plus those sessions in which a vulnerability was discovered. The **Traffic Monitor** selection allows you to display and review every HTTP request sent by WebInspect and the associated HTTP response received from the server.

To enable this option, click the **Edit** menu and select **Default Settings**; then, in the **Scan Settings** category, click **General** and select **Enable Traffic Monitor Logging**. Enabling this option while a scan is in progress will not activate the feature; it must be selected prior to beginning the scan.

See [Traffic Monitor](#) for additional information.

### Traffic Monitor Image



## Attachments

The **Attachments** selection displays a list of all session notes, vulnerability notes, flags for follow-up, and vulnerability screenshots that have been added to the scan. Each attachment is associated with a specific session. This form also lists scan notes (that is, notes that apply to the entire scan rather than to a specific session).

You can create a scan note, or you can edit or delete an existing attachment.

To create a scan note, click the **Add** menu (in the information display area).

To edit an attachment, select the attachment and click **Edit**.

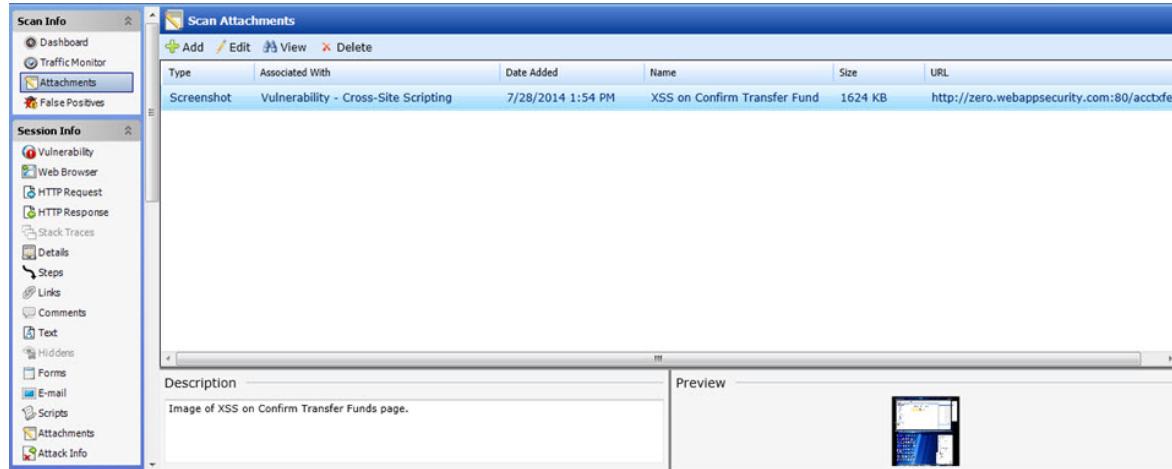
To create attachments in other area of the WebInspect user interface, you can either:

- Right-click a session in the navigation pane and select **Attachments** from the shortcut menu, or
- Right-click a URL on the **Vulnerabilities** tab of the summary pane and select **Attachments** from the shortcut menu.

WebInspect automatically adds a note to the session whenever you send a defect to HP Quality Center or IBM Rational ClearQuest.

See [Attachments - Scan Info](#) for more information.

### Attachments Image



## False Positives

This feature lists all URLs that WebInspect originally flagged as containing a vulnerability, but which a user later determined were false positives. Note that this option is not displayed until someone actually designates a vulnerability as a false positive.

Click the URL associated with a false positive to view a note that may have been entered when the user removed the vulnerability.

To reassign the vulnerability and remove the URL from the False Positive list, select a URL and click **Mark as Vulnerability**.

You can import from a previous scan a list of vulnerabilities that were identified as being false positives. WebInspect then correlates these false positives from a previous scan with vulnerabilities detected in the current scan and flags the new occurrences as false positives.

See [False Positives](#) for more information.

### False Positives Image

Risk	URL	Vulnerability	State	Source
State: Active False Positives (4 items)				
<input type="checkbox"/> Vulnerability: Backup File (Appended... .bak) (1 item)	<a href="http://zero.webappsec...">http://zero.webappsec...</a>	Backup File (Appended... Active False Positives		Site: http://zero.webappsecurity.com/ (Current Scan)
<input type="checkbox"/> Vulnerability: Possible Server Path Disclosure (unl) (1 item)	<a href="http://zero.webappsec...">http://zero.webappsec...</a>	Possible Server Path DL... Active False Positives		Site: http://zero.webappsecurity.com/ (Current Scan)
<input checked="" type="checkbox"/> Vulnerability: Form Auto Complete Active (1 item)	<a href="http://zero.webappsec...">http://zero.webappsec...</a>	Form Auto Complete A... Active False Positives		Site: http://zero.webappsecurity.com/ (Current Scan)
<input type="checkbox"/> Vulnerability: Potential filename found in comments (1 item)	<a href="http://zero.webappsec...">http://zero.webappsec...</a>	Potential filename fou... Active False Positives		Site: http://zero.webappsecurity.com/ (Current Scan)

### See Also

["Session Info Panel Overview " on page 67](#)

["Host Info Panel Overview" on page 75](#)

["User Interface Overview" on page 31](#)

["Dashboard " below](#)

["Traffic Monitor " on page 64](#)

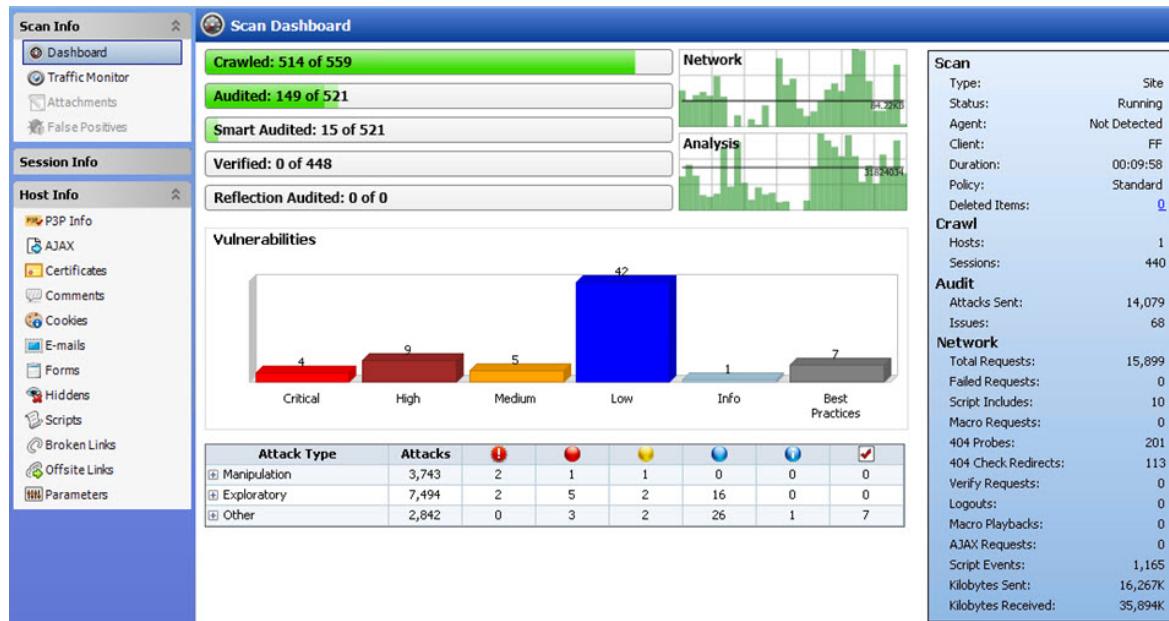
["Attachments - Scan Info " on page 65](#)

## Dashboard

The **Dashboard** selection displays a real-time summary of the scan results and a graphic representation of the scan progress.

### Dashboard Image

The following image displays the Scan Dashboard with a scan in progress.



## Progress Bars

Each bar represents the progress being made through that scanning phase.



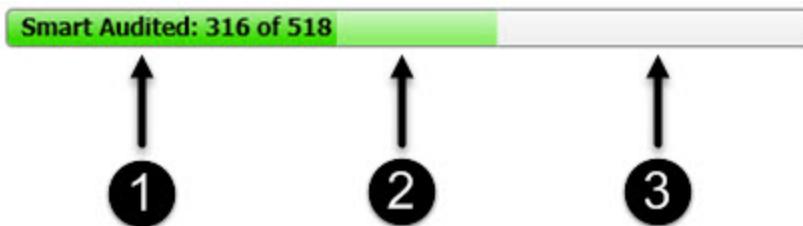
## Progress Bar Descriptions

The following table describes the progress bars:

Progress Bar	Description
<b>Crawled</b>	Number of sessions crawled / total number of sessions to crawl.
<b>Audited</b>	Number of sessions audited / total number of sessions to audit. The total number includes all checks except those pertaining to server type, which are handled by smart audit.

Progress Bar	Description
<b>Smart Audited</b>	<p>Number of sessions audited using smart audit / total number of sessions for smart audit.</p> <p>For smart audit, WebInspect detects the type of server on which the Web application is hosted. WebInspect runs checks that are specific to the server type and avoids checks that are not valid for the server type.</p>
<b>Verified</b>	<p>Number of persistent XSS vulnerable sessions verified / total number of persistent XSS vulnerable sessions to verify.</p> <p>When persistent XSS auditing is enabled, WebInspect sends a second request to all vulnerable sessions and examines all responses for probes that WebInspect previously made. When probes are located, WebInspect will record links between those pages internally.</p>
<b>Reflection Audited</b>	<p>Number of persistent XSS vulnerable linked sessions audited / total number of persistent XSS vulnerable linked sessions to audit.</p> <p>When persistent XSS auditing is enabled, this represents the work required for auditing the linked sessions found in the verification step for persistent XSS.</p>

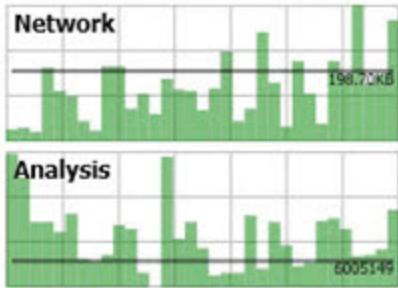
## Progress Bar Colors



1. Dark green indicates sessions that have been processed.
2. Light green indicates excluded, aborted, or rejected sessions (sessions that were considered for processing, but were skipped due to settings or other reasons).
3. Light gray indicates the unprocessed sessions.

## Activity Meters

WebInspect polls information about the activity occurring in the scan and displays the data in Activity Meters. The data presents a real-time snapshot of the scan activity. This information can help you to determine whether the scan is stalled or actively running.



## Activity Meter Descriptions

The following table describes the Activity Meters:

Meter	Description
<b>Network</b>	The amount of data being sent and received by WebInspect. The chart shows this data as B, KB, or MB sent/received over the last one second.
<b>Analysis</b>	The amount of work being done per second by WebInspect in processing all threads.

## Vulnerabilities Graphics

Graphic	Description
<b>Vulnerability Graph</b>	Total number of issues identified for the scan per severity level.
<b>Attack Stats Grid</b>	Number of attacks made and issues found, categorized by attack type and audit engine.

## Statistics Panel - Scan

Item	Description
<b>Type</b>	Type of scan: Site, Service, or Site Retest.
<b>Scan Status</b>	Status: Running, Paused, or Complete.

Item	Description
<b>Agent</b>	Refers to the WebInspect Agent and states either Detected or Not Detected. For certain checks (such as SQL injection, command execution, and cross-site scripting), WebInspect Agent intercepts WebInspect HTTP requests and conducts runtime analysis on the target module. If this analysis confirms that a vulnerability exists, WebInspect Agent appends the stack trace to the HTTP response. Developers can analyze this stack trace to investigate areas that require remediation.
<b>Client</b>	<p>The rendering engine specified for the scan. Options are:</p> <ul style="list-style-type: none"> <li>• IE (Internet Explorer)</li> <li>• FF (Firefox)</li> <li>• iPhone</li> <li>• iPad</li> <li>• Android</li> <li>• Windows Phone</li> <li>• Windows RT</li> </ul>
<b>Duration</b>	Length of time scan has been running (can be incorrect if the scan terminates abnormally).
<b>Policy</b>	Name of the policy used for the scan. For a retest, the field contains a dash ("-"), because the retest does not use the entire policy; see <a href="#">Review and Retest</a> .
<b>Deleted Items</b>	<p>The number of sessions and vulnerabilities removed by the user from the scan.</p> <p>To remove a session, right-click a session in the <a href="#">Navigation pane</a> and select <b>Remove Session</b> from the shortcut menu.</p> <p>To remove a vulnerability, right-click a vulnerability in the <a href="#">Summary pane</a> and select <b>Ignore Vulnerability</b> from the shortcut menu.</p> <p>To restore sessions or vulnerabilities that have been deleted:</p> <ol style="list-style-type: none"> <li>1. On the Scan Dashboard, click the number associated with deleted items. The Recover Deleted Items window appears.</li> <li>2. Select either <b>Vulnerabilities</b> or <b>Sessions</b> from the drop-down window.</li> <li>3. Select one or more items.</li> <li>4. Click <b>Recover</b>.</li> </ol>

## Statistics Panel - Crawl

Item	Description
<b>Hosts</b>	Number of hosts included in the scan.
<b>Sessions</b>	Total number of sessions (excluding AJAX requests, script and script frame includes, and WSDL includes).

## Statistics Panel - Audit

Item	Description
<b>Attacks Sent</b>	Total number of attacks sent.
<b>Issues</b>	Total number of issues found (all vulnerabilities, as well as best practices).

## Statistics Panel - Network

Item	Description
<b>Total Requests</b>	Total number of requests made.
<b>Failed Requests</b>	Total number of failed requests.
<b>Script Includes</b>	Total number of script includes.
<b>Macro Requests</b>	Total number of requests made as part of macro execution.
<b>404 Probes</b>	Number of file not found probes made to determine file not found status.
<b>404 Check Redirects</b>	Number of times a 404 probe resulted in a redirect.
<b>Verify Requests</b>	Requests made for detection of stored parameters.
<b>Logouts</b>	Number of times logout was detected and login macro executed.
<b>Macro Playbacks</b>	Number of times macros have been executed.
<b>AJAX Requests</b>	Total number of AJAX requests made.
<b>Script Events</b>	Total number of script events processed.
<b>Kilobytes Sent</b>	Total number of kilobytes sent.
<b>Kilobytes Received</b>	Total number of kilobytes received.

## See Also

- "Scan Info Panel Overview " on page 55
- "Session Info Panel Overview " on page 67
- "Host Info Panel Overview" on page 75

## Traffic Monitor

WebInspect normally displays in the [navigation pane](#) only the hierarchical structure of the Web site or Web service, plus those sessions in which a vulnerability was discovered. The **Traffic Monitor** allows you to display and review every HTTP request sent by WebInspect and the associated HTTP response received from the server.

To display this option, you can enable the feature in the default settings (click **Edit > Default Settings > Settings > General**) or when you start a scan through the Scan Wizard (by selecting **Enable Traffic Monitor** on the Detailed Scan Configuration window under Settings).

### Traffic Monitor Image

The screenshot shows the WebInspect interface with the 'Traffic Monitor' panel selected in the sidebar. The main area displays a table of traffic logs:

Time	Host	Method	Uri	Response Code	Engine
1/6/2011 2:53:36 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:53:37 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:53:53 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:53:53 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:53:53 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:53:53 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:54:14 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:54:14 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:54:15 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...

Below the table are two panes: 'Request Viewer' and 'Response Viewer'. The Request Viewer shows raw, details, and hex data for a selected POST request to /cda/hpdc/register.do. The Response Viewer shows raw, browser, and hex data for the corresponding HTTP/1.0 200 OK response.

## Button Functionality

Buttons at the top of the information display area are described in the following table.

Button	Description
HTTP Editor	Opens the HTTP editor loaded with the selected request and response session.

Button	Description
Session	Offers three choices: <ul style="list-style-type: none"> <li>• <b>Navigate to Session:</b> Navigate to the correlated session on this request in the site tree.</li> <li>• <b>Navigate to Parent Session:</b> Navigate to the correlated parent session on this request in the site tree.</li> <li>• <b>Highlight Parent Session:</b> Moves focus to the parent session of the selected session.</li> </ul>
Refresh	Updates display with most current information.
Auto Scroll	Automatically updates traffic monitor view with the latest traffic from WebInspect crawl and audit while scan is running. While in auto scroll mode, sorting is ascending by time, so user cannot sort without pausing the scan.
Columns	Allows user to select which traffic monitor database columns are displayed.

## See Also

["Scan Info Panel Overview " on page 55](#)

## Attachments - Scan Info

The **Attachments** selection displays a list of all session notes, vulnerability notes, flags for follow-up, and vulnerability screenshots that have been added to the scan. Each attachment is associated with a specific session. This form also lists scan notes (that is, notes that apply to the entire scan rather than to a specific session).

You can create a scan note, or you can edit or delete an existing attachment.

To view an attachment, select the attachment and click **View** (or simply double-click the attachment).

To create a scan note, click the **Add** menu (in the [information display area](#)).

To edit an attachment, select the attachment and click **Edit**. Note that screenshots cannot be edited.

These functions are also available by right-clicking an attachment and selecting an option from the shortcut menu. You may also select **Go to session**, which opens the Session Info - Attachments pane and highlights in the navigation pane the session associated with that attachment.

To create attachments in other areas of the WebInspect user interface, you can either:

- Right-click a session in the [navigation pane](#) and select **Attachments** from the shortcut menu, or
- Right-click a URL on the **Vulnerabilities** tab of the [summary pane](#) and select **Attachments** from the shortcut menu.

WebInspect automatically adds a note to the session whenever you send a defect to HP Quality Center or IBM Rational ClearQuest.

### See Also

["Scan Info Panel Overview " on page 55](#)

## False Positives

This feature lists all URLs that WebInspect originally flagged as containing a vulnerability and which a user later determined were false positives.

### Importing False Positives

You can also import from a previous scan a list of vulnerabilities that were analyzed as being false positive. WebInspect then correlates these false positives from a previous scan with vulnerabilities detected in the current scan and flags the new occurrences as false positives.

To illustrate, suppose a cross-site scripting vulnerability was detected in Scan No. 1 at URL <http://www.mysite.com/foo/bar> and, after further analysis, someone flagged it as a false positive. If you import false positives from Scan No. 1 into Scan No. 2 of [www.mysite.com](http://www.mysite.com), and if that second scan detects a cross-site scripting vulnerability at the same URL (<http://www.mysite.com/foo/bar>), then WebInspect automatically changes that vulnerability to a false positive.

### Inactive / Active False Positives Lists

Imported false positives are loaded first into a list labeled "Inactive False Positives." If a false positive in that list is matched with a vulnerability in the current scan, the item is moved from the Inactive False Positives list to the Active False Positives list. Unmatched items remain in the Inactive False Positives list.

### Loading False Positives

False positives from other scans can be manually loaded into the current scan at any time. Alternatively, you may instruct the Scan Wizard, while initiating a scan, that false positives are to be loaded from a specific file; in this case, WebInspect correlates the false positives as they are encountered during the scan. You can also see (on the scan dashboard) the false positives matched while the scan is running.

### Working with False Positives

1. Select **False Positives** from the **Scan Info** panel.
2. If necessary, click the plus sign  next to a vulnerability description to display the associated URLs and state.

3. Click a URL to view a comment (at the bottom of the Information pane) that may have been entered when the user removed the vulnerability.
4. To import false positives from other scans, click **Import False Positives**.
5. To change a false positive back to a vulnerability, select an item from the Active False Positive list and click **Mark as Vulnerability**.
6. To remove an item from the Inactive False Positive list, select the item and click **Remove From Inactive**.
7. To edit a comment associated with a false positive, select the item and click **Edit Comment**.

For information on how to designate a vulnerability as a false positive, see [Navigation Pane Shortcut menu](#) or [Summary Pane](#).

For more information on the WebInspect window, see [WebInspect User Interface](#).

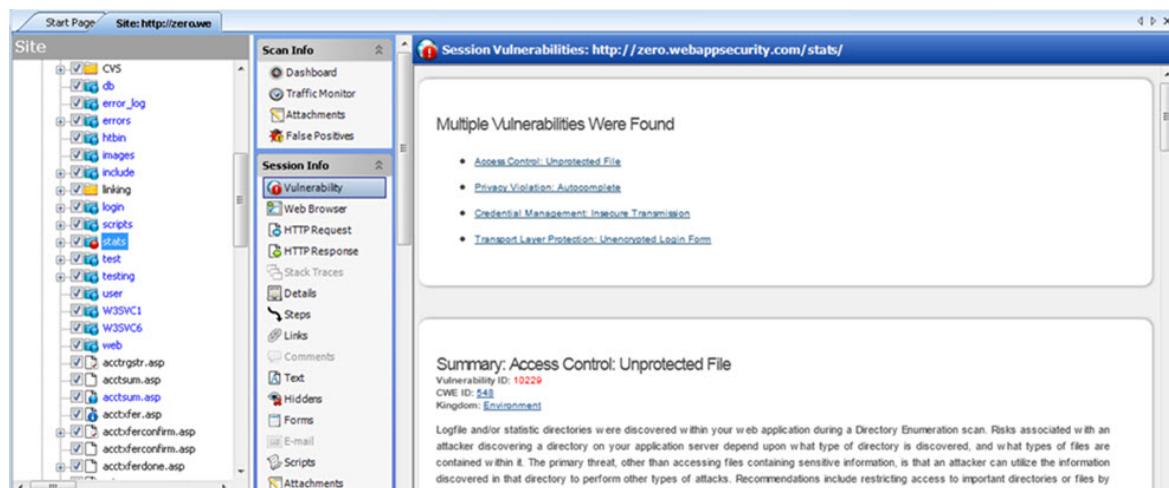
## Session Info Panel Overview

WebInspect lists each session created during a scan in the [navigation pane](#) using either the Site view or Sequence view. Select a session and then click one of the options in the **Session Info** panel to display related information about that session.

In the following example scan, WebInspect sent the HTTP request GET /stats/stats.html HTTP/1.1.

To see the vulnerability:

1. Select **Stats.html** in the navigation pane.
2. Click **Vulnerability** in the **Session Info** panel.



## Options Available

The following table lists the options available in the **Session Info** panel. Some options appear only for specific scans (Basic Scan or Web Service Scan). Also, options are enabled only if they are relevant to the selected session; for example, the **Forms** selection is not available if the session does not contain a form.

Option	Description
Vulnerability	Displays the vulnerability information for the session selected in the navigation pane.
Web Browser <sup>1</sup>	Displays the server's response as rendered by a Web browser for the session selected in the navigation pane.
HTTP Request	Displays the raw HTTP request sent by WebInspect to the server hosting the site you are scanning.
HTTP Response	<p>Displays the server's raw HTTP response to WebInspect's request.</p> <p>If the response contains one or more attack signatures (indicating that a vulnerability has been discovered) you can tab from one attack signature to the next by clicking these buttons:</p>  <p>If you select a Flash (.swf) file, WebInspect displays HTML instead of binary data. This allows WebInspect to display links in a readable format.</p>
Stack Traces	<p>This feature is designed to support WebInspect Agent when it is installed and running on the target server.</p> <p>For certain checks (such as SQL injection, command execution, and cross-site scripting), SecurityScope intercepts WebInspect HTTP requests and conducts runtime analysis on the target module. If this analysis confirms that a vulnerability exists, SecurityScope appends the stack trace to the HTTP response. Developers can analyze this stack trace to investigate areas that require remediation.</p>
Details <sup>1</sup>	<p>Lists request and response details, such as the size of the response and the request method. Note that the Response section contains two entries for content type: returned and detected. The <b>Returned Content Type</b> indicates the media type specified in the Content-Type entity-header field of the HTTP response. <b>Detected Content Type</b> indicates the actual content-type as determined by WebInspect.</p>
Steps <sup>1</sup>	Displays the route taken by WebInspect to arrive at the session selected in the navigation pane or the URL selected in the summary pane. Beginning with the parent session (at the top of the list), the sequence reveals the subsequent URLs visited and provides details about the scan methodology.

Option	Description
Links <sup>1</sup>	This option lists (under Linked From) all resources at the target site that contain links to the selected resource. The links may be rendered by HTML tags, scripts, or HTML forms. It also lists (under Linked To) all resources that are referenced by links within the HTTP response for the selected session.
Comments <sup>1</sup>	Displays all comments (in HTML) embedded in the HTTP response.
Text <sup>1</sup>	Displays all text contained in the HTTP response for the session selected in the <a href="#">navigation pane</a> .
Hiddens <sup>1</sup>	Displays the name attribute of each input element whose control type is "hidden."
Forms <sup>1</sup>	Displays the HTML interpreted by the browser to render forms.
E-mail <sup>1</sup>	Displays all e-mail addresses included in the response.
Scripts <sup>1</sup>	Displays all client-side scripts embedded in the server's response.
Attachments	<p>Displays all notes, flags, and screenshots associated with the selected object.</p> <p>To create an attachment, you can either:</p> <ul style="list-style-type: none"> <li>• Right-click a session (Basic or Guided Scan) or an operation or vulnerability (Web service scan) in the navigation pane and select <b>Attachments</b> from the shortcut menu, or</li> <li>• Right-click a URL on the <b>Vulnerabilities</b> tab of the <a href="#">summary pane</a> and select <b>Attachments</b> from the shortcut menu, or</li> <li>• Select a session (Basic Scan) or an operation or vulnerability (Web service scan) in the navigation pane, then select <b>Attachments</b> from the <b>Session Info</b> panel and click the <b>Add</b> menu (in the information pane).</li> </ul> <p>WebInspect automatically adds a note to the session information whenever you send a defect to HP Quality Center or IBM Rational ClearQuest.</p>
Attack Info <sup>1</sup>	Displays the attack sequence number, URL, name of the audit engine used, and the result of the vulnerability test. Attack information is usually associated with the session in which the attack was created and not with the session in which it was detected. If attack information does not appear for a selected vulnerable session, select the parent session and then click <b>Attack Info</b> .
XML Request <sup>2</sup>	Displays the SOAP envelope embedded in the request (available when selecting an operation during a Web Service Scan).
XML Response <sup>2</sup>	Displays the SOAP envelope embedded in the response (available when selecting an operation during a Web Service Scan).
Web Service Request <sup>2</sup>	Displays the web service schema and values embedded in the request (available when selecting an operation during a Web Service Scan).

Option	Description
Web Service Response <sup>2</sup>	Displays the web service schema and values embedded in the response (available when selecting an operation during a Web Service Scan).

<sup>1</sup> Basic or Guided Scan only

<sup>2</sup> Web Service Scan only

Most options provide a Search feature at the top of the information pane, allowing you to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

**Tip:** If you follow a link when viewing the vulnerability information, click the highlighted session in the navigation pane to return.

## See Also

["User Interface Overview" on page 31](#)

["Scan Info Panel Overview " on page 55](#)

["Host Info Panel Overview" on page 75](#)

## Vulnerability

This option displays the vulnerability information for the session selected in the [navigation pane](#) or for the vulnerability selected in the [summary pane](#). It typically includes a description of the vulnerability, vulnerability ID, Common Weakness Enumeration (CWE) ID, Kingdom, implications (how this vulnerability may affect you), and instructions on how to fix the vulnerability.

## Web Browser

This option displays the server's response as rendered by a Web browser for the session selected in the [navigation pane](#).

## HTTP Request

This option displays the raw HTTP request (for the session selected in the [navigation pane](#)) sent by WebInspect to the server hosting the site you are scanning.

## HTTP Response

This option displays the server's raw HTTP response to WebInspect's request, for the session selected in the [navigation pane](#).

If the response contains one or more attack signatures (indicating that a vulnerability has been discovered) you can tab from one attack signature to the next by clicking these buttons:



If you select a Flash (.swf) file, WebInspect displays HTML instead of binary data. This allows WebInspect to display links in a readable format.

## Stack Traces

This feature is designed to support WebInspect Agent when it is installed and running on the target server.

For certain checks (such as SQL injection, command execution, and cross-site scripting), WebInspect Agent intercepts WebInspect HTTP requests and conducts runtime analysis on the target module. If this analysis confirms that a vulnerability exists, WebInspect Agent appends the stack trace to the HTTP response. Developers can analyze this stack trace to investigate areas that require remediation.

## Details

This option lists request and response details, such as the size of the response and the request method, for the session selected in the [navigation pane](#).

Note that the Response section contains two entries for content type: returned and detected. The **Returned ContentType** indicates the media type specified in the Content-Type entity-header field of the HTTP response. **Detected ContentType** indicates the actual content-type as determined by WebInspect.

## Steps

This option displays the route taken by WebInspect to arrive at the session selected in the [navigation pane](#) or the URL selected in the [summary pane](#). Beginning with the parent session (at the top of the list), the sequence reveals the subsequent URLs visited and provides details about the scan methodology.

### See Also

["Session Info Panel Overview " on page 67](#)

## Links

This option lists (under Linked From) all resources at the target site that contain links to the selected resource. The links may be rendered by HTML tags, scripts, or HTML forms.

It also lists (under Linked To) all resources that are referenced by links within the HTTP response for the selected session.

If you double-click a listed link, WebInspect shifts focus in the [navigation pane](#) to the referenced session. Alternatively, you can browse to the linked resource by viewing the session in the Web browser (click **Web Browser**).

## Comments: Session Info

This option displays all comments embedded in the HTTP response for the session selected in the [navigation pane](#).

Developers sometimes leave critical information in comments that can be used to breach the security of a site. For example, something as seemingly innocuous as a comment referencing the required order of fields in a table could potentially give an attacker a key piece of information needed to compromise the security of your site.

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy comments to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

For more information on the WebInspect window, see [WebInspect User Interface](#).

## Text

This option displays all text contained in the HTTP response for the session selected in the [navigation pane](#).

## Hiddens: Session Info

WebInspect analyzes all forms and then lists all controls of the type "hidden" (i.e., controls that are not rendered but whose values are submitted with a form). Developers often include parameters in hidden controls that can be edited and resubmitted by an attacker.

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy the HTML text to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

For more information on the WebInspect window, see [WebInspect User Interface](#).

## Forms: Session Info

WebInspect lists all HTML forms discovered for the session selected in the [navigation pane](#).

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy forms to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

For more information on the WebInspect window, see [WebInspect User Interface](#).

## E-Mail

WebInspect lists all e-mail addresses contained in the session selected from the [navigation pane](#).

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy e-mail addresses to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

For more information on the WebInspect window, see [WebInspect User Interface](#).

## Scripts - Session Info

WebInspect lists all scripts discovered in a session.

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy the script to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

For more information on the WebInspect window, see [WebInspect User Interface](#).

## Attachments - Session Info

You can associate the following attachments with a session:

- Session Note
- Flag Session for Follow Up
- Vulnerability Note
- Vulnerability Screenshot

**Note:** You can also associate a note with a scan and view all attachments that have been added to the scan by selecting **Attachments** in the **Scan Info** panel.

The **Attachments** selection displays a list of all notes, flags, and screenshots that have been associated with the selected session.

## Viewing an Attachment

To view an attachment:

- Select the attachment and click **View** (or simply double-click the attachment).

## Adding a Session Attachment

To add a session attachment:

1. Select a session:
  - On the **Vulnerabilities** tab or the **Information** tab in the **Summary pane**, right-click a vulnerable URL, or
  - On the **Navigation pane**, right-click a session or URL.
2. On the shortcut menu, click **Attachments** and select an attachment type.

**Note:** An alternative method is to select a session in the Navigation pane, click **Attachments** in the **Session Info** panel, and then select a command from the **Add** menu (in the **information display area**).

3. Enter a comment related to the type of attachment you selected.
4. Select the check box next to one or more vulnerabilities.
5. If you selected **Vulnerability Screenshot**:
  - a. Enter a name for the screenshot in the **Name** box. Maximum length is 40 characters.
  - b. Click the Browse button  to locate the graphic file or, if you captured the image in memory, click **Copy from Clipboard**.
6. Click **OK**.

## Editing an Attachment

To edit an attachment:

1. Do one of the following:
  - To view all attachments that have been added to the scan, click **Attachments** in the **Scan Info** panel.
  - To view only those attachments that have been added to a specific session, click **Attachments** in the **Session Info** panel and then click a session in the Navigation pane. You can also select a URL in the Summary pane.
2. Select an attachment and click **Edit**.
3. Modify the comments as required.  
*Note:* Screenshot attachments cannot be edited.
4. Click **OK**.

**Tip:** Add, Edit, View, and Delete functions are also available by right-clicking an attachment in the information display area and selecting an option from the shortcut menu.

## Attack Info

For the session selected in the [navigation pane](#), this option displays the attack sequence number, URL, name of the audit engine used, and the result of the vulnerability test.

Attack information is usually associated with the session in which the attack was created and not with the session in which it was detected. If attack information does not appear for a selected vulnerable session, select the parent session and then click **Attack Info**.

Also, attack information for non-vulnerable sessions will not appear unless you have enabled the appropriate session storage option in the default settings; see [Session Storage](#) for more information.

## Web Service Request

This option displays the web service schema and values embedded in the request (available when selecting an operation during a Web Service Scan). It is available only during a Web Service scan.

## Web Service Response

This option displays the web service schema and values embedded in the response (available when selecting an operation during a Web Service Scan). It is available only during a Web Service scan.

## XML Request

This option displays the associated XML schema embedded in the selected request (available when selecting the WSDL object during a Web Service scan).

## XML Response

This option displays the associated XML schema embedded in the response for the session selected in the [navigation pane](#) (available when selecting the WSDL object during a Web Service scan).

## Host Info Panel Overview

When you click any item listed in this collapsible panel, WebInspect displays all instances of that item type that were discovered during a crawl or audit of the site (or host).

If you double-click an item, WebInspect highlights in the [navigation pane](#) the session that contains that item. You can copy items (such as e-mail addresses) to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

In most cases, you can use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using regular expressions, select the **Regex** button before clicking **Find**.

**Note:** The Host Info panel is not displayed when conducting a Web Service scan.

In the following illustration, selecting **Cookies** displays a list of all sessions in which cookies were detected. If you select an item from the list, WebInspect displays the cookies associated with the selected session.

### Host Info Panel Image

The screenshot shows the WebInspect interface with the 'Host Info' panel selected in the left sidebar. The main pane displays a table titled 'Host Cookies: http://zero.webappsecurity.com:80 (173)'. The table has columns for 'Source', 'URL', and 'Post Data'. Several rows are listed, including 'Start Macro', 'Html', 'Cookie Param Manipulation', 'Search', 'Path Truncation', and multiple entries for 'Html' with different URLs. Below the table, three cookie definitions are shown in the format 'Set-Cookie: [attribute] = [value]; path=/':

```

Set-Cookie: Keyed=Var2=Second+Value&Var1=First+Value; path=/
Set-Cookie: Second=Oatmeal+Chocolate; path=/
Set-Cookie: FirstCookie=Chocolate+Chip; path=/

```

### Options Available

Option	Description
P3P Info	Displays Platform for Privacy Preferences Project (P3P) information. <a href="#">Details</a> .
AJAX	Displays a list of all pages containing an AJAX engine, as well as the AJAX requests. <a href="#">Details</a> .
Certificates	Displays a list of all certificates associated with the site. <a href="#">Details</a> .
Comments	Displays a list of all URLs containing comments. <a href="#">Details</a> .
Cookies	Displays a list of all URLs containing cookies. <a href="#">Details</a> .
E-Mails	Displays a list of all URLs containing e-mail addresses in the response. <a href="#">Details</a> .
Forms	Displays a list of all URLs containing forms. <a href="#">Details</a> .
Hiddens	Displays a list of all URLs containing input elements whose control type is "hidden." <a href="#">Details</a> .

Option	Description
Scripts	Displays a list of all URLs containing client-side scripts embedded in the server's response. <a href="#">Details</a> .
Broken Links	Displays a list of all URLs containing hyperlinks to missing targets. <a href="#">Details</a> .
Offsite Links	Displays a list of all URLs containing hyperlinks to other sites. <a href="#">Details</a> .
Parameters	Displays a list of all URLs containing embedded parameters. <a href="#">Details</a> .

**See Also**

["Scan Info Panel Overview" on page 55](#)

## P3P Info

This option displays Platform for Privacy Preferences Project (P3P) information.

The World Wide Web Consortium's P3P enables Web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit.

A P3P-compliant Web site declares in a policy the kind of information it collects and how that information will be used. A P3P-enabled Web browser can decide what to do by comparing this policy with the user's stored preferences. For example, a user may set browser preferences so that information about their browsing habits should not be collected. When the user subsequently visits a Web site whose policy states that a cookie is used for this purpose, the browser automatically rejects the cookie.

## P3P User Agents

Microsoft Internet Explorer 6 can display P3P privacy policies and compare the P3P policy with your own settings to decide whether or not to allow cookies from a particular site.

The [Privacy Bird](#) (originally developed by AT&T) is a fully featured P3P user agent that automatically searches for privacy policies at every Web site the user visits. It then compares the policy with the user's stored privacy preferences and notifies the user of any discrepancies.

**See Also**

["Host Info Panel Overview" on page 75](#)

## AJAX

AJAX is an acronym for **A**synchronous **J**ava**S**cript **a**nd **X**ML**H**ttp**R**equest.

If you select this option, WebInspect displays all pages containing an AJAX engine, as well as the AJAX requests.

Type	URL
AJAX Page	http://officerdoofy:80/SampleWebSite/AlwaysVisibleControl/AlwaysVisibleControl.aspx
AJAX Page	http://officerdoofy:80/SampleWebSite/HoverMenu/HoverMenu.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/NumericUpDown/NumericUpDown.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/PopupControl/PopupControl.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/Rating/Rating.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/ReorderList/ReorderList.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/TextBoxWatermark/TextBoxWatermark.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/ToggleButton/ToggleButton.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/UpdatePanelAnimation/UpdatePanelAnimation.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/ValidatorCallout/ValidatorCallout.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/AlwaysVisibleControl/AlwaysVisibleControl.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/CascadingDropDown/CascadingDropDown.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/ConfirmButton/ConfirmButton.aspx
AJAX Page	http://officerdoofy:80/Sample Web Site/DropDown/DropDown.aspx

This page uses AJAX in script

There are two types of AJAX line items in this view:

- AJAX Page (as illustrated above)
- Request

If you click an item in the list, WebInspect displays "This page uses AJAX in script" (for a Page type) or it lists the query and/or POST data parameters (for a Request type).

## How AJAX Works

AJAX is not a technology per se, but a combination of existing technologies, including HTML or XHTML, Cascading Style Sheets, JavaScript, the Document Object Model, XML, XSLT, and the XMLHttpRequest object. When these technologies are combined in the AJAX model, Web applications are able to make quick, incremental updates to the user interface without reloading the entire browser page.

Instead of loading a Web page at the start of the session, the browser loads an AJAX engine that is responsible for both rendering the user interface and communicating with the server. Every user action that normally would generate an HTTP request takes the form of a JavaScript call to the AJAX engine instead. Any response to a user action that does not require communication with the server (such as simple data validation, editing data in memory, and even some navigation) is handled by the engine. If the engine needs to communicate with the server — submitting data for processing, loading additional interface code, or retrieving new data — the engine makes those requests asynchronously, usually using XML, without stalling a user's interaction with the application.

## Certificates

A certificate states that a specific Web site is secure and genuine. It ensures that no other Web site can assume the identity of the original secure site. A security certificate associates an identity with a public key. Only the owner of the certificate knows the corresponding private key, which allows the owner to make a "digital signature" or decrypt information encrypted with the corresponding public key.

## Comments - Host Info

Developers sometimes leave critical information in comments that can be used to breach the security of a site. For example, something as seemingly innocuous as a comment referencing the required order of fields in a table could potentially give an attacker a key piece of information needed to compromise the security of your site.

1. Select **Comments** from the **Host Info** panel to list all URLs that contain comments.
2. Click a **URL** to view the comments it contains.
3. Double-click an entry to locate in the [navigation pane](#) the session that contains the comment.  
Focus switches to the **Comments** choice in the **Session Info** panel.

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy comments to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

If you double-click a URL, WebInspect highlights in the [navigation pane](#) the session that contains the URL.

For more information on the WebInspect window, see [WebInspect User Interface](#).

### See Also

["Host Info Panel Overview" on page 75](#)

## Cookies

A cookie contains information (such as user preferences or configuration information) stored by a server on a client for future use. Cookies appear in two basic forms: as individual files or as records within one contiguous file. Often, there are multiple sets, the result of multiple browsers being installed in differing locations. In many cases, "forgotten" cookies contain revealing information that you would prefer others not see.

1. Select **Cookies** from the **Host Info** panel to list all URLs in which cookies were found during a crawl or audit.
2. Click a URL to view the cookies it contains.

3. Double-click an entry to locate in the [navigation pane](#) the session that contains the cookie. Focus switches to the **HTTP Response** choice in the **Session Info** panel.

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy cookie code to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

If you double-click a URL, WebInspect highlights in the [navigation pane](#) the session that contains the URL.

For more information on the WebInspect window, see [WebInspect User Interface](#).

#### See Also

["Host Info Panel Overview" on page 75](#)

## E-Mails - Host Info

WebInspect lists all e-mail addresses discovered during a scan.

1. Select **E-mail** from the **Host Info** panel to list all URLs that contain e-mail addresses.
2. Click a URL to view the e-mail addresses it contains.
3. Double-click an entry to locate in the [navigation pane](#) the session that contains the e-mail address. Focus switches to the **E-mail** choice in the **Session Info** panel.

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy e-mail addresses to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

If you double-click a URL, WebInspect highlights in the [navigation pane](#) the session that contains the URL.

For more information on the WebInspect window, see [WebInspect User Interface](#).

#### See Also

["Host Info Panel Overview" on page 75](#)

## Forms - Host Info

WebInspect lists all HTML forms discovered during a scan.

1. Select **Forms** from the **Host Info** panel to list all URLs that contain forms.
2. Click a URL to view the source HTML of the form it contains.

3. Double-click an entry to locate in the [navigation pane](#) the session that contains the form. Focus switches to the Forms choice in the **Session Info** panel.

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy forms to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

If you double-click a URL, WebInspect highlights in the [navigation pane](#) the session that contains the URL.

For more information on the WebInspect window, see [WebInspect User Interface](#).

#### See Also

["Host Info Panel Overview" on page 75](#)

## Hiddens - Host Info

WebInspect analyzes all forms and then lists all controls of the type "hidden" (i.e., controls that are not rendered but whose values are submitted with a form). Developers often include parameters in hidden controls that can be edited and resubmitted by an attacker.

1. Select **Hiddens** from the **Host Info** panel to list all URLs that contain hidden controls.
2. Click a URL to view the name and value attributes of the "hidden" controls contained in that URL.
3. Double-click an entry to locate in the [navigation pane](#) the session that contains the hidden control. Focus switches to the **Hiddens** choice in the **Session Info** panel.

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy the HTML text to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

If you double-click a URL, WebInspect highlights in the [navigation pane](#) the session that contains the URL.

For more information on the WebInspect window, see [WebInspect User Interface](#).

#### See Also

["Host Info Panel Overview" on page 75](#)

## Scripts - Host Info

WebInspect lists all e-mail addresses discovered during a scan.

1. Select **E-mail** from the **Host Info** panel to list all URLs that contain e-mail addresses.
2. Click a URL to view the e-mail addresses it contains.
3. Double-click an entry to locate in the [navigation pane](#) the session that contains the e-mail address.  
Focus switches to the **E-mail** choice in the **Session Info** panel.

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy e-mail addresses to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

If you double-click a URL, WebInspect highlights in the [navigation pane](#) the session that contains the URL.

For more information on the WebInspect window, see [WebInspect User Interface](#).

#### See Also

["Host Info Panel Overview" on page 75](#)

## Broken Links

WebInspect finds and documents all non-working hyperlinks on the site.

1. Select **Broken Links** from the **Host Info** panel to list all URLs that contain non-working hyperlinks.
2. Double-click an entry to locate in the [navigation pane](#) the session that contains a broken link.  
Focus switches to the **HTTP Response** choice in the **Session Info** panel.

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy the HTML text to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

If you double-click a URL, WebInspect highlights in the [navigation pane](#) the session that contains the URL.

For more information on the WebInspect window, see [WebInspect User Interface](#).

#### See Also

["Host Info Panel Overview" on page 75](#)

## Offsite Links

WebInspect finds and documents all hyperlinks to other sites.

1. Select **Offsite Links** from the **Host Info** panel to list all URLs that contain hyperlinks to other sites.
2. Double-click an entry to locate in the [navigation pane](#) the session that contains the offsite link. Focus switches to the **HTTP Response** choice in the **Session Info** panel.

Use the **Search** feature at the top of the information pane to locate the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy the HTML text to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

If you double-click a URL, WebInspect highlights in the [navigation pane](#) the session that contains the URL.

For more information on the WebInspect window, see [WebInspect User Interface](#).

#### See Also

["Host Info Panel Overview" on page 75](#)

## Parameters

A parameter can be either of the following:

- A query string submitted as part of the URL in the HTTP request (or contained in another header).
- Data submitted using the Post method.

To list all URLs that contain parameters:

1. Select **Parameters** from the **Host Info** panel.
2. Click a URL to view the parameters it contains.
3. Double-click an entry to locate in the [navigation pane](#) the session that contains the parameter.

Use the **Search** feature at the top of the information pane to search the selected URL for the text you specify. To conduct a search using [regular expressions](#), select the **Regex** button before clicking **Find**.

You can copy text to your clipboard by highlighting the text and selecting **Copy** from the shortcut menu.

If you double-click a URL, WebInspect highlights in the [navigation pane](#) the Session that contains the URL.

For more information on the WebInspect window, see [WebInspect User Interface](#).

#### See Also

["Host Info Panel Overview" on page 75](#)

## Summary Pane

When conducting or viewing a scan, use the horizontal summary pane at the bottom of the window to view a centralized display of vulnerable resources, quickly access vulnerability information, and view WebInspect logging information.

**Note:** You can also group and filter results on all tabs except **Scan Log**. For more information, see [Using Filters and Groups in the Summary Pane](#).

The screenshot shows the WebInspect interface with the 'Summary' tab selected. At the top, there are two tabs: 'Severity' (selected) and 'Check'. A search bar labeled 'Type filter criteria...' is positioned above the main table. The main area is a grid table with columns: Path, Method, Vuln Param, Parameters, Pending Status, and Published Stat. The rows are grouped by audit check. The first group, 'Check:Backup File (cgi.zip) (3 items)', contains three entries for URLs like 'http://zero.webappsecurity.com/admin/cgi.zip'. The second group, 'Check:Cross-Site Scripting (36 items)', contains two entries for URLs like 'http://zero.webappsecurity.com/acctxferconfirm.asp'. The bottom of the pane features a navigation bar with tabs: Vulnerabilities (selected), Not Found, Information, Best Practices, Scan Log, and Server Information.

Path	Method	Vuln Param	Parameters	Pending Status	Published Stat	
Check:Backup File (cgi.zip) (3 items)						
http://zero.webappsecurity.com/admin/cgi.zip	GET	-	?	Unknown	None	
http://zero.webappsecurity.com/cgi.zip	GET	-	?	Unknown	None	
http://zero.webappsecurity.com/test/cgi.zip	GET	-	?	Unknown	None	
Check:Cross-Site Scripting (36 items)						
http://zero.webappsecurity.com/acctxferconfirm.asp	POST	fromAcct	(Post)from...	?	Unknown	None
http://zero.webappsecurity.com/acctxferconfirm.asp	POST	amount	(Post)from...	?	Unknown	None

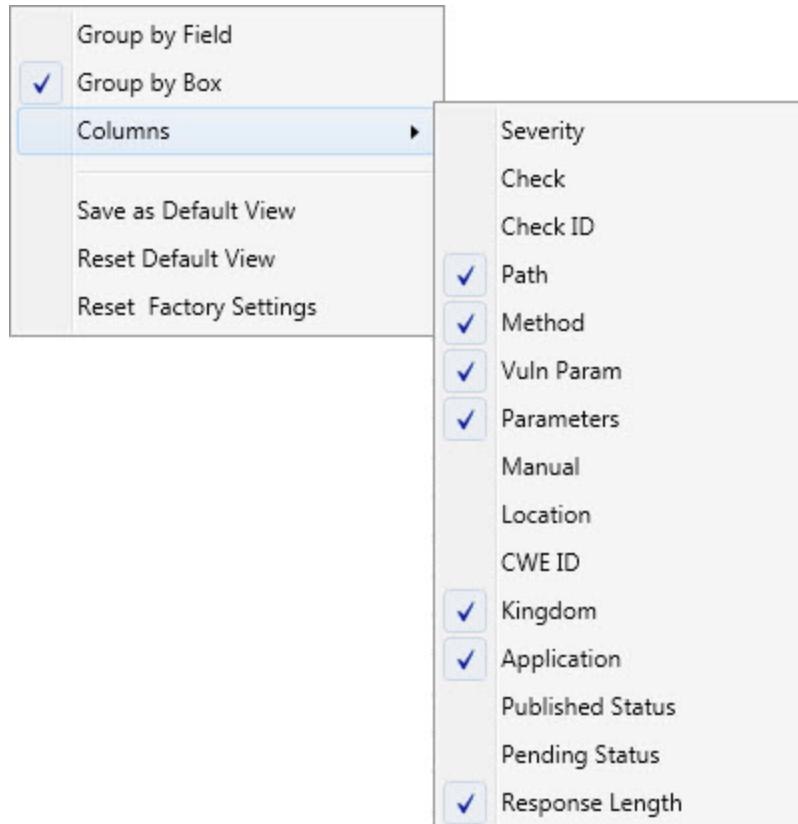
This pane has the following tabs:

- [Vulnerabilities](#)
- [Not Found](#)
- [Information](#)
- [Best Practices](#)
- [Scan Log](#)
- [Server Information](#)

## Vulnerabilities Tab

The **Vulnerabilities** tab lists information about each vulnerability discovered during an audit of your Web presence.

To select the information you want to display, right-click the column header bar and choose **Columns** from the shortcut menu.



The available columns are:

- **Severity:** A relative assessment of the vulnerability, ranging from low to critical. See below for associated icons.
- **Check:** A WebInspect probe for a specific vulnerability, such as cross-site scripting, unencrypted log-in form, etc.
- **Check ID:** The identification number of a WebInspect probe that checks for the existence of a specific vulnerability. For example, Check ID 742 tests for database server error messages.
- **Path:** The hierarchical path to the resource.
- **Method:** The HTTP method used for the attack.
- **Stack:** Stack trace information obtained from SecurityScope. Column is available only when SecurityScope is enabled during scan.
- **Vuln Param:** The name of the vulnerable parameter.
- **Parameters:** Names of parameters and values assigned to them.
- **Manual:** Displays a check mark if the vulnerability was manually created.

- **Duplicates:** Vulnerabilities detected by SecurityScope that are traceable to the same source. Column is available only when SecurityScope is enabled during scan.
- **Location:** Path plus parameters.
- **CWE ID:** The Common Weakness Enumeration identifier(s) associated with the vulnerability.
- **Kingdom:** The category in which this vulnerability is classified, using a taxonomy of software security errors developed by the HP Fortify Software Security Research Group.
- **Application:** The application or framework in which the vulnerability is found, such as ASP.NET or Microsoft IIS server.
- **Pending Status:** The status (assigned automatically by WebInspect or manually) if this scan were to be published.
- **Published Status:** The status as it exists in Software Security Center, if previously published.
- **Reproducible:** Values may be Reproduced, Not Found/Fixed, or New. Column is available for Site Retests only (Retest Vulnerabilities).
- **Response Length:** The response size in bytes for the vulnerable session.

The severity of vulnerabilities is indicated by the following icons.

Critical	High	Medium	Low

If you click an item in the list, the program highlights the related session in the [navigation pane](#) and displays associated information in the [information pane](#).

With a session selected, you can also view associated information by selecting an option from the [Session Info](#) panel.

For Post and Query parameters, click an entry in the **Parameters** column to display a more readable synopsis of the parameters.

If you right-click an item in the list, a shortcut menu allows you to:

- **Copy URL** - Copies the URL to the Windows clipboard.
- **Copy Selected Item(s)** - Copies the text of selected items to the Windows clipboard.
- **Copy All Items** - Copies the text of all items to the Windows clipboard.
- **Export** - Creates a comma-separated values (csv) file containing either all items or selected items and displays it in Microsoft Excel.
- **View in Browser** - Renders the HTTP response in a browser.

- **Filter by Current Value** - Restricts the display of vulnerabilities to those that satisfy the criteria you select. For example, if you right-click on "Post" in the Method column and then select **Filter by Current Value**, the list displays only those vulnerabilities that were discovered by sending an HTTP request that used the Post method.

**Note:** The filter criterion is displayed in the combo box in the upper right corner of the summary pane. Alternatively, you can manually enter or select a filtering criterion using this combo box. For additional details and syntax rules, see [Using Filters and Groups in the Summary Pane](#).

- **Modify Publish Status** - Change the status of a vulnerability/issue before publishing to HP Fortify Software Security Center. This command is available only when connected to WebInspect Enterprise.
- **Change Severity** - Allows you to change the severity level.
- **Edit Vulnerability** - Displays the [Edit Vulnerabilities dialog](#), allowing you to modify various vulnerability characteristics.
- **Review Vulnerability** - Allows you to retest the vulnerable session, mark it as false positive or ignored, or send it to HP Quality Center or IBM Rational ClearQuest. For more information, see [Vulnerability Review](#). This option is also invoked if you double-click a vulnerability.
- **Mark as** - Flags the vulnerability as either a false positive (and allows you to add a note) or as ignored. In both cases, the vulnerability is removed from the list. You can view a list of all false positives by selecting **False Positives** in the Scan Info panel. You can view a list of false positives and ignored vulnerabilities by selecting Dashboard in the Scan Info panel, and then clicking the hyperlinked number of deleted items in the statistics column.

**Note:** You can recover "false positive" and "ignored" vulnerabilities. See [Recover Deleted Items](#) for details.

- **Send to** - Converts the vulnerability to a defect and adds it to the HP Quality Center or IBM Rational ClearQuest database.
- **Remove Location** - Removes the selected session from the navigation pane (both Site and Sequence views) and also removes any associated vulnerabilities.

**Note:** You can recover removed locations (sessions) and their associated vulnerabilities. See [Recover Deleted Items](#) for details.

- **Crawl** - Recrawls the selected URL.
- **Tools** - Presents a submenu of available tools.
- **Attachments** - Allows you to create a note associated with the selected session, flag the session for follow-up, add a vulnerability note, or add a vulnerability screenshot.

If you right-click a group heading, a shortcut menu allows you to:

- **Collapse/Expand All Groups**
- **Collapse/Expand Group**
- **Copy Selected Item(s)**
- **Copy All Items**
- **Change Severity**
- **Mark as**
- **Send to**
- **Remove Location**

## Not Found Tab

This tab appears only after connecting to WebInspect Enterprise and after synchronizing a scan with Software Security Center. It lists vulnerabilities that were detected by a previous scan in a specific project version, but were not detected by the current scan. These vulnerabilities are not included in counts on the dashboard and are not represented in the site or sequence view of the navigation pane.

The shortcut menu options, grouping, and filtering capabilities are a subset of those described for the **Vulnerabilities** tab.

## Information Tab

The **Information** tab lists information discovered during a WebInspect scan. These are not considered vulnerabilities, but simply identify interesting points in the site or certain applications or Web servers. When you click a listed URL, the program highlights the related item in the navigation pane.

The shortcut menu options, grouping, and filtering capabilities are the same as described for the **Vulnerabilities** tab.

## Best Practices Tab

The **Best Practices** tab lists issues detected by WebInspect that relate to commonly accepted best practices for Web development. Items listed here are not vulnerabilities, but are indicators of overall site quality and site development security practices (or lack thereof).

The shortcut menu options, grouping, and filtering capabilities are the same as described for the **Vulnerabilities** tab.

## Scan Log Tab

Use the **Scan Log** tab to view information about your WebInspect scan action. For instance, the time at which certain audit methodologies are applied against your Web presence are listed here.

The screenshot shows the Scan Log tab interface. At the top, there are three filtering buttons: Error (checked), Warnings (unchecked), and Messages (unchecked). Below the buttons is a table with three columns: Time, Level, and Message. The Time column shows dates from June 27, 2012, at 8:19:25 AM to 8:21:16 AM. The Level column shows Info for all entries. The Message column contains log messages related to the scan start, scanner retry, recommendation modules, and various recommendation modules starting and completing. At the bottom of the table are navigation buttons: Vulnerabilities, Not Found, Information, Best Practices, Scan Log (selected), and Server Information.

Time	Level	Message
6/27/2012 8:19:25 AM	Info	Scan Start, ScanID:941fb508-4d44-4ea9-a3d3-0861c7367b2f Version:9.30.43.0, Location:C:\...
6/27/2012 8:21:15 AM	Info	Scanner Retry Start:
6/27/2012 8:21:15 AM	Info	Scanner Retry Stop:
6/27/2012 8:21:16 AM	Info	Recommendation Modules Started:
6/27/2012 8:21:16 AM	Info	Starting Recommendation Module: Web Macro:
6/27/2012 8:21:16 AM	Info	Starting Recommendation Module: Network Authentication:
6/27/2012 8:21:16 AM	Info	Starting Recommendation Module: File Not Found:
6/27/2012 8:21:16 AM	Info	Completed Recommendation Module: File Not Found:
6/27/2012 8:21:16 AM	Info	Completed Recommendation Module: Network Authentication:
6/27/2012 8:21:16 AM	Info	Starting Recommendation Module: Web Service:

! Vulnerabilities   
 ? Not Found   
 i Information   
 x Best Practices   
 s Scan Log   
 s Server Information

You can select the logging level (Debug, Info, Warn, Error, or Fatal) using the Logging option on the [Application Settings window](#).

You can filter the type of messages displayed using the **Errors**, **Warnings**, and **Messages** buttons at the top of the pane. To view detailed information about a specific entry in the scan log, select an entry and then click **Detail**.

You can also right-click an entry and select the following options from the shortcut menu:

- Copy selected row to clipboard.
- Copy all items to clipboard.
- Get more information about this message.

## Server Information Tab

This tab lists items of interest pertaining to the server. Only one occurrence of an item or event is listed per server.

### See Also

["User Interface Overview" on page 31](#)

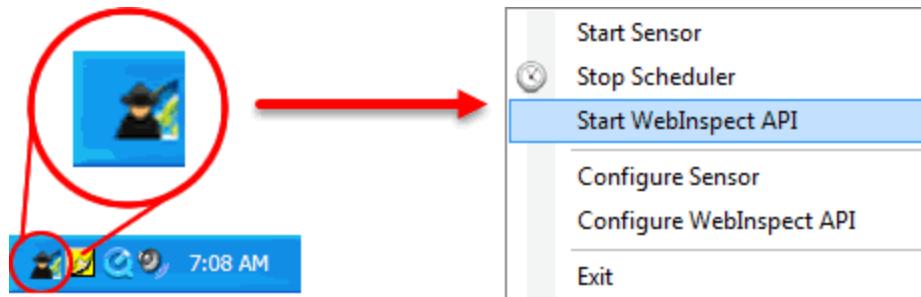
["Using Filters and Groups in the Summary Pane" on page 196](#)

["Reviewing a Vulnerability " on page 201](#)

## Fortify Monitor

The HP Fortify program, represented by an icon in the notification area of the taskbar, provides a context menu that allows you to:

- Start/stop the sensor service
- Start/stop the scheduler service
- Configure Enterprise Server sensor
- Start/configure the WebInspect API



Pop-up messages also appear whenever certain events occur.

This feature is provided primarily for users who install WebInspect as a standalone scanner, but subsequently want to connect to WebInspect Enterprise.

## Guided Scan Overview

Guided Scan directs you through the best steps for configuring a scan tailored to your application.

The first time you initiate a Guided Scan, WebInspect launches a tutorial. You can close the tutorial at any time, or click Tutorial in the top right corner or the wizard screen to launch the tutorial.

The Guided Scan progress display in the left pane allows you to easily see your progress as you specify settings for your scan. The right pane displays the scan options on each wizard page.

The Guided Scan Wizard allows you to:

- Verify connectivity to your application
- Test the entire application or only workflows
- Record your login procedure
- Review suggested configuration changes
- Explore your application to ensure proper coverage

Guided Scans are template based; you can select to use either a Predefined Template or a Mobile Template.

## Predefined Templates

There are three predefined templates options to choose from:

- **Standard Scan:** use this option to when you are interested in coverage. Larger sites could take days when using this template.
- **Quick Scan:** use this option when focusing on breadth and performance rather than digging deep. Especially good for very large sites.
- **Thorough Scan:** use to perform an exhaustive crawl on your site. It is recommended that you split your site into parts and only scan smaller chunks of your site with these settings. Not recommended for large sites.

## Mobile Templates

There are two mobile template options to choose from:

- **Mobile Scan:** use this option to scan a mobile site from the machine where your instance of WebInspect or WebInspect Enterprise is installed. WebInspect or WebInspect Enterprise will fetch

the mobile version of the site rather than the full site when this option is chosen.

- **Native Scan:** use this option to manually crawl a native mobile application and capture the Web traffic as a workflow macro. Generate the traffic on an Android, Windows, or iOS device or software emulator (Android and iOS only) running a mobile application.

After selecting a Guided Scan template, the stages and steps are displayed in the left pane, allowing you to easily navigate among them and specify the settings for your scan.

#### See Also

[About Guided Scan](#)

["Using the Predefined Template " on the next page](#)

["Using the Mobile Scan Template " on page 105](#)

["Using the Native Scan Template " on page 119](#)

## Running a Guided Scan

The first time you initiate a Guided Scan, WebInspect launches a tutorial. You can close the tutorial at any time, or click Tutorial in the top right corner or the wizard screen to launch the tutorial.

The Guided Scan progress display in the left pane allows you to easily see your progress as you specify settings for your scan. The right pane displays the scan options on each wizard page.

The first page of the Guided Scan presents you with the option to select the type of scan to run. There are three main types to choose from.

## Predefined Template (Standard, Quick, or Thorough)

There are three Predefined templates options to choose from:

- **Standard Scan:** Default scan settings are designed to focus more on coverage than performance. Larger sites could take days to crawl with these settings.
- **Quick Scan:** A scan that focuses on breadth and performance rather than digging deep. Especially good for very large sites.
- **Thorough Scan:** Thorough scan settings are designed to perform an exhaustive crawl of your site. It is recommended that you split your site up into parts and only scan smaller chunks of your site with these settings. Not recommended for large sites.

For more information, see [Using the Predefined Template](#).

## Mobile Scan Template

This template emulates a mobile device while scanning a Web application.

For more information, see [Using the Mobile Scan Template](#).

## Native Scan Template

This template manually crawls a native mobile application and captures Web traffic as a workflow macro.

For more information, see [Using the Native Scan Template](#).

### See Also

["Guided Scan Overview " on page 91](#)

["WebInspect Policies" on page 237](#)

[About Guided Scan](#)

## Using the Predefined Template

The Guided Scan wizard will step you through the necessary stages and steps required to scan your Web site. If you need to return to a previous step or stage, click the back navigation button, or click the step in the Guided Scan tree to be taken directly there.

## Launching a Guided Scan

To launch a Guided Scan:

- For WebInspect users, click the Start a Guided Scan option in the left pane, or select **File > New > Guided Scan** from the menu bar.
- For WebInspect Enterprise users, click **Guided Scan** under Actions on the Web Console.

The Guided Scan wizard launches and presents a list of Guided Scan templates. There are three Predefined templates options to choose from:

- **Standard Scan:** use this option to when you are interested in coverage. Larger sites could take days when using this template.
- **Quick Scan:** use this option when focusing on breadth and performance rather than digging deep. Especially good for very large sites.

- **Thorough Scan:** use to perform an exhaustive crawl on your site. It is recommended that you split your site into parts and only scan smaller chunks of your site with these settings. Not recommended for large sites.

Choose one of the **Predefined Templates**.

## About the Site Stage

During the Site stage, you will:

- Verify the Web site you want to scan
- Choose a scan type

## Verifying Your Web Site

To verify your Web site:

1. In the Start URL box, type or select the complete URL or IP address of the site to scan.

If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, WebInspect or WebInspect Enterprise will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

An invalid URL or IP address results in an error. If you want to scan from a certain point in your hierarchical tree, append a starting point for the scan, such as  
`http://www.myserver.com/myapplication/`.

Scans by IP address do not pursue links that use fully qualified URLs (as opposed to relative paths).

**Note:** WebInspect (beginning with version 8.1) supports Internet Protocol version 6 (IPv6) addresses in web site and web service scans. When you specify the Start URL, you must enclose the IPv6 address in brackets. For example:

- `http://[::1]`  
WebInspect scans "localhost."
- `http://[fe80::20c:29ff:fe32:bae1]/subfolder/`  
WebInspect scans the host at the specified address starting in the "subfolder" directory.

- `http://[fe80::20c:29ff:fe32:bae1]:8080/subfolder/`

WebInspect scans a server running on port 8080 starting in "subfolder."

WebInspect and WebInspect Enterprise support both Internet Protocol version 4 (IPV4) and Internet Protocol version 6 (IPV6). IPV6 addresses must be enclosed in brackets.

2. (Optional) To limit the scope of the scan to an area, select the **Restrict to Folder** check box, and then select one of the following options from the list:

**Directoryonly (self).** WebInspect and WebInspect Enterprise will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of `www.mycompany/one/two/`, WebInspect or WebInspect Enterprise will assess only the "two" directory.

**Directory and subdirectories.** WebInspect or WebInspect Enterprise will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.

**Directory and parent directories.** WebInspect or WebInspect Enterprise will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

3. Click **Verify**.
4. If you must access the target site through a proxy server, click **Proxy** in the lower left of the main screen to display the Proxy Settings area, and then select an option from the **Proxy Settings** list:

- **Direct Connection (proxy disabled)**
- **Autodetect proxy settings:** Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.
- **Use Internet Explorer proxy settings:** Import your proxy server information from Internet Explorer.
- **Use Firefox proxy settings:** Import your proxy server information from Firefox.
- **Configure proxy settings using a PAC File:** Load proxy settings from a Proxy Automatic Configuration (PAC) file. If you select this option, click Edit to enter the location (URL) of the PAC.
- **Explicitly configure proxy settings:** Specify proxy server settings as indicated. If you select this option, click Edit to enter proxy information.

**Note:** Electing to use browser proxy settings does not guarantee that you will access the

Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy server is not used.

When the Web site or directory structure appears, you have successfully verified your connection to the Start URL.

5. Click **Next**.

The Choose Scan Type window appears.

## Choosing a Scan Type

1. Type in a name for your scan in the **Scan Name** box.

2. Select one of the following scan types:

**Standard:** WebInspect or WebInspect Enterprise perform an automated analysis, starting from the target URL. This is the normal way to start a scan.

**Workflows:** If you select this option, an additional Workflows stage is added to the Guided scan.

3. In the Scan Method area, select one of the following scan methods:

- **Crawl Only.** This option completely maps a site's hierarchical data structure. After a crawl has been completed, you can click Audit to assess an application's vulnerabilities.

- **Crawl and Audit.** WebInspect or WebInspect Enterprise map the site's hierarchical data structure and audits each resource (page). Depending on the default settings you select, the audit can be conducted as each resource is discovered or after the entire site is crawled. For information regarding simultaneous vs. sequential crawl and audit, see "[Scan Settings: Method](#) " on page 278.

- **Audit Only.** WebInspect or WebInspect Enterprise apply the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.

4. In the Policy area, select a policy from the Policy list. For information about managing policies, see the "Policy" chapter in the Tools Guide for WebInspect Products.

5. In the Crawl Coverage area, select the level of coverage you want using the **Crawl Coverage** slider. For more information on crawl coverage levels, see [Specify Coverage and Thoroughness](#).

6. Click the **Next** button.

The Login stage appears with Network Authentication highlighted in the left pane.

## About the Login Stage

If the application you intend to scan requires login credentials, you can use the login stage to either select a pre-existing login macro or record one for use with the scan.

If your application does not require login credentials, you can skip this section of the Guided Scan wizard by clicking through the options without assigning values, or clicking Application in the Guided Scan tree to skip to the next stage.

In this stage you can:

- Configure network authorization
- Configure application authorization
- Create or assign a login macro

## Network Authentication Step

If your application requires either network or application level authentication, you can assign it here.

### Configuring Network Authentication

If your network requires user authentication, you can configure it here. If your network does not require user authentication, click the Next navigation button or the next appropriate step in the Guided Scan tree to continue on.

To configure network authentication:

1. Click the **Network Authentication** checkbox.
2. Select a **Method** from the drop-down list of authentication methods. The authentication methods are:
  - **Automatic.** Allow WebInspect or WebInspect Enterprise to determine the correct authentication type.
  - **Basic.** A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a user name and password. The Web browser then attempts to establish a connection to a server using the user's credentials. If the credentials are rejected, the browser displays an authentication window to re-enter the user's credentials. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers.
  - **NTLM.** NTLM (NT LanMan) is an authentication process that is used by all members of the

Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and WebInspect or WebInspect Enterprise has to pass through a proxy server to submit its requests to the Web server, WebInspect or WebInspect Enterprise may not be able to crawl or audit that Web site. Use caution when configuring WebInspect or WebInspect Enterprise for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

- **Digest.** The Windows Server operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.
- **Kerberos.** Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.
- **Negotiate.** The Negotiate authentication protocol begins with the option to negotiate for an authentication protocol. When the client requests access to a service, the server replies with a list of authentication protocols that it can support and an authentication challenge based on the protocol that is its first choice.

For example, the server might list Kerberos and NTLM, and send a Kerberos challenge. The client examines the contents of the reply and checks to determine whether it supports any of the specified protocols. If the client supports the preferred protocol, authentication proceeds. If the client does not support the preferred protocol, but does support one of the other protocols listed by the server, the client lets the server know which authentication protocol it supports, and the authentication proceeds. If the client does not support any of the listed protocols, the authentication exchange fails.

3. To use a client certificate for network authentication, select Client Certificate.
4. In the Certificate Store area, select one of the following, and then select either the **My** or **Root** radio button:
  - **Local Machine.** WebInspect uses a certificate on the local machine based on your selection in the Certificate Store area.
  - **Current User.** WebInspect uses a certificate for the current user based on your selection in the Certificate Store area.

5. To view certificate details in the Certificate Information area, select a certificate.
6. Click the **Next** button.

The Application Authentication page appears.

## Application Authentication Step

If your site requires authentication, you can use this step to create a login macro to automate the login process and increase the coverage of your site. A login macro is a recording of the activity that is required to access and log in to your application, typically by entering a user name and password and clicking a button such as Log In or Log On. You can select a previously recorded login macro or record a new one.

### Selecting a Login Macro

To select a previously recorded login macro:

1. Check the **Use a login macro for this site** checkbox.
2. Click the (**browse**) button to navigate to and select an existing login macro to use in the scan.

For details about recording a new login macro or using an existing login macro, see the "Unified Web Macro Recorder" chapter in the Tools Guide for WebInspect Products. That section also provides information about using macros that were recorded in previous versions of WebInspect using other web macro recorder tools.

3. Click the **Next** button.

The Organizational Tasks page appears with **Profile site for optimum settings** highlighted in the left pane.

## About the Workflows Stage

The Workflows stage only appears if you selected Workflows as the Scan Type in the Site stage. If you chose Standard, the Workflows stage will not appear. You can create a Workflow macro to ensure WebInspect audits the pages you specify in the macro. WebInspect audits only those URLs included in the macro and does not follow any hyperlinks encountered during the audit. A logout signature is not required. This type of macro is used most often to focus on a particular subsection of the application. If you select multiple macros, they will all be included in the same scan. In addition to allowing you to select multiple macros, you can also import Burp proxies to your scan.

To complete the Workflows settings, click any of the following in the Workflows table:

- **Record.** Opens the Unified Web Macro Recorder, allowing you to create a macro.
- **Edit.** Opens the Unified Web Macro Recorder and loads the selected macro.
- **Delete.** Removes the selected macro (but does not delete it from your disk).
- **Import.** Opens a standard file-selection window, allowing you to select a previously recorded macro and/or Burp Proxy captures.

**Note:** If you have installed HP Unified Functional Testing (UFT) on your computer, then WebInspect detects this automatically and displays an option to import a UFT .usr file.

See [Importing HP Unified Functional Testing \(UFT\) Files in a Guided Scan](#).

- **Export.** Opens a standard file-selection window, allowing you to save a recorded macro.

After you specify and play a workflow macro, it appears in the Workflows table and its Allowed Hosts are added to the **Guided Scan > Workflows > Workflows > Manager Workflow** page. You can enable or disable access to particular hosts. See [Allowed Hosts](#).

## To Add Burp Proxy results

If you have run Burp Proxy security tests, the traffic collected during those tests can be imported into a Workflow macro, reducing the time it would otherwise take to rescan the same areas.

To add Burp Proxy results to a workflow macro:

1. If you are not on the Workflows screen, click on the **Manage Workflows** step in the Guided Scan tree.
2. Click the **Import** button.

The Import Macro file selector appears.

3. Change the file type box filter from Web Macro (\*.webmacro) to Burp Proxy (\*.\*).
4. Navigate to your Burp Proxy files and select the desired file.
5. Click **Open**.

## About the Active Learning Stage

During the Active Learning stage:

- The WebInspect Profiler is run to see if any settings need to be modified.
- Set scan optimization option if necessary.
- Navigate to key locations in your site that should be fully exercised.

## Using the Profiler

The WebInspect Profiler conducts a preliminary examination of the target Web site to determine if certain settings should be modified. If changes appear to be required, the Profiler returns a list of suggestions, which you may accept or reject.

For example, the Profiler may detect that authorization is required to enter the site, but you have not specified a valid user name and password. Rather than proceed with a scan that would return significantly diminished results, you could follow the Profiler's suggestion to configure the required information before continuing.

Similarly, your settings may specify that WebInspect should not conduct "file-not-found" detection. This process is useful for Web sites that do not return a status "404 Not Found" when a client requests a resource that does not exist (they may instead return a status "200 OK," but the response contains a message that the file cannot be found). If the Profiler determines that such a scheme has been implemented in the target site, it would suggest that you modify the WebInspect setting to accommodate this feature.

To launch the Profiler:

1. Click **Profile**.

The Profiler runs. See [About Server Profiler](#) for detailed information.

Results appear in the Optimize scan for box in the Settings section.

2. Accept or reject the suggestions that appear in the Optimize scan for drop-down box. To reject the suggestion, select None or an alternate from the drop-down menu.
3. If necessary, provide any requested information.
4. Click the **Next** button.

Several options may be presented even if you do not run the Profiler, as described in the following sections.

### Autofill Web Forms

Select Auto-fill Web forms during crawl if you want WebInspect to submit values for input controls on forms it encounters while scanning the target site. WebInspect will extract the values from a prepackaged default file or from a file that you create using the Web Form Editor. See the "Web Form Editor" chapter in the Tools Guide for WebInspect Products. You may:

1. Click the ellipsis button (...) to locate and load a file.
2. Click **Edit** to edit the selected file (or the default values) using the Web Form Editor.
3. Click **Create** to open the Web Form Editor and create a file.

### Add Allowed Hosts

Use the Allowed Host settings to add domains to be crawled and audited. If your Web presence uses multiple domains, add those domains here. See [Allowed Hosts](#) for more information.

To add allowed domains:

1. Click **Add**.
2. In the **Specify Allowed Host** window, enter a URL (or a regular expression representing a URL) and click **OK**.

### Reuse Identified False Positives

Select scans containing vulnerabilities that were changed to false positives. If those false positives match vulnerabilities detected in this scan, the vulnerabilities will be changed to false positives. See [False Positives](#) for more information

To reuse identified false positives:

1. Select **Import False Positives**.
2. Click **Select Scans**.
3. Select one or more scans containing false positives from the same site you are now scanning.
4. Click **OK**.

### Apply Sample Macro

WebInspect's example banking application, zero.webappsecurity.com, uses a Web form login. If you scan this site, select **Apply sample macro** to run the prepackaged macro containing the login script.

### Traffic Analysis

Select **Launch and Direct Traffic through Web Proxy** to use the Web Proxy tool to examine the HTTP requests issued by WebInspect and the responses returned by the target server.

While scanning a Web site, WebInspect displays in the navigation pane only those sessions that reveal the hierarchical structure of the Web site, plus those sessions in which a vulnerability was discovered. However, if you select **Enable Traffic Monitor**, WebInspect adds the **Traffic Monitor** button to the Scan Info panel, allowing you to display and review each HTTP request sent by WebInspect and the associated HTTP response received from the server.

### Message

If the Profiler does not recommend changes, the Guided Scan wizard displays the message "No settings changes are recommended. Your current scan settings are optimal for this site."

The Enhance coverage of your web site task appears highlighted in the left pane.

### **Enhance coverage of your web site**

To enhance coverage of your application, navigate to key locations in your application to enhance coverage.

See "Unified Web Macro Recorder" in the Tools Guide for WebInspect Products for detailed information about using the Web Macro Recorder to navigate key locations in your application for Guided Scan to use during the scan.

See the Guided Scan Tutorial for more information about how to use this page of the Guided Scan wizard. To launch the tutorial, click **Tutorial** in the upper right corner of the page.

### **Web Form Values**

Guided Scan recorded all of the web form values that you entered while you explored your Web site. Here you can review and modify the values, which are part of the scan settings that are saved with the scan. In the Web Forms section of the toolbar, you can click **Export** to save the values to a separate file or click **Import** to use an existing set of values. The scan settings, including the web form values, serve as defaults that you can modify in future scans.

Click **Next**.

The Final Review page appears with **Configure Detailed Options** highlighted in the left pane.

## **About the Settings Stage**

To configure detailed options, specify any of the following settings.

### **Reuse Identified False Positives**

Select the **False Positives** box to reuse false positives that WebInspect has already identified.

### **Traffic Analysis**

1. To use the Web Proxy tool, select **Launch and Direct Traffic through Web Proxy** to use the Web Proxy tool to examine the HTTP requests issued by WebInspect and the responses returned by the target server.

Web Proxy is a stand-alone, self-contained proxy server that you can configure and run on your desktop. Web Proxy allows you to monitor traffic from a scanner, a Web browser, or any other tool that submits HTTP requests and receives responses from a server. Web Proxy is a tool for a debugging and penetration scan; you can view every request and server response while browsing a site.

2. Select the **Traffic Monitor** box to display and review each HTTP request sent by WebInspect and the associated HTTP response received from the server.

While scanning a Web site, WebInspect displays only those sessions that reveal the hierarchical structure of the Web site, plus those sessions in which a vulnerability was discovered. However,

if you select **Enable Traffic Monitor**, WebInspect allows you to display and review each HTTP request sent by WebInspect and the associated HTTP response received from the server.

3. Click **Next**.

The Validate Settings and Start Scan page appears with Configure Detailed Options highlighted in the left pane.

4. To save your scan settings, select **Click here to save settings**.
5. In the **Scan Now** area, review your scan settings, and then click **Start Scan** to begin the scan.

## Importing HP Unified Functional Testing (UFT) Files in a Guided Scan

If you have the HP Unified Functional Testing application installed, WebInspect detects it and allows you to import a UFT file (.usr) into your workflow scan to enhance the thoroughness and attack surface of your scan. For more information, see [HP Unified Functional Testing](#) on the HP Web site.

To import a UFT (.usr) file into a WebInspect Guided Scan:

1. Launch a Guided Scan, and then select Workflow Scan as the Scan Type. Additional text appears under the Workflows scan option: HP Unified Functional Testing has been detected. You can import scripts to improve the thoroughness of your security test.
2. Click the **Next** button.
3. In the Authentication section, Application Authentication is automatically selected. Complete the fields as indicated.
4. On the Manage Workflows screen, click **Import**. The Import Scripts dialog appears. On the Import Scripts dialog, you may:
  - Type the filename.
  - Browse to your file by clicking to locate your file with a .usr extension. Select **HP Unified Functional Testing** from the drop-down file type, and then navigate to the file.
  - Click **Edit** to launch the **HP Unified Functional Testing** application.
5. (Optional) On the Import Scripts dialog, you may select either of the following options:
  - **Show HP Unified Functional Testing UI during import**
  - **Open script result after import**
6. Select the file to import, and then click Import. After your file is successfully imported, the file appears in the Workflows table.
7. Select one of the following from the Workflows table:

- **Record** - launches the WebInspect Unified Macro Recorder. For more information, see "Unified Web Macro Recorder" in the Tools Guide for WebInspect Products guide.
- **Edit** - allows you to modify the file using the Unified Web Macro Recorder. See "Unified Web Macro Recorder" in the Tools Guide for WebInspect Products.
- **Delete** - deletes the script from the Workflows table.
- **Import** - import another file.
- **Export** - saves a file in .webmacro format with the name and location you specify.

8. Click the **Next** button.

When the first .usr script file is added to the list, its name (or default name) appears in the Workflows table and an Allowed Hosts table is added to the pane.

Adding another .usr script file can add more allowed hosts. Any host that is enabled is available to all the listed workflow .usr script files, not just the workflow.usr file for which it was added. The Guided Scan will play all the listed workflow files and make requests to all the listed allowed hosts, whether or not their check boxes are selected. If a check box for an allowed host is selected, WebInspect will crawl or audit the responses from that host. If a check box is not selected, WebInspect will not crawl or audit the responses from that host. In addition, if a particular workflow .usr script uses parameters, a Macro Parameters table is displayed when that workflow macro is selected in the list. Edit the values of the parameters as needed.

9. After you have completed changes or additions to the Workflows table, proceed in the Guided Scan wizard to complete your settings and run the scan. For more information about recording a new login macro or using an existing login macro, see the "Unified Web Macro Recorder" chapter in the Tools Guide for WebInspect Products manual. That chapter also provides information about using macros that were recorded in previous versions of WebInspect using other web macro recorder tools.

#### See Also

[About Guided Scan](#)

## Using the Mobile Scan Template

Using the Mobile Scan template to create a mobile Web site scan allows you to scan the mobile version of a Web site using the desktop version of your browser from within WebInspect or WebInspect Enterprise.

A Mobile Scan is nearly identical to a Web site scan and mirrors the settings options you will find when using one of the Predefined templates to do a Standard, Thorough, or Quick scan. The only difference is that you need to select a user agent header to allow your browser to emulate a mobile browser.

WebInspect and WebInspect Enterprise come with four mobile user agent options to choose from, but you can create a custom option and create a user agent for another version of Android, Windows

Phone, or other mobile device. For information creating a user agent header, see Creating a Custom User Agent Header.

## Launching a Mobile Scan

To launch a Mobile Scan:

1. Log into WebInspect or WebInspect Enterprise.
2. Start a Guided Scan:
  - a. For WebInspect, click **Start a Guided Scan** on the WebInspect Start page.
  - b. For WebInspect Enterprise, click **Guided Scan** under Actions on the Web Console.
3. Select **Mobile Scan** from the Mobile Templates section.
4. Click the **Mobile Client** icon in the tool bar.
5. Select the Rendering Engine you want to use.
6. Select the User Agent that represents the agent string you want your rendering engine to present to the site. If you created your own user string, it will appear as Custom. If the user agent is not listed, you can create a custom user agent. See Creating a Custom User Agent Header.

The Guided Scan wizard displays the first step in the Native Mobile Stage: Verify Web Site.

## Creating a Custom User Agent Header

WebInspect and WebInspect Enterprise include user agents for Android, Widows, and iOS devices. If you are using one of these options, you do not need to create a custom user agent header. If you want your Web browser to identify itself as a different mobile device or a specific OS version, create a custom user agent header.

To create a custom user agent:

1. Click the **Advanced** icon in the Guided Scan tool bar.
2. The Scan Settings window appears.
3. In the Scan Settings column, select **Cookies/Headers**.
4. In the Append Custom Headers section of the settings area, double-click the User-Agent string.  
The Specify Custom Header box appears.
5. Type in User-Agent: followed by the user agent header string for the desired device.

6. Click **OK**.

The new custom user agent will now be available to select as your Mobile Client.

## About the Site Stage

During the Site stage, you will:

- Verify the Web site you want to scan
- Choose a scan type

## Verifying Your Web Site

To verify your Web site:

1. In the **Start URL** box, type or select the complete URL or IP address of the site to scan.

If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, WebInspect or WebInspect Enterprise will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

An invalid URL or IP address results in an error. If you want to scan from a certain point in your hierarchical tree, append a starting point for the scan, such as <http://www.myserver.com/myapplication/>.

Scans by IP address do not pursue links that use fully qualified URLs (as opposed to relative paths).

WebInspect and WebInspect Enterprise support both Internet Protocol version 4 (IPV4) and Internet Protocol version 6 (IPV6). IPV6 addresses must be enclosed in brackets.

**Note:** WebInspect (beginning with version 8.1) supports Internet Protocol version 6 (IPv6) addresses in web site and web service scans. When you specify the Start URL, you must enclose the IPv6 address in brackets. For example:

- `http://[::1]`  
WebInspect scans "localhost."
- `http://[fe80::20c:29ff:fe32:bae1]/subfolder/`  
WebInspect scans the host at the specified address starting in the "subfolder" directory.

- `http://[fe80::20c:29ff:fe32:bae1]:8080/subfolder/`

WebInspect scans a server running on port 8080 starting in "subfolder."

2. (Optional) To limit the scope of the scan to an area, select the **Restrict to Folder** check box, and then select one of the following options from the list:
  - Directory only (self). WebInspect and WebInspect Enterprise will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of `www.mycompany/one/two/`, WebInspect or WebInspect Enterprise will assess only the "two" directory.
  - Directory and subdirectories. WebInspect or WebInspect Enterprise will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
  - Directory and parent directories. WebInspect or WebInspect Enterprise will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.
3. Click **Verify**.
4. If you must access the target site through a proxy server, click **Proxy** in the lower left of the main screen to display the Proxy Settings area, and then select an option from the Proxy Settings list:
  - **Direct Connection (proxy disabled)**
  - **Autodetect proxy settings:** Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.
  - **Use Internet Explorer proxy settings:** Import your proxy server information from Internet Explorer.
  - **Use Firefox proxy settings:** Import your proxy server information from Firefox.
  - **Configure proxy settings using a PAC File:** Load proxy settings from a Proxy Automatic Configuration (PAC) file. If you select this option, click Edit to enter the location (URL) of the PAC.
  - **Explicitly configure proxy settings:** Specify proxy server settings as indicated. If you select this option, click Edit to enter proxy information.

**Note:** Electing to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not

selected, then a proxy server is not used.

When the Web site or directory structure appears, you have successfully verified your connection to the Start URL.

5. Click **Next**.

The Choose Scan Type window appears.

## Choosing a Scan Type

1. Type in a name for your scan in the **Scan Name** box.
2. Select one of the following scan types:

**Standard:** WebInspect or WebInspect Enterprise perform an automated analysis, starting from the target URL. This is the normal way to start a scan.

**Workflows:** If you select this option, an additional Workflows stage is added to the Guided scan.

3. In the Scan Method area, select one of the following scan methods:
  - **Crawl Only.** This option completely maps a site's hierarchical data structure. After a crawl has been completed, you can click Audit to assess an application's vulnerabilities.
  - **Crawl and Audit.** WebInspect or WebInspect Enterprise map the site's hierarchical data structure and audits each resource (page). Depending on the default settings you select, the audit can be conducted as each resource is discovered or after the entire site is crawled. See [Crawl and Audit Mode](#) for information regarding simultaneous vs. sequential crawl and audit.
  - **Audit Only.** WebInspect or WebInspect Enterprise apply the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.
4. In the Policy area, select a policy from the Policy list. For information about managing policies, see the "Policy" chapter in the Tools Guide for WebInspect Products.
5. In the Crawl Coverage area, select the level of coverage you want using the **Crawl Coverage** slider. For more information on crawl coverage levels, see [Specify Coverage and Thoroughness](#).
6. Click the **Next** button.

The Login stage appears with Network Authentication highlighted in the left pane.

## About the Login Stage

If the application you intend to scan requires login credentials, you can use the login stage to either select a pre-existing login macro or record one for use with the scan.

If your application does not require login credentials, you can skip this section of the Guided Scan wizard by clicking through the options without assigning values, or clicking Application in the Guided Scan tree to skip to the next stage.

In this stage you can:

- Configure network authorization
- Configure application authorization
- Create or assign a login macro

## Network Authentication Step

If your application requires either network or application level authentication, you can assign it here.

### Configuring Network Authentication

If your network requires user authentication, you can configure it here. If your network does not require user authentication, click the Next navigation button or the next appropriate step in the Guided Scan tree to continue on.

To configure network authentication:

1. Click the **Network Authentication** checkbox.
2. Select a **Method** from the drop-down list of authentication methods. The authentication methods are:

#### **Automatic**

Allow WebInspect or WebInspect Enterprise to determine the correct authentication type.

#### **Basic**

A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a user name and password. The Web browser then attempts to establish a connection to a server using the user's credentials. If the credentials are rejected, the browser displays an authentication window to re-enter the user's credentials. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers.

## NTLM

NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and WebInspect or WebInspect Enterprise has to pass through a proxy server to submit its requests to the Web server, WebInspect or WebInspect Enterprise may not be able to crawl or audit that Web site. Use caution when configuring WebInspect or WebInspect Enterprise for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

## Digest

The Windows Server operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.

## Kerberos

Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.

## Negotiate

The Negotiate authentication protocol begins with the option to negotiate for an authentication protocol. When the client requests access to a service, the server replies with a list of authentication protocols that it can support and an authentication challenge based on the protocol that is its first choice.

For example, the server might list Kerberos and NTLM, and send a Kerberos challenge. The client examines the contents of the reply and checks to determine whether it supports any of the specified protocols. If the client supports the preferred protocol, authentication proceeds. If the client does not support the preferred protocol, but does support one of the other protocols listed by the server, the client lets the server know which authentication protocol it supports, and the authentication proceeds. If the client does not support any of the listed protocols, the authentication exchange fails.

3. To use a client certificate for network authentication, select **Client Certificate**.

**Note:** You can add a client certificate to a Windows phone, but the only way to subsequently remove it is to restore the phone to its default settings.

4. In the Certificate Store area, select one of the following, and then select either the **My** or **Root** radio button:
  - **Local Machine.** WebInspect uses a certificate on the local machine based on your selection in the Certificate Store area.
  - **Current User.** WebInspect uses a certificate for the current user based on your selection in the Certificate Store area.
5. To view certificate details in the Certificate Information area, select a certificate.
6. Click the **Next** button.

The Application Authentication page appears.

## Application Authentication Step

If your site requires authentication, you can use this step to create a login macro to automate the login process and increase the coverage of your site. A login macro is a recording of the activity that is required to access and log in to your application, typically by entering a user name and password and clicking a button such as Log In or Log On. You can select a previously recorded login macro or record a new one.

### Selecting a Login Macro

To select a previously recorded login macro:

1. Check the **Use a login macro for this site** checkbox.
2. Click the **(browse)** button to navigate to and select an existing login macro to use in the scan.

For details about recording a new login macro or using an existing login macro, see the "Unified Web Macro Recorder" chapter in the Tools Guide for WebInspect Products. That section also provides information about using macros that were recorded in previous versions of WebInspect using other web macro recorder tools.

3. Click the **Next** button.

The Organizational Tasks page appears with **Profile site for optimum settings** highlighted in the left pane.

## About the Workflows Stage

The Workflows stage only appears if you selected Workflows as the Scan Type in the Site stage. If you chose Standard, the Workflows stage will not appear.

You can create a Workflow macro to ensure WebInspect audits the pages you specify in the macro. WebInspect audits only those URLs included in the macro and does not follow any hyperlinks encountered during the audit.

You can create multiple Workflows macros; one for each use case on your site. A logout signature is not required. This type of macro is used most often to focus on a particular subsection of the application. If you select multiple macros, they will all be included in the same scan. In addition to allowing you to select multiple macros, you can also import Burp proxy captures and add them to your scan.

To complete the Workflows settings, click any of the following in the Workflows table:

- **Record.** Opens the Unified Web Macro Recorder, allowing you to create a macro.
- **Edit.** Opens the Unified Web Macro Recorder and loads the selected macro.
- **Delete.** Removes the selected macro (but does not delete it from your disk).
- **Import.** Opens a standard file-selection window, allowing you to select a previously recorded macro and/or Burp Proxy captures.

**Note:** If you have installed HP Unified Functional Testing (UFT) on your computer, then WebInspect detects this automatically and displays an option to import a UFT .usr file.

For more information, see [Importing HP Unified Functional Testing \(UFT\) Files in a Guided Scan](#).

- **Export** a recorded macro. After a macro is selected or recorded, you may optionally specify allowed hosts. Opens a standard file-selection window, allowing you to save a recorded macro.

After you specify and play a workflow macro, it appears in the Workflows table and its Allowed Hosts are added to the **Guided Scan > Workflows > Workflows > Manager Workflow** page. You can enable or disable access to particular hosts. See [Allowed Hosts](#).

## Adding Burp Proxy Results

If you have run Burp Proxy security tests, the traffic collected during those tests can be imported into a Workflows macro, reducing the time it would otherwise take to rescan the same areas.

### Adding Burp Proxy Results

To add Burp Proxy results to a workflow macro:

1. If you are not on the Workflows screen, click on the **Manage Workflows** step in the Guided Scan tree.

2. Click the **Import** button.

The Import Macro file selector appears.

3. Change the file type box filter from **Web Macro (\*.webmacro)** to **Burp Proxy (\*.\*)**.
4. Navigate to your Burp Proxy files and select the desired file.
5. Click **Open**.

## About the Active Learning Stage

During the Active Learning stage:

- The WebInspect Profiler is run to see if any settings need to be modified.
- Set scan optimization option if necessary.
- Navigate to key locations in your site that should be fully exercised.

## Using the Profiler

The WebInspect Profiler conducts a preliminary examination of the target Web site to determine if certain settings should be modified. If changes appear to be required, the Profiler returns a list of suggestions, which you may accept or reject.

For example, the Profiler may detect that authorization is required to enter the site, but you have not specified a valid user name and password. Rather than proceed with a scan that would return significantly diminished results, you could follow the Profiler's suggestion to configure the required information before continuing.

Similarly, your settings may specify that WebInspect should not conduct "file-not-found" detection. This process is useful for Web sites that do not return a status "404 Not Found" when a client requests a resource that does not exist (they may instead return a status "200 OK," but the response contains a message that the file cannot be found). If the Profiler determines that such a scheme has been implemented in the target site, it would suggest that you modify the WebInspect setting to accommodate this feature.

To launch the Profiler:

1. Click **Profile**.

The Profiler runs. See [About Server Profiler](#) for detailed information.

Results appear in the Optimize scan for box in the Settings section .

2. If necessary, provide any requested information.
3. Click the **Next** button.

Several options may be presented even if you do not run the Profiler, as described in the following sections.

### Autofill Web Forms

Select Auto-fill Web forms during crawl if you want WebInspect to submit values for input controls on forms it encounters while scanning the target site. WebInspect will extract the values from a prepackaged default file or from a file that you create using the Web Form Editor. See the "Web Form Editor" chapter in the Tools Guide for WebInspect Products. You may:

1. Click the browser button to locate and load a file.
2. Click **Edit** to edit the selected file (or the default values) using the Web Form Editor.
3. Click **Create** to open the Web Form Editor and create a file.

### Add Allowed Hosts

Use the Allowed Host settings to add domains to be crawled and audited. If your Web presence uses multiple domains, add those domains here. See [Allowed Hosts](#) for more information.

To add allowed domains:

1. Click **Add**.
2. In the Specify Allowed Host window, enter a URL (or a regular expression representing a URL) and click **OK**.

### Reuse Identified False Positives

Select scans containing vulnerabilities that were changed to false positives. If those false positives match vulnerabilities detected in this scan, the vulnerabilities will be changed to false positives. See [False Positives](#) for more information.

To reuse identified false positives:

1. Select **Import False Positives**.
2. Click **Select Scans**.
3. Select one or more scans containing false positives from the same site you are now scanning.
4. Click **OK**.

### Apply Sample Macro

WebInspect's example banking application, zero.webappsecurity.com, uses a Web form login. If you scan this site, select **Apply sample macro** to run the prepackaged macro containing the login script.

### Traffic Analysis

Select **Launch and Direct Traffic through Web Proxy** to use the Web Proxy tool to examine the HTTP requests issued by WebInspect and the responses returned by the target server.

While scanning a Web site, WebInspect displays in the navigation pane only those sessions that reveal the hierarchical structure of the Web site, plus those sessions in which a vulnerability was discovered. However, if you select **Enable Traffic Monitor**, WebInspect adds the **Traffic Monitor** button to the Scan Info panel, allowing you to display and review each HTTP request sent by WebInspect and the associated HTTP response received from the server.

### **Message**

If the Profiler does not recommend changes, the Guided Scan wizard displays the message "No settings changes are recommended. Your current scan settings are optimal for this site."

Click **Next**.

The **Enhance coverage of your web site** task appears highlighted in the left pane.

### **Enhance coverage of your web site**

To enhance coverage of your application, navigate to key locations in your application to enhance coverage.

See "Unified Web Macro Recorder" in the Tools Guide for WebInspect Products for detailed information about using the Web Macro Recorder to navigate key locations in your application for Guided Scan to use during the scan.

See the Guided Scan Tutorial for more information about how to use this page of the Guided Scan wizard. To launch the tutorial, click **Tutorial** in the upper right corner of the page.

### **Web Form Values**

Guided Scan recorded all of the web form values that you entered while you explored your Web site. Here you can review and modify the values, which are part of the scan settings that are saved with the scan. In the Web Forms section of the toolbar, you can click **Export** to save the values to a separate file or click **Import** to use an existing set of values. The scan settings, including the web form values, serve as defaults that you can modify in future scans.

Click **Next**.

The Final Review page appears with **Configure Detailed Options** highlighted in the left pane.

## About the Settings Stage

To configure detailed options, specify any of the following settings.

### **Reuse Identified False Positives**

Select the **False Positives** box to reuse false positives that WebInspect has already identified.

### **Traffic Analysis**

1. To use the Web Proxy tool, select Launch and Direct Traffic through Web Proxy to use the Web Proxy tool to examine the HTTP requests issued by WebInspect and the responses returned by the target server.

Web Proxy is a stand-alone, self-contained proxy server that you can configure and run on your desktop. Web Proxy allows you to monitor traffic from a scanner, a Web browser, or any other tool that submits HTTP requests and receives responses from a server. Web Proxy is a tool for a debugging and penetration scan; you can view every request and server response while browsing a site.

2. Select the **Traffic Monitor** box to display and review each HTTP request sent by WebInspect and the associated HTTP response received from the server.

While scanning a Web site, WebInspect displays only those sessions that reveal the hierarchical structure of the Web site, plus those sessions in which a vulnerability was discovered. However, if you select **Enable Traffic Monitor**, WebInspect allows you to display and review each HTTP request sent by WebInspect and the associated HTTP response received from the server.

3. Click **Next**.

The Validate Settings and Start Scan page appears with **Configure Detailed Options** highlighted in the left pane.

4. To save your scan settings, select **Click here to save settings**.
5. In the **Scan Now** area, review your scan settings, and then click **Start Scan** to begin the scan.

## Importing HP Unified Functional Testing (UFT) Files in a Guided Scan

If you have the HP Unified Functional Testing application installed, WebInspect detects it and allows you to import a UFT file (.usr) into your workflow scan to enhance the thoroughness and attack surface of your scan. For more information, see HP Unified Functional Testing on the HP Web site.

To import a UFT (.usr) file into a WebInspect Guided Scan:

1. Launch a Guided Scan, and then select Workflows Scan as the Scan Type. Additional text appears under the Workflows scan option:HP Unified Functional Testing has been detected. You can import scripts to improve the thoroughness of your security test.
2. Click the **Next** button.
3. In the Authentication section, **Application Authentication** is automatically selected. Complete the fields as indicated.
4. On the Manage Workflows screen, click **Import**. The Import Scripts dialog appears. On the Import Scripts dialog, you may:
  - Type the filename.
  - Browse to your file by clicking to locate your file with a .usr extension. Select **HP Unified Functional Testing** from the drop-down file type, and then navigate to the file.
  - Click **Edit** to launch the **HP Unified Functional Testing** application.

5. (Optional) On the Import Scripts dialog, you may select either of the following options:
    - **Show HP Unified Functional Testing UI during import**
    - **Open script result after import**
  6. Select the file to import, and then click **Import**. After your file is successfully imported, the file appears in the Workflows table.
  7. Select one of the following from the Workflows table:
    - **Record** - launches the WebInspect Unified Macro Recorder. For more information, see "Unified Web Macro Recorder" in the Tools Guide for WebInspect Products guide.
    - **Edit** - allows you to modify the file using the Unified Web Macro Recorder. See "Unified Web Macro Recorder" in the Tools Guide for WebInspect Products.
    - **Delete** - deletes the script from the Workflows table.
    - **Import** - imports another file.
    - **Export** - saves a file in .webmacro format with the name and location you specify
  8. Click the **Next** button.
- When the first .usr script file is added to the list, its name (or default name) appears in the Workflows table and an Allowed Hosts table is added to the pane.
- Adding another .usr script file can add more allowed hosts. Any host that is enabled is available to all the listed workflow .usr script files, not just the workflow.usr file for which it was added. The Guided Scan will play all the listed workflow files and make requests to all the listed allowed hosts, whether or not their check boxes are selected. If a check box for an allowed host is selected, WebInspect will crawl or audit the responses from that host. If a check box is not selected, WebInspect will not crawl or audit the responses from that host. In addition, if a particular workflows .usr script uses parameters, a Macro Parameters table is displayed when that workflow macro is selected in the list. Edit the values of the parameters as needed.
9. After you have completed changes or additions to the Workflows table, proceed in the Guided Scan wizard to complete your settings and run the scan. For more information about recording a new login macro or using an existing login macro, see the "Unified Web Macro Recorder" chapter in the Tools Guide for WebInspect Products manual. That chapter also provides information about using macros that were recorded in previous versions of WebInspect using other web macro recorder tools.

## See Also

[About Guided Scan](#)

## Using the Native Scan Template

WebInspect and WebInspect Enterprise allow you to scan the back-end traffic generated by your Android or iOS app or service. Traffic can be generated by running your application on an Android, Windows, or iOS device, or by running the software through an Android or iOS emulator.

The Guided Scan wizard includes a tutorial that runs the first time you launch a Guided Scan. If you don't require the tutorial, you can close it at any time and return to it later by clicking the **Tutorial** button at the top right of the display.

The Guided Scan wizard will step you through the necessary stages and steps required to scan your application back-end traffic. If you need to return to a previous step or stage, click the back navigation button, or click the step in the Guided Scan tree to be taken directly there.

## Setting Up Your Mobile Device

Running a native scan requires that you configure the mobile device to work with a secure proxy. In order to do that, you will need to:

[Set up a Mobile Device/Emulator Proxy](#)

[Install a Trusted Certificate](#)

## Guided Scan Stages

A Guided Scan using a mobile template consists of four or five stages, each of which has one or more steps. The stages are:

**Native Mobile:** where you choose a device or emulator, configure device/emulator proxy, and select the type of scan you want to run.

**Login:** where you define the type of authentication if back-end of your mobile application requires it.

**Application:** where you run your app, record Web traffic, and identify the hosts and RESTful endpoints to include in your scan.

**Settings:** where you review and validate your choices and run the scan.

## Supported Devices

WebInspect and WebInspect Enterprise support scanning the back-end traffic on Android, Windows, and iOS devices.

### Android Device Support

Any Android device, such as an Android-based phone or tablet.

### Windows Device Support

Any Windows device, such as a Windows phone or Surface tablet.

### iOS Device Support

Any iOS device, such as a iPhone or iPad, running the latest version of iOS.

## Supported Development Emulators

In addition to support for Android and iOS devices, you can run your application through your Android or iOS emulator in your development environment. When scanning traffic generated via your device emulator, you must ensure that the development machine is on the same network as WebInspect or WebInspect Enterprise and that you have set up a proxy between WebInspect or WebInspect Enterprise and your development machine.

## Launching a Native Scan

In order to launch a Native Scan, you will need to make sure your device or emulator is on the same network as WebInspect. In addition, you need to have authorization and access to the ports on the machine where you are running WebInspect in order to successfully create a proxy connection.

To launch a Native Scan:

1. Open WebInspect or WebInspect Enterprise.
2. Start a Guided Scan:
  - For WebInspect, click **Start a Guided Scan** on the WebInspect Start page.
  - For WebInspect Enterprise, click **Guided Scan** under Actions on the Web Console.
3. Select **Native Scan** from the Mobile Templates section.

The Guided Scan wizard displays the first step in the Native Mobile stage: Choose Device/Emulator.

## About the Native Mobile Stage

The first stage in the process is the Native Mobile stage. In this stage you will:

- Set up the device or emulator to use a proxy connection.
- Log the device or emulator on to the same network as your instance of WebInspect or WebInspect Enterprise.

- Install a client certificate on your device or emulator.
- Name the scan for future reference.
- Select a scan method.
- Select a scan policy.
- Select the crawl coverage amount.

## Choose Device/Emulator Type Step

After launching the Guided Scan, you will be provided with the following options:

Option	Description
Profile	The type of device or emulator you want to scan. Select a type from the drop-down menu. For more information, see <a href="#">Selecting a Profile</a> .
Mobile Device/Emulator Proxy	The IP address and port number for the proxy that Webinspect or WebInspect Enterprise creates for listening to the traffic between your device or emulator and the Web service or application being tested. Unless the IP address and/or port are reserved for other activities, use the default settings. For more information, see <a href="#">Setting the Mobile Device Proxy Address</a> .
Trusted Certificate	The port and URL to acquire a client certificate for your device or emulator. To download and install the certificate on your device or emulator, see <a href="#">Adding a Trusted Certificate</a> .

## Selecting a Profile

To set the device profile, select one of the following from the **Profile** drop-down textbox:

- iOS Device - An iPad or iPhone running the latest version of iOS.
- iOS Simulator - The iOS emulator that is part of the iOS SDK.
- Android Device - A phone or tablet running the Android operating system.
- Android Emulator - The Android emulator that is part of the Android SDK.
- Windows Device - A Windows phone or Surface tablet.

## Setting the Mobile Device Proxy Address

The Mobile Device/Emulator Proxy section lists the Host IP address and the Port number that will be used to establish a proxy connection between your device or emulator and Webinspect or WebInspect

Enterprise. Use the suggested settings unless the IP address or port number are unavailable on your system.

**Note:** If you are unable to connect to the server or access the Internet after setting your proxy, you may need to open up or change the port on your firewall specified in the Native Mobile stage. If it still does not work, you may need to select a different IP address. The IP address presented in the WebInspect/WebInspect Enterprise interface allows you to click the address and select an alternate from a drop-down list.

To set up a proxy on an iOS device:

1. Run the **Settings** application.
2. Select **Wi-Fi**.
3. Select the Wi-Fi network you are using to connect to WebInspect or WebInspect Enterprise.
4. Scroll down to the HTTP Proxy section and select **Manual**.

The screen displays the network configuration options for the network your device is connected to

5. Scroll down further and type in the Server IP address and the Port number provided by WebInspect or WebInspect Enterprise. If you don't have this information, see [Choose Device/Emulator Type](#) step.
6. In WebInspect or WebInspect Enterprise, click the **Verify** button in the Trusted Certificate section to verify the connection is working properly.

The Verify activity progress bar appears.

7. Launch the default browser on your device and visit any site to verify that WebInspect or WebInspect Enterprise is able to see the back-end traffic.

If everything is configured properly, after a few moments, the Verify activity progress bar will state that the traffic has been successfully verified.

8. Click **OK** to dismiss the verification progress bar and then click **Next** to select a scan type.

To set up a proxy on an Android or Windows device, consult your operator's instructions.

## Adding a Trusted Certificate

If your site requires a secure connection, each time you run a scan, WebInspect or WebInspect Enterprise generates a unique client certificate for your device or emulator. You will need to install the certificate into the device's (or emulator's) certificate repository.

**Note:** You can add a client certificate to a Windows phone, but the only way to subsequently

remove it is to restore the phone to its default settings.

There are three ways to add a certificate:

- Scan the QR code from the Trusted Certificate section of Guided Scan (requires QR reader software).
- Type the address into the built-in browser on your device or device emulator.
- Copy the certificate to your system clipboard for applying later (used when scanning with a device emulator).

Choose the option that best suits your needs.

**Note:** After completing the scan, you should remove the certificate from the repository on your device. See [Post Scan Steps](#).

To Add a Certificate to an iOS device or emulator:

1. After scanning the QR code or typing the provided URL into your browser, the Install Profile page appears.

**Note:** The HP WebInspect Root certificate status will display as Not Trusted until you add it to your root chain.

2. Tap the **Install** button.

A warning screen will appear stating that the certificate is not trusted. Once you add the certificate to the certificate repository on your device or emulator, the warning will go away.

3. Tap **Install** on the Warning screen.

The display changes to that of the current network your device or emulator is connected to. Make sure it is connected to the same network as WebInspect or WebInspect Enterprise.

## Choose Scan Type Step

After setting up your device or emulator to work with WebInspect or WebInspect Enterprise during the first part of the Native Mobile stage, you will need to select the type of scan you would like to run.

Set the options listed below:

Option	Description
Scan Name	Type a name for the scan so that later you can identify the scan on the Manage Scans page.

Option	Description
Scan Method	<p>Choose the type of scan you want from the following list:</p> <p><b>Crawl Only:</b> maps the attack surface of the specified workflow(s).</p> <p><b>Crawl and Audit:</b> maps the attack surface of the specified workflow(s) and scans for vulnerabilities.</p> <p><b>Audit Only:</b> only attack the specified workflows.</p>
Policy	Select a policy for the scan from the drop-down menu. For more information on policies, see " <a href="#">"WebInspect Policies" on page 237</a> ". For information on creating and editing policies, see the "Policy Manager" chapter in the Tools Guide for WebInspect Products.
Crawl Coverage	Select the level of coverage you want using the Crawl Coverage slider.

## About the Login Stage

If the application you intend to scan requires login credentials, you can use the login stage to either select a an existing login macro or record one for use with the scan.

If your application does not require login credentials, you can skip this section of the Guided Scan wizard by clicking through the options without assigning values, or clicking the next step in the Guided Scan tree to skip to the next stage.

In this stage you can:

- Configure network authorization
- Configure application authorization
- Create or assign a login macro

## Network Authentication Step

If your application requires either network or application level authentication, you can assign it here.

### Configuring Network Authentication

If your network requires user authentication, you can configure it here. If your network does not require user authentication, click the Next navigation button or the next appropriate step in the Guided Scan tree to continue on.

To configure network authentication:

1. Click the **Network Authentication** checkbox.
2. Select a **Method** from the drop-down list of authentication methods. The authentication methods are:

#### **Automatic**

Allow WebInspect or WebInspect Enterprise to determine the correct authentication type.

#### **Basic**

A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a user name and password. The Web browser then attempts to establish a connection to a server using the user's credentials. If the credentials are rejected, the browser displays an authentication window to re-enter the user's credentials. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers.

#### **NTLM**

NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and WebInspect or WebInspect Enterprise has to pass through a proxy server to submit its requests to the Web server, WebInspect or WebInspect Enterprise may not be able to crawl or audit that Web site. Use caution when configuring WebInspect or WebInspect Enterprise for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

#### **Digest**

The Windows Server operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.

#### **Kerberos**

Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.

#### **Negotiate**

The Negotiate authentication protocol begins with the option to negotiate for an authentication

protocol. When the client requests access to a service, the server replies with a list of authentication protocols that it can support and an authentication challenge based on the protocol that is its first choice.

For example, the server might list Kerberos and NTLM, and send a Kerberos challenge. The client examines the contents of the reply and checks to determine whether it supports any of the specified protocols. If the client supports the preferred protocol, authentication proceeds. If the client does not support the preferred protocol, but does support one of the other protocols listed by the server, the client lets the server know which authentication protocol it supports, and the authentication proceeds. If the client does not support any of the listed protocols, the authentication exchange fails.

3. Type in the **User Name** and **Password**.

## Configuring a Client Certificate

If your network is set up to accept a client certificate rather than a user name and password, you can configure WebInspect or WebInspect Enterprise to provide the client certificate upon request.

To configure a client certificate:

1. Click the **Client Certificate** checkbox.
2. Select **Local Machine** if the certificate is located on the local machine, or Current User to select among the certificates owned by the currently logged-in user.
3. Select **My** or **Root** from the drop-down menu to identify the type of certificate required.

The Certificate box is populated with the certificates that meet the selected criteria.

4. Select the certificate you want to use from the Certificate box.

For verification purposes, certificate information, including validity dates, is listed in the Certificate Information section below the selection box.

## Application Authentication Step

If the back-end of your mobile application requires authentication, you can use this step to create a login macro to automate the login process and increase the coverage of your site. A login macro is a recording of the activity that is required to access and log in to your application, typically by entering a user name and password and tapping a button such as Log In or Log On. You can select a previously recorded login macro or record a new one.

## Selecting a Login Macro

To select a login macro:

1. Click the **Use a login macro for this site** check box.
2. Click the ... button to select a macro you have saved.

## Creating a Login Macro

To select a login macro:

1. Click the **Use a login macro for this site** check box.
2. Click the **Create** button to create a new one.

## Recording a Login Macro

To create a login macro:

1. Click the **Use a login macro for this site** checkbox.
2. Click the **Create** button.
3. When the macro recorder opens, click the **Record** button.
4. On your device or emulator, use your application to log in to your site. Once you have logged in, click the **Stop** button.
5. Click **Play** to test your macro.
6. Confirm the macro played back correctly or start over and recreate the macro.

## Specifying a Logout Condition

In some cases, after playing back your macro, a logout condition will need to be manually specified. If so, see the "Logout Condition Editor" section of the "Unified Web Macro Recorder" chapter of the Tools Guide for WebInspect Products.

## About the Application Stage

The Application Stage is where you run your application. During the application stage:

- Run the mobile application to generate and collect Web traffic.
- Identify the hosts and RESTful endpoints you want to include.

## Run Application Step

To run the application and generate and collect Web traffic:

1. Click the **Record** button.
2. Exercise the application, navigating through the interface as your customers will.
3. When you have generated enough traffic, click the **Stop** button.
4. Click **Play** to verify your workflow.

## Finalizing Allowed Hosts and RESTful Endpoints

After running the application and collecting Web traffic, a list will be generated of the Allowed Hosts and potential RESTful Endpoints.

To select the hosts to include in your audit, click the check boxes in the **Enabled** column of the Allowed Hosts table.

The list of RESTful endpoints is generated by listing every possible combination that could be a RESTful endpoint. Select the actual RESTful endpoints from the list by selecting their Enabled check boxes. To reduce the list to a more likely subset, click the Detect button. Heuristics are applied, filtering out some of the less likely results. Select the Enabled check boxes from the resultant list.

If WebInspect or WebInspect Enterprise didn't find all of the RESTful endpoints, you can add them manually.

To set up a new RESTful endpoint rule:

1. Click the **New Rule** button.

A new rule input box appears in the RESTful Endpoints table.

2. Following the sample format in the input box, type in a RESTful Endpoint.

To Import a List of RESTful Endpoints:

1. Click the **Import** button.

A file selector appears.

2. Select a Web Application Description Language (.wadl) file.
3. Click **OK**.

## About the Settings Stage

During the final stage, you can set a number of options that affect how the collected traffic is audited. The available options vary, based on the selections you have made.

## Final Review Step

### Configure Detailed Options

The Configure Detailed Options step allows you to set detailed options. These options will change from scan to scan, as they are dependent on the choices made in the Guided Scan wizard. Some of the options include:

**Reuse Identified False Positives.** Select a previous scan to identify vulnerabilities that have already been identified as false positives.

**Traffic Analysis.** You can use a self-contained proxy server on your desktop. With it you can monitor traffic from a scanner, a browser, or any other tool that submits HTTP requests and receives responses from a server. You can also enable the Traffic Monitor and display the hierarchical structure of the Web site or Web service in a WebInspect navigation pane. It allows you to display and review every HTTP request sent by WebInspect and the associated HTTP response received from the server.

**Scan Mode.** A crawl-only feature. Allows you to set Discovery (Path Truncation) Path truncation allows you to make requests for known directories without file names. This can cause directory listings to be displayed. You can also select the Passive Analysis (Keyword Search) option to examine every response from the Web server for (error messages, directory listings, credit card numbers, etc.) not properly protected by the Web site.

## Validate Settings and Start Scan

The Validate Settings and Start Scan step provides information on your scan, allows you to save your scan settings, and allows you to launch your scan.

To launch a scan:

- Read the **Warnings and Informationals** section to see if there are any final tasks or corrections that need to be made.
- Click the **Click here to save settings** link if you would like to save your scan settings for future use.
- Click the **Scan** button.

## Post Scan Steps

After you have completed your scan and run WebInspect or WebInspect Enterprise, you will need to reset your Android, Windows, or iOS device or emulator to its former state. The following steps show how to reset your iOS device to the way it was before you began. Steps for other devices and emulators are similar, but depend on the version of the OS you are running.

To remove the HP Certificate on an iOS device:

Run the Settings application.

1. Select **General** from the Settings column.
2. Scroll down to the bottom of the list and select **Profile HP WebInspect Root**.
3. Tap the **Remove** button.

To Remove the Proxy Settings on an iOS device:

1. Run the **Settings** application.
2. Select **Wi-Fi** from the **Settings** column.
3. Tap the **Network** name.

Delete the Server IP address and the Port number.

#### See Also

[About Guided Scan](#)

## Running a Web Service Scan

When performing a Web service scan, WebInspect crawls the WSDL site and submits a value for each parameter in each operation it discovers. These values are extracted from a file that you must create using the Web Service Test Designer. It then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection.

See [Auditing Web Services](#) for more information on how a Web services vulnerability scan differs from other types of scan actions.

**Note:** If you conducted a Web Service scan using a version of WebInspect prior to 9.0 and attempt to import that scan into version 10.0 or greater, results will be less than optimal. HP recommends that you rescan your Web service using WebInspect 10.0 or greater. See "[Importing Legacy Web Service Scans](#)" on page 174 for additional details.

Use the following procedure to conduct a Web Service scan.

1. On the WebInspect **Start Page**, click **Start a Web Service Scan**.

The Web Service ScanWizard appears.

2. Enter a name for the scan in the **Scan Name** box.
3. Select one of the following:

- **Configure a Web Service Scan** - Enter or select the full path and name of a Web Service Definition Language (WSDL) file, or click  to open a standard file-selection dialog and

choose a WSDL file. You will import the WSDL file and later launch the Web Service Test Designer to configure a file containing values for each operation in the service.

**Note:** For instructions on conducting a Web service scan of the HP WebInspect test site, click [here](#).

- **Scan with Existing Design File** - Click  to open a standard file-selection dialog and choose a Web Service Test Design (WSD) file that you previously created using the Web Service Test Designer. This file contains values for each operation in the service.

4. Click **Next**.

Note: On any window presented by the Web Service Scan Wizard, you can click **Settings** (at the bottom of the window) to modify the default settings or to load a settings file that you previously saved. Any changes you make will apply to this scan only and will not be retained in the default settings file. To make and retain changes to default settings, click the WebInspect **Edit** menu and select **Default Scan Settings**.

## Authentication and Connectivity

1. If you need to access the target site through a proxy server, select **NetworkProxy** and then choose an option from the **Proxy Profile** list:
  - **Autodetect**: Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.
  - **Use Internet Explorer**: Import your proxy server information from Internet Explorer.
  - **Use PAC File**: Load proxy settings from a Proxy Automatic Configuration (PAC) file. If you select this option, click **Edit** to enter the location (URL) of the PAC.
  - **Use Explicit Proxy Settings**: Specify proxy server settings. If you select this option, click **Edit** to enter proxy information.
  - **Use Mozilla Firefox**: Import your proxy server information from Firefox.

**Note:** Electing to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy server will not be used.

2. If server authentication is required, select **Network Authentication** and then select an authentication method and enter your network credentials. The authentication methods are:

### Basic

A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a user name and password. The Web browser then attempts to establish a connection to a server using the user's credentials. If the credentials are rejected, the browser displays an authentication window to re-enter the user's credentials. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers.

### NTLM

NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and WebInspect has to pass through a proxy server to submit its requests to the Web server, WebInspect may not be able to crawl or audit that Web site. Use caution when configuring WebInspect for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

### Automatic

Allow WebInspect to determine the correct authentication type.

### Digest

The Windows Server operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.

### Negotiate

The Negotiate authentication protocol begins with the option to negotiate for an authentication protocol. When the client requests access to a service, the server replies with a list of authentication protocols that it can support and an authentication challenge based on the protocol that is its first choice. For example, the server might list Kerberos and NTLM, and send a Kerberos challenge.

The client examines the contents of the reply and checks to determine whether it supports any of the specified protocols. If the client supports the preferred protocol, authentication proceeds. If the client does not support the preferred protocol, but does support one of the other protocols listed by the server, the client lets the server know which authentication protocol it supports, and the authentication proceeds. If the client does not support any of the listed protocols, the authentication exchange fails.

3. Click **Next**.

## Detailed Scan Configuration

1. If you are creating a design test file, a message prompts you to launch the Web Service Test Designer. The Scan Wizard will not advance until you use the designer to create a WSD file.
2. If you already selected a design test file, you may click **Design** to open the Web Service Test Designer and edit a web service design (WSD) file containing values that should be submitted to the WSDL file during the scan.
3. (Optional) You may select the following options:
  - Launch and Direct Traffic through Web Proxy. (This option is not available if you are scheduling a scan.)
  - Enable Traffic Monitor.
4. Click **Next**.

## Congratulations

1. If you anticipate running this scan again, you can save the settings in an XML file. Click the **Save** hyperlink to name and save the file.

When starting a scan through the Web Service Scan Wizard, you can click **Settings** (at the bottom of the window) to load this settings file.
2. If you are scheduling a scan, you can also elect to generate a report when the scan completes. Select the **Generate Report** check box, and then click the **Select reports** hyperlink.
3. Click **Scan** (or click **Schedule**, if you are scheduling a scan).

## Running a Basic Scan

The options displayed by default on this and subsequent windows are extracted from the WebInspect default settings. Any changes you make will be used for this scan only. If you click **Settings (Default)** at the bottom of the window to access the full complement of [WebInspect Settings](#), any selections you make are also temporary. To change the default settings, you must select **Default Scan Settings** from the **Edit** menu.

## Basic Scan Options

1. In the **Scan Name** box, enter a name or brief description of the scan.
2. Select one of the following scan modes:
  - **Crawl Only:** This option completely maps a site's hierarchical data structure. After a crawl has been completed, you can click **Audit** to assess an application's vulnerabilities.
  - **Crawl and Audit:** WebInspect maps the site's hierarchical data structure and audits each resource (page). Depending on the default settings you select, the audit can be conducted as each resource is discovered or after the entire site is crawled. For information regarding simultaneous vs. sequential crawl and audit, see [Scan Settings - Method](#).
  - **Audit Only:** WebInspect applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.
  - **Manual:** Manual mode allows you to navigate manually to whatever sections of your application you choose to visit, using Internet Explorer. It does not crawl the entire site, but records information only about those resources that you encounter while manually navigating the site. This feature is used most often to enter a site through a Web form logon page or to define a discrete subset or portion of the application that you want to investigate. Once you finish navigating through the site, you can audit the results to assess the security vulnerabilities related to that portion of the site that you recorded.

**Note:** Manual mode is not available when scheduling scan.

3. Select one of the following scan types:
  - **Standard Scan:** WebInspect performs an automated analysis, starting from the target URL. This is the normal way to start a scan.
  - **Manual Scan:** Manual Crawl (Step Mode) allows you to navigate manually to whatever sections of your application you choose to visit, using Internet Explorer. This choice appears only if you select the Manual Scan mode (above).
  - **List-Driven Scan:** Perform a scan using a list of URLs to be scanned. Each URL must be fully qualified and must include the protocol (for example, `http://` or `https://`). You can use a text file, formatted as comma-separated list or one URL per line, or the XML file generated by the [FilesToURLs utility](#).
  - **Workflow-Driven Scan:** WebInspect audits only those URLs included in the [macro](#) that you previously recorded and does not follow any hyperlinks encountered during the audit. A logout signature is not required. This type of macro is used most often to focus on a particular

subsection of the application. If you select multiple macros, they will all be included in the same scan.

4. If you select **Standard Scan**, follow these instructions:

- a. In the **Start URL** box, type or select the complete URL or IP address of the site you want to examine.

If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, WebInspect will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

An invalid URL or IP address will result in an error. If you want to scan from a certain point in your hierarchical tree, append a starting point for the scan, such as <http://www.myserver.com/myapplication/>.

Scans by IP address will not pursue links that use fully qualified URLs (as opposed to relative paths).

WebInspect supports both Internet Protocol version 4 (IPV4) and Internet Protocol version 6 (IPV6). IPV6 addresses must be enclosed in brackets. See [Internet Protocol Version 6](#).

- b. If you select **Restrict to folder**, you can limit the scope of the scan to the area you choose from the drop-down list. The choices are:

- **Directory only** - WebInspect will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, WebInspect will assess only the "two" directory.
- **Directory and subdirectories** - WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
- **Directory and parent directories** - WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

5. If you select **Manual Scan**, enter a URL and, if desired, select **Restrict to folder**. See Standard Scan (above).

6. If you select **List-Driven Scan**, do one of the following:

- Click **Import** and select a text file or XML file containing the list of URLs you want to scan.
- Click **Manage** to create or modify a list of URLs.

7. If you select **Workflow-Driven Scan**, do one of the following:

- Click **Manage** to select, edit, record, import, export, or remove a macro.
- Click **Record** and create a macro.

**Note:** You can include more than one macro in a scan.

8. Click **Next**.

## Authentication and Connectivity

1. If you need to access the target site through a proxy server, select **NetworkProxy** and then choose an option from the **Proxy Profile** list:
  - **Autodetect:** Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.
  - **Use Internet Explorer:** Import your proxy server information from Internet Explorer.
  - **Use PAC File:** Load proxy settings from a Proxy Automatic Configuration (PAC) file. If you select this option, click **Edit** to enter the location (URL) of the PAC.
  - **Use Explicit Proxy Settings:** Specify proxy server settings. If you select this option, click **Edit** to enter proxy information.
  - **Use Mozilla Firefox:** Import your proxy server information from Firefox.

**Note:** Electing to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy server will not be used.

2. Select **Network Authentication** if server authentication is required. Then select an authentication method and enter your network credentials. The authentication methods are:

### Basic

A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a user name and password. The Web browser then attempts to establish a connection to a server using the user's credentials. If the credentials are rejected, the browser displays an authentication window to re-enter the user's credentials. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers.

## NTLM

NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and WebInspect has to pass through a proxy server to submit its requests to the Web server, WebInspect may not be able to crawl or audit that Web site. Use caution when configuring WebInspect for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

### Automatic

Allow WebInspect to determine the correct authentication type.

### Digest

The Windows Server operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.

### Kerberos

Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.

### Negotiate

The Negotiate authentication protocol begins with the option to negotiate for an authentication protocol. When the client requests access to a service, the server replies with a list of authentication protocols that it can support and an authentication challenge based on the protocol that is its first choice.

For example, the server might list Kerberos and NTLM, and send a Kerberos challenge. The client examines the contents of the reply and checks to determine whether it supports any of the specified protocols. If the client supports the preferred protocol, authentication proceeds. If the client does not support the preferred protocol, but does support one of the other protocols listed by the server, the client lets the server know which authentication protocol it supports, and the authentication proceeds. If the client does not support any of the listed protocols, the authentication exchange fails.

3. Select **Site Authentication** to use a recorded macro containing a user name and password that allows you to log on to the target site. The macro must also contain a "logout condition," which

indicates when an inadvertent logout has occurred so WebInspect can rerun this macro to log on again.

- Click  to select a macro. If, after selecting a macro, you want to modify the macro using the Web Macro Recorder, click **Edit**.

**Note:** To erase the macro name, clear the **Site Authentication** check box.

- Click  to create a macro.
- The **Login Macro Parameters** grid appears if, when recording the macro, you selected the Smart Credentials option (when using the traffic-mode or event-based web macro recorders) or if you created input parameters when using the TruClient web macro recorder. Enter a user name and password. When scanning the page containing the input control associated with this entry, WebInspect will substitute these credentials for those used in the macro. This feature allows you to create a macro using your user name and password, yet when other persons run the scan using this macro, they can substitute their own user credentials.

**Note:** For help creating login parameters with the HP WebInspect web macro recorder, see [Web Macro Recorder Help](#). For help with Smart Credentials using the event-based web macro recorder, see [Event-based WMR Help](#). For help with Smart Credentials using the traffic-mode web macro recorder, see [Traffic-mode WMR Help](#).

4. Click **Next**.

## Coverage and Thoroughness

1. To optimize settings for an application built using either Oracle Application Development Framework Faces components or IBM WebSphere Portal, select **Framework** and then choose **Oracle ADF Faces** or **WebSphere Portal** from the **Optimize scan for** list. HP may develop other settings overlays and make them available through Smart Update.

For more information about scanning a WebSphere portal, see [WebSphere Portal FAQ](#).

2. Use the **CrawlCoverage** slider to specify the crawler settings.

This slider may or may not be enabled, depending on the scan mode you selected. The label associated with this slider also depends on your selection. If enabled, the slider allows you to select one of four crawl positions. Each position represents a specific collection of settings, as represented by the following labels:

### Thorough

A Thorough crawl is an automated crawl that uses the following settings:

- Redundant Page Detection: **OFF**
- Maximum Single URL Hits: **20**
- Maximum Web Form Submissions: **7**
- Create Script Event Sessions: **ON**
- Maximum Script Events Per Page: **2000**
- Number of Dynamic Forms Allowed Per Session: **Unlimited**
- Include Parameters In Hit Count: **True**

### Default

A Default crawl is an automated crawl that uses the following (default scan) settings:

- Redundant Page Detection: **OFF**
- Maximum Single URL Hits: **5**
- Maximum Web Form Submissions: **3**
- Create Script Event Sessions: **OFF**
- Maximum Script Events Per Page: **1000**
- Number of Dynamic Forms Allowed Per Session: **Unlimited**
- Include Parameters In Hit Count: **True**

### Moderate

A Normal crawl is an automated crawl that uses the following settings:

- Redundant Page Detection: **OFF**
- Maximum Single URL Hits: **5**
- Maximum Web Form Submissions: **2**
- Create Script Event Sessions: **OFF**
- Maximum Script Events Per Page: **300**

- Number of Dynamic Forms Allowed Per Session: **1**

- Include Parameters In Hit Count: **False**

#### Quick

A quick crawl uses the following settings

- Redundant Page Detection: **ON**
- Maximum Single URL Hits: **3**
- Maximum Web Form Submissions: **1**
- Create Script Event Sessions: **OFF**
- Maximum Script Events Per Page: **100**
- Number of Dynamic Forms Allowed Per Session: **0**
- Include Parameters In Hit Count: **False**

If you click **Settings** (to open the Advanced Settings dialog) and change a setting that conflicts with any setting established by one of the four slider positions, the slider creates a fifth position labeled **Customized Coverage Settings**.

3. Select a policy from the **AuditDepth (Policy)** list.

This list may or may not be enabled, depending on the scan mode you selected in Step 1. For descriptions of policies, see [WebInspect Policies](#).

4. Click **Next**.

## Detailed Scan Configuration

### Profiler

WebInspect conducts a preliminary examination of the target Web site to determine if certain settings should be modified. If changes appear to be required, the Profiler returns a list of suggestions, which you may accept or reject.

For example, the Server Profiler may detect that authorization is required to enter the site, but you have not specified a valid user name and password. Rather than proceed with a scan that would return significantly diminished results, you could follow the Server Profiler's suggestion to configure the required information before continuing.

Similarly, your settings may specify that WebInspect should not conduct "file-not-found" detection. This process is useful for Web sites that do not return a status "404 Not Found" when a client requests a resource that does not exist (they may instead return a status "200 OK," but the response contains a

message that the file cannot be found). If the Profiler determines that such a scheme has been implemented in the target site, it would suggest that you modify the WebInspect setting to accommodate this feature.

To launch the Profiler each time you access this page, select **Run Profiler Automatically**.

To launch the Profiler manually, click **Profile**. See [Server Profiler](#) for detailed information.

Results appear in the Settings section.

## Settings

1. Accept or reject the suggestions. To reject, clear the associated check box.
2. If necessary, provide the requested information.
3. Click **Next**.

Several options may be presented even if you do not run the Profiler. They include:

- Auto fill Web forms
- Add allowed hosts
- Reuse identified false positives
- Apply sample macro
- Traffic analysis

## Auto Fill Web Forms

Select **Auto-fill Web forms during crawl** if you want WebInspect to submit values for input controls on forms it encounters while scanning the target site. WebInspect will extract the values from a prepackaged default file or from a file that you create using the [Web Form Editor](#). You may:

- Click the ellipsis button  to locate and load a file.
- Click Edit  to edit the selected file (or the default values) using the Web Form Editor.
- Click Create  to open the Web Form Editor and create a file.

## Add Allowed Hosts

Use the Allowed Host settings to add domains to be crawled and audited. If your Web presence uses multiple domains, add those domains here. See [Allowed Hosts](#) for more information.

To add allowed domains:

1. Click **Add**.
2. On the Specify Allowed Host window, enter a URL (or a regular expression representing a URL) and click **OK**.

## Reuse Identified False Positives

Select scans containing vulnerabilities that were changed to false positives. If those false positives match vulnerabilities detected in this scan, the vulnerabilities will be changed to false positives. See [False Positives](#) for more information.

To reuse identified false positives:

1. Select **Import False Positives**.
2. Click **SelectScans**.
3. Select one or more scans containing false positives from the same site you are now scanning.
4. Click **OK**.

**Note:** You cannot import false positives when scheduling a scan or conducting an Enterprise scan.

## Sample Macro

WebInspect's example banking application, zero.webappsecurity.com, uses a Web form login. If you scan this site, select **Apply sample macro** to run the sample macro containing the login script.

## Traffic Analysis

Select **Launch and Direct Traffic through Web Proxy** to use the Web Proxy tool to examine the HTTP requests issued by WebInspect and the responses returned by the target server.

While scanning a Web site, WebInspect displays in the navigation pane only those sessions that reveal the hierarchical structure of the Web site, plus those sessions in which a vulnerability was discovered. However, if you select **Enable Traffic Monitor**, WebInspect adds the **Traffic Monitor** button to the Scan Info panel, allowing you to display and review each HTTP request sent by WebInspect and the associated HTTP response received from the server.

## Message

If the profiler does not recommend changes, the Scan Wizard displays the message, "No settings changes are recommended. Your current scan settings are optimal for this site."

## Congratulations

The contents of this window vary, depending your choices and configuration.

## Upload to WebInspect Enterprise Scan Template

When connected to an enterprise server (WebInspect Enterprise), you can send the settings for this scan to WebInspect Enterprise, which will create a scan template. However, you must be assigned to a role that allows you to create scan templates.

## Save Settings

You can save the settings you configured for this scan, which would allow you to reuse the settings for a future scan.

## Generate Reports

If you are scheduling a scan, you can instruct WebInspect to generate a report when the scan completes.

1. Select **Generate Reports**.
2. Click the **Select reports** hyperlink.
3. (Optional) Select a report from the **Favorites** list.

A "favorite" is simply a named collection of one or more reports and their associated parameters. To create a favorite once you have selected reports and parameters, click the **Favorites** list and select **Add to favorites**.

4. Select one or more reports.
5. Provide information for any parameters that may be requested. Required parameters are outlined in red.
6. Click **Next**.
7. If you select **Automatically Generate Filename**, the name of the report file will be formatted as <reportname> <date/time>. <extension>. For example, if creating a compliance report in pdf format and the report is generated at 6:30 on April 5, the file name would be "Compliance Report 04\_05\_2009 06\_30.pdf." This is useful for recurring scans.

Reports are written to the directory specified for generated reports in the Application settings.

8. If you did not select **Automatically Generate Filename**, enter a name for the file in the **Filename**

box.

9. Select the report format from the **Export Format** list.
10. If you selected multiple reports, you can combine them all into one report by selecting **Aggregate reports into one report**.
11. Select a template that defines the headers and footers used for the report and, if necessary, provide the requested parameters.
12. Click **Finished**.
13. Click **Schedule**.

## Running an Enterprise Scan

An enterprise scan provides a comprehensive overview of your Web presence from an enterprise network perspective. WebInspect will automatically discover all available ports for a range of IP addresses. You can then select which servers to assess for vulnerabilities from all servers that are discovered.

To start an Enterprise Scan:

1. Do one of the following to launch the Enterprise Scan Wizard:
  - On the WebInspect **Start Page**, click **Start an Enterprise scan**.
  - Click **File > New > Enterprise Scan**.
  - Click the drop-down arrow on the **New** icon (on the toolbar) and select **Enterprise Scan**.
  - On the WebInspect **Start Page**, click **Manage Scheduled Scans**, click **Add**, and then select **Enterprise Scan**.
2. On Step 1 of the Enterprise Scan Wizard, specify when you want to conduct the scan. The choices are:
  - **Immediately**: The scan will run immediately after finishing the Scheduled Scan Wizard.
  - **Run Once Date / Time**: Modify the date and time when the scan should begin. You can click the drop-down arrow to reveal a calendar for selecting the date.
  - **Recurrence Schedule**: Use the slider to select a frequency (Daily, Weekly, or Monthly). Then specify the time when the scan should begin and (for Weekly or Monthly) provide other schedule information.
3. Click **Next**.

4. On Step 2 of the Enterprise Scan Wizard, in the **Enterprise Scan Name** box, enter a unique name for this enterprise scan.

At this point, you can perform one or more of the following functions:

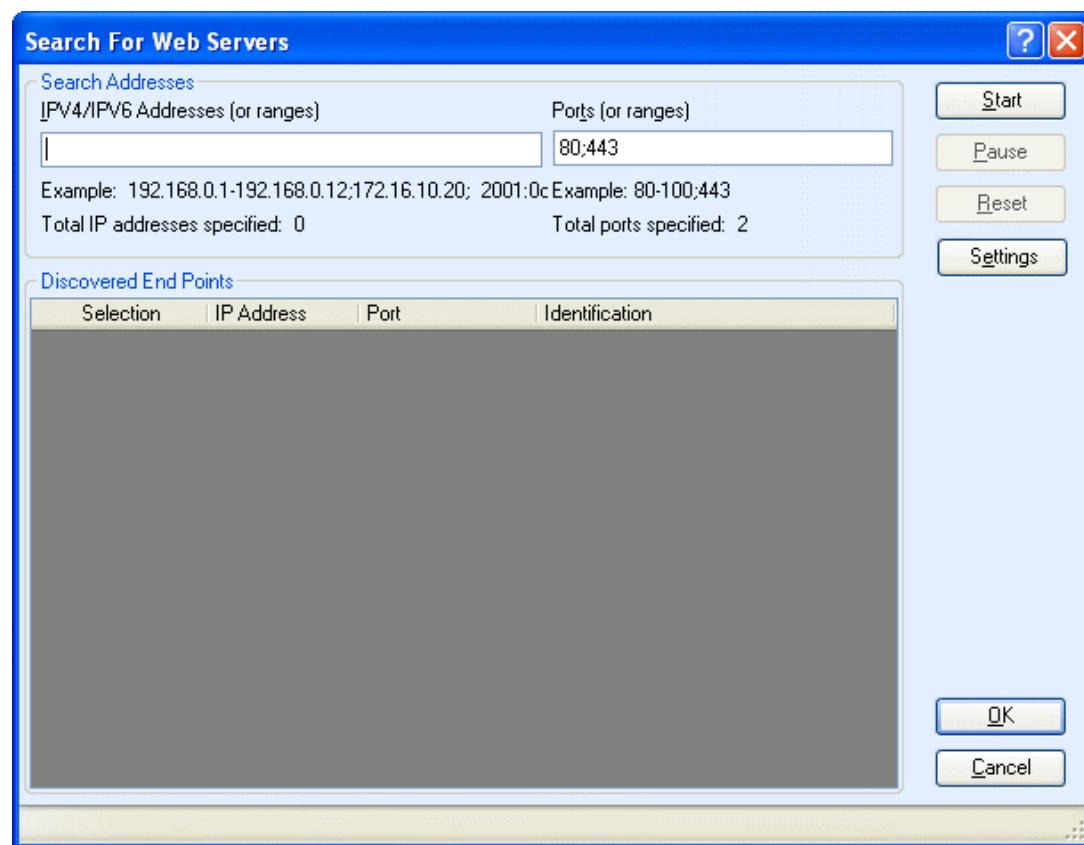
- Instruct WebInspect to discover all available servers within a range of IP addresses and ports that you specify.

Click Discover.

Follow the steps below to discover Web servers.

- a. Click **Discover**.

The Search for Web Servers window appears.



- b. In the **IPV4/IPv6 Addresses (or ranges)** box, type one or more IP addresses or a range of IP addresses.
  - Use a semicolon to separate multiple addresses.  
Example: 172.16.10.3;172.16.10.44;188.23.102.5

- Use a dash or hyphen to separate the starting and ending IP addresses in a range.  
Example: 10.2.1.70-10.2.1.90.

**Note:** IPV6 addresses must be enclosed in brackets. See [Internet Protocol Version 6](#).

- c. In the **Ports (or ranges)** box, type the ports you want to scan.
    - Use a semicolon to separate multiple ports.  
Example: 80;8080;443
    - Use a dash or hyphen to separate the starting and ending ports in a range.  
Example: 80-8080.
  - d. (Optional) Click **Settings** to modify the number of sockets and timeout parameters used for the discovery process.
  - e. Click **Start** to initiate the discovery process.
- Results display in the **Discovered End Points** area.
- Click an entry in the **IP Address** column to view that site in a browser.
  - Click an entry in the **Identification** column to open the Session Properties window, where you can view the raw request and response.
- f. To remove a server from the list, clear the associated check box in the **Selection** column.
  - g. Click **OK**.

The IP addresses appear in the "Hosts to Scan" list.

- Enter individual URLs or IP addresses of hosts to scan.

Click Add.

Follow the steps below to manually enter a list of URLs or IP addresses you want to scan.

- a. Click **Add**.

The Scan Wizard opens.

- b. Provide the information described in [Basic Scan](#).
  - c. Repeat for additional servers.
- Import a list of servers that you want to scan (using a list that you previously created).

Click Import.

If you previously used the Enterprise Scan feature or the [Web Discovery tool](#) to detect servers and

then exported your findings to a text file, you can load those results by clicking **Import** and then selecting the saved file.

## Edit the 'Hosts to Scan' List

After building a list of servers using one or more of the above methods, you can modify the list using the following procedure:

To modify the settings for a specific scan:

1. Select a server.
2. Click **Edit**.  
The Scan Wizard opens.
3. Change the settings.
4. Click **Finish** (on the Edit Basic Scan window)

To delete a server from the list:

1. Select a server.
2. Click **Delete**.

## Export a List

To save the "Hosts to Scan" list:

1. Click **Export**.
2. Using a standard file-selection window, specify the file name and location.

## Start the Scan

To begin the enterprise scan, click **Schedule**. Each server's scan results will automatically be saved upon completion in your default Scans folder. The name of the server, along with a date and time stamp, will be included in the file name.

**Note:** WebInspect licenses permit users to scan specific IP addresses or a range of addresses. If a server has an IP address that is not permitted by your license, that server will not be included in the scan.

## Running a Manual Scan

A manual scan (also referred to as Step Mode) is a Basic Scan option that allows you to navigate manually to whatever sections of your application you choose to visit, using Internet Explorer. It does not crawl the entire site, but records information only about those resources that you encounter while manually navigating the site. This feature is used most often to enter a site through a Web form logon page or to define a discrete subset or portion of the application that you want to investigate. Once you finish navigating through the site, you can audit the results to assess the security vulnerabilities related to that portion of the site that you recorded.

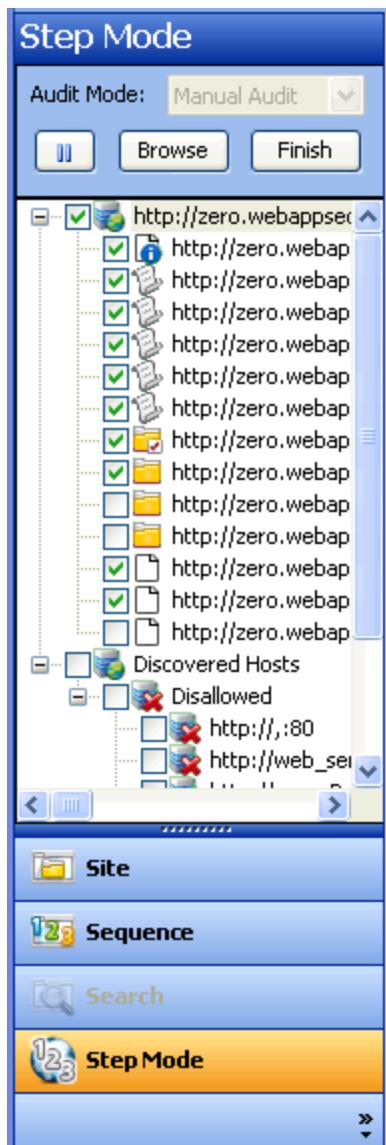
To conduct a manual scan:

1. On the WebInspect **Start Page**, select **Start A Basic Scan**.
2. Follow the instructions for configuring a Basic Scan as described in [Basic Scan Wizard](#), selecting **Manual** as the scan method.
3. Click **Scan**.
4. When Internet Explorer opens, use it to navigate through the site, visiting the areas you want to record.

**Note:** If you want to visit certain areas of the application without recording the sessions, return to WebInspect and click the **Pause** button  displayed in the Step Mode view of the [navigation pane](#). To resume recording sessions, click the **Record** button .

5. When done, close the browser.

WebInspect displays the Step Mode view in the [navigation pane](#), which lists the URL of each resource you visited.



6. Do one of the following:

- To resume browsing the application, select a session and click **Browse**.
- To import the sessions into the scan, click **Finish**. You can exclude an individual session from the import by clearing its associated check box.

7. To audit the recorded sessions, click (on the toolbar).

## Scan Status

Unless otherwise specified, the scan status is read directly from the database. Scan statuses are as follows:

Status	Description
Running	A scheduled scan or a scan initiated through the command-line interface (CLI) is currently running on the local machine.
Locked	Another instance of WebInspect has initiated the scan, which is running and its heartbeat has not expired.  Note: Applies to remote SQL Server (full version) only.
Open	A user on the local machine has the scan open in WebInspect. The user may be the current user (in which case, the scan can be seen on the Scan tab) or it may be another user on the same machine (when using Terminal services, for example). The state stored in the scan database is ignored.
Interrupted	The WebInspect or CLI instance that was last using the scan crashed. The following conditions must be met: <ul style="list-style-type: none"> <li>• The remote database has a status of "Running."</li> <li>• The heartbeat has expired.</li> <li>• The scan is not open on the local machine.</li> </ul>
Incomplete	The user has paused the scan and closed it. It has not finished running.
Complete	The scan has finished.

## Updates to Information in the Scan Manager

The scan manager is not intended to give real-time status information on any of the scans currently being displayed, with three notable exceptions:

- A new scan has been created or opened. In this case, the scan manager will list the new scan with a status of Open.
- A scan that was previously opened by the current user is closed. For example, a user opens/creates a scan, then closes it. The status in the scan manager for the scan is updated to reflect the status of the scan at the time it was closed (for example, Completed, Incomplete, etc.). All statistics will be refreshed for the single scan only.
- The duration field is not always accurate or available while a scan is open. Therefore, when a scan

is in the Open, Running, or Locked state, the **Duration** column will show that the value is unavailable (instead of a number the user will see "-").

To see any other status changes or updated count information, the user MUST click the refresh button.

#### See Also

["Scheduled Scan Status " on page 165](#)

## Opening a Saved Scan

Use one of the following procedures to open a saved file containing the results of a previous scan.

Using the Menu or Tool bar:

- Click **File > Open > Scan**.
- Click the drop-down arrow on the **Open** button and select **Scan**.

From the Start Page tab:

- Click **Start a Basic Scan**.
- On the Home pane, click an entry in the **Recently Opened Scans** list.
- On the Manage Scans pane, select a scan and click **Open** (or double-click the scan name).

WebInspect loads the scan data and displays it on a separate tab.

## Comparing Scans

You can compare the vulnerabilities revealed by two different scans of the same target and use this information to:

- Verify fixes: Compare vulnerabilities detected in the initial scan with those in a subsequent scan of the same site after the vulnerabilities were supposedly fixed.
- Check on scan health: Change scan settings and verify that those changes expand the attack surface.
- Find new vulnerabilities: Determine if new vulnerabilities have been introduced in an updated version of the site.
- Investigate Issues: Pursue anomalies such as false positives or missed vulnerabilities.
- Compare authorization access: Conduct scans using two different user accounts to discover vulnerabilities that are unique or common to both accounts.

**Note:** Data from both scans must be stored in the same database type (SQL Server Express Edition or SQL Server Standard/Enterprise Edition).

## Selecting Scans to Compare Scans

To compare two scans, do one of the following:

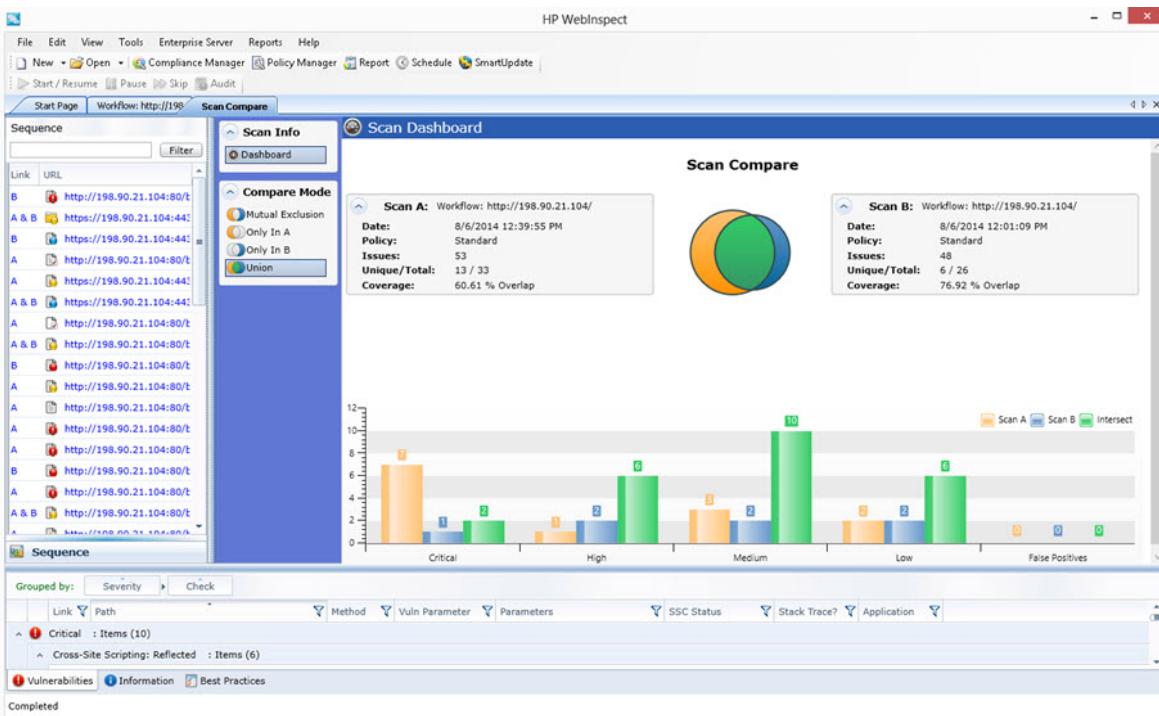
- From the Manage Scans page, select two scans and click **Compare**.
- From a tab containing an open scan (which will be Scan A in the comparison):
  - a. Click **Compare**.
  - b. Select a scan from the list on the Scan Comparison window. This scan will be Scan B in the comparison.
  - c. Click **Compare**.

**Note:** If the open scan is a "site retest" (resulting from **Rescan > Retest Vulnerabilities**), WebInspect automatically selects the parent scan for comparison. For example, if you created a scan named "zero," and then verified vulnerabilities for that scan, the resulting scan would be named (by default) "site retest - zero." With the retest scan open, if you select **Compare**, WebInspect will compare "site retest - zero" with the parent scan "zero."

A warning message appears if the selected scans have different start URLs or used different scan policies, or if the scans are of a different type (such as a Basic Scan vs. a Web service scan). You can choose to continue, or you can terminate the function.

You cannot conduct a comparison if either of the scans is currently running.

## Scan Compare Image



## Reviewing the Scan Dashboard

The Scan Dashboard displays the scan comparison results.

### Scan Descriptions



The Scan A and Scan B boxes provide the following information of the scans:

- Scan A or Scan B:** Name of the scan.
- Date:** Date and time the original scan was conducted.
- Policy:** Policy used for the scan; see [WebInspect Policies](#) for more information.

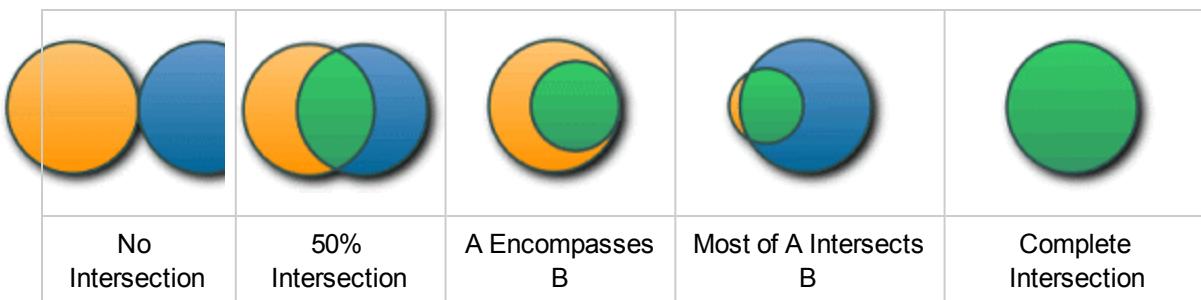
- **Issues:** Total number of issues identified on the Vulnerabilities tab, the Information tab, and the Best Practices tab, as well as false positives detected.
- **Unique/Total:** Number of unique sessions created for this scan (that is, the number of sessions that appear in this scan and not the other scan), compared to the total number of sessions for this scan.
- **Coverage:** Percentage of sessions that are common to both scans.

## The Venn Diagram

The Venn diagram depicts the session coverage of Scan A (represented by a yellow circle) and the session coverage of Scan B (represented by a blue circle). The intersection of the two sets is represented by the green overlap. (In prior releases, the Venn diagram represented the overlap of vulnerabilities.)

The Venn diagram is scaled to reflect the actual relationship between the sets.

Several examples of session coverage overlap are illustrated below.



## Vulnerabilities Bar Chart

In separate groupings for each vulnerability severity and for False Positives, the bottom of the Scan Dashboard displays a set of bar charts that show the number of vulnerabilities found in Scan A, in Scan B, and in their intersection (**Intersect**). The same color coding is used as in the Venn diagram. These bar charts do not change based on the selected **Compare Mode**.

## Effect of Scheme, Host, and Port Differences on Scan Comparison

WebInspect does not ignore the scheme, host, and port when comparing scans from two duplicate sites that are hosted on different servers.

For example, the following site pairs would not be correlated in a scan comparison because of differences in scheme, host, or port:

- **Scheme**
  - Site A - http://zero.webappsecurity.com/
  - Site B - https://zero.webappsecurity.com/
- **Host**
  - Site A - http://dev.foo.com/index.html?par1=123&par2=123
  - Site B - http://qa.foo.com/index.html?par1=123&par2=123
- **Port**
  - Site A - http://zero.webappsecurity.com:80/
  - Site B - http://zero.webappsecurity.com:8080/

## Compare Modes

You can select one of the following options in the **Compare Mode** section to the left of the Scan Dashboard to display different data in the **Sequence** area in the left pane (the data in the Scan Dashboard is not affected):

- **Mutual Exclusion:** Lists sessions that appear in Scan A or Scan B, but not in both scans
- **Only In A:** Lists sessions that appear only in Scan A
- **Only in B:** Lists sessions that appear only in Scan B
- **Union** (the default): Lists sessions that appear in Scan A, Scan B, or both Scans A & B

## Session Filtering

The **Sequence** pane lists each session that matches the selected Compare Mode. An icon to the left of the URL indicates the severity of the vulnerability, if any, for that session. The severity icons are:

Critical	High	Medium	Low

At the top of the **Sequence** pane, you can specify a filter and click **Filter** to limit the set of displayed sessions in the following ways:

- You can enter the URL with only its starting characters, as a "starts with" match. Your entry must begin with the protocol (http:// or https://).
- You can search for an exact match by specifying the URL in quotes. Your entry must begin with the quotes and protocol ("http:// or "https://")
- You can use an asterisk (\*) as a wildcard character at the beginning or end of the string you enter.
- You can use asterisks (\*) at both the beginning and end of the string you enter, which requires matches to contain the string between the asterisks.
- You can enter a question mark (?) followed by a full query parameter string to find matches to that query parameter.

## Using the Session Info Panel

When you select a session in the **Sequence** pane, the **Session Info** panel opens below the **Compare Mode** options. With a session selected, you can select an option in the **Session Info** panel to display more details about that session to the right of the **Session Info** panel. If the session contains data for both scans, the data for some functions such as **Web Browser**, **HTTP Request**, and **Steps** are shown in a split view with Scan A on the left side and Scan B on the right side.

**Note:** The **Steps** option displays the path taken by WebInspect to arrive at the session selected in the **Sequence** pane or the URL selected in the **Summary** pane. Beginning with the parent session (at the top of the list), the sequence reveals the subsequent URLs visited and provides details about the scan methodology. In a scan comparison, if any of the steps for the session are different between the scans, the **In Both** column is added to the **Steps** table (as the first column). A value of **Yes** in the column for a particular step indicates that the step is the same for that session for both scans A and B. A value of **No** in the column for a particular step indicates that the step is different for that session between scans A and B.

## Using the Summary Pane to Review Vulnerability Details

When comparing scans, the horizontal Summary pane at the bottom of the window provides a centralized table of vulnerable resources and allows you to quickly access vulnerability information. You can drag the horizontal divider above the table to show or hide more of the Summary pane.

The **Vulnerabilities** tab at the bottom of the page is selected by default. The **Information** and **Best Practices** tabs display analogous data.

The set of entries (rows) displayed in the table depends on the option selected for **Compare Mode**, as reflected in the **Link** column in the table.

## Grouping and Sorting Vulnerabilities

For information on grouping and sorting vulnerabilities, see "Summary Pane" on page 84 and "Using Filters and Groups in the Summary Pane" on page 196.

## Filtering Vulnerabilities

You can click the filter icon () at the right of any column heading to open a filter that allows you to choose a variety of conditions regarding that column that must be met in order for a vulnerability (row) to remain listed in the table after filtering. The available conditions include the full set of current values in the column, and you can also specify logical expressions regarding the content of that column.

For example, in the filter for the **Vuln Parameter** column, suppose you:

1. Leave the top set of check boxes as is.
2. Below the **Show rows with value that** text, select **Contains** from the drop-down menu.
3. Type **Id** in the text box below the drop-down menu.
4. Click **Filter**.

Then the table will show only rows that contain the text "Id" in the **Vuln Parameter** column. This would include rows for which the value of **Vuln Parameter** is **accountId** or **payeeId** or any other entry that includes "Id."

You can specify filters for multiple columns, one column at a time, and they will all be applied.

If a filter for a column has been specified, its icon becomes a darker blue than the icons for unused filters.

To quickly clear a filter, click **Clear Filter** while the filter is open to be specified.

## Working with Vulnerabilities

Right-clicking an item in the Summary pane displays a shortcut menu containing the following commands:

- **Copy URL:** Copies the URL to the Windows clipboard.
- **Copy Selected Item(s):** Copies the text of selected items to the Windows clipboard.
- **Copy All Items:** Copies the text of all items to the Windows clipboard.
- **Export:** Creates a comma-separated values (csv) file containing either all items or selected items and displays it in Microsoft Excel.
- **View in Browser:** Renders the HTTP response in a browser.

- **Review Vulnerability:** Allows you to retest the vulnerability. If the vulnerability was detected in only one scan, the Vulnerability Review window opens; if the vulnerability was detected in both scans, you are first prompted to select a scan. See [Vulnerability Review](#) for more information.

**Note:** For Post and Query parameters, click an entry in the **Parameters** column to display a more readable synopsis of the parameters.

#### See also

["Summary Pane" on page 84](#)

["Using Filters and Groups in the Summary Pane" on page 196](#)

## Manage Scans

To manage scans:

1. On the **Start Page**, click **Manage Scans**.



A list of scans appears in the right-hand pane of the **Start Page**.

By default, WebInspect lists all scans saved in the SQL Server Express Edition on your machine and in SQL Server Standard Edition (if configured). The current state of the scan is indicated in the [Status column](#).

2. (Optional) To group scans into categories based on the column headings, drag the heading and drop it on the grouping area.
3. Use the toolbar buttons to perform the functions listed below.
  - To open scans, select one or more scans and click **Open** (or simply double-click an entry in the list). WebInspect loads the scan data and displays each scan on a separate tab.
  - To launch the Scan Wizard prepopulated with settings last used for the selected scan, click **Rescan > Scan Again**.
  - To rescan only those sessions that contained vulnerabilities revealed during a previous scan, select a scan and click **Rescan > Retest Vulnerabilities**.
  - To rename a selected scan, click **Rename**.
  - To delete the selected scan(s), click **Delete**.
  - To import a scan, click **Import**.

- To export a scan or scan details, or to export a scan to Software Security Center, click the drop-down button on **Export**.
- To compare scans, select two scans (using **Ctrl + click**) and click **Compare**.
- By default, WebInspect lists all scans saved in the local SQL Server Express Edition and in a configured SQL Server Standard Edition. To select one or both databases, or to specify a SQL Server connection, click **Connections**.
- When necessary, click **Refresh** to update the display.
- To select which columns should be displayed, click **Columns**. You can rearrange the order in which columns are displayed using the **Move Up** and **Move Down** buttons or, on the **Manage Scans** list, you can simply drag and drop the column headers.

**Note:** You can also perform most of these functions by right-clicking an entry and selecting a command from the shortcut menu. In addition, you can also choose to generate a report; see [Generating a Report](#) for more information.

#### See Also

["Managing Scheduled Scans " on page 161](#)

["Start Page " on page 35](#)

## Schedule a Scan

You can schedule a Basic Scan, a Web Service Scan, or an Enterprise Scan to occur at a date and time of your choosing.

The options and settings you select are saved in a special file and accessed by a Windows service that starts WebInspect (if necessary) and initiates the scan. It is not necessary for WebInspect to be running at the time you specify for the scan to begin.

**Note:** To access scheduled scans after they are complete, select the **Start Page** tab and click **Manage Scans**.

Follow the steps below to schedule a scan.

1. Do one of the following:
  - Click the **Schedule** icon on the WebInspect toolbar.
  - Click **Manage Scheduled Scans** on the WebInspect **Start Page**.
2. When the Manage Scheduled Scans window appears, click **Add**.

3. In the **Type of Scan** group, choose one of the following:
  - **Basic Scan**
  - **Web Service Scan**
  - **Enterprise Scan**
4. To conduct the scan one time only, select **Run Once** and then edit the **Start Date** and **Time**. If you click the drop-down arrow, you can use a calendar to select the date.
5. To scan a site periodically:
  - a. Select **Recurring** (or **Recurrence Schedule**), then specify the start time and choose a frequency: **Daily**, **Weekly**, or **Monthly**.
  - b. If you select **Weekly** or **Monthly**, provide the additional requested information.
6. Click **Next**.

For additional instructions, click the type of scan you are conducting:

["Running a Basic Scan" on page 133](#)

["Running a Web Service Scan " on page 130](#)

["Running an Enterprise Scan " on page 144](#)

#### See Also

["Configuring Time Interval for Scheduled Scan " below](#)

## Configuring Time Interval for Scheduled Scan

To configure when to run a scan or to set up recurring scans:

1. In the **Type of Scan** group, choose one of the following:
  - Basic Scan
  - Web Service Scan
  - Enterprise Scan
2. To conduct a scan now, select **Immediately**.
3. To conduct a one-time-only scan at a later date or time:

- a. Select **Run Once**.
- b. Modify the date and time when the scan should begin.

**Tip:** Click the drop-down arrow to reveal a calendar for selecting the date.

4. To scan a site periodically:
  - a. Select **Recurring**.
  - b. Specify the time when the scan should start.
  - c. Choose a frequency: Daily, Weekly, or Monthly.
5. Click **Next**.

For additional instructions, click the type of scan you are conducting:

["Running a Basic Scan" on page 133](#)

["Enter a name for the scan in the Scan Name box." on page 130](#)

["At this point, you can perform one or more of the following functions:" on page 145](#)

## Managing Scheduled Scans

You can instruct WebInspect to conduct a scan at a time and date you specify. The options and settings you select are saved in a special file and accessed by a Windows service that starts WebInspect (if necessary) and initiates the scan. It is not necessary for WebInspect to be running at the time you designate the scan to begin.

**Note:** Note: Scheduled scans, when complete, do not appear in the Recent Scans list that displays on the WebInspect Start page. To access scheduled scans after they are complete, select the Start page and click Manage Scans.

On the **Start Page**, click **Manage Schedule**.



A list of scans you previously scheduled appears in the right-hand pane of the **Start Page**.

The current state of the scan is indicated in the **Status column**.

You can perform the following tasks:

Delete a Scan

To delete a scan from the list, select a scan and click **Delete**.

## Edit Scan Settings

To edit settings for a scheduled scan, select a scan and click **Edit**.

## Run a Scan Immediately

To run a scan immediately, without waiting for the scheduled time, select a scan and click **Start** (or right-click a scan and select **Start Scan** from the shortcut menu). As with all scheduled scans, the scan runs in the background and does not appear on a tab.

## Stop a Scheduled Scan

To stop a scheduled scan, select a scan that is running and click **Stop** (or right-click a running scan and select **Stop Scan** from the shortcut menu).

## Schedule a Scan

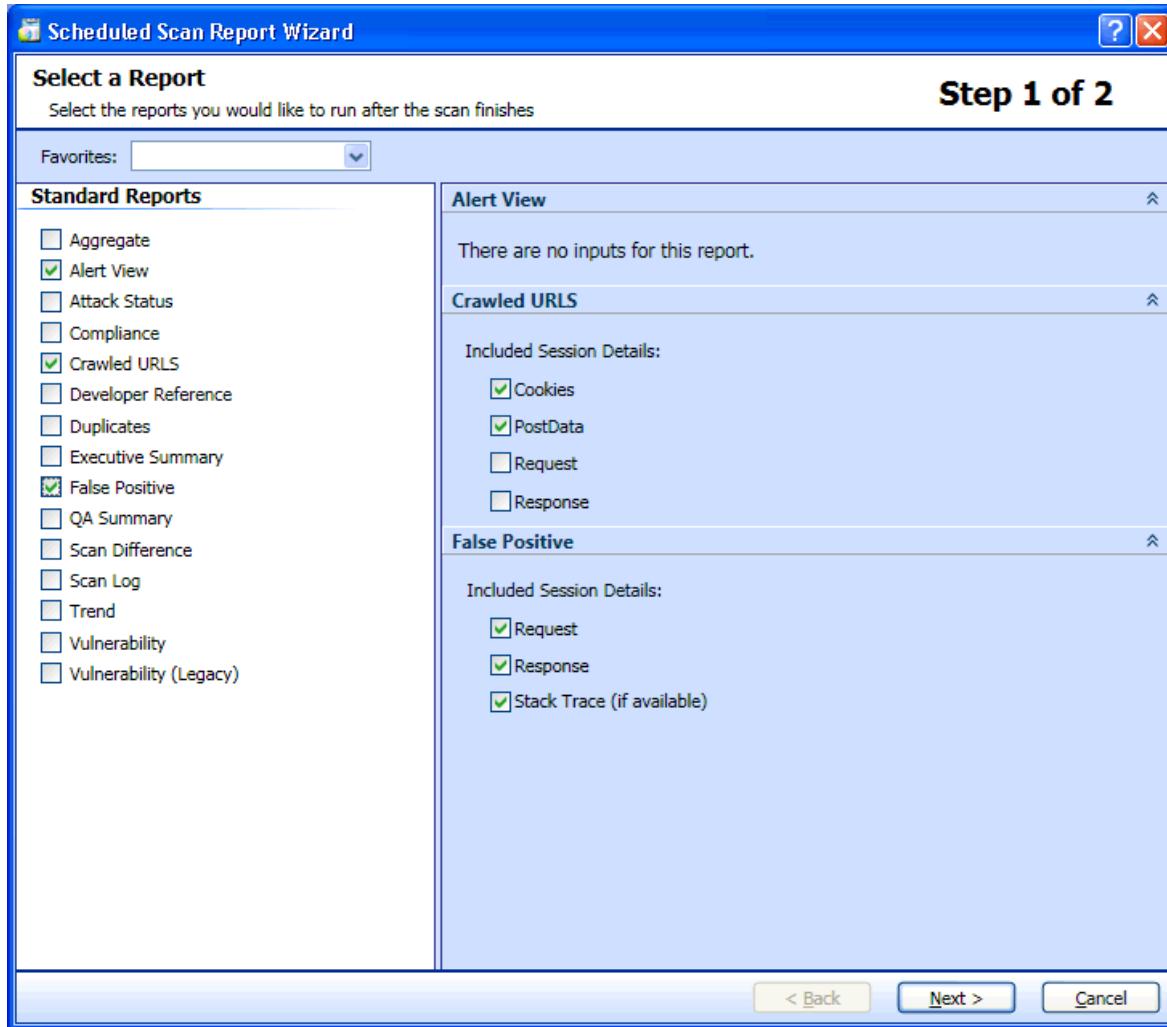
To schedule a scan:

1. Click **Add**.
2. In the Type of Scan group, choose one of the following:
  - Basic Scan
  - Web Service Scan
  - Enterprise Scan
3. Specify when you want to conduct the scan. The choices are:
  - Immediately
  - Run Once: Modify the date and time when the scan should begin. You can click the drop-down arrow to reveal a calendar for selecting the date.
  - Recurrence Schedule: Use the slider to select a frequency (Daily, Weekly, or Monthly). Then specify the time when the scan should begin and (for Weekly or Monthly) provide other schedule information.
4. Click **Next**.
5. Enter the settings for the type of scan you selected.
6. For Web Site and Web Service Scans only, you can elect to run a report at the conclusion of the scan:
  - a. Select **Generate Reports** and click the **Select Reports** hyperlink.
  - b. Continue with Selecting a Report (below).
7. To schedule the scan without generating a report, click **Schedule**.

## Selecting a Report

If you opted to include a report with the scheduled scan, the Scheduled Scan Report Wizard dialog appears:

Scheduled Scan Report Wizard (Step 1 of 2) Image



1. (Optional) Select a report from the **Favorites** list.

A "favorite" is simply a named collection of one or more reports and their associated parameters. To create a favorite once you have selected reports and parameters, click the **Favorites** list and select **Add to favorites**.

2. Select one or more reports.
3. Provide information for any parameters that may be requested. Required parameters are outlined

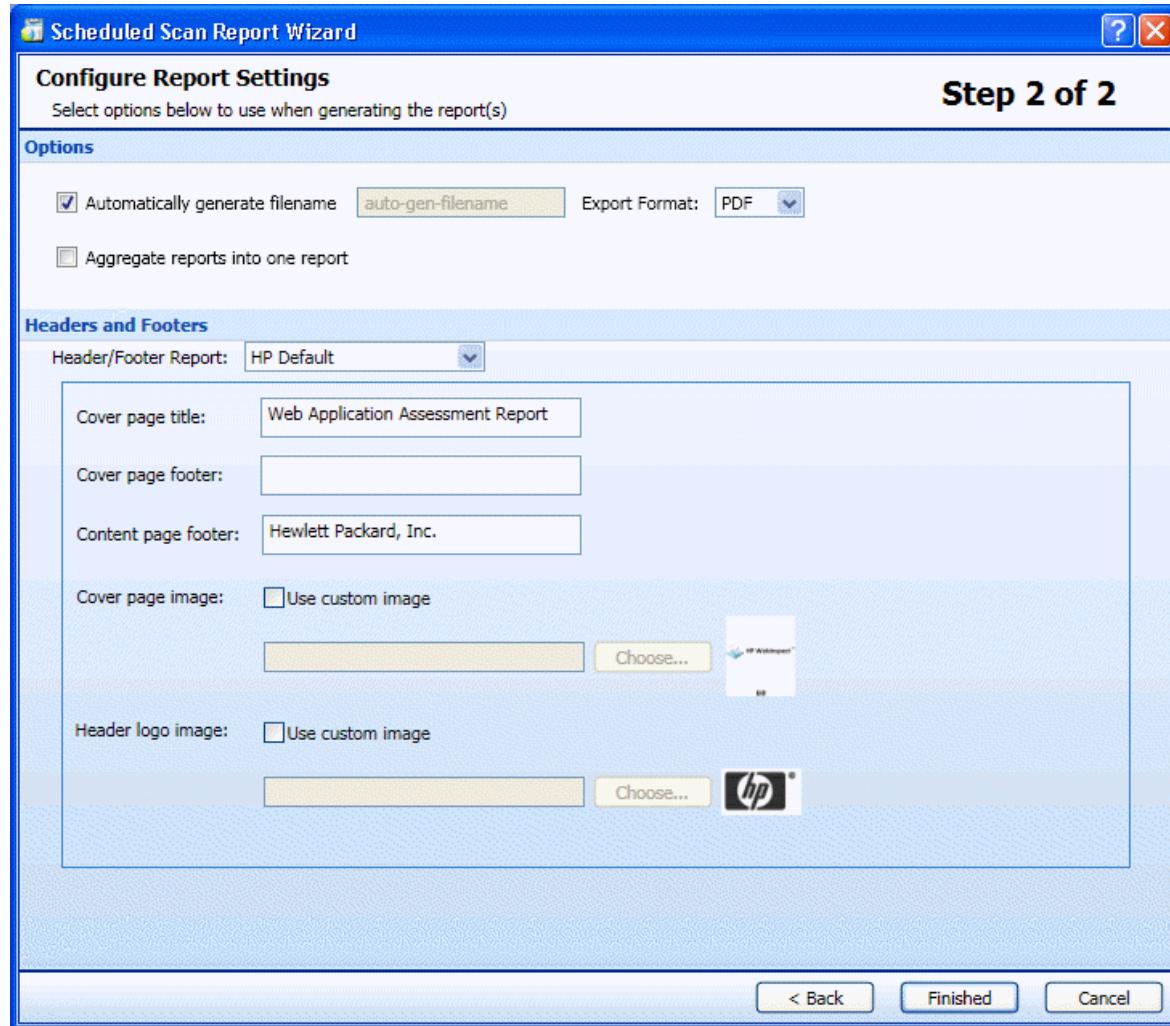
in red.

4. Click **Next**.

The Configure Report Settings dialog appears.

## Configuring Report Settings

Scheduled Scan Report Wizard (Step 2 of 2) Image



1. If you select **Automatically Generate Filename**, the name of the report file will be formatted as <reportname> <date/time>. <extension>. For example, if creating a compliance report in pdf format and the report is generated at 6:30 on April 5, the file name would be "Compliance Report 04\_05\_2009 06\_30.pdf." This is useful for recurring scans.  
Reports are written to the directory specified for generated reports in the Application settings.

2. If you did not select **Automatically Generate Filename**, enter a name for the file in the **Filename** box.
3. Select the report format from the **Export Format** list.
4. If you selected multiple reports, you can combine them all into one report by selecting **Aggregate reports into one report**.
5. Select a template that defines the headers and footers used for the report and, if necessary, provide the requested parameters.
6. Click **Finished**.
7. Click **Schedule**.

#### See Also

- ["Start Page" on page 35](#)  
["Manage Scans" on page 158](#)  
["Scheduled Scan Status" below](#)

## Stopping a Scheduled Scan

To halt a scheduled scan while it is running, select the scan from the Manage Schedule list and click  **Stop** (or right-click the scan and select **Stop Scan** from the shortcut menu).

To restart a stopped scan, select the scan from the Manage Schedule list and click  **Start** (or right-click the scan and select **Start Scan** from the shortcut menu).

## Scheduled Scan Status

The status of each scheduled scan appears in the **Last Run Status** column on the **Manage Schedule** pane. The possible statuses are defined in the following table.

Status	Definition
Failure	WebInspect was unable to perform the scan.
Success	The scan was conducted without error.
Not Yet Run	The scan is queued to run at the scheduled time, which has not yet occurred.
Skipped	The scheduled scan was not run because the service was down for some period of time.

Status	Definition
Stopping	The user clicked the <b>Stop</b> button, but the scan has not yet stopped.
Stopped	The scan has been stopped by the user.
Running	The scheduled scan is in progress.
Running with Error	The scan could not stop; see log for further details.

## Exporting a Scan

Use the Export Scan function to save information collected during a WebInspect crawl or audit.

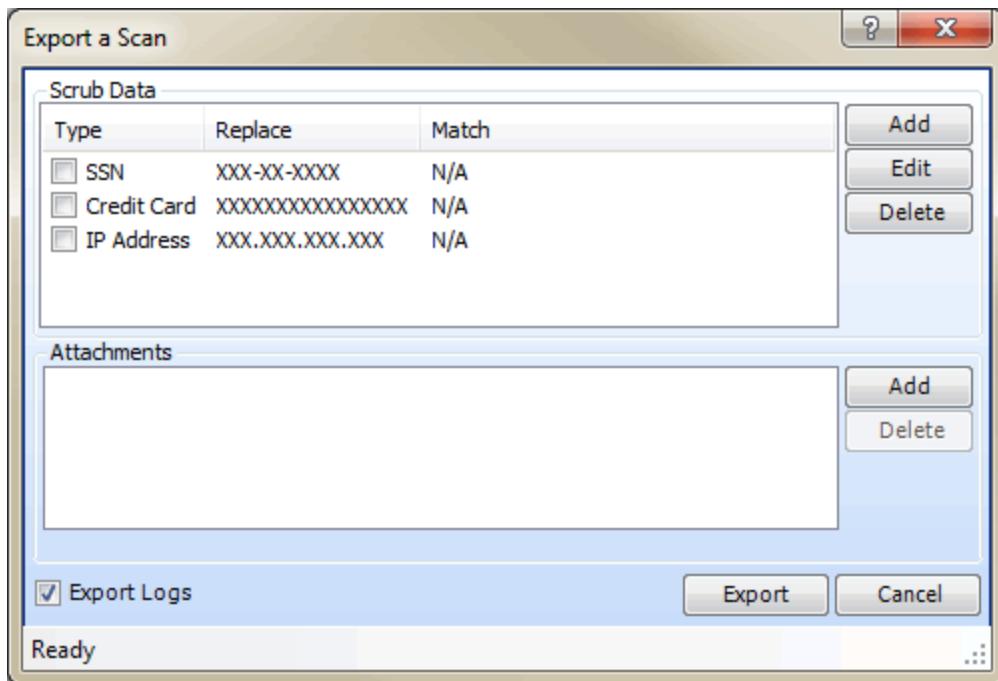
**Note:** When exporting to Software Security Center (SSC), after exporting to the .fpr format, you must manually upload the .fpr file to SSC. HP does not support uploading both WebInspect FPR artifacts and WebInspect Enterprise FPR artifacts to the same project version in SSC.

Follow the steps below to export a scan.

1. Do one of the following:

- Open a scan (or click a tab containing an open scan), click **File > Export** and select either **Scan** or **Scan to Software Security Center**
  
- On the Manage Scans pane of the Start page, select a scan, click the drop-down arrow on the **Export** button and select either **Export Scan** or **Export Scan to Software Security Center**.

The Export a Scan window (or the Export Scan to Software Security Center window) appears.



2. The **Scrub Data** group contains, by default, three non-editable regular expression functions that will substitute X's for each digit in a string formatted as a Social Security number, credit card number, or IP address. To include a search-and-replace function, select its associated check box. This feature prevents any sensitive data from being included in the export.
3. To create a Scrub Data function:
  - a. Click **Add**.
  - b. On the Add Scrub Entry window, select either **Regex** or **Literal** from the **Type** list.
  - c. In the **Match** box, enter the string (or a regular expression representing a string) that you want to locate. If using a regular expression, you can click the ellipsis button [...] to open the Regular Expression Editor, with which you can create and test your regular expression.
  - d. In the **Replace** box, enter the string that will replace the target specified by the **Match** string.
  - e. Click **OK**.
4. If you are exporting to Software Security Center, go to Step 7.
5. If you want to include an attachment:
  - a. In the **Attachments** group, click **Add**.
  - b. Using the standard file-selection window, navigate to the directory that contains the file you

want to attach.

- c. Select a file and click **Open**.
6. To include the scan's log files, select **Export Logs**.
7. Click **Export**.
8. Using the standard file-selection window, select a location and click **Save**.

#### See Also

["Importing a Scan " on page 173](#)

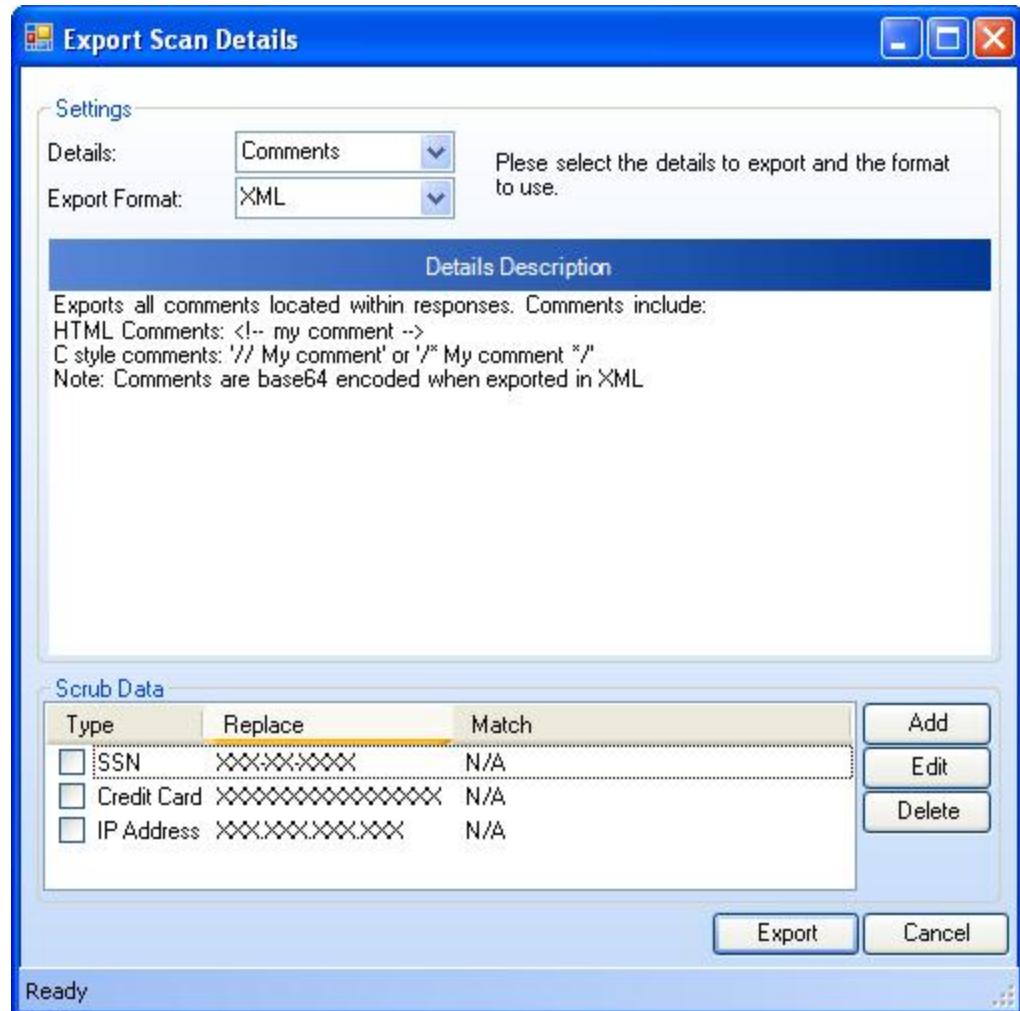
["Exporting Scan Details " below](#)

## Exporting Scan Details

Use this function to save information collected during a WebInspect crawl or audit.

1. Open a scan, or click a tab containing a scan.
2. Click **File > Export > Scan Details**.

The Export Scan Details window appears.



3. From the **Details** list, select the type of information you want to export. The options are as follows:
  - Comments
  - Emails
  - Full (all details)
  - Hidden Fields
  - Offsite Links
  - Parameters
  - Requests

- Script
- Sessions
- Set Cookies
- URLs
- Vulnerabilities
- Web Crawl Dump
- Site Tree Dump
- Web Forms

**Note:** Not all choices are available for a Web Service scan.

4. Choose a format (either Text or XML) from the **Export Format** list.
5. The **Scrub Data** group contains, by default, three non-editable regular expression functions that will substitute X's for each digit in a string formatted as a Social Security number, credit card number, or an IP address. To include this search-and-replace function for a data type, select its associated check box. This feature prevents any sensitive data from being included in the export.
6. To create a Scrub Data function:
  - a. Click **Add**.
  - b. On the Add Scrub Entry window, select either **Regex** or **Literal** from the **Type** list.
  - c. In the **Match** box, enter the string (or a regular expression representing a string) that you want to locate. If using a regular expression, you can click the ellipsis button [...] to open the Regular Expression Editor, with which you can create and test your regular expression.
  - d. In the **Replace** box, enter the string that will replace the target specified by the **Match** string.
  - e. Click **OK**.
7. Click **Export**.
8. Using a standard file-selection window, specify a name and location for the exported file and click **Save**.

## See Also

["Exporting a Scan " on page 166](#)

# Export Scan to Software Security Center

This feature allows you to export the results of a WebInspect scan in a format (.fpr format) that can be consumed by HP Fortify Software Security Center (SSC).

**Note:** After exporting to the .fpr format, you must manually upload the .fpr file to SSC. HP does not support uploading both WebInspect FPR artifacts and WebInspect Enterprise FPR artifacts to the same project version in SSC.

1. Do one of the following:
  - Open a scan (or click a tab containing an open scan) and click **File > Export > Scan to Software Security Center**.
  - On the Manage Scans pane of the Start page, select a scan, click the drop-down arrow on the **Export** button and select **Export Scan to Software Security Center**.
- The Export Scan to Software Security Center window appears.
2. The **Scrub Data** group contains, by default, three non-editable regular expression functions that will substitute X's for each digit in a string formatted as a Social Security number, credit card number, or IP address. To include a search-and-replace function, select its associated check box. This feature prevents any sensitive data from being included in the export.
3. To create a Scrub Data function:
  - a. Click **Add**.
  - b. On the Add Scrub Entry window, select either **Regex** or **Literal** from the **Type** list.
  - c. In the **Match** box, enter the string (or a regular expression representing a string) that you want to locate. If using a regular expression, you can click the ellipsis button [...] to open the Regular Expression Editor, with which you can create and test your regular expression.
  - d. In the **Replace** box, enter the string that will replace the target specified by the **Match** string.
  - e. Click **OK**.
4. Click **Export**.
5. Using the standard file-selection window, select a location and click **Save**.

# Exporting Protection Rules to HP TippingPoint

Use the export function to create an .xml file that can be imported into the TippingPoint Digital Vaccine Toolkit, based on vulnerabilities detected by HP WebInspect during a scan of your web application.

The Digital Vaccine Toolkit can then create and import filters into the HP TippingPoint Security Management System for distribution across a network of Intrusion Prevention System (IPS) devices.

To create the file that can be imported into the TippingPoint Digital Vaccine Toolkit:

1. Open the scan of interest (or click a tab containing an open scan) and click **File > Export > Protection Rules to HP TippingPoint**.
2. Specify the **Export Path**, that is, the directory to which you want the new file to be saved.
3. The **Destination Address** is optional.
4. Click **Export**.

The mapped vulnerabilities are transformed and exported to some of all of the following files on the path you specified:

- TpXssRules.xml
- TpSqlnjRules.xml
- TpFileIncludeRules.xml

5. In the TippingPoint Digital Vaccine Toolkit, click **File > Import XML** to import each of the .xml files, one at a time. Ignore all Filter Validation messages (click **Yes** in them to continue).

The content of the imported files accumulates in one .csv file of filters.

6. Click **File > Save As** and save the accumulated file as a .csv file.
7. To import the .csv file into TippingPoint Security Management System, click **Profiles**, then click **DV Toolkit Packages**, and then click **Import** and select the .csv file. When the import completes, click **Activate**, and when the activation completes, click **Distribute** and select the device to which you want to distribute the file. In the IPS Profiles, block your filters. For more information, see the TippingPoint Security Management System documentation.

# Exporting Protection Rules to Web Application Firewall

To generate and save a full export (.xml) file based on vulnerabilities detected by HP WebInspect during a scan of your web application:

1. Open the scan of interest (or click a tab containing an open scan) and click **File > Export > Protection Rules to Web Application Firewall**.
2. Specify the scrub data types in the same way as for the **File > Export > Scan** option. The **Scrub Data** group contains, by default, three non-editable regular expression functions that will substitute an X for each digit in a string formatted as a Social Security Number, credit card number, or IP address. To include this search-and-replace function for a data type, select its associated check box. This feature prevents any sensitive data from being included in the export.
3. Click **Export**.
4. Specify the path and filename to which you want to save the exported data and click **Save**.

A full export (.xml) file is saved as you specified.

# Importing a Scan

Follow the steps below to import a scan.

1. Click **File > Import Scan**.
2. Using a standard file-selection window, select an option from the **Files Of Type** list:
  - Scan files (\*.scan) - scan files designed for or created by WebInspect versions beginning with 7.0.
  - SPA files (\*.spa) - scan files created by versions of WebInspect prior to release 7.0.
3. Choose a file and click **Open**.

If attachments were exported with the scan, those attachments will be imported and saved in a subdirectory of the imported scan. The default location is C:\Documents and Settings\<username>\Local Settings\Application Data\HP\HP WebInspect\ScanData\Imports\<DirectoryName>\<filename>, whereDirectoryName is the ID number of the exported/imported scan.

## See Also

["Exporting a Scan " on page 166](#)

## Importing False Positives

You can import from a previous scan a list of vulnerabilities that were analyzed as being false positive. WebInspect then correlates these false positives from a previous scan with vulnerabilities detected in the current scan and flags the new occurrences as false positives.

Select a scan containing false positives from the same site you are now scanning.

**Note:** You cannot import false positives when scheduling a scan or conducting an Enterprise scan.

To import false positives:

1. In the scan currently being conducted, select **False Positives** in the **Scan Info** panel.

The Scan False Positives window appears.

2. Click **Import False Positives**.

The Select a Scan to Import False Positives window appears.

3. Select the checkbox(es) for the scan or scans from which you want to import false positives, and click **OK**.

The Importing False Positives window appears, displaying the progress of the import.

4. When the import is complete, do one of the following:

- Click **Details** to view a log file for the import.
- Click **Close** to view the false positive(s) in the Scan False Positives window.

## Importing Legacy Web Service Scans

WebInspect 10.0 and greater offers minimal support for Web Service scans that were created with versions of WebInspect earlier than 9.0. These scans do not contain all the information required to render them properly in the current user interface and will exhibit the following attributes:

- The tree view may not show the correct structure.
- Even if the operations do not appear in the tree view, the vulnerabilities will appear in the vulnerability list. You should be able to select these vulnerabilities and view the vulnerability information, as well as the request and the response.

- Nothing will display in the XmlGrid.
- The rescan functionality should launch the Web Services scan wizard and select the first option having the selected WSDL already populated. This should force the Web Service Test Designer to open on page 3.
- The "Vulnerability Review" feature should be disabled.
- All reports should work as in previous WebInspect releases.
- The Scan view should render in "ReadOnly" mode, which disables the **Start**, **Audit** and **Current Settings** buttons.

HP recommends that you rescan your Web service.

## Changing Import/Export Settings

If you require different settings for different scan actions, you can save your settings in an XML file and load them when needed. You can also reload the WebInspect factory default settings.

**Tip:** You can also create, edit, delete, import, and export scan settings files from the Manage Settings window. Click **Edit** and select **Manage Settings**

1. Click **Edit > Default Settings**.

The Default Settings window appears.

2. To export settings:
  - a. Click **Save settings as** (at the bottom of the left pane).

On the Save Scan Settings window, select a folder and enter a file name.

c. Click **Save**.

3. To import settings:
  - a. Click **Load settings from file** (at the bottom of the left pane).

On the Open Scan Settings File window, select a file.

c. Click **Open**.

4. To restore factory default settings:

- a. Click **Restore factory defaults** (at the bottom of the left pane).
- b. When prompted to confirm your selection, click **Yes**.

## Downloading a Scan from Enterprise Server

Use the following procedure to download a scan from the enterprise server (WebInspect Enterprise) to WebInspect.

1. Click the WebInspect **Enterprise Server** menu and select **Download Scan**.
2. On the Download Scan(s) window, select one or more scans from the list of available scans.
3. Click **OK**.

The downloaded scan is added to the list of scans on the [Manage Scans pane](#). The scan date becomes the date you downloaded the scan, not the date on which the site originally was scanned.

### See Also

["Uploading a Scan to Enterprise Server" below](#)

## Uploading a Scan to Enterprise Server

Use the following procedure to upload a scan file from WebInspect to an enterprise server (WebInspect Enterprise).

1. Click the WebInspect **Enterprise Server** menu and select **Upload Scan**.
2. On the Upload Scan(s) window, select one or more WebInspect scans from the **Scan Name** column.

**Note:** To access scans in a different database, click **Connections** and, in the Database application settings, change options under **Connection Settings for Scan Viewing**.

3. For each scan, select a **Project** and **Project Version** from the appropriate drop-down lists.

The program attempts to select the correct project and project version based on the "Scan URL" in the scan file, but you may select an alternative.

4. Click **Upload**.

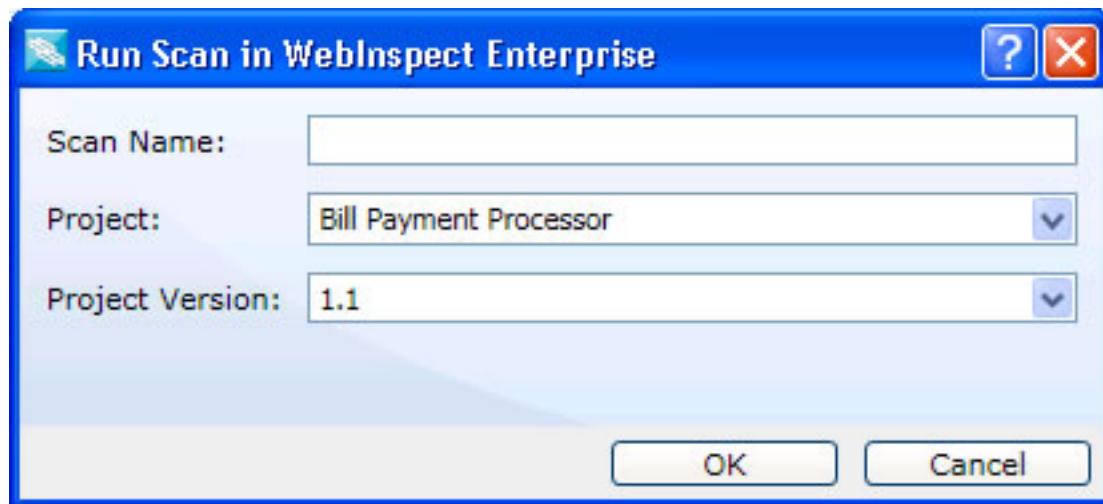
### See Also

["Downloading a Scan from Enterprise Server" above](#)

## Running a Scan in Enterprise Server

This feature is designed for users who prefer to configure a scan in WebInspect rather than WebInspect Enterprise. You can modify the settings and run the scan in WebInspect, repeating the process until you achieve what you believe to be the optimal settings. You can then send the open scan's settings to WebInspect Enterprise, which creates a scan request and places it in the scan queue for the next available sensor.

1. Open a scan.
2. If you are not connected to an enterprise server, click the **Enterprise Server** menu and select **Connect to WebInspect Enterprise**.
3. Click the **Scan** menu and select **Run in WebInspect Enterprise** (or simply click the appropriate button on the toolbar).
4. On the **Run Scan in WebInspect Enterprise** dialog, enter a name for the scan.



5. Select a **Project** and a **Project Version**.
6. Click **OK**.

If you pass all permission checks, the scan is created and the priority assigned to the scan is the highest priority allowed by your role (up to 3, which is the default).

## Transferring Settings to/from Enterprise Server

Use this feature to:

- Create a WebInspect Enterprise scan template based on a WebInspect settings file and upload it from WebInspect to an enterprise server (WebInspect Enterprise).
- Create a WebInspect settings file based on an enterprise server scan template and download it to WebInspect.

WebInspect settings files and WebInspect Enterprise scan templates do not have the same format; not all settings in one format are replicated in the other. Note the warnings that follow descriptions of the conversion procedure.

## To Create a WebInspect Enterprise Scan Template

1. Click the WebInspect **Enterprise Server** menu and select **Transfer Settings**.
2. On the Settings Transfer window, select a WebInspect settings file from the **Local Settings Filelist**.
3. (Optional) Click **View** to review the settings as they appear in a WebInspect settings file. To continue, click **Close**.
- Note:** This is a read-only file. Any changes you make will not be persisted.
4. Select the **Project** and **Project Version** to which the template will be transferred in WebInspect Enterprise.
5. If necessary, click **Refresh** to ensure the lists include the latest settings files and scan templates.
6. Enter the name of the scan template that will be created. You cannot duplicate the name of an existing template.
7. Click **Upload**.

All template settings that are not extracted from WebInspect will use the WebInspect Enterprise template default settings.

- The scan template will not specify the policy used by the WebInspect settings file. Instead, it will contain the "Use Any" option.
- Any client certificate information that may be included in the WebInspect settings file is transferred to the scan template, but the certificates are not transmitted.
- All WebInspect settings are preserved in the scan template, even if they are not used by WebInspect Enterprise. Therefore, if you subsequently create a WebInspect settings file based on the scan template you created from the original settings file, the WebInspect settings will be retained.

## To Create a WebInspect Settings File

1. Click the WebInspect **Enterprise Server** menu and select **Transfer Settings**.
2. Select the **Project** and **Project Version** from which the template will be transferred in WebInspect Enterprise.
3. On the Settings Transfer window, select a scan template from the list.
4. (Optional) Click **View** to review the settings as they would appear in a WebInspect settings file. To continue, click **Close**.

**Note:** This is a read-only file. Any changes you make will not be persisted.

5. If necessary, click **Refresh** to ensure the lists include the latest settings files and scan templates.
6. Click **Download**.
7. Using a standard file-selection window, name the settings file, select a location in which to save it, and click **Save**.

The WebInspect settings file will not specify the policy used by the scan template. Instead, it will specify the Standard policy.

## Publishing a Scan (WebInspect Enterprise Connected)

Use the following procedure to transmit scan data from WebInspect to an HP Fortify Software Security Center server, via WebInspect Enterprise.

**Note:** For information about managing the SSC status of vulnerabilities when conducting multiple scans of the same Web site or application, see [Integrating with WebInspect Enterprise](#).

1. Configure WebInspect Enterprise and Software Security Center.
2. Run a scan in WebInspect (or use an imported or downloaded scan).
3. Click the **Enterprise Server** menu and select **Connect to WebInspect Enterprise**. You will be prompted to submit credentials.
4. If a scan is open on a tab that has focus, and you want to publish only that scan:

- a. Click  **Synchronize**.
  - b. Select a project and version, then click **OK**.
  - c. Examine the results. Columns will appear in the Summary pane specifying "Published Status" and "Pending Status." The Published Status is the status of the vulnerability the last time this scan was published to WebInspect Enterprise. The Pending Status is what the status of the vulnerability will be after this scan is published. Depending on the Pending Status, you can modify it to specify whether the vulnerability has been resolved or is still existing (see Step 7 below). In addition, a new tab named "Not Found" appears; this tab contains vulnerabilities that were detected in previous scans but not in the current scan. You can add screenshots and comments to vulnerabilities or mark vulnerabilities as false positive or ignored. You can also review and retest vulnerabilities, modifying the scan results until you are ready to publish.
  - d. Click  **Publish**. Go to step 7.
5. To select from a list of scans:
    - a. Click the **Enterprise Server** menu and select **Publish Scan**.
    - b. On the Publish Scan(s) to Software Security Center dialog, select one or more scans.
    - c. Select a project and project version.
    - d. Click **Next**. WebInspect automatically synchronizes with SSC.
  6. WebInspect lists the number of vulnerabilities to be published, categorized by status and severity.

To determine the status, WebInspect compares previously submitted vulnerabilities (obtained by synchronizing with SSC) with those reported in the current scan. If this is the first scan submitted to a project version, all vulnerabilities will be "New."

If a vulnerability was previously reported, but is not in the current scan, it is marked as "Not Found." You must determine if it was not found because it has been fixed or because the scan was configured differently (for example, you may have used a different scan policy, or you scanned a different portion of the site, or you terminated the scan prematurely). When examining the results (step 4c), you can change the "pending status" of individual vulnerabilities detected by all but the first scan (by right-clicking a vulnerability in the Summary pane). However, when publishing, you must specify how WebInspect should handle any remaining "Not Found" vulnerabilities.

To retain these "Not Found" vulnerabilities in Software Security Center (indicating that they still exist), select **Retain: Assume all vulnerabilities still marked "Not Found" in the scan are still present**.

To remove them (implying that they have been fixed), select **Remove: Assume all vulnerabilities still marked "Not Found" in the scan are fixed**.

7. If this scan was conducted in response to a scan request initiated at HP Fortify Software Security Center, select **Associate scan with an "In Progress" scan request for the current project version.**
8. Click **Publish**.

## Integrating with WebInspect Enterprise

HP Fortify Software Security Center (SSC) is a suite of tightly integrated solutions for identifying, prioritizing, and fixing security vulnerabilities in software. It uses HP Fortify Static Code Analyzer to conduct static analysis and HP WebInspect to conduct dynamic application security testing.

WebInspect Enterprise provides a central location for managing multiple WebInspect scanners and correlating scan results that can be published directly to individual project versions within SSC.

WebInspect Enterprise maintains a history of all vulnerabilities for a particular SSC project version. After WebInspect conducts a scan, it synchronizes with WebInspect Enterprise to obtain that history, compares vulnerabilities in the scan with those in the history, and then assigns a status to each vulnerability as follows:

SSC Status	Description
New	A previously unreported issue.
Existing	A vulnerability in the scan that is already in the history.
Not Found	A vulnerability in the history that is not found in the scan. This can occur because (a) the vulnerability has been remediated and no longer exists, or (b) because the latest scan used different settings, or scanned a different portion of the site, or for some other reason did not discover the vulnerability.
Resolved	A vulnerability that has been fixed.
Reintroduced	A vulnerability that appears in a current scan but was previously reported as "Resolved."
Still an Issue	A vulnerability that was "Not Found" in the current scan does, in fact, exist.

To change the SSC status for an individual vulnerability, right-click a vulnerability on the **Vulnerability** tab and select **Modify Publish Status**. This option appears only after connecting to WebInspect Enterprise and is enabled only after you have synchronized WebInspect with Software Security Center.

The following example demonstrates a hypothetical series of scans for integrating vulnerabilities into HP Fortify Software Security Center.

## First scan

1. Scan the target site with WebInspect. In this example, assume that only one vulnerability (Vuln A) is discovered.
2. Examine the results. You can add screenshots and comments to vulnerabilities or mark vulnerabilities as false positive or ignored. You can also review, retest, and delete vulnerabilities.
3. Synchronize the scan with a project version in SSC, then publish the scan.

## Second scan

1. The second scan again reveals Vuln A, but also discovers four more vulnerabilities (Vulns B, C, D, and E).
2. Synchronize the scan with the project version in SSC.
3. Now examine the results. If you added audit data (such as comments and screenshots) to Vuln A when publishing the first scan, the data will be imported into the new scan.
4. Publish the scan to SSC. Vuln A will be marked "Existing," Vulns B-E will be marked "New," and five items will exist in the SSC system.

## Third scan

1. The third scan discovers Vulns B, C, and D, but not Vuln A or Vuln E.
2. Synchronize the scan with the project version in SSC.
3. After retesting Vuln A, you determine that it does, in fact, exist. You change its pending status to "Still an Issue."
4. After retesting Vuln E, you determine that it does not exist. You change its pending status to "Resolved."
5. Publish the scan to SSC. Vulns B, C, and D will be marked "Existing." Five items will exist in the SSC system.

## Fourth Scan

1. The fourth scan does not find Vuln A or Vuln B. The scan does find Vulns C, D, E, and F.
2. Synchronize the scan with the project version in SSC.
3. Vuln E was previously declared to be resolved and so its status is set to "Reintroduced."
4. You examine the vulnerabilities that were not found (A and B, in this example). If you determine that the vulnerability still exists, update the pending status to "Still an Issue." If a retest verifies that the vulnerability does not exist, update the pending status to "Resolved."
5. Publish the scan to SSC. Vulns C and D remain marked "Existing."

# Using Macros

Use the [Web Macro Recorder](#) tool to record login macros. A macro is a recording of the events that occur when you access and log in to a website. You can subsequently instruct WebInspect to begin a scan using this recording. Macros that were recorded in a Basic Scan or a Guided Scan can be used in either type of scan.

There are two types of macros:

- A log-in macro is a recording of the events that occur when you access and log in to a Web site using the event-based Web Macro Recorder. You can subsequently instruct WebInspect to begin a scan using this recording. You can specify a log-in macro when you select **Site Authentication** on Step 2 of the Guided Scan Wizard.
- A workflow macro is a recording of HTTP events that occur as you navigate through a Web site using the session-based Web Macro Recorder. WebInspect audits only those URLs included in the macro that you previously recorded and does not follow any hyperlinks encountered during the audit. You can specify a workflow macro when you select a **Workflows** scan in the Guided Scan or Basic Scan wizards.

Any activity you record in a macro will override the scan settings. For example, if you specify a URL in the Excluded URL setting, and then you actually navigate to that URL when creating a macro, WebInspect will ignore the exclusion when it crawls and audits the site.

**Note:** When you play a macro, WebInspect will not send any cookie headers that may have been incorporated in the recorded macro. Macros that were recorded in a Basic Scan or a Guided Scan can be used in either type of scan.

## Recommendation

HP strongly recommends that you use the WebInspect version 10.0 or greater Web Macro Recorder to record all new login macros and workflow macros.

### See Also

["Running a Guided Scan" on page 92](#)

[Select Workflow Macro](#)

["Using the Unified Web Macro Recorder" on page 186](#)

## Unified Web Macro Recorder Overview

While the Unified Web Macro Recorder is the only directly accessible macro recording tool provided in WebInspect version 10.0 or greater, it provides (or provides access to) the capabilities of the three web macro recorders of previous WebInspect versions. Due to its versatility, the version 10.0 or greater Web Macro Recorder is also known as the Unified Web Macro Recorder.

The Web Macro Recorder can be launched in several ways—while configuring a [Guided Scan](#) or a [Basic Scan](#), or outside of either scan in what is known as “stand-alone” mode.

**Tip:** For more detailed information about the Unified Web Macro Recorder, see the [Tools > Web Macro Recorder Help](#).

The Web Macro Recorder tool enhances the functionality of the three web macro recorders that were available in previous versions, and its enhancements make [login macro](#) recording more automatic, more complete, and more successful.

The Web Macro Recorder operates by default using underlying Firefox browser technology to record and play macros. It can also operate using Internet Explorer browser technology (also referred to here as IE technology) to record and display web traffic data. Note the following:

- The Web Macro Recorder does not support the recording of Flash or Silverlight applications.
- The TruClient technology used in the Web Macro Recorder is an adaptation of the Ajax TruClient technology originally developed for use with HP LoadRunner and HP Performance Center. It does not incorporate or support all the capabilities of the fully-featured version in those products.
- When you play a macro, WebInspect does not send any cookie headers that may have been incorporated in the recorded macro.
- If a URL is in a macro, the request is always sent when the macro is played, regardless of any exclusion rules in scan settings.
- When launching the Web Macro Recorder, you may receive the following error message: “Exc in ev handl: TypeError: this.oRoot.enable is not a function.” This can occur if the McAfee SiteAdvisor is installed. Simply acknowledge the message and continue.

## Traffic-Mode Web Macro Recorder of Previous WebInspect Versions (Obsolete)

WebInspect version 10.0 or greater does not include the Traffic-Mode Web Macro Recorder that was provided in previous versions. However, the version 10.0 or greater Web Macro Recorder allows you to open, play back, and edit existing traffic-mode macros created in previous WebInspect versions, and create new traffic-mode macros, using its Internet Explorer browser technology (IE technology) option. Based on its versatility, the version 10.0 or greater Web Macro Recorder is also known as the Unified

Web Macro Recorder. When recording new macros, the version 10.0 or greater Web Macro Recorder first uses event-based recording and Firefox browser technology by default, but if that fails for some reason, the Web Macro Recorder automatically switches to its traffic-mode IE technology as an alternative recording method.

## Event-Based IE Compatible Web Macro Recorder of Previous WebInspect Versions (Hidden in user interface)

WebInspect version 10.0 or greater includes one Web Macro Recorder tool. By default, it uses event-based functionality and Firefox browser technology to record new macros. The functionality of the separate Event-Based IE Compatible Web Macro Recorder that was provided in previous versions is no longer directly accessible in WebInspect menus. However, the version 10.0 or greater Web Macro Recorder allows you to open, play back, and edit existing event-based macros created in previous WebInspect versions, and create new macros, in the earlier Event-Based IE Compatible Web Macro Recorder.

### See Also

["Using the Unified Web Macro Recorder" below](#)

[Login Macro](#)

## Using the Unified Web Macro Recorder

While the Unified Web Macro Recorder is the only directly accessible macro recording tool provided in WebInspect version 10.0 or greater, it provides (or provides access to) the capabilities of the three web macro recorders of previous WebInspect versions. The Web Macro Recorder can be launched in several ways—while configuring a Guided Scan or a Basic Scan, or outside of either scan in what is known as “stand-alone” mode.

The Web Macro Recorder tool. It enhances the functionality of the three web macro recorders that were available in previous versions, and its enhancements make login macro recording more automatic, more complete, and more successful.

The Web Macro Recorder operates by default using underlying Firefox browser technology to record and play macros. It can also operate using Internet Explorer browser technology (also referred to here as IE technology) to record and display web traffic data. Note the following:

- Web Macro Recorder does not support the recording of Flash or Silverlight applications.
- The TruClient technology used in the Web Macro Recorder is an adaptation of the Ajax TruClient technology originally developed for use with HP LoadRunner and HP Performance Center. It does not incorporate or support all the capabilities of the fully-featured version in those products.
- When you play a macro, WebInspect does not send any cookie headers that may have been incorporated in the recorded macro.

- If a URL is in a macro, the request is always sent when the macro is played, regardless of any exclusion rules in scan settings.
- When launching the Web Macro Recorder, you may receive the following error message: "Exc in ev handl: TypeError: this.oRoot.enable is not a function." This can occur if the McAfee SiteAdvisor is installed. Simply acknowledge the message and continue.

## Upgrade Impacts

If you have upgraded from a previous version of WebInspect, review the following aspects of the version 10.0 or greater Web Macro Recorder, as compared to the web macro recorders of previous versions:

- The version 10.0 or greater Web Macro Recorder includes and enhances the TruClient Web Macro Recorder functionality of previous versions of WebInspect, and by default it uses this enhanced functionality to record a new macro. The automatic detection of logout conditions has been significantly improved from previous versions. As a result, usually you should not need to manually identify a logout condition as part of recording a login macro.
- Macros that were recorded using the TruClient Web Macro Recorder in any previous version of WebInspect can be used in a Guided Scan or a Basic Scan in WebInspect version 10.0 or greater.
- When using Internet Explorer browser technology (also referred to here as IE technology), the version 10.0 or greater Web Macro Recorder can open macros that were created in the Traffic-Mode Web Macro Recorder of previous WebInspect versions. For more information, see [Opening Macros Recorded with the Traffic-Mode Web Macro Recorder](#).
- Also, if the Web Macro Recorder cannot successfully record a new macro using the default Firefox browser technology, it automatically switches to IE technology to record the macro. IE technology can also be manually selected.

## Traffic-Mode Web Macro Recorder of Previous WebInspect Versions (Obsolete)

WebInspect version 10.0 or greater does not include the Traffic-Mode Web Macro Recorder that was provided in previous versions. However, the version 10.0 or greater Web Macro Recorder allows you to open, play back, and edit existing traffic-mode macros created in previous WebInspect versions, and create new traffic-mode macros, using its Internet Explorer browser technology (IE technology) option. When recording new macros, the version 10.0 or greater Web Macro Recorder first uses event-based recording and Firefox browser technology by default, but if that fails for some reason, the Web Macro Recorder automatically switches to its traffic-mode IE technology as an alternative recording method.

## Event-Based IE Compatible Web Macro Recorder of Previous WebInspect Versions (Hidden in user interface)

WebInspect version 10.0 or greater includes one Web Macro Recorder tool. By default, it uses event-based functionality and Firefox browser technology to record new macros. The functionality of the separate Event-Based IE Compatible Web Macro Recorder that was provided in previous versions is no longer directly accessible in WebInspect menus. However, the version 10.0 or greater Web Macro Recorder allows you to open, play back, and edit existing event-based macros created in previous WebInspect versions, and create new macros, in the earlier Event-Based IE Compatible Web Macro Recorder.

### See Also

["Using Macros" on page 184](#)

[Login Macro](#)

## Server Profiler

Use the Server Profiler to conduct a preliminary examination of a Web site to determine if certain WebInspect settings should be modified. If changes appear to be required, the Profiler returns a list of suggestions, which you may accept or reject.

For example, the Server Profiler may detect that authorization is required to enter the site, but you have not specified a valid user name and password. Rather than proceed with a scan that would return significantly diminished results, you could follow the Server Profiler's prompt to configure the required information before continuing.

Similarly, your settings may specify that WebInspect should not conduct "file-not-found" detection. This process is useful for Web sites that do not return a status "404 Not Found" when a client requests a resource that does not exist (they may instead return a status "200 OK," but the response contains a message that the file cannot be found). If the Profiler determines that such a scheme has been implemented in the target site, it would suggest that you modify the WebInspect setting to accommodate this feature.

The Server Profiler can be selected during a Guided Scan, or enabled in the Application settings. For specific information, see [Application Settings - Server Profiler](#).

## Using the Server Profiler

You can use either of two methods to invoke the Server Profiler:

Launch Server Profiler as a Tool

Follow these steps to launch the Server Profiler:

1. Click the WebInspect **Tools** menu and select **ServerProfiler**.
2. In the **URL** box, enter or select a URL or IP address.
3. (Optional) If necessary, modify the **Sample Size**. Large Web sites may require more than the default number of sessions to sufficiently analyze the requirements.
4. Click **Analyze**.

The Profiler returns a list of suggestions (or a statement that no modifications are necessary).

5. To reject a suggestion, clear its associated check box.
6. For suggestions that require user input, provide the requested information.
7. (Optional) To save the modified settings to a file:
  - a. Click **Save Settings**.
  - b. Using a standard file-selection window, save the settings to a file in your Settings directory.

#### Invoke Server Profiler when Starting a Scan

Follow these steps to launch the profiler when beginning a scan:

1. Start a scan using one of the following methods:
  - On the WebInspect **Start Page**, click **Start a Basic Scan**.
  - Click **File > New > Basic Scan**.
  - Click the drop-down arrow on the **New** icon (on the toolbar) and select **Basic Scan**.
  - On the WebInspect **Start Page**, click **Manage Scheduled Scans**, click **Add**, and then select **Basic Scan**.
2. On step 4 of the Scan Wizard (Detailed Scan Configuration), click **Profile** (unless **Run Profiler Automatically** is selected).

The Profiler returns a list of suggestions (or a statement that no modifications are necessary).

3. To reject a suggestion, clear its associated check box.
4. For suggestions that require user input, provide the requested information.
5. Click **Next**.

## Inspecting the Results

This topic describes inspecting the results for a Basic Scan and a Web Services Scan.

## Basic Scan

As soon as you start a Basic Scan, WebInspect begins scanning your Web application and displays in the [navigation pane](#) an icon depicting each session (using either the Site or Sequence view). It also reports possible vulnerabilities on the **Vulnerabilities** tab and **Information** tab in the [summary pane](#).

If you click a URL listed in the summary pane, the program highlights the related session in the [navigation pane](#) and displays its associated information in the [information pane](#).

Sometimes the attack that detected a vulnerable session is not listed under attack information. That is, if you select a vulnerable session in the navigation pane and then click **Attack Info** in the [Session Info](#) panel, the attack information does not appear in the information pane. This is because attack information is usually associated with the session in which the attack was created and not with the session in which it was detected. When this occurs, select the parent session and then click **Attack Info**.

## Working with a Vulnerability

If you right-click a vulnerability in the summary pane, a shortcut menu allows you to:

- **Copy URL** - Copies the URL to the Windows clipboard.
- **Copy Selected Item(s)** - Copies the text of selected items to the Windows clipboard.
- **Copy All Items** - Copies the text of all items to the Windows clipboard.
- **Export** - Copies the item to a CSV file.
- **View in Browser** - Renders the HTTP response in a browser.
- **Filter by Current Value** - Restricts the display of vulnerabilities to those that satisfy the criteria you select. For example, if you right-click on "Post" in the Method column and then select **Filter by Current Value**, the list displays only those vulnerabilities that were discovered by sending an HTTP request that used the Post method.

**Note:** The filter criterion is displayed in the combo box in the upper right corner of the summary pane. Alternatively, you can manually enter or select a filtering criterion using this combo box. For additional details and syntax rules, see [Using Filters and Groups in the Summary Pane](#).

- **Change Severity** - Allows you to change the severity level.
- **Edit Vulnerability** - Displays the [Edit Vulnerabilities dialog](#), allowing you to modify various vulnerability characteristics.
- **Review Vulnerability** - Allows you to retest the vulnerable session, mark it as a false positive, or send it to HP Quality Center or IBM Rational ClearQuest. For more information, see [Vulnerability](#)

[Review](#).

- **Mark as** - Flags the vulnerability as either a false positive (and allows you to add a note) or as ignored. In both cases, the vulnerability is removed from the list. You can view a list of all false positives by selecting **False Positives** in the Scan Info panel. You can view a list of false positives and ignored vulnerabilities by selecting Dashboard in the Scan Info panel, and then clicking the hyperlinked number of deleted items in the statistics column.

**Note:** You can recover "false positive" and "ignored" vulnerabilities. See [Recover Deleted Items](#) for details.

- **Send to** - Converts the vulnerability to a defect and adds it to the HP Quality Center or IBM Rational ClearQuest database.
- **Remove Location** - Removes the selected session from the navigation pane (both Site and Sequence views) and also removes any associated vulnerabilities.

**Note:** You can recover removed locations (sessions) and their associated vulnerabilities. See [Recover Deleted Items](#) for details.

- **Crawl** - Recrawls the selected URL.
- **Tools** - Presents a submenu of available tools.
- **Attachments** - Allows you to create a note associated with the selected session, flag the session for follow-up, add a vulnerability note, or add a vulnerability screenshot.

## Working with a Group

If you right-click a group, a shortcut menu allows you to:

- Collapse/Expand All Groups
- Collapse/Expand Group
- Copy Selected Item(s)
- Copy All Items
- Export
- Change Severity
- Mark as

- Send to
- Remove Location

## Understanding the Severity

The relative severity of a vulnerability listed in the summary pane is identified by its associated icon, as described in the following table.

Icon	Description
	A vulnerability wherein an attacker might have the ability to execute commands on the server or retrieve and modify private information.
	Generally, the ability to view source code, files out of the Web root, and sensitive error messages.
	Indicates non-HTML errors or issues that could be sensitive.
	Interesting issues, or issues that could potentially become higher ones.
	An interesting point in the site, or detection of certain applications or Web servers.

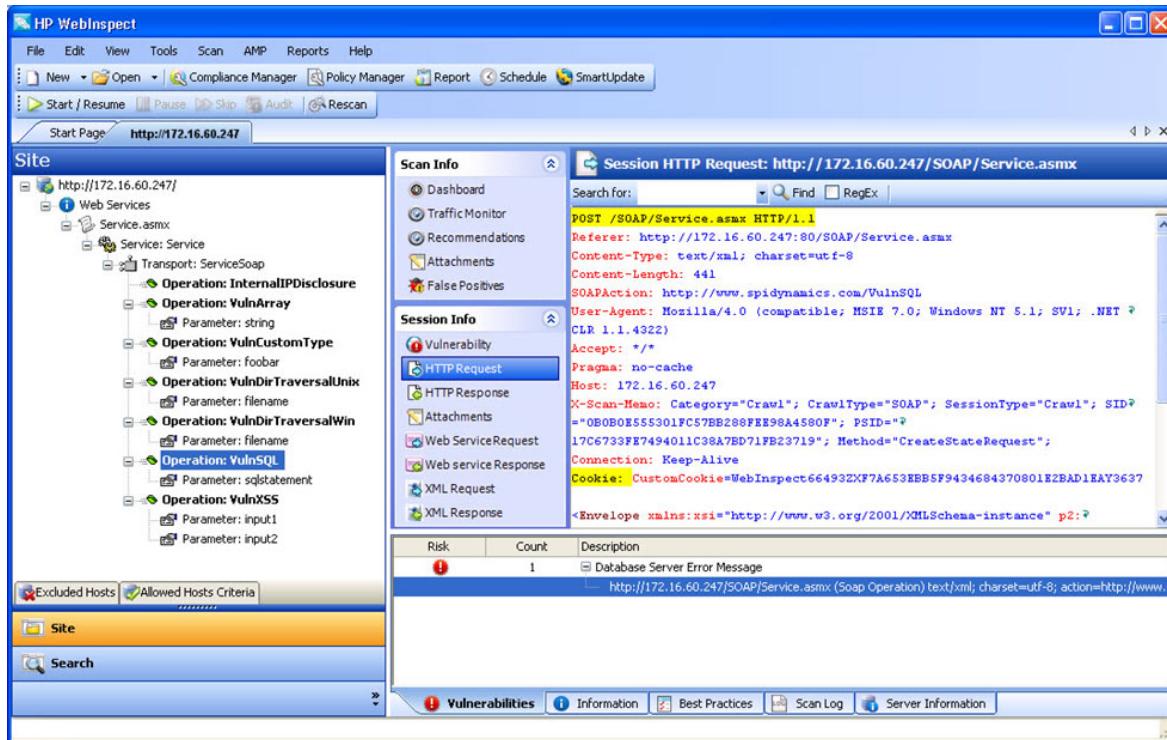
## Working in the Navigation Pane

You can also select an object or session in the [navigation pane](#) and investigate the session using the options available on the [Session Info panel](#).

## Web Services Scan

Web services are programs that communicate with other applications (rather than with users) and answer requests for information. Most Web services use Simple Object Access Protocol (SOAP) to send XML data between the Web service and the client Web application that initiated the information request. XML provides a framework to describe and contain structured data. The client Web application can readily understand the returned data and display that information to the end user.

## Web Services Scan Image



A client Web application that accesses a Web service receives a Web Services Definition Language (WSDL) document so that it understands how to communicate with the service. The WSDL document describes the procedures included in the Web service, the parameters those procedures expect, and the type of return information the client Web application will receive.

After selecting a session object in the [navigation pane](#) or on the **Vulnerabilities** tab of the [summary pane](#), you can select options from the [Session Info](#) panel.

### See Also

["Reviewing and Retesting" on page 211](#)

["Auditing Web Services " on page 199](#)

["Editing Vulnerabilities" on page 204](#)

["User Interface Overview" on page 31](#)

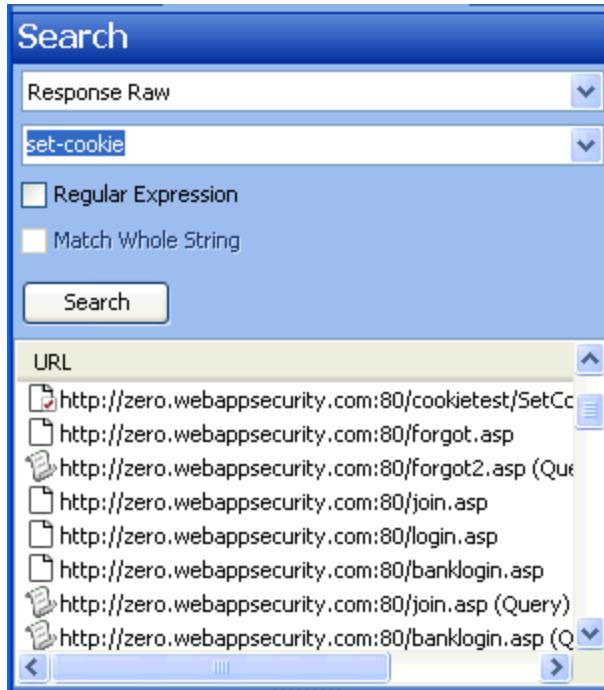
["Reviewing a Vulnerability " on page 201](#)

["Recovering Deleted Items" on page 214](#)

## Search View

The Search view allows you to search across all sessions for various HTTP message components. For example, if you select **Response Raw** from the drop-down and specify **set-cookie** as the search

string, WebInspect lists every session whose raw HTTP response includes the "set-cookie" command.



To use the Search view:

1. In the **navigation pane**, click **Search** (at the bottom of the pane).

If all buttons are not displayed, click the **Configure Buttons** drop-down at the bottom of the button list and select **Show More Buttons**.

2. From the top-most list, select an area to search. The choices are:
  - Status Code
  - URL
  - Request Raw
  - Request Method
  - Request Post Data
  - Request Post Data Name
  - Request Post Data Value
  - Request Headers
  - Request Header Name

- Request Header Value
- Request Query
- Request Query Name
- Request Query Value
- Request Cookies
- Request Cookie Name
- Request Cookie Value
- Request File Name and Extension
- Request File Name
- Request File Extension
- Request Path
- Response Raw
- Response Headers
- Response Header Name
- Response Header Value
- Response Cookies
- Response Cookie Name
- Response Cookie Value

3. In the combo box, type or select the string you want to locate.
4. If the string represents a **regular expression**, select the **Regular Expression** check box.
5. To find an entire string in the HTTP message that exactly matches the search string, select the **Match Whole String** check box. The exact match is not case-sensitive.

This option is not available for certain search targets.

6. Click **Search**.

#### See Also

["Navigation Pane " on page 45](#)

["User Interface Overview" on page 31](#)

# Using Filters and Groups in the Summary Pane

This topics describes how to use filters and groups in the Summary Pane.

## Using Filters

You can display a subset of items that match the criteria you specify using either of two methods:

- Enter filter criteria using the combo box in the top right corner of the pane.  
Note: Click the filter criteria box and press CTRL + Space to view a pop-up list of all available filter criteria, and then enter a value for that criterion.
- Right-click a value in any column and select **Filter by Current Value** from the shortcut menu.

This filtering capability is available on all Summary pane tabs except **Scan Log**.

## No Filters

The following example shows unfiltered items on the **Vulnerabilities** tab.

Summary Pane with No Filters Image

Path	Method	Vuln Param	Parameters	Pending Status	Published Status
http://zero.webappsecurity.com/test/cgi.zip	GET	-	?	Unknown	None
<b>Check:Cross-Site Scripting (36 items)</b>					
http://zero.webappsecurity.com/acctxferconfirm.asp	POST	fromAcct	(Post)from...	?	Unknown
http://zero.webappsecurity.com/acctxferconfirm.asp	POST	amount	(Post)from...	?	Unknown
http://zero.webappsecurity.com/acctxferconfirm.asp	POST	toAcct	(Post)from...	?	Unknown
http://zero.webappsecurity.com/banklogin.asp	GET	err	(Query)err...	?	Unknown
http://zero.webappsecurity.com/cookiestest/ShowCook...	GET	-	?	Unknown	None
http://zero.webappsecurity.com/cookiestest/ShowCook...	GET	-	?	Unknown	None
<input checked="" type="radio"/> Vulnerabilities <input type="radio"/> Not Found <input type="radio"/> Information <input type="radio"/> Best Practices <input type="radio"/> Scan Log <input type="radio"/> Server Information					

## Filtered by Method:Get

The following example is rendered after entering "Method:Get" in the filter criteria box.

## Summary Pane with Filters Image

Path	Method	Vuln Param	Parameters	Pending Status	Published Status
Check:Backup File (cgi.zip) (3 items)					
http://zero.webappsecurity.com/admin/cgi.zip	GET	-	Unknown	None	
http://zero.webappsecurity.com/cgi.zip	GET	-	Unknown	None	
http://zero.webappsecurity.com/test/cgi.zip	GET	-	Unknown	None	
Check:Cross-Site Scripting (25 items)					
http://zero.webappsecurity.com/banklogin.asp	GET	err	(Query)err...	Unknown	None
http://zero.webappsecurity.com/cookietest>ShowCook...	GET	-	Unknown	None	

Filter Criteria: Method:Get

Buttons at the bottom: Vulnerabilities, Not Found, Information, Best Practices, Scan Log, Server Information.

Note that the filtering criteria (Method:Get) appears in the combo box, which also contains a red X. Click it to remove the filter and return the list to the original contents.

## Specifying Multiple Filters

To specify multiple filters when typing criteria in the filter criteria combo box, insert a comma between filters (such as Parameter:noteid, Method:GET).

## Filter Criteria

You can enter the following identifiers:

- check - Check name
- cookienamerp - Cookie name in the HTTP response
- cookienamerq - Cookie name in the HTTP request
- cookievaluerp - Cookie value in the HTTP response
- cookievaluerq - Cookie value in the HTTP request
- duplicates - Duplicates detected by SecurityScope
- filerq - File name and extension in the HTTP request
- headernamerp - Header name in the HTTP response
- headernamerq - Header name in the HTTP request
- headervaluerp - Header value in the HTTP response
- headervaluerq - Header value in the HTTP request

- location - Path plus parameters identifying the resource
- manual - A location added manually (syntax is manual:True or manual:False)
- method - HTTP method (GET, POST)
- methodrq - Method specified in HTTP request
- parameters - Parameters specified in the HTTP request
- path - Path identifying the resource (without parameters)
- rawrp - Raw HTTP response
- rawrq - Raw HTTP request
- sessiondataid - Session data identifier (right-click on a session in the Navigation pane and select Filter by Current Session)
- severity - Severity assigned to a vulnerability (critical, high, medium, low)
- stack - Stack tracereturned by SecurityScope (syntax is stack:True or stack:False)
- statuscode - HTTP status code
- typerq - Type of request: query, post, or SOAP
- vparam - The vulnerability parameter

## Using Groups

You can group items into categories based on the column headings. To do so, simply drag the heading and drop it on the grouping area at the top of the pane.

Vulnerabilities in the following illustration are grouped by risk and then by check name.

### Summary Pane Using Groups Image

The screenshot shows the WebInspect interface with the 'Check' tab selected. The main area displays a table of vulnerabilities. The columns are: Path, Method, Vuln Param, Parameters, Pending Status, and Published Stat. The table is grouped under two categories: 'Check:Backup File (cgi.zip) (3 items)' and 'Check:Cross-Site Scripting (36 items)'. Each group contains multiple rows of vulnerabilities with their respective details.

Path	Method	Vuln Param	Parameters	Pending Status	Published Stat	
Check:Backup File (cgi.zip) (3 items)						
http://zero.webappsecurity.com/admin/cgi.zip	GET	-	?	Unknown	None	
http://zero.webappsecurity.com/cgi.zip	GET	-	?	Unknown	None	
http://zero.webappsecurity.com/test/cgi.zip	GET	-	?	Unknown	None	
Check:Cross-Site Scripting (36 items)						
http://zero.webappsecurity.com/acctxferconfirm.asp	POST	fromAcct	(Post)from...	?	Unknown	None
http://zero.webappsecurity.com/acctxferconfirm.asp	POST	amount	(Post)from...	?	Unknown	None

Below the table, there is a navigation bar with icons for Vulnerabilities, Not Found, Information, Best Practices, Scan Log, and Server Information.

If you right-click a column header, WebInspect displays the following shortcut menu:

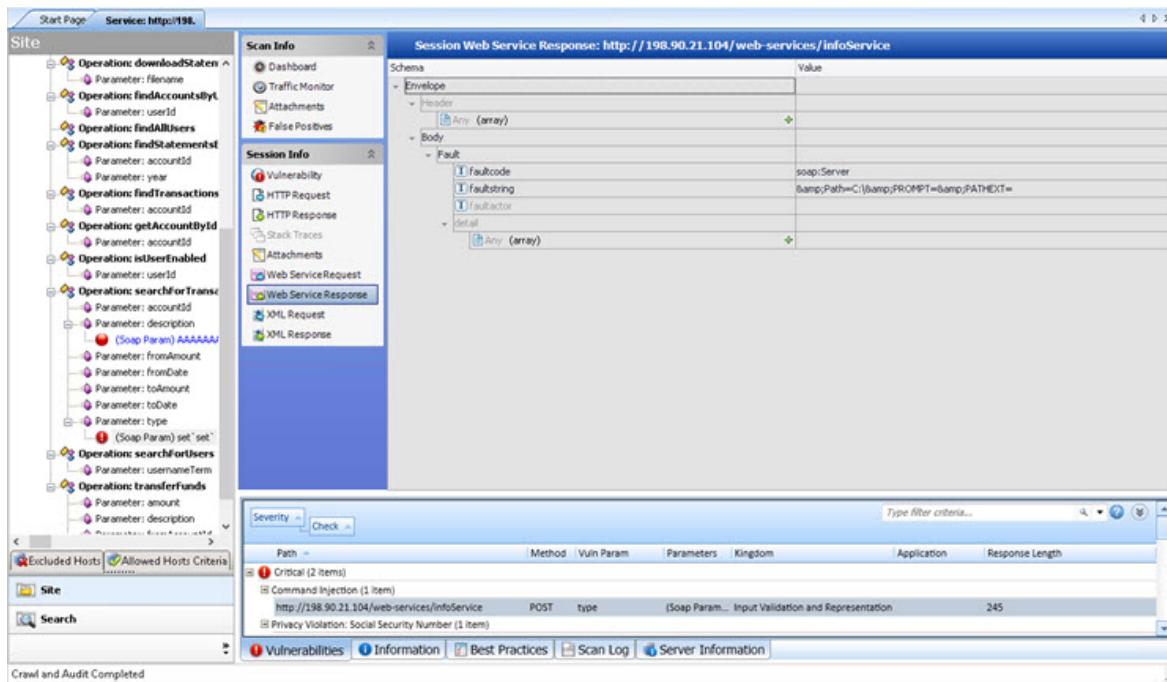
- Group by Field - Groups vulnerabilities according to the field you selected.
- Group by Box - Shows the "Group By" area in which you can arrange grouping by column headers.
- Columns - Allows you to select which columns are displayed.
- Save as Default View - Saves the current grouping paradigm as the default for all scans.
- Reset Default View - Restores the grouping paradigm to the default view that you created.
- Reset Factory Settings - Restores the grouping paradigm to the original view (Severity > Check).

## Auditing Web Services

Web services are programs that communicate with other applications (rather than with users) and answer requests for information. Most Web services use Simple Object Access Protocol (SOAP) to send XML data between the Web service and the client Web application that initiated the information request. Unlike HTML, which only describes how Web pages are displayed, XML provides a framework to describe and contain structured data. The client Web application can readily understand the returned data and display that information to the end user.

A client Web application that accesses a Web service receives a Web Services Description Language (WSDL) document so that it understands how to communicate with the service. The WSDL document describes what programmed procedures the Web service includes, what parameters those procedures expect, and the type of return information the client Web application will receive.

## Web Services Scan Image



## Options Available from the Session Info Panel

The following table describes the options that are available from the Session Info panel.

Option	Definition
Vulnerability	Displays the vulnerability information for the session selected in the <a href="#">navigation pane</a> .
HTTP Request	Displays the raw HTTP request sent by WebInspect to the server hosting the site you are scanning.
HTTP Response	Displays the server's raw HTTP response to WebInspect's request.  Note: If you select a Flash (.swf) file, WebInspect displays HTML instead of binary data. This allows WebInspect to display links in a readable format.

Option	Definition
Stack Traces	<p>This feature is designed to support WebInspect Agent when it is installed and running on the target server. For certain checks (such as SQL injection, command execution, and cross-site scripting), WebInspect Agent intercepts WebInspect HTTP requests and conducts runtime analysis on the target module. If this analysis confirms that a vulnerability exists, WebInspect Agent appends the stack trace to the HTTP response. Developers can analyze this stack trace to investigate areas that require remediation.</p>
Attachments	<p>Displays all notes, flags, and screenshots associated with the selected session.</p> <p>To create an attachment, you can either:</p> <ul style="list-style-type: none"> <li>• Right-click an operation or vulnerability in the navigation pane and select <b>Attachments</b> from the shortcut menu, or</li> <li>• Right-click a URL on the <b>Vulnerabilities</b> tab of the <a href="#">summary pane</a> and select <b>Attachments</b> from the shortcut menu, or</li> <li>• Select an operation or vulnerability in the navigation pane, then select <b>Attachments</b> from the <b>Session Info</b> panel and click the <b>Add</b> menu (in the information pane).</li> </ul> <p>WebInspect automatically adds a note to the session information whenever you send a defect to HP Quality Center or IBM Rational ClearQuest.</p>
Web Service Request	<p>Displays an exploded view of the SOAP envelope, header, and body elements for the request.</p>
Web Service Response	<p>Displays an exploded view of the SOAP envelope, header, and body elements for the response.</p>
XML Request	<p>Displays the associated XML schema embedded in the request (available when selecting the WSDL object during a Web Service scan).</p>
XML Response	<p>Displays the associated XML schema embedded in the response (available when selecting the WSDL object during a Web Service scan).</p>

For more information on how to conduct a Web services vulnerability scan, see [Web Service Scan](#).

## Reviewing a Vulnerability

After you conduct a scan and report discovered vulnerabilities, developers may correct their code and update the site. You can then open the original scan, select the once-vulnerable session (now

supposedly remediated), and select **Review Vulnerability** from the shortcut menu. Assuming that the fundamental architecture of the site has not changed, you can verify that the threat no longer exists without rescanning the entire site (which, in some cases, could require several hours or even days).

Alternatively, you can use this feature simply to double-check a reported vulnerability, even while the scan is still running.

1. Right-click a session from the [Navigation pane](#) (or right-click a URL on the **Vulnerability** tab of the [Summary pane](#)).
2. Select **Review Vulnerability** from the shortcut menu.

The Retest Vulnerability window appears.

3. If you want to access the site through Web Proxy, click **Options** and select **Launch and Direct Traffic through Web Proxy**.
4. If multiple vulnerabilities are associated with the selected session, choose one from the **Vulnerabilities to Review** list.
5. Use the tabs to display information about the original session (as selected in the lower pane under the **URL** column):
  - **Browser** - The server's response, as rendered in a browser.
  - **Request** - The raw HTTP request message.
  - **Response** - The raw HTTP response message.
  - **Stack Trace** - A report of the active stack frames at a certain point in time during the execution of a program. This tab is present only when SecurityScope is running on the target server.
  - **Vulnerability** - A description of the vulnerability, its implications, and suggestions on how to fix it.
  - **Attachments** - Notes and screen shots, which you may add, view, edit, or delete.
6. To retest the session for the selected vulnerability, click **Retest**.

Results of the retest appear on the Status bar and in the lower pane in the **Response Match Status** column.

The status is reported as either "Complete (Vulnerability Detected)" or "Complete (Vulnerability Not Detected)."

The reliability of the reported findings is mitigated by the Response Match Status, which may have the following values:

- **Match** - The resource has not changed significantly; WebInspect was able to access the session via the same path used by the original scan.

- **Inconclusive** - Based on the HTTP response, the resource has changed in a manner that may or may not substantiate the finding that a vulnerability has or has not been detected during the retest.
  - **Different** - The HTTP response is radically different from the response received during the original scan, suggesting major changes to the resource.
7. If you think that WebInspect has erroneously determined that the vulnerability exists, you can remove the vulnerability by clicking **Mark as** and selecting **False Positive** from the drop-down list.
  8. To ignore the vulnerability, click **Mark as** and select **Ignored** from the drop-down list.
  9. To convert one or more vulnerabilities to defects and add them to either the HP Quality Center or IBM Rational ClearQuest database, click **Send To**.

**Note:** If you access the Vulnerability Review window from the Vulnerability Compare window, the **Mark As** and **Send To** buttons are not enabled.

#### See Also

["Reviewing and Retesting" on page 211](#)

["Sending Vulnerabilities to a Defect Tracking System " on page 215](#)

["Mark As False Positive" on page 207](#)

## Adding/Viewing Vulnerability Screenshot

To add a vulnerability screenshot:

1. Do one of the following to select a vulnerability:
    - On the **Vulnerabilities** tab or the **Information** tab in the **Summary pane**, right-click a vulnerable URL.
    - On the **Navigation pane**, right-click a vulnerable session or URL.
  2. On the shortcut menu, click **Attachments > Add Vulnerability Screenshot**.
- Note:** An alternative method is to select a vulnerability, click **Attachments** in the **Session Info** panel, and then select a command from the **Add** menu (in the **information display area**).
3. If you selected a session with multiple vulnerabilities, select the check box next to one or more vulnerabilities.
  4. Enter a name (40 characters max.) for the screenshot in the **Name** box.

5. Select an image file, using one of the following methods:
  - Click the browse button  and choose a file with the standard file-selection window.
  - Click **Copy from Clipboard** to save the contents of the Windows clipboard.

**Note:** You can specify only one image file even if you have selected multiple vulnerabilities.

6. (Optional) Enter a note related to the vulnerability screenshot you selected.
7. Click **OK**.

## Viewing Screenshots for a Selected Session

You can view notes, flags, and screenshots for a selected session by clicking **Attachments** on the Session Info panel.

## Viewing Screenshots for All Sessions

You can view notes, flags, and screenshots for all sessions by clicking **Attachments** on the Scan Info panel.

### See Also

["Vulnerability Note" on page 210](#)

["Flag Session for Follow-Up" on page 208](#)

["Scan Note" on page 208](#)

## Editing Vulnerabilities

After WebInspect assesses your application's vulnerabilities, you may want to edit and save the results for a variety of reasons, including:

- **Security** - If an HTTP request or response contains passwords, account numbers, or other sensitive data, you may want to delete or modify this information before making the scan results available to other persons in your organization.
- **Correction** - WebInspect occasionally reports a "false positive." This occurs when WebInspect detects indications of a possible vulnerability, but further investigation by a developer determines that the problem does not actually exist. You can delete the vulnerability from the session or delete

the entire session. Alternatively, you can designate it as a false positive (right-click the session in either the Site or Sequence view and select **Mark As False Positive**).

- **Severity Modification** - If you disagree with WebInspect's ranking of a vulnerability, you can assign a different level, using the following scale:

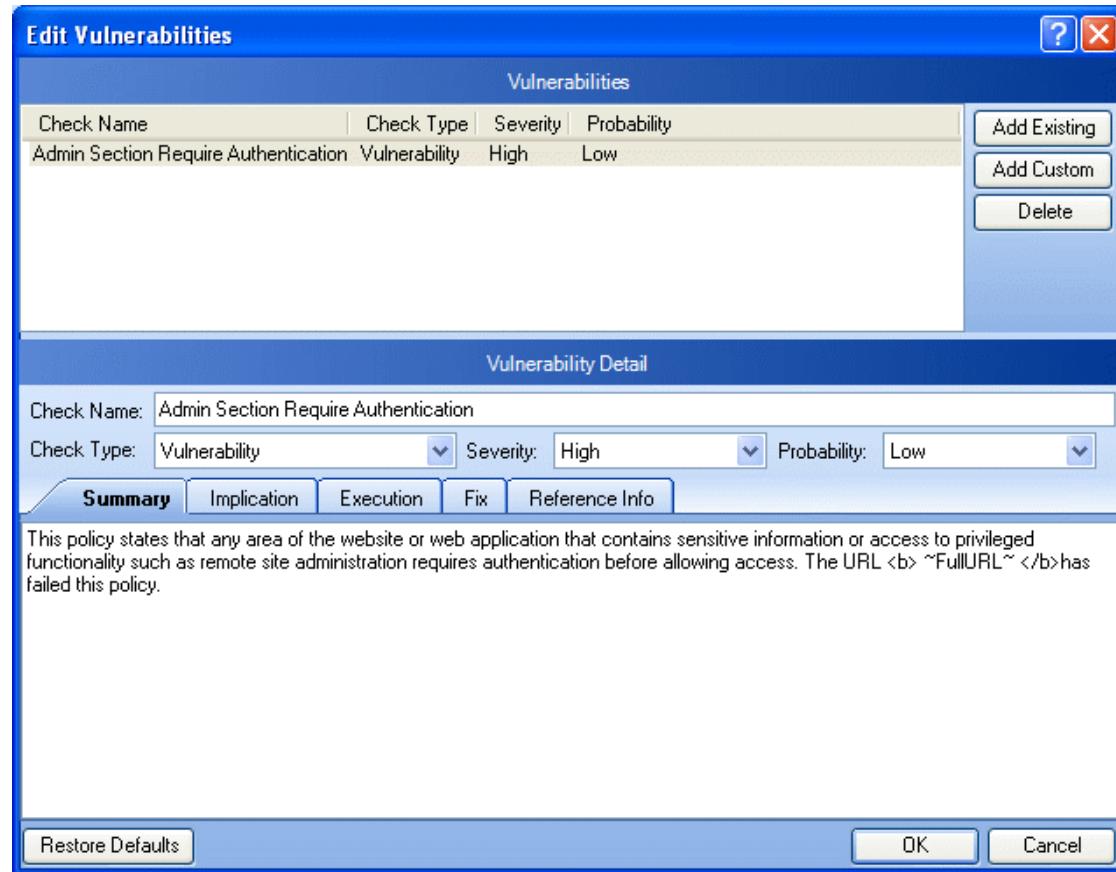
Range	Severity
0 - 9	Normal
10	Information
11 - 25	Low
26 - 50	Medium
51 - 75	High
76 - 100	Critical

- **Record Keeping** - You can modify any of the report fields associated with an individual vulnerability (Summary, Execution, Recommendation, Implementation, Fixes, and References). For example, you could add a paragraph to the Fixes section describing how you actually fixed the problem.
- **Enhancement**- If you discover a new vulnerability, you could define it and add it to a session as a custom vulnerability

Follow the steps below to edit a vulnerable session.

1. Select a session:
  - On the **Vulnerabilities** tab or the **Information** tab in the **Summary** pane, right-click a vulnerable URL , or
  - On the [navigation pane](#), right-click a session or URL.
2. Select **Edit Vulnerability** from the shortcut menu.

The Edit Vulnerabilities window opens.



3. Select a vulnerability (if the session includes multiple vulnerabilities).
4. To add an existing vulnerability to the session (that is, one that exists in the database), click **Add Existing**.
  - a. On the Add Existing Vulnerability window, enter part of a vulnerability name, or a complete vulnerability ID number or type.
 

**Note:** The \* and % characters can be used interchangeably as wildcards. However, a wildcard is allowed only at the beginning, at the end, or at the beginning and end of a string. If placed within a string (such as "mic\*soft,"), these characters will not function as wildcards.
  - b. Click **Search**.
  - c. Select one or more of the vulnerabilities returned by the search.
  - d. Click **OK**.
5. To add a custom vulnerability, click **Add Custom**.

You can then edit the vulnerability as described in Step 7.

6. To delete the vulnerability from the selected session, click **Delete**.
7. To modify the vulnerability, select different options from the **Vulnerability Detail** section. You can also change the descriptions that appear on the Summary, Implication, Execution, Fix, and Reference Info tabs.
8. Click **OK** to save the changes.

## Mark As False Positive

If you think that WebInspect has erroneously determined that a session contains a vulnerability, you can remove the vulnerability from the session.

1. Select the check box associated with one or more URLs.
2. (Optional) Enter a comment.
3. (Optional) To notify HP support personnel that you have found what you believe to be a false positive, select **Send to HP Support**.

If you select this option, you may also select **Preview Data Upload**, which allows you to view the contents of the data being sent to HP Support. At that time, you can copy the data to the Windows clipboard, cancel the upload, or allow it to proceed (by clicking **OK**).

4. Click **OK**.

**Tip:** To view a list of all sessions that have been marked as false positives, select **False Positives** from the **Scan Info** panel. Note that this option is not displayed until you actually declare a vulnerability as a false positive.

## Mark As Vulnerability

If you think that someone has erroneously reclassified a detected vulnerability as a false positive, you can restore the vulnerability to its original session.

1. Select the check box associated with one or more URLs.
2. (Optional) Enter a comment.
3. Click **OK**.

## Flag Session for Follow-Up

To flag a session for follow-up:

1. Do one of the following to select a session:
  - On the **Vulnerabilities** tab or the **Information** tab in the **Summary pane**, right-click a vulnerable URL.
  - On the **Navigation pane**, right-click a session or URL.
2. On the shortcut menu, click **Attachments > Flag Session for Follow Up**.

**Note:** You can also flag a session for follow-up by selecting a vulnerability or session, clicking **Attachments** in the Session Info panel, and then click the **Add** menu (in the information display area).

3. Enter a note related to the session you selected.
4. Click **OK**.

## Viewing Flags for a Selected Session

You can view notes, flags, and screenshots for a selected session by clicking **Attachments** on the **Session Info** panel.

## Viewing Flags for All Sessions

You can view notes, flags, and screenshots for all sessions by clicking **Attachments** on the **Scan Info** panel.

## Scan Note

To add a scan note:

1. Click **Attachments** on the **Scan Info** panel.
2. Click **Add** and select **Scan Note**.

3. On the Add Scan Note dialog, enter a note related to the scan.
4. Click **OK**.

To delete a scan note (or any attachment):

1. Select the attachment.
2. Click **Delete**.

#### See Also

["Adding/Viewing Vulnerability Screenshot" on page 203](#)

["Vulnerability Note" on the next page](#)

["Flag Session for Follow-Up" on the previous page](#)

## Session Note

To add a session note:

1. Select a session:
  - On the **Vulnerabilities** tab or the **Information** tab in the **Summary pane**, right-click a vulnerable URL , or
  - On the **Navigation pane**, right-click a session or URL.
2. On the shortcut menu, click **Attachments > Add Session Note**.

**Note:** You can also add a session note by selecting a vulnerability or session, clicking **Attachments** in the Session Info panel, and then clicking the **Add** menu (in the **information display area**).

3. Enter a note related to the session you selected.
4. Click **OK**.

## Viewing Notes for a Selected Session

You can view notes, flags, and screenshots for a selected session by clicking **Attachments** on the **Session Info** panel.

## Viewing Notes for All Sessions

You can view notes, flags, and screenshots for all sessions by clicking **Attachments** on the **Scan Info** panel.

## Vulnerability Note

To add a vulnerability note:

1. Do one of the following to select a vulnerability:
    - On the **Vulnerabilities** tab or the **Information** tab in the **Summary pane**, right-click a vulnerable URL.
    - On the **Navigation pane**, right-click a vulnerable session or URL.
  2. On the shortcut menu, click **Attachments > Add Vulnerability Note**.
- Note:** An alternative method is to select a vulnerability, click **Attachments** in the Session Info panel, and then click the **Add** menu (in the **information display area**).
3. If you selected a session with multiple vulnerabilities, select the check box next to one or more vulnerabilities.
  4. Enter a note related to the vulnerability (or vulnerabilities) you selected.
  5. Click **OK**.

## Viewing Notes for a Selected Session

You can view notes, flags, and screenshots for a selected session by clicking **Attachments** on the **Session Info** panel.

## Viewing Notes for All Sessions

You can view notes, flags, and screenshots for all sessions by clicking **Attachments** on the **Scan Info** panel.

# Reviewing and Retesting

WebInspect offers several methods for reviewing or retesting discovered vulnerabilities. You may:

- Retest an individual vulnerability
- Verify all vulnerabilities discovered in a scan
- Rescan the entire site
- Compare two scans of the same site

**Caution:** If you have a previous version of WebInspect, HP recommends that you do not perform a Retest or Vulnerability Review as HP does not support these features from previous versions. The current version of WebInspect may display different results if you proceed.

## Review Individual Vulnerability

The Review feature is an extremely powerful tool for confirming that developers have fixed a specific vulnerability without having to conduct an entirely new scan.

1. Open a scan.
2. Right-click a vulnerable session in the [Navigation pane](#) or right-click a single vulnerability on the **Vulnerability** tab of the [Summary pane](#).
3. Select **Review Vulnerability** from the shortcut menu.
4. On the Vulnerability Review window, click **Retest**.

WebInspect resubmits the entire vulnerability path to the server, compares each result to the original response, and displays the percentage of retest responses that match the original. This indicates whether the vulnerability was accurately reproduced. Each HTTP request and response for the original session and the retest session can be compared side by side, instantly revealing any significant variations. Once the item has been confirmed as a vulnerability, you can submit the defect to either HP Quality Center or IBM Rational ClearQuest.

For more information, see [Vulnerability Review](#).

## Retest Vulnerabilities

This type of scan examines only those portions of the target site in which vulnerabilities were detected during the original scan. WebInspect does not conduct a new crawl of the site, but simply retraces the

path of vulnerable sessions (as recorded in the original scan) and attacks the resources using the same checks previously employed.

To retest all vulnerabilities:

1. Do one of the following:
  - Open a scan.
  - Select a scan on the Manage Scans pane of the Start page.
2. Click **Rescan** and select **Retest Vulnerabilities**.

The default name of the scan is "Site Retest - <original scan name>"; for example, the retest of a site that originally resulted in a scan named MySite would produce a scan named Site Retest - MySite. However, you can specify a different name when launching the scan.

Use the **Vulnerability** tab in the [Summary pane](#) to view the results. The grid contains an additional column named "Reproducible," which may contain the following values:

- **Not Found/Fixed** - The vulnerability detected in the original scan was not found by the retest. These vulnerabilities are displayed with gray text. You can conduct a vulnerability review and retest of these items. The percentage in parentheses indicates a heuristic confidence level for the determination.
- **Complete** - Both the original scan and the retest detected the same vulnerability. In other words, the vulnerability still exists.
- **New** - The retest detected a vulnerability that was not reported in the original scan. This is most likely attributable to content that was added to the resource after the original scan was conducted.

**Note:** This bulk retest feature uses only those portions of a scan policy that revealed vulnerabilities in the original scan. If new vulnerabilities have been introduced since then, they may be detectable only by checks that were not used during the retest.

Also, because the retest does not use the entire policy, the name of the policy listed in the dashboard statistics will be a dash (-).

## Rescan the Site

The Rescan feature allows you to transition easily from an open or selected scan into the scan wizard with the original scan settings preloaded. You may wish to conduct an identical scan of an updated site (using the same settings that were used for the original scan) to determine if previously discovered vulnerabilities have been fixed and if new ones have been introduced. Alternatively, you might want to tweak some of the settings to improve the crawl or audit.

The rescan functionality is available in two areas: the **Rescan** button on the scan toolbar and the **Rescan** button (and shortcut menu) for a selected scan on the Manage Scans pane.

1. Do one of the following:
  - Open a scan, click **Rescan** and select **Scan Again**.
  - On the WebInspect Start page, click **Manage Scans**; then select a scan and click **Rescan**.
2. Using the Scan Wizard, you may optionally modify the settings that were used for the original scan.

**Note:** The scan name is set by default to <original\_scan\_name>-1. If you conduct a rescan or a rescan, the integer appended to the default name will be incremented by one.

3. On the last step of the Scan Wizard, click **Scan**.

**Note:** You cannot rescan the results of a "Retest Vulnerabilities" function.

## Compare Scans

This feature allows you to compare the vulnerabilities revealed by two different scans of the same target. You can use this information to:

- **Verify fixes:** Compare vulnerabilities detected in the initial scan with those in a subsequent scan of a site in which the vulnerabilities were supposedly fixed.
- **Check on scan health:** Change scan settings and verify that those changes expand the attack surface.
- **Find new vulnerabilities:** Determine if new vulnerabilities have been introduced in an updated version of the site.
- **Investigate Issues:** Pursue anomalies such as false positives or missed vulnerabilities.
- **Compare authorization access:** Conduct scans using two different user accounts to discover vulnerabilities that are unique or common to both accounts.
- **Compare two instances of the same site:** Conduct scans on two instances of the same site, such as Production vs. Development, and compare findings.

**Note:** Data from both scans must be stored in the same database type (SQL Server Express Edition vs. SQL Server Standard/Enterprise Edition).

To compare two scans, do one of the following:

- From the Manage Scans page, select two scans and click **Compare**.
- From a tab containing an open scan (which will be Scan A in the comparison):

- a. Click **Compare**.
- b. Select a scan from the list on the Scan Comparison window. This scan will be Scan B in the comparison.
- c. Click **Compare**.

**Note:** If the open scan is a "site retest" (resulting from **Rescan > Retest Vulnerabilities**), WebInspect automatically selects the parent scan for comparison. For example, if you created a scan named "zero," and then verified vulnerabilities for that scan, the resulting scan would be named (by default) "site retest - zero." With the retest scan open, if you select **Compare**, WebInspect will compare "site retest - zero" with the parent scan "zero."

#### See Also

["Comparing Scans " on page 151](#)

["Reviewing a Vulnerability " on page 201](#)

## Recovering Deleted Items

When you remove a session or "ignore" a vulnerability, WebInspect deletes the item from the Navigation pane (in both the Site and Sequence views) and from the **Vulnerabilities** tab in the Summary pane. It also omits those items from any reports you may generate.

The number of deleted items is displayed on the Dashboard (under the Scan category). You can recover removed sessions and ignored vulnerabilities using the following procedure.

1. Click the highlighted number that appears next to the Deleted Items header.  
The Recover Deleted Items window displays a list of deleted items.
2. Click the drop-down list to toggle between ignored vulnerabilities and removed sessions.
3. Select the check box next to one or more items you want to recover.
4. To view detailed information about the items, select **Show details when selected**.
5. Click **Recover** and then click **Yes** when prompted to verify your selection.

Recovered vulnerabilities reappear in the Navigation pane in both the Site and Sequence views (along with their parent sessions) and also reappear in the **Vulnerabilities** tab in the Summary pane. Recovered sessions also reappear in the Navigation pane along with any child sessions and their vulnerabilities.

#### See Also

["Session Info Panel Overview " on page 67](#)

# Sending Vulnerabilities to a Defect Tracking System

You can convert one or more vulnerabilities to defects and add them to either the HP Quality Center or IBM Rational ClearQuest database (depending on which option you select).

1. Right-click a vulnerability in either the [Navigation pane](#) or the [Summary pane](#).
2. Select **Send to** and choose either **HP Quality Center** or **IBM Rational ClearQuest**.
3. On the Send to dialog, choose a profile from the **Profile** list.

If you need to create or edit a profile, click **Manage** to access the WebInspect [Application Settings](#).

**Note:** If the selected profile maps a WebInspect vulnerability to "Do not publish" (based on its severity level), the vulnerability will not be exported.

4. To force the creation of a defect even if it has been previously reported, select **Allow duplicate defect assignment**.

WebInspect recognizes duplicates only within the same scan. If you scan a site and send a specific vulnerability to Quality Center or ClearQuest, you can prevent WebInspect from sending that same vulnerability if it is encountered again during that scan. However, if you conduct a subsequent scan of that site and WebInspect again encounters that same vulnerability, WebInspect is not programmatically aware that the vulnerability was sent to Quality Center or ClearQuest during the previous scan.

5. To close this dialog after sending the defect(s), select **Close when finished**.
6. If you have selected multiple vulnerabilities, you can exclude a vulnerability by removing the check mark next to the ID number.
7. Click **Send**.

## Additional Information Sent

WebInspect will also add a note to the session information indicating that the vulnerability/defect was sent to HP Quality Center or IBM Rational ClearQuest, as illustrated by the following example:

Defect #30 was created in Quality Center.  
Check ID: 182  
CheckName: Dan-o Log Information Disclosure  
Profile: Thack  
Server URL: <http://qbakervm2003/qcbin>  
Project: test3

Priority: 3-High  
Severity: 1-Low

**Note:** If you receive the error message, "Error authenticating with Quality Center," see [Disabling Data Execution Prevention](#).

## Disabling Data Execution Prevention

When you attempt to integrate with HP Quality Center, you may receive the error message, "Error authenticating with Quality Center." If so, you must disable Microsoft's Data Execution Prevention (DEP) using one of the procedures described below.

### For Microsoft Windows XP Service Pack 2 (or later)

1. Right-click **My Computer** and select **Properties**.
2. Click the **Advanced** tab.
3. In the **Startup and Recovery** section, click **Settings**.
4. In the **System Startup** section, click **Edit**.
5. Locate the text "/NoExecute=OptIn" and replace OptIn (which the default) with AlwaysOff. Your boot.ini file should contain the following entry:

/NoExecute=AlwaysOff

Be sure to enter this text carefully and exactly. Failure to do so could prevent your computer from booting.

6. Click **File** and select **Save**.
7. Click **OK** to close the Startup and Recovery window.
8. Click **OK** to close the System Properties window.
9. Restart your computer.

### For Windows Vista (32-bit)

1. Click the Windows Vista Start orb.
2. In the **Start** menu, navigate to **All Programs** and select **Accessories**.

3. In the **Accessories** menu, right-click **Command Prompt** and select **Run as administrator**.

You may need to provide Administrator credentials at this point.

4. In the Command Prompt window, type the following:

```
bcdedit.exe /set {current} nx AlwaysOff
```

5. Press **Enter**.

The message "The operation completed successfully" should be displayed.

6. Close the Command Prompt window.

7. Restart your computer.

**Note:** Setting DEP to AlwaysOff does not provide any DEP coverage for any part of the system, regardless of hardware DEP support.

## Generating a Report

You can launch the Report Generator using a variety of methods:

- On the Start page, click **Generate a Report** in the left pane of the client area.
- On the WebInspect toolbar, click **Reports**.
- Click the **Reports** menu and select **Generate Report**.
- On the Manage Scans form, right-click a scan name and select **Generate Report**.
- With a scan open, right-click a session in the **Site view** and select **Generate Session Report**.
- When scheduling scans.
- When using the Report Designer.

Follow the steps below to generate a report.

1. Launch the Report Generator using one of the options listed above.
2. Select one or more scans from the Select a Scan window.
3. (Optional) Click **Advanced** (at the bottom of the window) to select options for saving reports and for selecting a template for headers and footers.

4. Click **Next**.
5. (Optional) Select a report from the **Favorites** list.

**Tip:** "Favorites" is simply a named collection of one or more reports and their associated parameters. To create a favorite once you have selected reports and parameters, click the **Favorites** list and select **Add to favorites**.

6. Select one or more reports. See [Standard Reports](#) for report descriptions.
7. Provide information for any parameters that may be requested. An exclamation mark  indicates a required parameter.
8. If you want to display each report on a separate tab (rather than combining all reports on one tab), select **Open Reports in Separate Tabs**.
9. Click **Finish**.

## Saving a Report

After WebInspect generates and displays the report, you can save it by clicking **Save As** on the Report Viewer toolbar.

Reports can be saved in the following formats:

- Adobe Portable Data Format (.pdf)
- Hypertext Markup Language (.html)
- Native WebInspect internal format (.raw)
- Rich Text Format (.rtf)
- Text (.txt)
- Microsoft Excel (.xls)

### See Also

- ["Standard Reports" on the next page](#)
- ["Advanced Report Options" on the next page](#)
- ["Compliance Templates " on page 221](#)
- ["Application Settings: Reports" on page 357](#)

## Advanced Report Options

The following table describes the advanced report options:

Option	Description
<b>Save reports to disk</b>	Select this option to output a report to a file.
<b>Automatically generate file name</b>	<p>If you select this option when saving the report to disk, the name of the report file will be formatted as &lt;reportname&gt; &lt;date/time&gt;. &lt;extension&gt;.</p> <p>For example, if creating a compliance report in pdf format and the report is generated at 6:30 on April 5, the file name would be "Compliance Report 04_05_2009 06_30.pdf." This is useful for recurring scans.</p> <ul style="list-style-type: none"> <li>• If you select more than one report type, then &lt;reportname&gt; will be "Combined Reports."</li> <li>• Reports are written to the directory specified for generated reports in the Application settings.</li> </ul> <p>If you do not select <b>Automatically generate filename</b>, replace the default name "auto-gen-filename" with a file name.</p>
<b>Export Format</b>	Select a report format.
<b>Header/Footer Report</b>	Select a format for the report's header and footer, and then enter or select the components.

## Standard Reports

The following standard reports are available:

Report	Description
Aggregate	This report is designed for multiple scans. You can select which severity categories to report, report sections (server content and vulnerability detail), and session information (responses and requests). Stack traces can also be reported, when available.
Alert View	This report lists all vulnerabilities sorted by severity, with a hyperlink to each HTTP request that elicited the vulnerability. It also includes an appendix that describes each vulnerability in detail.

Report	Description
Attack Status	For each attack agent (check) employed during the scan, this report lists the vulnerability ID number, check name, vulnerability severity, whether or not the check was enabled for the scan, whether or not the check passed or failed (i.e., did or did not detect the vulnerability), and (if it failed) the number of URLs where the vulnerability was detected. You can select to report vulnerabilities of a certain severity as well as the pass/fail status.
Compliance	This report provides a qualitative analysis by grading how well your application complies with certain government-mandated regulations or corporate-defined guidelines.
Crawled URLs	<p>For each URL encountered during the crawl, this report lists any cookies sent and the raw HTTP request and response.</p> <p><b>Note:</b> If WebInspect is unable to complete this report or if the report generates slowly, modify the report as follows:</p> <ol style="list-style-type: none"> <li>1. Open Report Designer.</li> <li>2. Open the Crawled URLs - Non-unique Subreport.</li> <li>3. For the RichTextBoxes underneath GroupHeaderRequest and GroupHeaderResponse, set the MaxLength property to 4096.</li> <li>4. Save the report.</li> </ol>
Developer Reference	Totals and detailed description of each form, JavaScript, e-mail, comment, hidden control, and cookie discovered on the Web site. You can select one or more of these reference types.
Duplicates	This report contains information about vulnerabilities detected by SecurityScope that were traceable to the same source. It begins with a bar chart comparing the total number of uncorrelated vulnerabilities to the number of unique vulnerabilities.
Executive Summary	This report lists basic statistics, plus charts and graphs that reflect your application's level of vulnerability.
False Positives	This report displays information about URLs that WebInspect originally classified as vulnerabilities, but were subsequently determined by a user to be false positives.
QA Summary	This report lists the URLs of all pages containing broken links, server errors, external links, and timeouts. You can select one or more of these categories.

Report	Description
Scan Difference	This report compares two scans and reports the differences, such as vulnerabilities, pages, and file-not-found responses that occur in one Web site but not the other.
Scan Log	Sequential list of the activities conducted by WebInspect during the scan (as the information appears on the <b>Scan Log</b> tab of the summary pane).
Trend	This report allows you to monitor your development team's progress toward resolving vulnerabilities. For example, you save the results of your initial scan and your team begins fixing the problems. Then once a week, you rescan the site and archive the results. To quantify your progress, you run a trend report that analyzes the results of all scans conducted to date. The report includes a graph showing the number of vulnerabilities, by severity, plotted on a timeline defined by the date on which each scan was conducted. Important: To obtain reliable results, make sure you conduct each scan using the same policy.
Vulnerability (Legacy)	This is a detailed report of each vulnerability, with recommendations concerning remediation.
Vulnerability	This report also presents detailed information about discovered vulnerabilities, sorted by severity.

## Compliance Templates

The available compliance templates are described below. Additional templates may be downloaded through SmartUpdate as they become available.

### 21CFR11

Part 11 of Title 21 of the United States Code of Federal Regulation (commonly abbreviated as "21 CFR 11") includes requirements for electronic records and electronic signatures. To assist medical companies in compliance, the US Food and Drug Administration (FDA) has published guidance for the proper use of electronic records and electronic signatures for records that are required to be kept and maintained by FDA regulations. The guidance outlines "criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper."

Due to the law and FDA guidance, medical companies and organizations dealing with highly sensitive medical information are being required to ensure that electronic records and electronic signatures are trustworthy, reliable, and generally an equivalent substitute for paper records and handwritten signatures. As interaction between equipment, operators, and computers becomes commonplace, it is important to establish a secure means to communicate and store information.

## Basel II

Basel II is a round of deliberations by central bankers from around the world, under the auspices of the Basel Committee on Banking Supervision (BCBS) in Basel, Switzerland, aimed at producing uniformity in the way banks and banking regulators approach risk management across national borders. The BCBS is the international rule-making body for banking compliance. In 2004, central bank governors and the heads of bank supervisory authorities in the Group of Ten (G10) countries endorsed the publication of "International Convergence of Capital Measurement and Capital Standards: a Revised Framework," the new capital adequacy framework commonly known as Basel II.

Basel II essentially requires banks to increase their capital reserves or demonstrate that they can systematically and effectively control their credit and operational risk. The framework defines operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events," and highlights hacking and information theft through inadequate systems security as loss events. While banks around the world are experts at managing risk by virtue of operating in global financial markets, they are relatively new at understanding and controlling the risks inherent with operating online banking systems and keeping customer data secure.

Banks that practice effective information and systems security are able to demonstrate to regulators that they should qualify for lower capital reserves through reduced operational risk. The Basel II framework insists that banks demonstrate that an effective system of policies and processes are in place to protect information and that compliance to these policies and processes is ensured, but is not prescriptive in how banks should implement security policies and processes. The international standard ISO/IEC 17799 Code of Practice for Information Security Management provides guidelines for implementing and maintaining information security and is commonly used as a model for managing and reporting operational risk related to information security in the context of Basel II.

## CA OPPA

The California Online Privacy Protection Act (OPPA) was established in 2003 to require all businesses and owners of commercial web sites in the state of California to conspicuously post and comply with a privacy policy that clearly states the policies on the collection, use, and sharing of personal information. The policy identifies the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information.

Any business, organization, or individual that operates a Web site that collects private personal information for a person residing in the state of California is bound by the provisions of the law, so the California OPPA has a much greater impact nationally than is typical for state legislation.

## CASB 1386

California Senate Bill 1386 has established the most specific and restrictive privacy breach reporting requirements of any state in the United States. The law was enacted to force businesses, organizations, and individuals holding private personal information for legitimate business purposes to inform consumers immediately when their personal information has been compromised. The law also gives consumers the right to sue businesses in civil court for damages incurred through the compromise of information. Any business, organization, or individual that holds private personal information for a person residing in the state of California is bound by the provisions of the law.

## COPPA

The Children's Online Privacy Protection Act (COPPA) was enacted in 2000 to protect the online collection of personal information about children under the age of 13. COPPA's goal was to protect children's privacy and safety online in recognition of the easy access that children often have to the

Web. The law requires that Web site operators post a privacy policy on the site and outlines requirements for Web site operators to seek parental consent to collect children's personal information in certain circumstances.

The law applies not only to Web sites that are clearly directed toward children but to any Web site that contains general audience content where the Web site operators have actual knowledge that they are collecting personal information from children. An operator must post a link to a notice of its information practices on the home page of its Web site or online service and at each area where it collects personal information from children. An operator of a general audience site with a separate children's area must post a link to its notice on the home page of the children's area.

#### DCID

This directive establishes the security policy and procedures for storing, processing, and communicating classified intelligence information in information systems. For purposes of this directive, intelligence information refers to sensitive compartmented information and special access programs for intelligence under the purview of the Director of Central Intelligence.

#### DoD Application Security Checklist Version 2

DISA Field Security Operations (FSO) conducts Application SRRs to provide a minimum level of assurance to DISA, Joint Commands, and other Department of Defense (DoD) organizations that their applications are reasonably secure against attacks that would threaten their mission. The complexity of most mission critical applications precludes a comprehensive security review of all possible security functions and vulnerabilities in the time frame allotted for an Application SRR. Nonetheless, the SRR helps organizations address the most common application vulnerabilities and identify information assurance (IA) issues that pose an unacceptable risk to operations.

Ideally, IA controls are integrated throughout all phases of the development life cycle. Integrating the Application Review process into the development lifecycle will help to ensure the security, quality, and resilience of an application. Since the Application SRR is usually performed close to or after the applications release, many of the Application SRR findings must be fixed through patches or modifications to the application infrastructure. Some vulnerabilities may require significant application changes to correct. The earlier the Application Review process is integrated into the development life cycle, the less disruptive the remediation process will be.

#### DoD Application Security and Development STIG V3 R2

This compliance template reports all applicable web application components of the Application Security and Development Security Technical Implementation Guide (STIG) Version 3, Release 1. The STIG provides security guidance for use throughout the application development lifecycle. Defense Information Systems Agency (DISA) encourages sites to use these guidelines as early as possible in the application development process.

#### EU Data Protection

The European Commission's Directive on Data Protection protects the fundamental rights of European Union citizens to privacy with respect to the processing of personal data. The primary focus of the directive is on the acceptable use and protection of personal data. Like all other European Union privacy legislation, this directive also requires that personal data be collected, stored, changed or disseminated only with a citizen's express consent and with full disclosure as to the use of the data. The directive also prohibits the transfer of personal data from European organizations to non-European Union nations and organizations that do not adequately protect the safety and privacy of personal data. The United States has developed a Safe Harbor framework for U.S. organizations that are required to

comply with this directive.

#### EU Directive on Privacy and Electronic Communications

European Union Directive on Privacy and Electronic Communications is part of a broader "telecoms package" of legislation that governs the electronic communications sector in the European Union. The directive reinforces a basic European Union principle that all member states must ensure the confidentiality of communications made over public communications networks and the personal and private data inherent in those communications. The directive governs the physical communication networks as well as the personal data that is carried on it.

#### FISMA

The United States Congress passed the E-Government Act of 2002 in recognition of the importance of information security to the economic and national security interests of the United States. Title III of the act, entitled the Federal Information Security Management Act (FISMA), tasked the National Institute of Standards and Technology with developing standards and guidelines to be used by all U.S. federal government agencies in implementing adequate information security as part of their information systems, underpinned by three security objectives for information systems: confidentiality, integrity and availability. FISMA requires the head of each federal agency to provide information security protections commensurate with the risk and magnitude of the harm that may result from unauthorized access, use, disclosure, disruption, modification or destruction of its information and information systems. The protection should apply not only within the agency, but also within contractor or other organizations working on behalf of the agency.

#### GLBA

The Gramm-Leach-Bliley Act (GLBA) mandates that financial institutions must protect consumers' personal financial information. The main provision affecting Web application security in the financial industry is the GLBA Safeguards Rule.

#### HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) mandates the privacy and security of personal health information from the various threats and vulnerabilities associated with information management.

#### ISO17799

This is the most commonly accepted international standard for information security management. Use this policy as a baseline in crafting a compliance policy to meet the needs of your organization and its security policy.

#### ISO27001

ISO/IEC 27001 is an information security management system standard published in October 2005 by the International Organization for Standardization and the International Electrotechnical Commission. The basic objective is to help establish and maintain an effective information management system using a continual improvement approach. ISO 27001 specifies the requirements for the security management system itself. It is the standard, as opposed to ISO 17799, against which certification is offered. Additionally, ISO 27001 is "harmonized" with other management standards, such as ISO 9001 and ISO 14001.

#### JPIPA

Japan enacted the Personal Information Protection Act (JPIPA) in 2003 to protect individuals' rights

and personal information while preserving the usefulness of information technology and personal information for legitimate purposes. The law establishes responsibilities for businesses that handle personal information for citizens of Japan and outlines potential fines and punishments for organizations that do not comply. The act requires businesses to communicate their purpose in collecting and using personal information. They must also take reasonable steps to protect personal information from disclosure, unauthorized use or destruction.

#### NERC

The North American Electric Reliability Council (NERC) was established in 1968 with the mission of ensuring that the electric system of the United States is reliable, adequate and secure. After President Bill Clinton issued Presidential Decision Directive 63 in 1998 to define infrastructure industries critical to the United States' national economy and public well-being, the U.S. Department of Energy designated the NERC to act as the coordinating agency for the electricity industry, which was named one of the eight critical infrastructure industries.

#### NIST 800-53

The United States Congress passed the E-Government Act of 2002 in recognition of the importance of information security to the economic and national interests of the United States. Title III of the act, entitled the Federal Information Security Management Act (FISMA), tasked the National Institute of Standards and Technology with developing standards and guidelines to be used by all U.S. federal government agencies in implementing adequate information security as part of their information systems, underpinned by three security objectives for information systems: confidentiality, integrity, and availability.

#### OMB

This policy addresses major application security sections that were defined in December 2004 by the Office of Management and Budget for federal agency public Web sites. These are information resources funded in whole or in part by the federal government and operated by an agency, contractor, or other organization on behalf of the agency. They present government information or provide services to the public or a specific non-federal user group and support the proper performance of an agency function.

#### OWASP Top Ten 2004/2007/2010

Many government agencies suggest testing for the Open Web Application Security Project (OWASP) Top Ten Web application vulnerabilities as a best practice in ensuring the security of your Web application.

#### PCI Data Security 1.2, 2.0

The Payment Card Industry (PCI) Data Security Policy requires that all PCI Data Security members, merchants, and service providers that store, process or transmit cardholder data verify all purchased and custom Web applications, including internal and external applications.

#### PIPEDA

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) is a new law that protects personal information in the hands of private sector organizations and provides guidelines for the collection, use and disclosure of that information in the course of commercial activity. The Act, based on ten privacy principles developed by the Canadian Standards Association, is overseen by the Privacy Commissioner of Canada and the Federal Court. As of January 1, 2004, all Canadian businesses are required to comply with the privacy principles set out by PIPEDA. The Act covers both

traditional, paper-based and on-line business.

#### Safe Harbor

The European Commission's Directive on Data Protection prohibits the transfer of personal data from European organizations to non-European Union nations and organizations that do not adequately protect the safety and privacy of personal data. Upon passage of this comprehensive European legislation, all businesses and organizations in the United States that share data with European Union organizations were obligated to comply with the regulations, which could have disrupted many types of trans-Atlantic business transactions. Due to the differences in approaches taken by the United States and European Union nations in protecting personal data privacy, the U.S. Department of Commerce, in consultation with the European Commission, developed a streamlined "Safe Harbor" framework through which U.S. organizations could comply with the Directive on Data Protection.

Organizations participating in the Safe Harbor are committed to complying with these seven principles designed to ensure that personal data is properly used, controlled and protected: Notice, Choice, Onward Transfer, Access, Security, Data Integrity and Enforcement. Of particular significance to information technology:

- The Notice principle requires organizations to inform individuals about the purposes for which it collects information, such as through a privacy policy.
- The Security principle states that organizations will take reasonable precautions to protect personal data.
- The Enforcement principle mandates that organizations have procedures in place for verifying that security commitments are satisfied, such as through comprehensive security testing.

#### SANS CWE Top 25

The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. The SANS Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors is a list of the most widespread and critical programming errors that can lead to serious software vulnerabilities. They are dangerous because they frequently allow attackers to completely take over the software, steal data, or prevent the software from functioning. This compliance template reports all applicable web application components of this list.

#### Sarbanes-Oxley

The Sarbanes-Oxley Act, which falls under the umbrella of the U.S. Securities and Exchange Commission (SEC), was enacted on July 30, 2002. It focuses on regulating corporate behavior for the protection of financial records, rather than enhancing the privacy and security of confidential customer information.

#### UK Data Protection

The European Commission's Directive on Data Protection protects the fundamental rights of European Union citizens to privacy with respect to the processing of personal data. The primary focus of the directive is on the acceptable use and protection of personal data. The United Kingdom implemented the protections mandated by the directive through its Data Protection Act of 1998, summarized as follows:

- Personal data should be processed fairly and lawfully and only with consent.
- Personal data should be obtained only for specified and lawful purposes, and should not be further processed in any manner incompatible with those purposes.
- Personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data should be accurate and kept up to date.
- Personal data processed for any purpose should not be kept for longer than is necessary for that purpose.
- Personal data should be processed in accordance with the rights of data subjects.
- Appropriate technical and organizational measures should be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data should not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

#### WASC

This compliance template is based on the Web Application Security Consortium threat classes. The WASC Threat Classification is a cooperative effort to clarify and organize the threats to the security of a web site. When used in conjunction with the All Checks policy, you can generate a compliance report that includes each vulnerability check contained in SecureBase.

## Managing Settings

This feature allows you to create, edit, delete, import, and export scan settings files.

You can also load and save settings and restore factory default settings from the Default Settings window. Click **Edit** and select **Default Scan Settings**.

From the WebInspect **Edit** menu, select **Manage Settings**.

The Manage Settings window opens.

## Creating a Settings File

To create a settings file:

1. Click **Add**.
2. On the Create New Settings window, change settings.
3. When finished, click **OK**.
4. Using a standard file-selection dialog, name and save the file.

## Editing a Settings File

To edit a settings file:

1. Select a file.
2. Click **Edit**.
3. On the Create New Settings window, change settings.
4. When finished, click **OK**.

## Deleting a Settings File

To delete a settings file:

1. Select a file.
2. Click **Delete**.

## Importing a Settings File

To import a settings file:

1. Click **Import**.
2. Using a standard file-selection dialog, select a settings file and click **Open**.

## Exporting a Settings File

To export a settings file:

1. Select a file.
2. Click **Export**.

3. Using a standard file-selection dialog, name the file and select a location.
4. Click **Save**.

## Scanning with a Saved Settings File

To scan with a saved settings file:

1. From the WebInspect **Edit** menu, select **Default Settings**.
2. At the bottom of the Default Settings window, in the left column, click **Load settings from file**.
3. Using a standard file-selection dialog, select the settings file you want to use and click **Open**.

The file you select is now your default settings file.

## SmartUpdate

The WebInspect SmartUpdate feature contacts the Hewlett-Packard data center via the Internet to check for new or updated adaptive agents, vulnerability checks, and policy information. SmartUpdate will also ensure that you are using the latest version of WebInspect, and will prompt you if a newer version of the product is available for download.

You can configure WebInspect settings to conduct a SmartUpdate each time you start the application (select **Application Settings** from the **Edit** menu and choose **Smart Update**).

You can also run SmartUpdate on demand through the WebInspect user interface by selecting **Start SmartUpdate** from the WebInspect **Start Page**, by selecting **SmartUpdate** from the **Tools menu**, or by clicking the **SmartUpdate** button on the **standard toolbar**.

**Caution:** For enterprise installations, if SmartUpdate changes or replaces certain files used by WebInspect, the sensor service may stop and the sensor will display a status of "off line." You must launch the WebInspect application and restart the service. To do so:

1. Click **Edit > Application Settings**.
2. Select **Run as a Sensor**.
3. Click the **Start** button in the Sensor Status area.

## Performing a SmartUpdate

1. Do one of the following:
  - From the toolbar, click **SmartUpdate**.
  - Select **SmartUpdate** from the **Tools** menu.
  - Select **Start SmartUpdate** from the WebInspect **Start Page**.

If updates are available, the SmartUpdate window displays up to three separate collapsible panes for downloading the following:

- New and updated checks
- WebInspect software
- SmartUpdate software

2. Select the check box associated with one or more of the download options.
3. To install the updates, click **Download**.

## Downloading Checks without Updating WebInspect

If you download checks without also downloading available new versions of WebInspect, HP will continue to offer updates to your installed knowledgebase for only 10 days. Beyond that period, updates will not be available to you until you download the new WebInspect software.

## WebSphere Portal FAQ

### How do you know if an application is running on WebSphere Portal?

WebSphere Portal applications typically have very long urls that begin with /wps/portal or /wps/myportal followed by encoded sections. For example:

[http://myhost.com/wps/portal/internet/customers/home/!ut/p/b1/fY7BcolwFAC\\_xS94T4QCx6Rpk6qlo20x5tIJShElJolD0q-vnfFq97Yze1hQIEEdV8W-lzaozZ\\_rh6-HjkRfrhERBZ4-EKESBmde5ggzEEVxmbXNGW7-sIsKdgTW3c\\_B3xmpzBfnacLv6QuIfxVHKJGhmNfzToue8nWdKg4fx8jtaT9MJpB2zQPgqlp9GrADyey0tvvL1F9Sntm\\_y0cbuw8Xbmvg2NN6412wlsQP27GAa3AO9AEBJhmxxcnWHlk8kverBIBQ!!/dl4/d5/L2dBISEvZ0FBIS9nQSEh/](http://myhost.com/wps/portal/internet/customers/home/!ut/p/b1/fY7BcolwFAC_xS94T4QCx6Rpk6qlo20x5tIJShElJolD0q-vnfFq97Yze1hQIEEdV8W-lzaozZ_rh6-HjkRfrhERBZ4-EKESBmde5ggzEEVxmbXNGW7-sIsKdgTW3c_B3xmpzBfnacLv6QuIfxVHKJGhmNfzToue8nWdKg4fx8jtaT9MJpB2zQPgqlp9GrADyey0tvvL1F9Sntm_y0cbuw8Xbmvg2NN6412wlsQP27GAa3AO9AEBJhmxxcnWHlk8kverBIBQ!!/dl4/d5/L2dBISEvZ0FBIS9nQSEh/)

### Which versions of WebSphere Portal are supported?

Versions 6.1 and later are supported.

### **Why does WebInspect require special settings to scan a WebSphere Portal application?**

The encoded sections of the URL include what is called "navigation state," which contains information about how to display elements in the current page (similar to VIEWSTATE in .Net) plus the navigation history. It is this navigation history that is troublesome for automated crawlers. As the crawler visits each link, the navigation state is being updated. This causes links on a page that the crawler may have already visited to continuously change. Since these look like new links, the crawler visits them and becomes trapped in an endless cycle.

When the WebSphere Portal overlay is selected, WebInspect can decode the navigation state in a URL and determine if the URL has already been visited. This prevents the crawler from continuously visiting the same page over and over again.

### **How does WebInspect decode the navigation state?**

WebSphere Portal 6.1 and later include a URL decoding service. When the WebSphere Portal overlay is selected, WebInspect can pass a URL to the decoding service and evaluate the response to determine if this URL has already been visited. Although the decoding service is on by default, it is possible to turn it off in your WebSphere Portal server configuration. To get a good scan of your site with WebInspect, the decoding service must be enabled.

### **Is the navigation state just a special kind of session ID?**

No. Navigation state does not contain any session information. Session is maintained via cookies.

### **Any special instructions when recording a login macro?**

Make sure that the cookies JSESSIONID and LtpaToken are set as state parameters.

### **Why does the site tree contain deeply nested folders?**

WebInspect's site tree does not currently understand how to parse the navigation state in WebSphere Portal URLs. It treats each section as a directory. These are, of course, not real directories. You will generally need to drill down to the lowest level of each branch to see the real content.

### **Is there any limitation on what types of attacks WebInspect can perform on WebSphere Portal applications?**

WebInspect can perform all manipulation attacks on WebSphere Portal applications. This includes (but is not limited to) XSS, SQL Injection, CSRF, RFI, LFI and others. WebInspect will not perform any site search attacks when scanning a WebSphere Portal site. These include searching for backup files (.bak, .old), hidden files, hidden directories and platform specific configuration files. The reason for this exclusion is because almost any request will result in a 200 response to the default portal view and so there is no way to distinguish between an error response and a valid response.

### **How can you tell if the crawler is working correctly on a WebSphere Portal site?**

The WebSphere Portal decoding service must be enabled and reachable on the server for the crawler to perform optimally. You can confirm if this is working by manually decoding a URL. Copy a URL from your site and modify it like this:

`http://myhost.com/wps/poc?uri=state: path with navigation state>&mode=download`

You should get an xml response. Alternatively, start a scan of your site with the WebSphere Portal overlay selected. Enable Traffic Monitor or run the scan through the Web Proxy. You should see periodic requests to the decoder service in the following format:

`http://myhost.com/wps/poc?uri=state: path with navigation state>&mode=download.`

Another thing to consider is that the path of the decoding service can be changed on the server. If this is the case, you will need to modify your scan settings manually. Contact [HP technical support](#) for assistance.

It is also possible to modify the navigation state marker. By default this is !ut/p. If this is changed from the default on the server, you will need to modify your scan settings manually. Contact [HP technical support](#) for assistance.

## Command Line Execution

You can initiate several WebInspect functions via a command line interface using the program WI.exe. Use the following syntax when typing a command:

```
wi.exe -u url [-s file] [-db] [-ws file] [-o|c][-n name] [-b filepath] [-d filepath -m filename] [-i[erdx] scanid] [-x|xd|xa|xn] [-Framework name] [-Crawl|Coverage name][ -ps policyID | -pc path] [-a[bndakm] {creds}] [-e [abcdefgijklmnopst] file] [-v] [-r report_name -w report_favorite -ag -y report_type -f report_export_file -g[phacxe] [-t compliance_template_file] [-?]
```

To run multiple scans from the command line, create and execute a batch file, using a format similar to the following:

```
c:  
cd \program files\HP\HP WebInspect  
wi.exe -u http://172.16.60.19 -ps 4  
wi.exe -u http://www.mywebsite.com  
wi.exe -u http://172.16.60.17  
wi.exe -u http://172.16.60.16
```

## Options

The options are defined in the following table. Items in italics require a value.

Category	Parameter	Definition
General	?	Show usage.

Category	Parameter	Definition
	u {url}	<p>URL or IP address.</p> <p>Caution 1: When using the -u parameter with -s (a settings file), be sure to specify an -x, -xa, -xd, or -xn parameter to restrict a scan to folders, if desired. Failure to do so may result in an unrestricted audit under certain conditions.</p> <p>Caution 2: If the URL contains an ampersand (&amp;), you must enclose the URL within quotation marks.</p>
	s {filename}	Settings file [Note that command line parameters take precedence over values in a settings file].
	db	Use database defined in settings file. If omitted, WebInspect defaults to database connection defined in application settings.
	ws {filename}	Web Service Design file.
	o	Audit only.
	c	Crawl only.
	n {name}	Scan name.
	b {filepath}	Use given SecureBase file. For path, specify the full path and file name.
	d {filepath}	Move database to filepath.
	m {filename}	Move database to filename.
	ie {scanid}	Start configured scan with the specified scan ID (GUID).
	ir {scanid}	Resume scan with the specified scan ID (GUID).
	ix {scanid}	Use existing scan with the specified scan ID (GUID), but do not continue the scan.
	id {scanid}	Delete scan with the specified scan ID (GUID).
Restrict to Root Folder	x	Restrict to directory only (self).
	xa	Restrict to directory and parents (ancestors).
	xd	Restrict to directory and subdirectories (descendants).

Category	Parameter	Definition
	xn	Ignore “restrict to folder” rules in referenced settings file. Restrict to folder parameters (x xa xb xn) can be in their own category (as report or output).
Framework	framework {framework_name}	Name of framework; currently only Oracle ADF Faces (Oracle) and IBM WebSphere Portal (WebSpherePortal) are supported. Optimizes scanning of application built with either of these technologies.
Crawl Coverage	CrawlCoverage {Coveragename}	Values for Coveragename are: Thorough = Exhaustive crawl of entire site Default = Focus more on coverage than performance Moderate = Balance of coverage and speed Quick = Focus on breadth and performance
Audit Policy	ps {policy id}	Use a non-custom policy. Values for <i>policy id</i> are: 1 = Standard 2 = Assault 3 = SOAP 4 = Quick 5 = Safe 6 = Development 7 = Blank 16 = QA 17 = Application 18 = Platform 1001 = SQL Injection 1002 = Cross-Site Scripting 1003 = OWASP Top 10 Application Security Risks 2007 1004 = All Checks 1005 = Passive 1008 = Critical and High Vulnerabilities 1009 = OWASP Top 10 Application Security Risks 2010 1010 = Aggressive SQL Injection 1011 = NoSQL and Node.js 1012 = OWASP Top 10 Application Security Risks 2013 1013 = Mobile 1014 = OpenSSL Heartbleed 1015 = Apache Struts
	pc {policy path}	Use a custom policy. For path, specify the full path and file name, such as: C:\MyPolicies\MyCustomPolicy.policy

<b>Category</b>	<b>Parameter</b>	<b>Definition</b>
Authentication	ab { <i>id:password</i> }	Basic mode (user name and password).
	an { <i>id:password</i> }	NTLM mode (user name and password).
	ad { <i>id:password</i> }	Digest mode (user name and password).
	aa { <i>id:password</i> }	Automatic mode (user name and password).
	ak { <i>id:password</i> }	Kerberos mode (user name and password).
	am { <i>path</i> }	Web macro (path and macro name).
Output	ea { <i>filepath</i> }	Export scan in legacy full XML format.
	eb { <i>filepath</i> }	Export scan details (Full) in legacy XML format.
	ec { <i>filepath</i> }	Export scan details (Comments) in legacy XML format.
	ed { <i>filepath</i> }	Export scan details (Hidden Fields) in legacy XML format.
	ee { <i>filepath</i> }	Export scan details (Script) in legacy XML format.
	ef { <i>filepath</i> }	Export scan details (Set Cookies) in legacy XML format.
	eg { <i>filepath</i> }	Export scan details (Web Forms) in legacy XML format.
	eh { <i>filepath</i> }	Export scan details (URLs) in legacy XML format.
	ei { <i>filepath</i> }	Export scan details (Requests) in legacy XML format.
	ej { <i>filepath</i> }	Export scan details (Sessions) in legacy XML format.
	ek { <i>filepath</i> }	Export scan details (E-mails) in legacy XML format.
	el { <i>filepath</i> }	Export scan details (Parameters) in legacy XML format.
	em { <i>filepath</i> }	Export scan details (Web Dump) in legacy XML format.
	en { <i>filepath</i> }	Export scan details (Offsite Links) in legacy XML format.
	eo { <i>filepath</i> }	Export scan details (Vulnerabilities) in legacy XML format.
	ep { <i>filepath</i> }	Export scan in FPR format to specified file.
	es { <i>filepath</i> }	Export scan in .scan format to specified file.
	et { <i>filepath</i> }	Export scan with logs in .scan format to specified file.
	v	Verbose output.

Category	Parameter	Definition
Reports	r {report_name} For multiple reports, separate report names with a semicolon. All reports will be contained in a single file.	Name of the report to run. Valid values for <i>report_name</i> are: Aggregate Alert View Attack Status Compliance Crawled URLs Developer Reference Duplicates Executive Summary False Positive QA Summary Scan Difference Scan Log Trend Vulnerability Vulnerability (Legacy)
		<b>Note:</b> Report names containing a space must be enclosed in quotation marks.
	w {favorite_name}	Name of the report favorite to run.
	ag	Aggregate reports in report favorite.
	y {report_type}	The type of report: Standard or Custom.
	f {export_file}	File path and file name where the report will be saved.
	gp	Export as Portable Document Format (PDF) file.
	gh	Export as HTML file in .zip file.
	ga	Export as raw report file.
	gc	Export as rich text format (RTF) file.
	gx	Export as text file.
	ge	Export as Excel file.
	t {filepath}	Use specified compliance template file.

## Examples

The following examples illustrate command line execution as if executed from the WebInspect home directory:

```
wi.exe -u www.anywebsite.com -ps 1 -ab MyUsername:Mypassword  
wi -u https://zero.webappsecurity.com -s c:\program  
files\webinspect\scans\scripted\  
-f c:\program files\webinspect\scans\scripted\zero051105.xml
```

If you do not specify a policy, WebInspect will crawl (but not audit) the Web site.

If you specify an invalid policy number, WebInspect will not conduct the scan.

## Hyphens in Command Line Arguments

You can use hyphens in command line arguments (output files, etc.) only if the argument is enclosed in double quotes, as illustrated by the "export path" argument in the following command:

```
wi.exe -u http://zero.webappsecurity.com -ea "c:\ temp\command-line-test-export.xml"  
"
```

**Note:** To initiate a command line, select **Run** from the Windows **Start** menu, type "cmd" in the **Open** box, and click **OK**. This will ensure proper handling of long file names. The process, as it appears in the Task Manager, is WI.exe. Scan data will be cached temporarily in the Working directory and then moved to the Scans directory.

## WebInspect Policies

A policy is a collection of vulnerability checks and attack methodologies that WebInspect deploys against a Web application. Each policy is kept current through WebInspect's Smart Update functionality, ensuring that scans are accurate and capable of detecting the most recently discovered threats.

WebInspect contains the following packaged policies that you can use to determine the vulnerability of your Web application.

## Best Practices

This group contains policies designed to test applications for the most pervasive and problematic Web application security vulnerabilities.

Policy	Description
OWASP Top 10 - 2013	This policy provides a minimum standard for Web application security. The OWASP Top 10 represents a broad consensus about what the most critical Web application security flaws are. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.
Standard	A Standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the Web server, Web application server and Web application layers. A Standard scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.

## By Type

The By Type group contains policies designed with a specific application layer, type of vulnerability, or generic function as its focus. For instance, the Application policy contains all checks designed to test an application, as opposed to the operating system.

Policy	Description
Aggressive SQL Injection	This policy performs a comprehensive security assessment of your Web application for SQL injection vulnerabilities. SQL injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the Web application for execution by a backend database.
Application	The Application policy performs a security scan of your Web application by submitting known and unknown Web application attacks, and only submits specific attacks that assess the application layer. When performing scans of enterprise level Web applications, use the Application Only policy in conjunction with the Platform Only policy to optimize your scan in terms of speed and memory usage.
Blank	This policy is a template that you can use to build your own policy. It includes an automated crawl of the server and no vulnerability checks. Edit this policy to create custom policies that only scan for specific vulnerabilities.
Criticals and Highs	Use the Criticals and Highs policy to quickly scan your Web applications for the most urgent and pressing vulnerabilities while not endangering production servers. This policy checks for SQL Injection, Cross-Site Scripting, and other critical and high severity vulnerabilities. It does not contain checks that may write data to databases or create denial-of-service conditions, and is safe to run against production servers.

Policy	Description
Cross-Site Scripting	This policy performs a security scan of your Web application for cross-site scripting (XSS) vulnerabilities. XSS is an attack technique that forces a Web site to echo attacker-supplied executable code, such as HTML code or client-side script, which then loads in a user's browser. Such an attack can be used to bypass access controls or conduct phishing expeditions.
Dev	A Developer scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the Web application layer only. The policy does not execute checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
NoSQL and node.js	A NoSQL and Node.js scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities targeting databases based on NoSQL such as MongoDB and server side infrastructures based on JavaScript such as NodeJS. This policy includes checks that are available to WebInspect release 9.3 and above.
Mobile	A mobile scan will detect security flaws based on the communication observed between a mobile application and the supporting backend services.
OWASP Top 10 - 2010	This policy provides a minimum standard for Web application security. The OWASP Top 10 represents a broad consensus about what the most critical Web application security flaws are. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.
OWASP Top 10 - 2007	This policy provides a minimum standard for Web application security. The OWASP Top 10 represents a broad consensus about what the most critical Web application security flaws are. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.
Passive	The Passive Scan policy scans an application for vulnerabilities detectable without active exploitation, making it safe to run against production servers. Vulnerabilities detected by this policy include issues of path disclosure, error messages, and others of a similar nature.
Platform	The Platform policy performs a security scan of your Web application platform by submitting attacks specifically against the Web server and known Web applications. When performing scans of enterprise-level Web applications, use the Platform Only policy in conjunction with the Application Only policy to optimize your scan in terms of speed and memory usage.

Policy	Description
QA	The QA policy is designed to help QA professionals make project release decisions in terms of Web application security. It performs checks for both known and unknown Web application vulnerabilities. However, it does not submit potentially hazardous checks, making it safe to run on production systems.
Quick	A Quick scan includes an automated crawl of the server and performs checks for known vulnerabilities in major packages and unknown vulnerabilities at the Web server, Web application server and Web application layers. A quick scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
Safe	A Safe scan includes an automated crawl of the server and performs checks for most known vulnerabilities in major packages and some unknown vulnerabilities at the Web server, Web application server and Web application layers. A safe scan does not run any checks that could potentially trigger a denial-of-service condition, even on sensitive systems.
SQL Injection	The SQL Injection policy performs a security scan of your Web application for SQL injection vulnerabilities. SQL injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the Web application for execution by a backend database.

## Custom

The Custom group contains all user-created policies, any custom policies modified by a user, and the policy listed below.

Policy	Description
Hacme Bank	A custom policy for scanning an example Web site maintained by OWASP. For more information, visit <a href="https://www.owasp.org/index.php/Hacme_Bank">https://www.owasp.org/index.php/Hacme_Bank</a> .

## Hazardous

The Hazardous group contains a policy with potentially dangerous checks, such as a denial-of-service attack, that could cause production servers to fail. Use this policy against non-production servers and systems only.

Policy	Description
All Checks	<p>An All Checks scan includes an automated crawl of the server and performs all active checks from SecureBase, the WebInspect database. This scan includes all checks that are listed in the compliance reports that are available in Hewlett-Packard Web application and Web services vulnerability scan products. This includes checks for known and unknown vulnerabilities at the Web server, Web application server, and Web application layers.</p> <p><b>Caution:</b> An All Checks scan includes checks that may write data to databases, submit forms, and create denial-of-service conditions. It is strongly recommended that All Checks scans be used only in test environments.</p>
Assault	<p>An Assault scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the Web server, Web application server, and Web application layers.</p> <p><b>Caution:</b> An Assault scan includes checks that can create denial-of-service conditions. It is strongly recommended that assault scans only be used in test environments.</p>

## Regular Expressions

Special metacharacters and sequences are used in writing patterns for regular expressions. The following table describes some of these characters and includes short examples showing how the characters are used. Another recommended resource is the [Regular Expression Library](#).

To verify the syntax of regular expressions you create, use the [Regular Expression Editor](#) (if it is installed on your system).

Character	Description
\	Marks the next character as special. /n/ matches the character " n ". The sequence /n/ matches a line feed or newline character.
^	<p>Matches the beginning of input or line.</p> <p>Also used with character classes as a negation character. For example, to exclude everything in the content directory except /content/en and /content/ca, use: /content/[^ (en ca)]. */.* . Also see \S \D \W.</p>
\$	Matches the end of input or line.

Character	Description
*	Matches the preceding character zero or more times. /zo*/ matches either " z " or "zoo."
+	Matches the preceding character one or more times. /zo+/ matches "zoo" but not "z."
?	Matches the preceding character zero or one time. /a?ve?/ matches the "ve" in "never."
.	Matches any single character except a newline character.
[xyz]	A character set. Matches any one of the enclosed characters. /[abc]/ matches the "a" in "plain."
\b	Matches a word boundary, such as a space. /ea*\rb/ matches the "er" in "never early."
\B	Matches a nonword boundary. /ea*\r\B/ matches the "ear" in "never early."
\d	Matches a digit character. Equivalent to [0-9].
\D	Matches a nondigit character. Equivalent to [^0-9].
\f	Matches a form-feed character.
\n	Matches a line feed character.
\r	Matches a carriage return character.
\s	Matches any white space including space, tab, form-feed, and so on. Equivalent to [\f\n\r\t\v]
\S	Matches any nonwhite space character. Equivalent to [^\f\n\r\t\v]
\w	Matches any word character including underscore. Equivalent to [A-Za-z0-9_].
\W	Matches any nonword character. Equivalent to [^A-Za-z0-9_].

WebInspect developers have also created and implemented extensions to the normal regular expression syntax. For more information, see [Regex Extensions](#).

## Regex Extensions

Hewlett-Packard engineers have developed and implemented extensions to the normal regular expression (regex) syntax. When building a regular expression, you can use the tags and operators described below.

## Regular Expression Tags

- STATUSCODE]
- [BODY]
- [ALL]
- [URI]
- [HEADERS]
- [COOKIES]
- [STATUSLINE]
- [STATUSDESCRIPTION]
- [SETCOOKIES]
- [METHOD]
- [REQUESTLINE]
- [VERSION]
- [POSTDATA]
- [TEXT]

## Regular Expression Operators

- AND
- OR
- NOT
- [ ]
- ( )

## Examples

- To detect a response in which (a) the status line contains a status code of "200" and (b) the phrase "logged out" appears anywhere in the message body, use the following regular expression:

```
[STATUSCODE]200 AND [BODY]logged\sout
```

- To detect a response indicating that the requested resource resides temporarily under a different URI (redirection) and having a reference to the path "/Login.asp" anywhere in the response, use the following:

```
[STATUSCODE]302 AND [ALL]Login.asp
```

- To detect a response containing either (a) a status code of "200" and the phrase "logged out" or "session expired" anywhere in the body, or (b) a status code of "302" and a reference to the path "/Login.asp" anywhere in the response, use the following regular expression:

```
( [STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired ) OR  
( [STATUSCODE]302 AND [ALL]Login.asp )
```

**Note:** You must include a space (ASCII 32) before and after an "open" or "close" parenthesis; otherwise, the parenthesis will be erroneously considered as part of the regular expression.

- To detect a redirection response where "login.aspx" appears anywhere in the redirection Location header, use the following regular expression:

```
[STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx
```

- To detect a response containing a specific string (such as "Please Authenticate") in the Reason-Phrase portion of the status line, use the following regular expression:

```
[STATUSDESCRIPTION]Please\sAuthenticate
```

### See Also

["Regular Expressions" on page 241](#)

## WebInspect API

This topic provides information on the WebInspect API.

## About the WebInspect API

The WebInspect API provides an interface between your systems and WebInspect. It runs as a lightweight Windows service (WebInspect API) that is installed automatically when you install WebInspect. You configure, start, and stop the service using the HP Fortify Monitor tool. You can use the WebInspect API to add security audit capabilities to your existing automation scripts.

WebInspect API provides a RESTful interface for remotely controlling the proxy and scanner.

## Configuring the WebInspect API

Before you can use the WebInspect API, you must configure it.

1. From the Windows Start menu, click **All Programs > HP > HP WebInspect > HP Fortify Monitor.**

The HP Fortify Monitor icon appears in the system tray.

2. Right-click the **HP Fortify Monitor** icon.
3. From the right-click menu, select **Configure WebInspect API**.

The Configure WebInspect API dialog box appears.

4. Configure the API Server settings.

Settings	Value
Host	Both WebInspect and the WebInspect API must reside on the same machine. The default setting, +, is a wild card that tells the WebInspect API to intercept all request on the port identified in the Port field. If you have another service running on the same port and want to define a specific hostname just for the API service, this value can be changed.
Port	Use the provided value or change it using the up/down arrows to an available port number.

Settings	Value
Authentication	<p>Choose None, Windows, or Basic from the Authentication drop-down selector.</p> <p>If you chose Basic as the authentication type, you will need to provide user name(s) and password(s). Click the Edit access tokens button and select a text editor. The wircserver.keys file will open in the text editor. Add a username and password, separated by a colon, for each user to be authenticated. There should be only one username and password per line. Save the file.</p>
Log Level	Choose the level of log information you want to collect.
Use HTTP	<p>Select this checkbox if you want to access the server over an HTTPS connection.</p> <p>To run the server over HTTPS, you will need to create a server certificate and bind it to the API service using the following command:</p> <pre>netsh http add sslcert ipport=0.0.0.0:&lt;port&gt;certhash=&lt;thumbprint&gt;aappid={160e1003-0b46-47c2-a2bc-01ea1e49b9dc}</pre>

5. Use the provided Listener Address in the Proxy Service Configuration section, or change it to the network address of the API server.
6. Click the **Start** button to start the WebInspect API service.

## About Automating WebInspect

You can use the WebInspect API to add WebInspect to your to your existing automation scripts. As long as the user agent can access the Service Router, the scripts can live in an entirely different environment from WebInspect.

## About the WebInspect API Service Providers

The WebInspect API comes with two service providers: Proxy and Scanner.

### Proxy

The proxy service provider provides a control mechanism for the proxies in use.

Method	URI	Path params	Request params	Description
DELETE	/webinspect/proxy/<instanceID>	instanceID (required)	None	Completely deletes a proxy instance and any data it contains. Any subsequent GET to that instanceID will return a 404.
GET	/webinspect/proxy/	None	None	Retrieves the list of all running proxies.
GET	/webinspect/proxy/<instanceID>.<extension>	instanceID (required) extension (required)- valid values for extension are psf, webmacro, and <i>xml</i> .	None	Gets the proxy results in the format specified by the extension. For example, a request for /12345.psf will get the proxy results in psf format.
GET	/webinspect/proxy/<instanceID>	instanceID (required)	None	Gets host and port for a specific instance.

Method	URI	Path params	Request params	Description
POST	/webinspect/proxy/	None	instanceID  (optional) – user can specify an instanceID, or system will generate if blank  port  (optional) – user can specify	Creates a new proxy instance. Returns instanceID, port, and proxy IP address.
PUT	/webinspect/proxy/<instanceID>	instanceID (required) – instanceID to be updated	action (required)	action=rese t will clear the proxy traffic without deleting the proxy instance.
PUT	/webinspect/proxy/<instanceID>.<extensi on>	instanceID (required)  extension (required) -- valid values for extension are psf, webmacro, and xml.	action (required)	action=sav e will save the proxy results to the WebInspect settings directory on the server. This saves the round trip of having to download the proxy results and then reupload them."

## Scanner

The scanner service provider allows remote access to start, stop, and query scans. The following RESTful API covers all v1.0 supported functionality:

Meth od	URI	Path params	Request params	Description
GET	/webinspect/scanner/settings/	None	None	<p>Gets a list of scan settings file names from WebInspect's default scan settings directory.</p> <p><b>Note:</b> All settings must be in this directory to be used with the remote scanner.</p>

Method	URI	Path params	Request params	Description
GET	/webinspect/scanner/scans/	None	query (options) – a JSON serialized list of constraints for scans to be returned. Accepted values are: <i>Name</i> , <i>Status</i> , <i>StartsAfter</i> , and <i>EndsBefore</i> . All query terms are ANDed together.	<p>Gets a list of known scan information in JSON with the following fields for each scan: ID (as GUID), Name, StartTime and Status. These results can be filtered by sending the optional "query" parameter.</p> <p><b>Note:</b> Currently, if you are using SQL Express to store your scans, only scans created with the WebInspect API will be returned.</p>

Method	URI	Path params	Request params	Description
GET	/webinspect/scanner/<scanId>	scanId: The ID of the scan represented as a GUID.	action <i>WaitForStatusChange</i> will block until the status of the scan changes.  action <i>GetCurrentStatus</i> will immediately return the current scan status.	Retrieves the status of the specified scan. A request with action <i>waitForstatuschange</i> will block until the status of the scan changes (i.e. waiting for a scan to stop). If the scan has already been stopped, the request will return immediately. A request with action <i>getcurrentstatus</i> with the current status of the scan. The scan status is returned in the body of the response.

Method	URI	Path params	Request params	Description
GET	/webinspect/scanner/<scanId>.scan	scanId: The ID of the scan represented as a GUID.	None	<p>Exports the specified scan. Returns a binary scan file in the body of the response.</p> <p><b>Note:</b> Currently only scans created via the Webinspect API will have the scan logs exported along with it. Scans not created via the API can be exported via the API but the scan logs will be absent.</p>
GET	/webinspect/scanner/<scanId>.details	scanId: The ID of the scan represented as a GUID.	detailType: The type of scan detail to export. Currently supported detail types: <i>Full</i> , <i>Comments</i> , <i>HiddenFields</i> , <i>Script</i> , <i>SetCookies</i> , <i>WebForms</i> , <i>Urls</i> , <i>Requests</i> , <i>Sessions</i> , <i>Emails</i> , <i>Parameters</i> , <i>OffsiteLinks</i> , <i>Vulnerabilities</i> .	Exports the 'detail' of the specified scan in XML format. The 'detail' of a scan consists of individual parts of a scan (i.e. a list of the URLs discovered, or a list of the emails found).

Method	URI	Path params	Request params	Description
GET	/webinspect/scanner/policies	None	None	Returns a list of policy names and IDs.

Method	URI	Path params	Request params	Description
POST	/webinspect/scanner/	None	<p>settingsName – The name (lacking ext) of the settings file to use. The named file is expected to have the .xml extension and is expected to be in the default WebInspect settings directory.</p> <p>overrides (optional) – A JSON serialized list of settings overrides to be applied to the scan settings selected. The following settings overrides are supported:</p> <ul style="list-style-type: none"> <li>ScanName -- The name of the scan.</li> <li>StartURL -- The URL of the site to scan.</li> <li>CrawlAuditMode -- Accepted values are <i>auditonly</i>, <i>crawlonly</i>, and <i>crawlandaudit</i>.</li> <li>StartOption -- Accepted values are macro and URL. If using the macros start option you can supply a workflow macro.</li> <li>LoginMacro -- The name of the macro. Macro files are currently looked for</li> </ul>	<p>Creates a new scan with settings referred to by the provided settings file name. The scan will be started.</p> <p><b>Note:</b> The HTTP request will be blocked until after the scan has been started and the scan ID (represented as a GUID) is returned in the response body.</p>

Method	URI	Path params	Request params	Description
			<p>in the scan settings directory. All hosts in the given macro will be added to allowed hosts.</p> <p>WorkflowMacros -- A list of workflow macro file names for use within the scan. <i>StartOption</i> should be set to macro.</p> <p>AllowedHosts -- A list of host names allowed to be scanned.</p> <p>PolicyID -- The ID of the policy to use for the audit.</p> <p>ScanScope -- A folder restriction rule. Accepted values are <i>unrestricted</i>, <i>self</i>, <i>children</i>, and <i>ancestors</i>.</p> <p>ScopedPaths -- For use in conjunction with the ScanScope value <i>children</i>. This is a whitelist of child folders that are allowed to be scanned.</p>	

Method	URI	Path params	Request params	Description
PUT	/webinspect/scanner/<scanId>	scanId: The ID of the scan represented as a GUID.	action: The action to take on a particular scan. Currently supported actions: Stop: Stops currently running scan.  Continue: Continues a previously paused or interrupted scan.	Performs the specified action on the specified scan (i.e. stop's the scan with ID of scanId).
PUT	/webinspect/scanner/settings	None	None	Send the raw file contents in the request body.

Method	URI	Path params	Request params	Description
PUT	/webinspect/scanner/<scanId>	scanId: The ID of the scan represented as a GUID.	host: string port: number protocol: string (usually http or https) requestBase64: string (base64 encoded request data, including headers and body) responseBase64: string (base64 encoded response data, including headers and body) issues: array of objects with the following format (or null to indicate no vulnerabilities): name: string (the issue name) severity: number (0=None, 1=Low, 2=Medium, 3=High, 4=Critical) probability: number (0=None, 1=Low, 2=Possible, 3=Certain, 4=Confirmed) summary: string (report information)	Add a new session (or sessions) to the scan with an optional list of issues.

Method	URI	Path params	Request params	Description
			execution: string (report information)  fix: string (report information)  referenceInfo: string (report information)	

## Example Proxy Automation Script Using cURL

The following script is an example Proxy Server automation script.

```
#!/bin/bash
#example automation script using curl to drive webinspect's proxy
API_SCHEME="http"
API_HOST="10.10.203.20"
API_PORT="80"
API_ENDPOINT="$API_SCHEME://$API_HOST:$API_PORT/webinspect/proxy"
echo $API_ENDPOINT#Create a new proxy with a specific id on a specific port.
#Send an empty POST body and a new proxy will be created with random instance id on
first available port.
#The instance id and port are returned in the response.
curl -d "instanceId=12345&port=8123" $API_ENDPOINT

#Get a list of all running proxies.
curl $API_ENDPOINT

#Get information about a specific proxy.
curl $API_ENDPOINT/12345

#Send some traffic through the proxy (note that this is not the same endpoint as
the WIRC command server).
curl -x http://10.10.203.20:8123 http://zero.webappsecurity.com

#Send a HEAD request (-I option) to get information about proxy capture as psf
(content length is the most useful).
curl -I $API_ENDPOINT/12345.psf

#Get proxy capture as psf (WebInspect native proxy capture).
curl -o ./12345.psf $API_ENDPOINT/12345.psf

#Get proxy capture as webmacro.
curl -o ./12345.webmacro $API_ENDPOINT/12345.webmacro
```

```
#Get proxy capture as scan settings (scan setting is configured as an audit only
workflow scan using the proxy traffic as the workflow macro).
curl -o ./12345.xml $API_ENDPOINT/12345.xml

#Save the proxy as a settings file to the WI machine without needing to download it
locally.
curl -X PUT -d "action=save" $API_ENDPOINT/12345.xml

#If you want to reuse the proxy, don't do a DELETE. Instead, send PUT action=reset
and its results will be cleared out and ready for a new run.
curl -X PUT -d "action=reset" $API_ENDPOINT/12345

#Completely shutdown the proxy (the WIRC server continues to run, these commands
only affect proxy instances).
curl -X DELETE $API_ENDPOINT/12345
```

## Example Scanner Automation Script Using cURL

The following script is an example Scanner automation script.

```
#!/bin/bash
#example automation script using curl to drive webinspect's scanner
API_SCHEME="http"
API_HOST="10.10.203.20"
API_PORT="80"
API_ENDPOINT="$API_SCHEME://$API_HOST:$API_PORT/webinspect/scanner"
echo $API_ENDPOINT

#Get a list of scan setting
curl $API_ENDPOINT/settings

#Upload a settings file, it will be placed in the WebInspect settings directory as
defined by your WebInspect application setting
curl -X PUT -F "file=@/local/path/to/settings.xml" $API_ENDPOINT/settings

#Start a scan specifying a settings file to use
curl -d "settingsName=Default" $API_ENDPOINT

#Start a scan specifying a settings file to use and additional overrides. Overrides
are optional, you can use any or all or none.
#Full list of overrides (field names and values are case sensitive):
#ScanName - any string, does not need to be unique
#StartUrl - a valid, fully qualified url with scheme host and port
#(http://zero.webappsecurity.com:80)
#CrawlAuditMode - one of: CrawlOnly, AuditOnly, CrawlAndAudit
#StartOption one of: Url, Macro
#LoginMacro: name of webmacro file, this file must exist in the settings directory
on the webinspect machine
#WorkflowMacros: an array of webmacro names to be used as workflow macros, these
files must exist in the settings directory on the webinspect machine
#AllowedHosts: array of allowed hosts
#PolicyId: an integer representing the policy id
```

```
curl -d "settingsName=Default&overrides=
{\"ScanName\":\"testing\",\"StartUrl\":\"http://zero.webappsecurity.com:80\",\"Craw
lAuditMode\":\"CrawlOnly\",\"StartOption\":\"Url\",\"LoginMacro\":\"test.webmacro\"
,\"AllowedHosts\":[\"http://zero.webappsecurity.com:80\"],\"PolicyId\":1000}" $API_
ENDPOINT

#stop a running scan
curl -X PUT -d "action=stop" $API_ENDPOINT/<scan_id>

#continue a stopped scan
curl -X PUT -d "action=continue" $API_ENDPOINT/<scan_id>

#get a list of all scans
curl $API_ENDPOINT/scans

#get a list of all scans with the filter specified by "query" applied
#query is a json blob, all fields are optional
#{
# Name: <regex that will match on scan name>,
# Status: <one of: Running, NotRunning, Interrupted, Complete, Amp>,
# StartsAfter: <date>,
# EndsBefore: <date>
#}

curl -G $API_ENDPOINT/scans --data-urlencode "query=
{\\"Name\":\"zero\\\",\\\"Status\\\":\\\"Complete\\\"}"

#get status of a specific scan (returns one of
Running/NotRunning/Complete/Interrupted)
curl $API_ENDPOINT/<scan_id>?action=getcurrentstatus

#get specific scan as a WebInspect .scan file (full xml scan report)
curl $API_ENDPOINT/<scan_id>.scan

#get specific scan as .fpr file (Fortify SSC format)
curl $API_ENDPOINT/<scan_id>.fpr

#get specific scan as a WebInspect simplified export (same report as File...Export
Details..Vulnerabilities from UI)
curl $API_ENDPOINT/<scan_id>.details?detailType=Vulnerabilities

#get scan settings used for specific scan
curl $API_ENDPOINT/<scan_id>.settings
```

## WebInspect API Server Logs

If you need to troubleshoot the WebInspect API Server, you can use the Windows' Event Viewer to review the WebInspect API log.

To check the status of the server, from a browser, log on to [http\(s\)://hostname:port/webinspect](http://hostname:port/webinspect).

# About the Burp API Extension

The Burp Suite is a toolkit for performing security testing of web applications. WebInspect includes a Burp extension that allows Burp Suite users to connect WebInspect to Burp via the WebInspect API.

## Benefits of Using the Burp API Extension

Connecting WebInspect to Burp provides the following benefits:

- Create Burp issues with vulnerabilities from a WebInspect scan
  - Request vulnerabilities detected in a currently running or completed scan
  - Request vulnerabilities based on a specified criteria, such as Severity

**Note:** WebInspect check IDs and names do not map to Burp issue IDs and names.

- Select sessions in Burp and send to WebInspect

**Note:** Sessions could be selected for the following reasons:

- Locations that need to be added to WebInspect's crawl in a running scan
- New vulnerabilities that need to be added to a running scan
- New vulnerabilities that need to be added to a completed scan

- Get Scan Information from WebInspect
  - Get status of a specific scan
  - Get a list of scans available in the currently connected WebInspect database
  - Get a list of scans based on scan status (Running/Complete)

## Supported Versions

The WebInspect Burp API extension is compatible with the new Burp Extension API.

### See Also

["WebInspect API " on page 244](#)

["Using the Burp API Extension" on the next page](#)

# Using the Burp API Extension

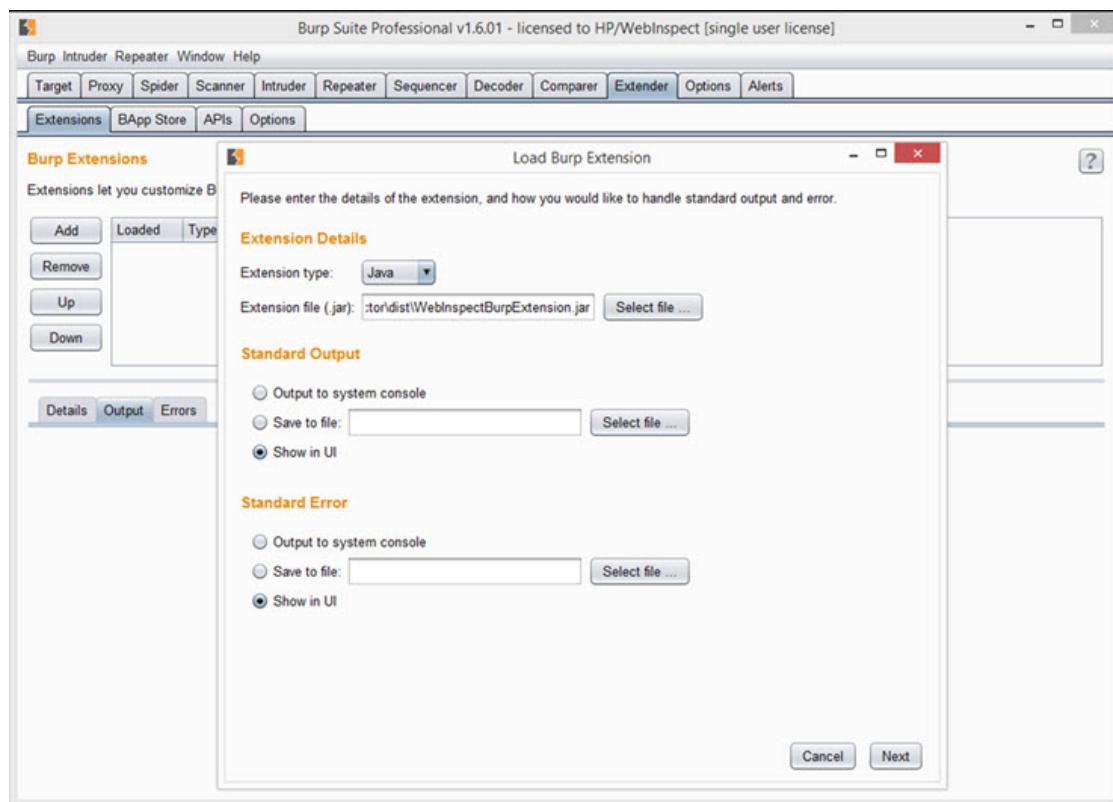
This topic describes how to set up and use the WebInspect Burp extension.

## Loading the Burp Extension

Perform the following steps in Burp to load the WebInspect Burp extension:

1. On the **Extender** tab, select **Extensions** and click **Add**.

The Load Burp Extension window appears.



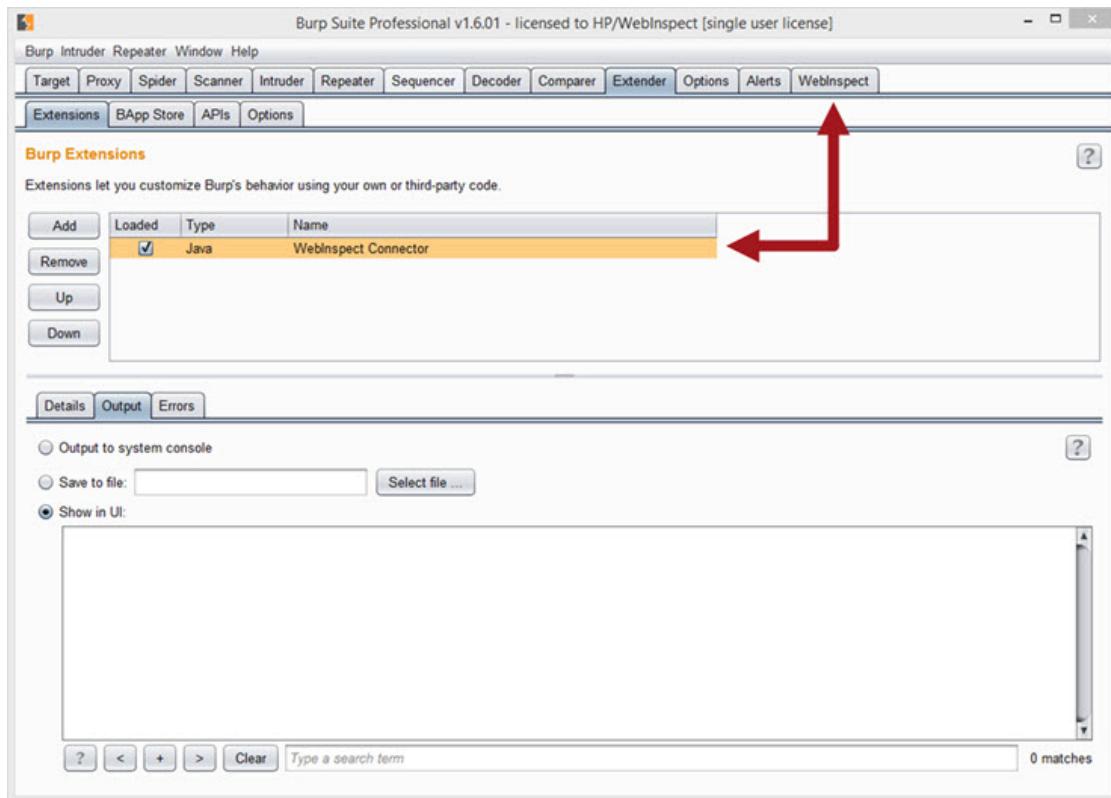
2. In the **Extension file (.jar)** field, click **Select file** and navigate to the WebInspectBurpExtension.jar file.

**Tip:** The WebInspectBurpExtension.jar file can be found in the Extensions directory in the WebInspect installation location. The default location is one of the following:

```
C:\Program Files\HP\HP WebInspect\Extensions  
C:\Program Files (x86)\HP\HP WebInspect\Extensions
```

3. Ensure that the **Show in UI** option is selected under the **Standard Output** and **Standard Error** sections.
4. Click **Next**.

WebInspect Connector appears in the list of Burp Extensions and a tab labeled "WebInspect" is added to the Burp user interface. If you do not see the WebInspect tab, then the Burp extension did not load correctly. In this case, look in the Output and Errors tabs for information that may help you to troubleshoot the issue.

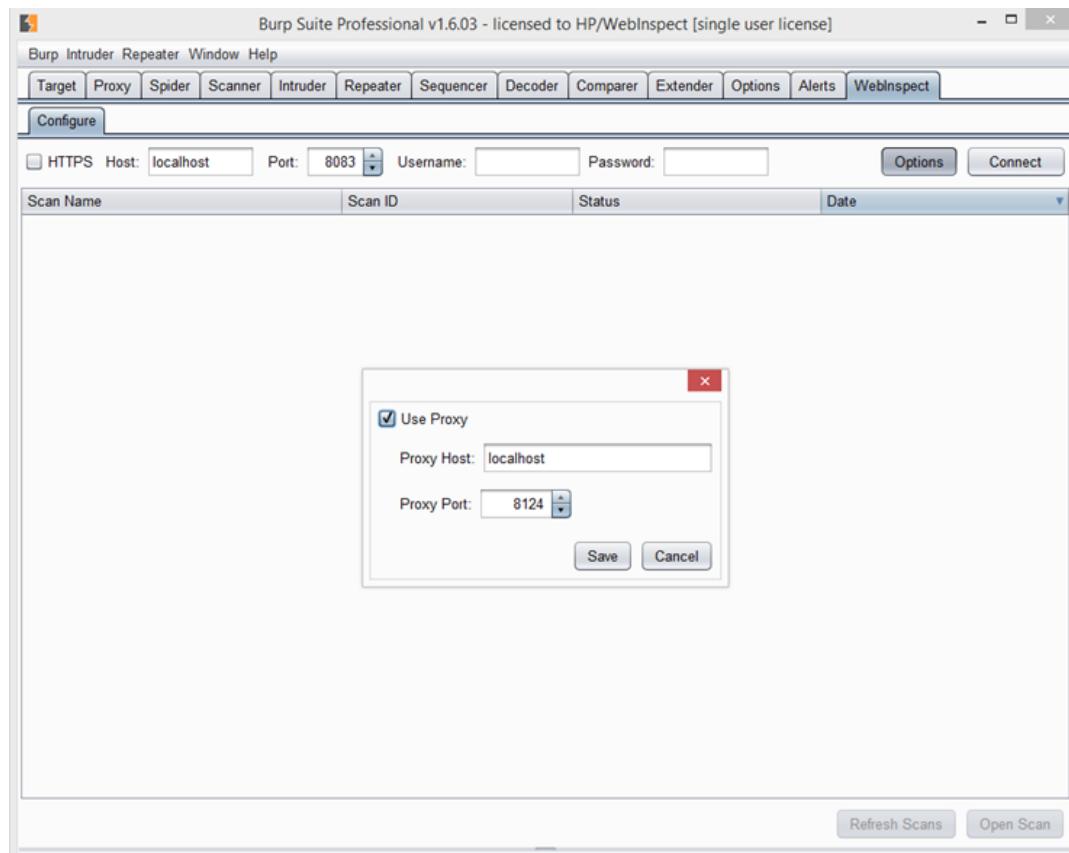


## Connecting to WebInspect

Perform the following steps in Burp to connect to WebInspect:

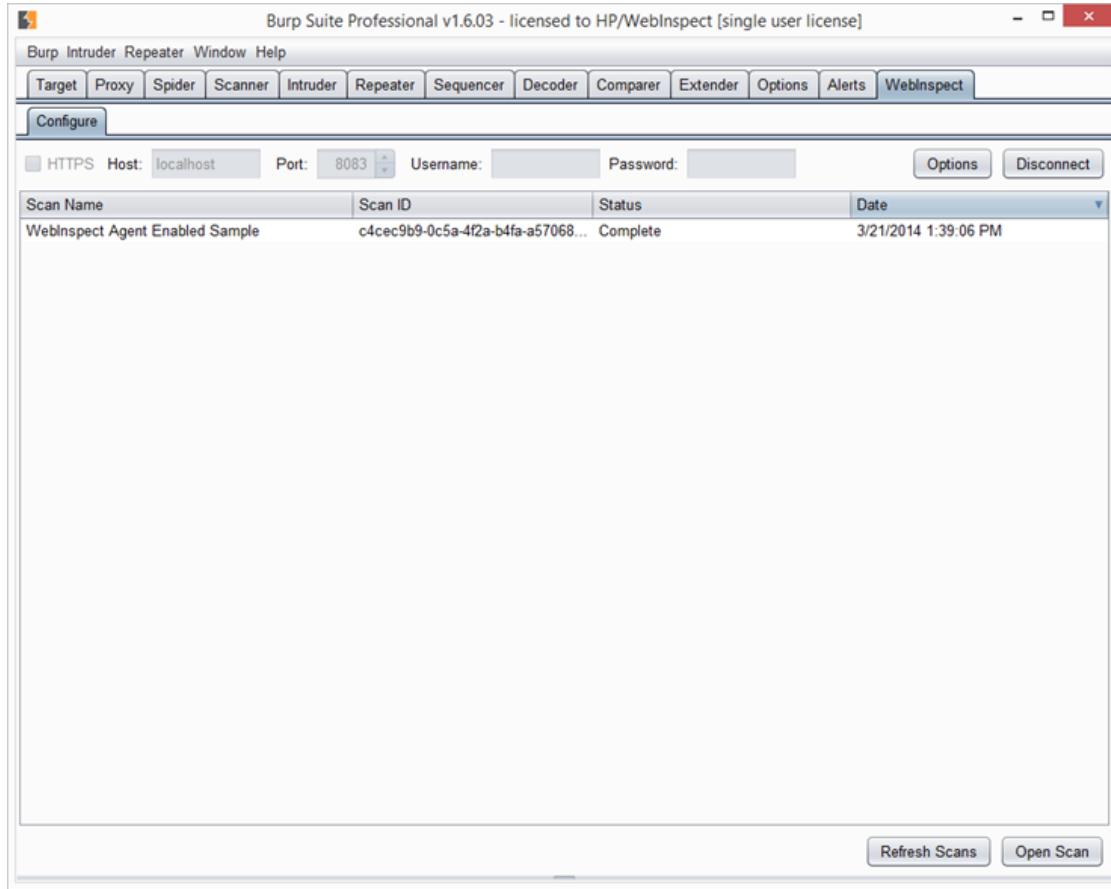
1. Ensure that the Webinspect API service is running. See [Fortify Monitor](#) for more information.
2. On the **WebInspect > Configure** tab, do the following:
  - a. If the API requires HTTPS authentication, select the **HTTPS** check box.
  - b. Type the **Host** name and **Port** number for the WebInspect API service.
  - c. If the API is configured to require authentication, type the **Username** and **Password**.
  - d. Click **Options** to configure proxy settings for the API HTTP requests.

A proxy settings window appears.



- e. Select the **Use Proxy** checkbox, and type the **Proxy Host** name and the **Proxy Port** number.
- f. Click **Save**.
3. Click **Connect**.

A list of WebInspect scans should appear in the WebInspect tab.



## Refreshing the List of Scans

To update the list of WebInspect scans, click **Refresh Scans**.

## Working with a Scan in Burp

Perform the following steps in Burp to work with a WebInspect scan:

1. Do one of the following to open a scan:
  - Double-click on a scan in the list.
  - Select a scan in the list and click **Open Scan**.

The scan opens in a new tab under the WebInspect tab, with Crawl sessions and Vulnerable sessions listed. The list of sessions is automatically sorted by Type with Vulnerabilities first followed by Crawl sessions.

The screenshot shows the Burp Suite Professional interface with the 'WebInspect' tab selected. The main window displays a table of session results for the site <http://zero.webappsecurity.com/>. The columns are Host, Method, URL, Type, Severity, and Name. The table lists numerous entries, primarily 'Vulnerability' type sessions, with severities ranging from High to Low. Some entries include descriptive names like 'Credential Management: I...', 'Transport Layer Protection...', etc. Below the table, there are tabs for 'Raw' and 'Hex', and a search bar with the placeholder 'Type a search term'. At the bottom right, there are buttons for 'Refresh Sessions', 'Resume Scan', and 'Close Tab'.

2. To re-sort on a sorted column in reverse order, click the column heading. To sort the list using different sort criteria, click the heading of the column you want to sort by. The following table provides some sort scenarios:

If you...	Then Sort By...
Have multiple hosts in the scan and want to group sessions by hosts	Host
Want to see all sessions that used a specific method	Method and scroll to the specific method you want
Want to see all sessions affecting a specific page in your Web site	URL and scroll to the specific page you want
Want to select all sessions with Critical and High severities and send them to a Burp tool	Severity and scroll to the sessions with Critical and High severities
Want to select all sessions with the same check name	Name and scroll to the specific check name you want

3. To update the list of sessions—such as when Burp is connected to a scan that is still running—click **Refresh Sessions**.
4. To view the request for a session, click the session in the list.

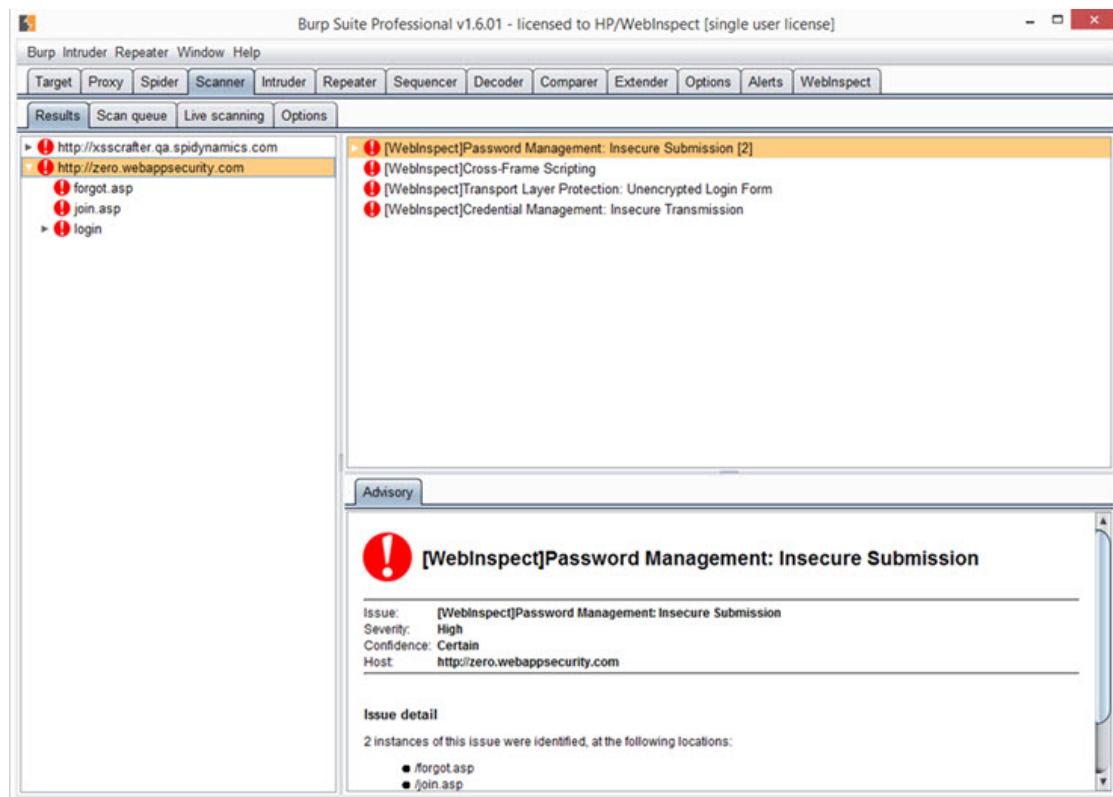
The session request information appears at the bottom of the window. Click the request to see the response.

5. To send one or more sessions to a Burp tool for further analysis, select the session(s), right-click and select the appropriate "**Send To**" option.

**Note:** Current options are Send To Spider, Send To Intruder, and Send To Repeater. For more information about Burp tools, see the Burp Suite documentation.

6. To create an issue for a Vulnerable session and add it to the Scanner tab in Burp, right-click on the session and select **Create Issue**.

The issue is populated with report data from WebInspect and the issue name is tagged with [WebInspect] to indicate that the issue was added from an external resource.



**Note:** The Create Issue option is only available in the Burp Professional Edition and is not

available for Crawl sessions.

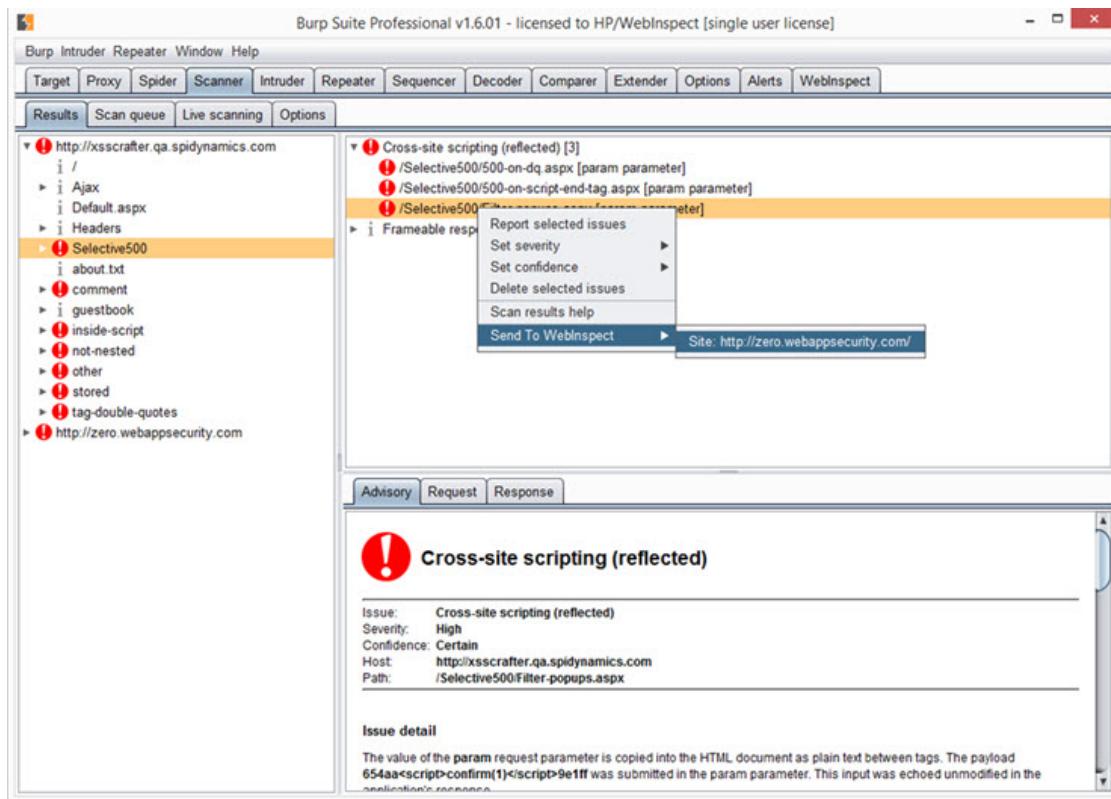
7. To continue a stopped scan, click **Resume Scan**.
8. To close the scan tab, click **Close Tab**.

## Sending Items from Burp to WebInspect

Perform the following steps in Burp to send requests/responses and issues to WebInspect to be crawled:

1. Ensure that the desired WebInspect scan is open in the **WebInspect** tab.

**Tip:** The Send To WebInspect option will not be available in the context menu if a WebInspect scan is not open in Burp.
2. Click the **Scanner** tab and then the **Results** tab.
3. To send a request/response to WebInspect to be crawled, right click the request and select **Send To WebInspect > [scan name]**.

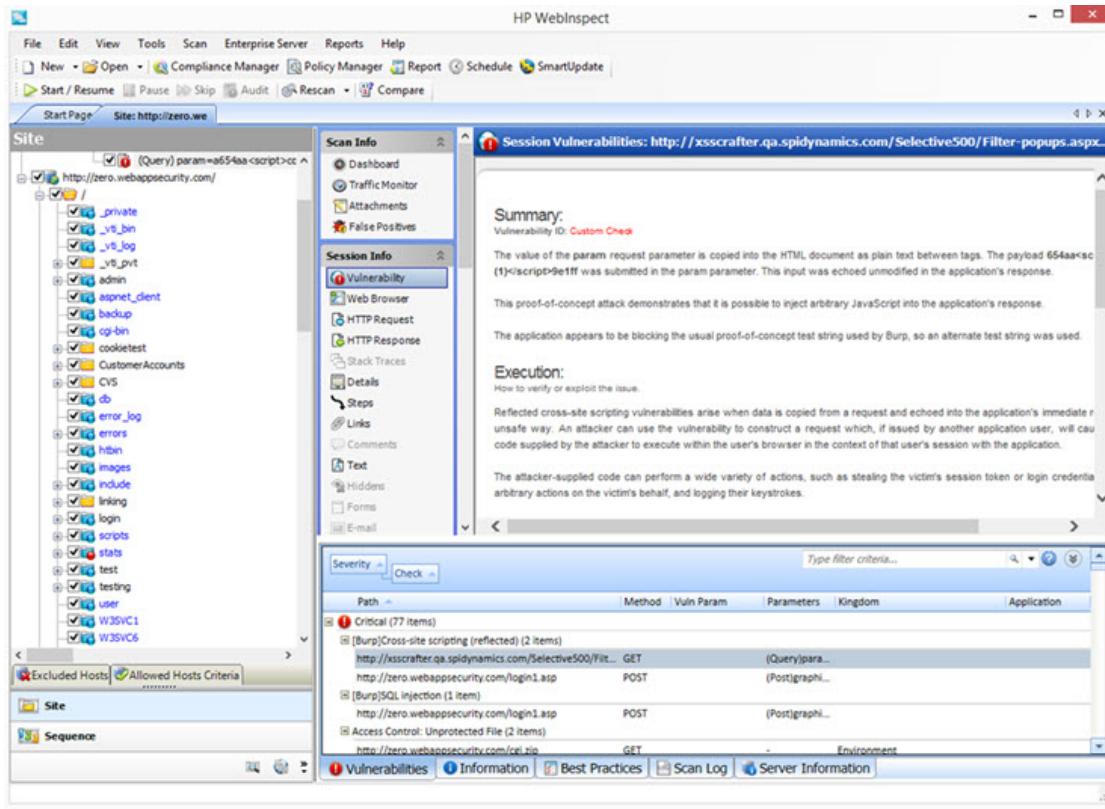


WebInspect creates a session for the request that is ready to be crawled. You can return to the scan in the **WebInspect** tab and click **Resume Scan** to crawl the session.

**Note:** Scan settings for the open scan apply to the session being sent. This may affect what WebInspect does with the session. For instance, if the open scan is for Host A and you send a session from Host B, but Host B is not in the Allowed Hosts list for the open scan, the session will be excluded and will not be crawled.

4. To send an issue to WebInspect as a manual finding, right click the issue and select **Send To WebInspect > [scan name]**.

The issue is populated with report data from Burp and the issue name is tagged with [Burp] to indicate that the issue was added from an external resource.



## See Also

["About the Burp API Extension" on page 261](#)

["WebInspect API " on page 244](#)

["Fortify Monitor " on page 90](#)

## Add Page or Directory

If you use manual inspection or other security analysis tools to detect resources that WebInspect did not discover, you can add these locations manually and assign a vulnerability to them. Incorporating the data into a WebInspect scan allows you to report and track vulnerabilities using WebInspect features.

**Note:** When creating additions to the data hierarchy, you must manually add resources in a logical sequence. For example, to create a subdirectory and page, you must create the subdirectory before creating the page.

1. Replace the default name of the page or directory with the name of the resource to be added.
2. If necessary, edit the HTTP request and response. Do not change the request path.
3. You can send a request to the resource and record the response in the session data. This will also verify the existence of the resource that was not discovered by WebInspect:
  - a. Click **HTTP Editor** to open the WebInspect HTTP Editor.
  - b. If necessary, modify the request.
  - c. Click  **Send**.
  - d. Close the HTTP Editor.
  - e. When prompted to use the modified request and response, select **Yes**.
4. (Optional) To delete all request and response modifications, click **Reset**.
5. When finished, click **OK**.

## Add Variation

If you use manual inspection or other security analysis tools to detect resources that WebInspect did not discover, you can add these locations manually and assign a vulnerability to them. Incorporating the data into a WebInspect scan allows you to report and track vulnerabilities using WebInspect features.

A variation is a subnode of a location that lists particular attributes for that location. For example, the login.asp location might have the variation:

(Post) uid=12345&Password=foo&Submit=Login

Variations, like any other location, can have vulnerabilities attached to them, as well as subnodes.

1. In the **Name** box, replace the default "attribute=value"with the actual parameters to be sent (for example, uid=9999&Password=kungfoo&Submit=Login).
2. Select either **Post** or **Query**.
3. If necessary, edit the HTTP request and response. Do not change the request path.
4. You can send a request to the resource and record the response in the session data. This will also verify the existence of the resource that was not discovered by WebInspect:
  - a. Click **HTTP Editor** to open the WebInspect HTTP Editor.
  - b. If necessary, modify the request.

- c. Click .
- d. Close the HTTP Editor.
- e. When prompted to use the modified request and response, select **Yes**.
5. (Optional) To delete all request and response modifications, click **Reset**.
6. When finished, click **OK**.

## Fortify Monitor: Configure Enterprise Server Sensor

This configuration information is used for integrating WebInspect into the WebInspect Enterprise as a sensor. After providing the information and starting the sensor service, you should conduct scans using the WebInspect Enterprise Web console, not the WebInspect graphical user interface.

Item	Description
<b>Manager URL</b>	Enter the URL or IP address of the Enterprise Server Manager.
<b>Sensor Authentication</b>	Enter a user name (formatted as domain\username) and password, then click <b>Test</b> to verify the entry.
<b>Enable Proxy</b>	If WebInspect must go through a proxy server to reach the Enterprise Server manager, select <b>Enable Proxy</b> and then provide the IP address and port number of the server. If authentication is required, enter a valid user name and password.
<b>Override Database Settings</b>	WebInspect normally stores scan data in the device you specify in the <a href="#">Application Settings for WebInspect Database</a> . However, if WebInspect is connected to WebInspect Enterprise as a sensor, you can select this option and then click <b>Configure</b> to specify an alternative device.
<b>Service Account</b>	You can log on to the sensor service using either the LocalSystem account or an account you specify.
<b>Sensor Status</b>	This area displays the current status of the Sensor Service and provides buttons allowing you to start or stop the service.

## After Configuring as a Sensor

After configuring WebInspect as a sensor, click **Start**.

## Blackout Period

When WebInspect is connected to WebInspect Enterprise, a user may attempt to conduct a scan during a blackout period, which is a block of time during which scans are not permitted by the enterprise manager. When this occurs, the following error message appears:

"Cannot start Scanner because the start URL is under the following blackout period(s)..."

You must wait until the blackout period ends before conducting the scan.

Similarly, if a scan is running when a blackout period begins, the enterprise manager will suspend the scan, place it in the pending job queue, and finish the scan when the blackout period ends. In cases where a blackout is defined for multiple IP addresses, the enterprise manager will suspend the scan only if the scan begins at one of the specified IP addresses. If the scan begins at a non-excluded IP address, but subsequently pursues a link to a host whose IP address is specified in the blackout setting, the scan will not be suspended.

## Create Exclusion

To add exclusion/rejection criteria:

1. Click **Add** (on the right side of the **Excluded or Rejected URLs and Hosts** list).  
The Create Exclusion window opens.
2. Select an item from the **Target** list.
3. If you selected Query Parameter or Post Parameter as the target, enter the **Target Name**.
4. From the **Match Type** list, select the method to be used for matching text in the target:
  - Matches Regex - Matches the regular expression you specify in the **Match String** box.
  - Matches Regex Extension - Matches a syntax available from HP's [regular expression extensions](#) you specify in the **Match String** box.
  - Matches - Matches the text string you specify in the **Match String** box.
  - Contains - Contains the text string you specify in the **Match String** box.
5. In the **Match String** box, enter the string or regular expression for which the target will be searched. Alternatively, if you selected a regular expression option in the **Match Type**, you can click the drop-down arrow and select **Create Regex** to launch the Regular Expression Editor.
6. Click .

7. (Optional) Repeat steps 2-6 to add more conditions. Multiple matches are ANDed.
8. If you are working in Current Settings, you can click **Test** to process the exclusions on the current scan. Any sessions from that scan that would have been filtered by the criteria will appear in the test screen, allowing you to modify your settings if required.
9. Click **OK**.
10. When the exclusion appears in the **Excluded or Rejected URLs or Hosts** list, select either **Reject**, **Exclude**, or both.

## Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following exclusion and select **Reject**.

Target	Target Name	Match Type	Match String
URL	N/A	contains	Microsoft.com

## Example 2

Enter "logout" as the match string. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the "logout" example, WebInspect would exclude or reject URLs such as logout.asp or applogout.jsp.

Target	Target Name	Match Type	Match String
URL	N/A	contains	logout

## Example 3

The following example rejects or excludes a session containing a query where the query parameter "username" equals "John."

Target	Target Name	Match Type	Match String
Query parameter	username	matches	John

## Example 4

The following example excludes or rejects the following directories:

<http://www.test.com/W3SVC55/>

<http://www.test.com/W3SVC5/>

<http://www.test.com/W3SVC550/>

Target	Target Name	Match Type	Match String
URL	N/A	matches regex	/W3SVC[0-9]*/

## FilesToURLs Utility

As part of the normal installation procedure, WebInspect installs two command line utilities (FilesToURLs.exe and FilesToURLs.py) designed to enhance the discovery and evaluation of all resources on your Web site. When executed on your server, the utility examines all files on the target site and creates an XML file containing a URL for each resource it detects. Then, when using the new Basic Scan Wizard, you can select the List-Driven scan method and submit this XML file to WebInspect.

**Note:** FilesToURLs.exe is for a Windows server and requires .NET Framework 2.0 or later.  
FilesToURLs.py is for a UNIX server and requires Python 2.6.

To create the XML file and include it in a scan:

1. Locate FilesToURLs.exe (or FilesToURLs.py, for UNIX systems).

**Tip:** The default location is C:\Program Files\HP\HP WebInspect\ .

2. Using a network share (or after copying the file to your Web server) run the utility, according to the usage described below.
3. Launch WebInspect.
4. On Step 1 of the Scan Wizard, select **List-Driven Scan**.
5. Click the Browse button and select the XML file generated by the FilesToURLs utility.

6. Complete the wizard and start the scan.

WebInspect will crawl your site in the normal fashion and then crawl each listed URL.

## Usage for FilesToURLs.exe

The FilesToURLs.exe syntax is similar to the following:

```
FilesToURLs.exe /docroot c:\docroot /outfile outfile.xml [/include filename.xml] [/hostname example.com] [/baseurl baseurl] [/port port] [/secure] [/?] [/help]
```

The following table describes the arguments that can be used with FilesToURLs.exe.

Argument	Description
/docroot	The local path where web files are stored (required).
/outfile	The name of the XML file to be created (required).
/include	An existing file whose contents should be included in the output.
/hostname	The hostname from which files are served (default: local hostname).
/baseurl	The base URL from which files are served (default: / ).
/port	The port that the web server is listening in (default: 80 or 443).
/secure	Specifies that the port is using SSL.

## Usage for FilesToURLs.py

The following table describes the FilesToURLs.py [options].

Option	Description
-h, --help	Show help message and exit.
-d DOCROOT, --docroot=DOCROOT	Apache's DocumentRoot or other directory from which files are served.
-o FILE, --outfile=FILE	Write output to FILE (defaults to STDOUT).
-i FILE, --include=FILE	Include the contents of FILE in the output.
-n HOSTNAME, --hostname=HOSTNAME	Hostname of the web server (defaults to local hostname).
-b BASEURL, --baseurl=BASEURL	Base URL from which files are served (defaults to / ).

Option	Description
-p PORT, --port=PORT	Port that service is listening on (defaults to 80 or 443).
-s, --secure	Specifies that the listening port is using SSL (defaults to False).

## List-Driven Scan

The List-Driven Scan option can also use a manually created plain text file instead of the XML file generated by the FilesToURLs utility. List one URL per line. Each URL must be fully qualified and must include the protocol (for example, http:// or https://).

# Default Scan Settings

Use Default Settings to establish scanning parameters for your scan actions. WebInspect will use these options unless you specify alternatives while initiating a scan (using the options available through the Scan Wizard or by accessing Current Settings).

## See Also

["Crawl Settings" on page 325](#)

["Audit Settings" on page 330](#)

## Scan Settings: Method

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Method**.

## Scan Mode

The following options are available:

Option	Description
Crawl Only	This option completely maps a site's tree structure. After a crawl has been completed, you can click <b>Audit</b> to assess an application's vulnerabilities.
Crawl and Audit	As WebInspect maps the site's hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content may possibly change before the crawl can be completed. This is described in the Default Settings <a href="#">Crawl and Audit Mode</a> option called "Simultaneously."
Audit Only	WebInspect applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.
Manual  (Not available for Guided Scan)	Manual mode allows you to navigate manually to whatever sections of your application you choose to visit. It does not crawl the entire site, but records information only about those resources that you encounter while manually navigating the site. This feature is used most often to enter a site through a Web form logon page or to define a discrete subset or portion of the application that you want to investigate. After you finish navigating through the site, you can audit the results to assess the security vulnerabilities related to that portion of the site that you recorded.

## Crawl and Audit Mode

The following options are available:

Option	Description
Simultaneously	As WebInspect maps the site's hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content may possibly change before the crawl can be completed.
Sequentially	<p>In this mode, WebInspect crawls the entire site, mapping the site's hierarchical data structure, and then conducts a sequential audit, beginning at the site's root.</p> <p>If you select <b>Sequentially</b>, you can specify the order in which the crawl and audit should be conducted:</p> <ul style="list-style-type: none"> <li>• <b>Test each engine type per session (engine driven):</b> WebInspect audits all sessions using the first audit engine, then audits all sessions using the second audit engine, continuing in sequence until all engine types have been deployed.</li> <li>• <b>Test each session per engine type (session driven):</b> WebInspect runs all audit engines against the first session, then runs all audit engines against the second session, continuing in sequence until all sessions are audited.</li> </ul>

## Crawl and Audit Details

The following options are available:

Option	Description
Include search probes (send search attacks)	If you select this option, WebInspect will send requests for files and directories that might or might not exist on the server, even if those files are not found by crawling the site. This option is selected by default only when the Scan Mode is set to Crawl & Audit. The option is cleared(unchecked) by default when the Scan Mode is set to Crawl Only or Audit Only.
Crawl links on File Not Found responses	If you select this option, WebInspect will look for and crawl links on responses that are marked as "file not found." This option is selected by default when the Scan Mode is set to Crawl Only or Crawl & Audit. The option is not available when the Scan Mode is set to Audit Only.

## Navigation

The following options are available:

Option	Description
Auto-fill Web forms during crawl	<p>If you select this option, WebInspect submits values for input controls found on all forms. The values are extracted from a file you create using the Web form editor. Use the browse button to specify the file containing the values you want to use. Alternatively, you can select the <b>Edit</b> button (to modify the currently selected file) or the <b>Create</b> button (to create a Web form file).</p> <p><b>Caution:</b> Do not rely on this feature for authentication. If the crawler and the auditor are configured to share state, and if WebInspect never inadvertently logs out of the site, then using values extracted by the Web Form Editor for a login form may work. However, if the audit or the crawl triggers a logout after the initial login, then WebInspect will not be able to log in again and the auditing will be unauthenticated. To prevent WebInspect from terminating prematurely if it inadvertently logs out of your application, go to Scan Settings - Authentication and select <a href="#">Use a login macro for forms authentication</a>.</p>
Prompt for Web form values	<p>If you select this option, WebInspect pauses the scan when it encounters an HTTP or JavaScript form and displays a window that allows you to enter values for input controls within the form. However, if you also select <b>Only prompt for tagged inputs</b>, WebInspect will not pause for user input unless a specific input control has been designated <b>Mark as Interactive Input</b> (using the <a href="#">Web Form Editor</a>). This pausing for input is termed "interactive mode" and you can cancel it at any time during the scan.</p>
Use Web Service Design	<p>This option applies only to Web Service scans.</p> <p>When performing a Web service scan, WebInspect crawls the WSDL site and submits a value for each parameter in each operation. These values are contained in a file that you create using the Web Service Test Designer tool. WebInspect then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection.</p> <p>Use the browse button to specify the file containing the values you want to use. Alternatively, you can select the <b>Edit</b> button (to modify the currently selected file) or the <b>Create</b> button (to create a SOAP values file).</p>

## SSL/TLS Protocols

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols provide secure HTTP (HTTPS) connections for Internet transactions between Web browsers and Web servers. SSL/TLS protocols enable server authentication, client authentication, data encryption, and data integrity for Web applications.

Select the SSL/TLS protocol(s) used by your Web server. The following options are available:

- Use SSL 2.0
- Use SSL 3.0
- Use TLS 1.0
- Use TLS 1.1
- Use TLS 1.2

If you do not configure the SSL/TLS protocol to match your Web server, WebInspect will still connect to the site, though there may be a performance impact.

For example, if the setting in WebInspect is configured to Use SSL 3.0 only, but the Web server is configured to accept TLS 1.2 connections only, WebInspect will first try to connect with SSL 3.0, but will fail. WebInspect will then implement each protocol until it discovers that TLS 1.2 is supported. The connection will then succeed, although more time will have been spent in the effort. The correct setting (Use TLS 1.2) in WebInspect would have succeeded on the first try.

### See Also

- ["Scan Settings: Allowed Hosts" on page 298](#)
- ["Scan Settings: Authentication" on page 315](#)
- ["Scan Settings: Content Analyzers" on page 287](#)
- ["Scan Settings: Cookies/Headers " on page 310](#)
- ["Scan Settings: Custom Parameters" on page 305](#)
- ["Scan Settings: File Not Found " on page 320](#)
- ["Scan Settings: Filters" on page 308](#)
- ["Scan Settings: General" on the next page](#)
- ["Scan Settings: HTTP Parsing " on page 300](#)
- ["Scan Settings: Policy " on page 322](#)
- ["Scan Settings: Proxy " on page 312](#)
- ["Scan Settings: Requestor" on page 289](#)
- ["Scan Settings: Session Exclusions" on page 294](#)

["Scan Settings: Session Storage " on page 292](#)

## Scan Settings: General

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **General**.

### Scan Details

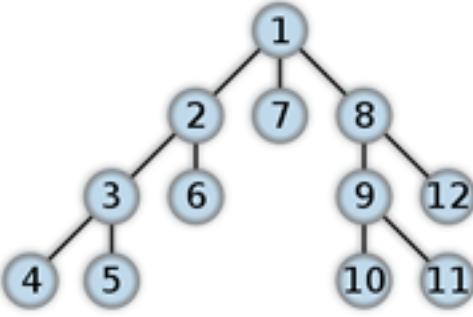
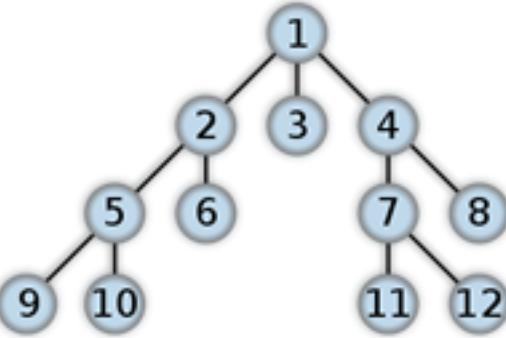
The Scan Details options are described in the following table:

Option	Description
Enable Path Truncation	<p>Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. WebInspect truncates paths, looking for directory listings or unusual errors within each truncation.</p> <p><b>Example:</b> If a link consists of  <a href="http://www.site.com/folder1/folder2/file.asp">http://www.site.com/folder1/folder2/file.asp</a>, then truncating the path to look for <a href="http://www.site.com/folder1/folder2/">http://www.site.com/folder1/folder2/</a> and  <a href="http://www.site.com/folder1/">http://www.site.com/folder1/</a> may cause the server to reveal directory contents or may cause unhandled exceptions.</p>
Case-sensitive request and response handling	Select this option if the server at the target site is case-sensitive to URLs.
Recalculate correlation data	This option is used only for comparing scans. The setting should be changed only upon the advice of HP Support personnel.
Compress response data	If you select this option, WebInspect saves disk space by storing each HTTP response in a compressed format in the database.
Enable Traffic Monitor Logging	During a Basic Scan, WebInspect displays in the navigation pane only those sessions that reveal the hierarchical structure of the Web site plus those sessions in which a vulnerability was discovered. However, if you select the Traffic Monitor option, WebInspect adds the <b>Traffic Monitor</b> button to the Scan Info panel (as shown below), allowing you to display and review every single HTTP request sent by WebInspect and the associated HTTP response received from the server.
Encrypt Traffic Monitor File	<p>All sessions are normally recorded in the traffic monitor file as clear text. If you are concerned about storing sensitive information such as passwords on your computer, you can elect to encrypt the file.</p> <p>Encrypted files cannot be compressed. Selecting this option will significantly increase the size of exported scans containing log files.</p>

Option	Description
Maximum crawl-audit recursion depth	When an attack reveals a vulnerability, WebInspect crawls that session and follows any link that may be revealed. If that crawl and audit reveals a link to yet another resource, the depth level is incremented and the discovered resource is crawled and audited. This process can be repeated until no other links are found. However, to avoid the possibility of entering an endless loop, you may limit the number of recursions. The default value is 2. The maximum recursion level is 1,000.

## Crawl Details

The Crawl Details options are described in the following table:

Option	Description
Crawler	<p>WebInspect can crawl a site in two different ways, depending on which option you select.</p> <p><b>Depth-First Tree</b></p> <p>Depth-first crawling accommodates sites that enforce order-dependent navigation (where the browser must visit page A before it can visit page B). This type of search progresses by expanding the first child node (link) and crawling deeper and deeper until it reaches a node that has no children. The search then backtracks, returning to the most recent node it hasn't finished exploring and drilling down from there. The following illustration depicts the order in which linked pages are accessed using a depth-first crawl. Node 1 has links to nodes 2, 7, and 8. Node 2 has links to nodes 3 and 6.</p>  <pre> graph TD     1((1)) --- 2((2))     1 --- 7((7))     1 --- 8((8))     2 --- 3((3))     2 --- 6((6))     8 --- 9((9))     8 --- 10((10))     8 --- 11((11))     9 --- 10     9 --- 11   </pre> <p><b>Breadth-First Tree</b></p> <p>By contrast, breadth-first crawling begins at the root node and explores all the neighboring nodes (one level down). Then for each of those nearest nodes, it explores their unexplored neighbor nodes, and so on, until all resources are identified. The following illustration depicts the order in which linked pages are accessed using a breadth-first crawl. Node 1 has links to nodes 2, 3, and 4. Node 2 has links to nodes 5 and 6.</p>  <pre> graph TD     1((1)) --- 2((2))     1 --- 3((3))     1 --- 4((4))     2 --- 5((5))     2 --- 6((6))     4 --- 7((7))     4 --- 8((8))     4 --- 11((11))     4 --- 12((12))     9 --- 10((10))   </pre>

Option	Description
Enable keyword search audit	A keyword search, as its name implies, uses an attack engine that examines server responses and searches for certain text strings that typically indicate a vulnerability. Normally, this engine is not used during a crawl-only scan, but you can enable it by selecting this option.
Perform redundant page detection	Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, WebInspect would never be able to finish the scan. This option, however, allows WebInspect to identify and exclude processing of redundant resources.
Limit maximum single URL hits to	Sometimes, the configuration of a site will cause a crawl to loop endlessly through the same URL. Use this field to limit the number of times a single URL will be crawled. The default value is 5.
Include parameters in hit count	<p>If you select <b>Limit maximum single URL hits to</b> (above), a counter is incremented each time the same URL is encountered. However, if you also select <b>Include parameters in hit count</b>, then when parameters are appended to the URL specified in the HTTP request, the crawler will crawl that resource up to the single URL limit. Any differing set of parameters is treated as unique and has a separate count.</p> <p>For example, if this option is selected, then "page.aspx?a=1" and "page.aspx?b=1" will both be counted as unique resources (meaning that the crawler has found two pages).</p> <p>If this option is not selected, then "page1.aspx?a=1" and "page.aspx?b=1" will be treated as the same resource (meaning that the crawler has found the same page twice).</p>
Limit maximum link traversal sequence to	<p>This option restricts the number of hyperlinks that can be sequentially accessed as WebInspect crawls the site. For example, if five resources are linked as follows</p> <ul style="list-style-type: none"> <li>• Page A contains a hyperlink to Page B</li> <li>• Page B contains a hyperlink to Page C</li> <li>• Page C contains a hyperlink to Page D</li> <li>• Page D contains a hyperlink to Page E</li> </ul> <p>and if this option is set to "3," then Page E will not be crawled. The default value is 15.</p>

Option	Description
Limit maximum crawl folder depth to	<p>This option limits the number of directories that may be included in a single request. The default value is 15.</p> <p>For example, if the URL is</p> <p><code>http://www.mysite.com/Dir1/Dir2/Dir3/Dir4/Dir5/Dir6/Dir7</code></p> <p>and this option is set to "4," then the contents of directories 5, 6, and 7 will not be crawled.</p>
Limit maximum crawl count to	<p>This feature restricts the number of HTTP requests sent by the crawler and should be used only if you experience problems completing a scan of a large site.</p>
Limit maximum Web form submission to	<p>Normally, when WebInspect encounters a form that contains controls having multiple options (such as a list box), it extracts the first option value from the list and submits the form; it then extracts the second option value and resubmits the form, repeating this process until all option values in the list have been submitted. This ensures that all possible links will be followed.</p> <p>There are occasions, however, when submitting the complete list of values would be counterproductive. For example, if a list box named "State" contains one value for each of the 50 states in the United States, there is probably no need to submit 50 instances of the form.</p> <p>Use this setting to limit the total number of submissions that WebInspect will perform. The default value is 3.</p>

## Audit Details

If you select a depth-first crawl, you can also elect to retrace the crawl path for each parameter attack, as opposed to applying all attacks as the crawl progresses. This considerably increases the time required to conduct a scan.

### See Also

- ["Scan Settings: Allowed Hosts" on page 298](#)
- ["Scan Settings: Authentication" on page 315](#)
- ["Scan Settings: Content Analyzers" on the next page](#)
- ["Scan Settings: Cookies/Headers" on page 310](#)
- ["Scan Settings: Custom Parameters" on page 305](#)
- ["Scan Settings: File Not Found" on page 320](#)
- ["Scan Settings: Filters" on page 308](#)
- ["Scan Settings: HTTP Parsing" on page 300](#)

- "Scan Settings: Method " on page 278
- "Scan Settings: Policy " on page 322
- "Scan Settings: Proxy " on page 312
- "Scan Settings: Requestor" on page 289
- "Scan Settings: Session Exclusions" on page 294
- "Scan Settings: Session Storage " on page 292

## Scan Settings: Content Analyzers

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Content Analyzers**.

### Flash

If you enable the Flash analyzer, WebInspect analyzes Flash files, Adobe's vector graphics-based resizable animation format.

### JavaScript/VBScript

The JavaScript/VBScript analyzer is always enabled. It allows WebInspect to crawl links defined by JavaScript or VisualBasic script, and to create and audit any documents rendered by JavaScript.

**Tip:** To increase the speed at which WebInspect conducts a crawl while analyzing script, change your browser options so that images/pictures are not displayed.

Configure the settings in the lower pane of the window, as described below.

Option	Description
Crawl links found from script execution	If you select this option, the crawler will follow dynamic links (i.e., links generated during JavaScript execution).

Option	Description
Reject script include file requests to offsite hosts	<p>Pages downloaded from a server may contain scripts that retrieve files and dynamically render their content. An example JavaScript "include file" request is:</p> <pre data-bbox="535 418 1155 481">&lt;script type="text/javascript" src="www.badsite.com/yourfile.htm"&gt;&lt;/script&gt;</pre> <p>WebInspect will download and parse such files, regardless of their origin or file type, unless you select the Reject Script option. It will then download the files only if permitted by the parameters normally governing file handling (such as session and attack exclusions, allowed hosts, etc.).</p>
Create script event sessions	WebInspect creates and saves a session for each change to the Document Object Model (DOM).
Verbose script parser debug logging	If you select this setting AND if the <a href="#">Application setting for logging level</a> is set to Debug, WebInspect logs every method called on the DOM object. This can easily create several gigabytes of data for medium and large sites.
Log JavaScript errors	WebInspect logs JavaScript parsing errors from the script parsing engine.
Enable JS Framework UI Exclusions	With this option selected, the WebInspect JavaScript parser ignores common JQuery and Ext JS user interface components, such as a calendar control or a ribbon bar. These items are then excluded from JavaScript execution during the scan.
Max script events per page	Certain scripts endlessly execute the same events. You can limit the number of events allowed on a single page to a value between 1 and 9999. The default value is 1000.
Enable classic script engine	The script engine first provided in WebInspect 10.00 operates more like a browser and supports more web applications than did the script engine used in previous WebInspect versions. You can select this option to use the previous script engine instead.
Enable Advanced JS Framework Support	When this option is selected, WebInspect can recognize certain JavaScript frameworks and more intelligently execute script by recognizing patterns that these frameworks use. This option is available only for the new script engine of WebInspect 10.0 and is disabled if you select the Enable classic script engine option.
Enable Site-Wide Event Reduction	When this option is selected, the crawler and JavaScript engine recognize common functional areas that appear among different parts of the website, such as common menus or page footers. This eliminates the need to find within HTML content the dynamic links and forms that have already been crawled, resulting in quicker scans. This option is enabled by default and should not normally be disabled.

## Silverlight

If you enable the Silverlight analyzer, WebInspect analyzes Silverlight applications, which provide functionalities similar to those in Adobe Flash, integrating multimedia, graphics, animations and interactivity into a single runtime environment.

### See Also

- ["Scan Settings: Allowed Hosts" on page 298](#)
- ["Scan Settings: Authentication" on page 315](#)
- ["Scan Settings: Cookies/Headers " on page 310](#)
- ["Scan Settings: File Not Found " on page 320](#)
- ["Scan Settings: Filters" on page 308](#)
- ["Scan Settings: General" on page 282](#)
- ["Scan Settings: HTTP Parsing " on page 300](#)
- ["Scan Settings: Method " on page 278](#)
- ["Scan Settings: Policy " on page 322](#)
- ["Scan Settings: Proxy " on page 312](#)
- ["Scan Settings: Requestor" below](#)
- ["Scan Settings: Session Exclusions" on page 294](#)
- ["Scan Settings: Session Storage " on page 292](#)

## Scan Settings: Requestor

A requestor is the software module that handles HTTP requests and responses.

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Requestor**.

## Requestor Performance

The following options are available:

Option	Description
Use a shared requestor	<p>If you select this option, the crawler and the auditor use a common requestor when scanning a site, and each thread uses the same state, which is also shared by both modules. This replicates the technique used by previous versions of WebInspect and is suitable for use when maintaining state is not a significant consideration. You also specify the maximum number of threads (up to 75).</p>
Use separate requestors	<p>If you select this option, the crawler and auditor use separate requestors. Also, the auditor's requestor associates a state with each thread, rather than having all threads use the same state. This method results in significantly faster scans.</p> <p>When performing crawl and audit, you can specify the maximum number of threads that can be created for each requestor. The <b>Crawl requestor thread count</b> can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the default setting is 5. The <b>Audit requestor thread count</b> can be set to a maximum of 50; the default setting is 10. Increasing the thread counts may increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.</p> <p><b>Note:</b> Depending on the capacity of the application being scanned, increasing thread counts may increase request failures due to increased load on the server, causing some responses to exceed the <b>Request timeout</b> setting. Request failures may reduce scan coverage because the responses that failed may have exposed additional attack surface or revealed vulnerabilities. If you notice increased request failures, you might reduce them by either increasing the <b>Request timeout</b> or reducing the <b>Crawl requestor thread count</b> and <b>Audit requestor thread count</b>.</p> <p>Also, depending on the nature of the application being scanned, increased crawl thread counts may reduce consistency between subsequent scans of the same site due to differences in crawl request ordering. By reducing the default <b>Crawl requestor thread count</b> setting to 1, consistency may be increased.</p>

## Requestor Settings

The following options are available:

Option	Description
Limit maximum response size to	Select this option to limit the size of accepted server responses, and then specify the maximum size (in kilobytes). The default is 1000 kilobytes. Note that Flash files (.swf) and JavaScript "include" files are not subject to this limitation.
Request retry count	Specify how many times WebInspect will resubmit an HTTP request after receiving a "failed" response (which is defined as any socket error or request timeout). The value must be greater than zero.
Request timeout	Specify how long WebInspect will wait for an HTTP response from the server. If this threshold is exceeded, WebInspect resubmits the request until reaching the retry count. If it then receives no response, WebInspect logs the timeout and issues the first HTTP request in the next attack series. The default value is 20 seconds.

## Stop Scan if Loss of Connectivity Detected

There may be occasions during a scan when a Web server fails or becomes too busy to respond in a timely manner. You can instruct WebInspect to terminate a scan by specifying a threshold for the number of timeouts.

**Note:** If these options are selected and the **Request timeout** setting (above) is reached, the scan may stop when the server does not respond within the period set for the Request timeout. The first time a timeout occurs, WebInspect will extend the timeout period to confirm that the server is unresponsive. If the server responds within the extended Request timeout period, then the extended period becomes the new Request timeout for the current scan.

The following options are available:

Option	Description
Consecutive "single host" retry failures to stop scan	Enter the number of consecutive timeouts permitted from one specific server. The default value is 75.
Consecutive "any host" retry failures to stop scan	Enter the total number of consecutive timeouts permitted from all hosts. The default value is 150.
Nonconsecutive "single host" retry failures to stop scan	Enter the total number of nonconsecutive timeouts permitted from a single host. The default value is "unlimited."
Nonconsecutive "any host" request failures to stop scan	Enter the total number of nonconsecutive timeouts permitted from all hosts. The default value is 350.

Option	Description
If first request fails, stop scan	Selecting this option will force WebInspect to terminate the scan if the target server does not respond to WebInspect's first request.
Response codes to stop scan if received	Enter the HTTP status codes that, if received, will force WebInspect to terminate the scan. Use a comma to separate entries; use a hyphen to specify an inclusive range of codes.

## See Also

- ["Scan Settings: Allowed Hosts" on page 298](#)
- ["Scan Settings: Authentication" on page 315](#)
- ["Scan Settings: Content Analyzers" on page 287](#)
- ["Scan Settings: Cookies/Headers " on page 310](#)
- ["Scan Settings: Custom Parameters" on page 305](#)
- ["Scan Settings: File Not Found " on page 320](#)
- ["Scan Settings: Filters" on page 308](#)
- ["Scan Settings: General" on page 282](#)
- ["Scan Settings: HTTP Parsing " on page 300](#)
- ["Scan Settings: Method " on page 278](#)
- ["Scan Settings: Policy " on page 322](#)
- ["Scan Settings: Proxy " on page 312](#)
- ["Scan Settings: Session Exclusions" on page 294](#)
- ["Scan Settings: Session Storage " below](#)

## Scan Settings: Session Storage

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Session Storage**.

## Log Rejected Session to Database

You can specify which rejected sessions should be saved to the WebInspect database. This saved information can be used for two purposes.

- If you pause a scan, change any of the settings associated with the Reject Reasons in this panel, and then resume the scan, WebInspect retrieves the saved data and sends HTTP requests that previously were suppressed.
- Hewlett-Packard support personnel can extract the generated (but not sent) HTTP requests for analysis.

Sessions may be rejected for the reasons cited in the following table:

Reject Reason	Explanation
Invalid Host	Any host that is not specified in Default (or Current) Scan Settings/Scan Settings/Allowed Hosts.
Excluded File Extension	Files having an extension that is excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded or Rejected File Extensions; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded or Rejected File Extensions; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded or Rejected File Extensions.
Excluded URL	URLs or hosts that are excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded or Rejected URLs and Hosts; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded or Rejected URLs and Hosts; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded or Rejected URLs and Hosts.
Outside Root URL	If the <b>Restrict to Folder</b> option is selected when starting a scan, any resource not qualified by the available options (Directory Only, Directory and Subdirectories, or Directory and Parent Directories).
Maximum Folder Depth Exceeded	HTTP requests were not sent because the value specified by the <b>Limit maximum crawl folder depth to</b> option in Default (or Current) Scan Settings/Scan Settings/General has been exceeded.
Maximum URL Hits	HTTP requests were not sent because the value specified by the <b>Limit Maximum Single URL hits to</b> option in Default (or Current) Scan Settings/Scan Settings/General has been exceeded.
404 Response Code	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option <b>Determine File Not Found (FNF) using HTTP response codes</b> is selected and the response contains a code that matches the requirements.
Solicited File Not Found	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option <b>Auto detect FNF page</b> is selected and WebInspect determined that the response constituted a "file not found" condition.

Reject Reason	Explanation
Custom File Not Found	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option <b>Determine FNF from custom supplied signature</b> is selected and the response contains one of the specified phrases.
Rejected Response	Files having a MIME type that is excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded MIME Types; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded MIME Types; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded MIME Types.

## Session Storage

WebInspect normally saves only those attack sessions in which a vulnerability was discovered. To save all attack sessions, select **Save non-vulnerable attack sessions**.

### See Also

- ["Scan Settings: Allowed Hosts" on page 298](#)
- ["Scan Settings: Authentication" on page 315](#)
- ["Scan Settings: Content Analyzers" on page 287](#)
- ["Scan Settings: Cookies/Headers " on page 310](#)
- ["Scan Settings: Custom Parameters" on page 305](#)
- ["Scan Settings: File Not Found " on page 320](#)
- ["Scan Settings: Filters" on page 308](#)
- ["Scan Settings: General" on page 282](#)
- ["Scan Settings: HTTP Parsing " on page 300](#)
- ["Scan Settings: Method " on page 278](#)
- ["Scan Settings: Policy " on page 322](#)
- ["Scan Settings: Proxy " on page 312](#)
- ["Scan Settings: Requestor" on page 289](#)
- ["Scan Settings: Session Exclusions" below](#)

## Scan Settings: Session Exclusions

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Session Exclusions**.

These settings apply to both the crawl and audit phases of a WebInspect vulnerability scan. To specify exclusions for only the crawl or only the audit, use the [Crawl Settings: Session Exclusions](#) or the [Audit Settings: Session Exclusions](#).

## Excluded or Rejected File Extensions

You can identify a file type and then specify whether you want to exclude or reject it.

- **Reject** - WebInspect will not request files of the type you specify.
- **Exclude** - WebInspect will request the files, but will not attack them (during an audit) and will not examine them for links to other resources.

By default, most image, drawing, media, audio, video, and compressed file types are rejected.

Follow the steps below to add a file extension:

1. Click **Add**.

The Exclusion Extension window opens.

2. In the **File Extension** box, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **OK**.

## Excluded MIME Types

WebInspect will not process files associated with the MIME type you specify. By default, image, audio, and video types are excluded.

Follow the steps below to add a MIME Type:

1. Click **Add**.

The Provide a Mime-type to Exclude window opens.

2. In the **Exclude Mime-type** box, enter a MIME type.
3. Click **OK**.

## Other Exclusion/Rejection Criteria

You can identify various components of an HTTP message and then specify whether you want to exclude or reject a session that contains that component.

- **Reject** - WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude** - During a crawl, WebInspect will not examine the specified URL or host for links to other resources. During the audit portion of the scan, WebInspect will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

## Editing Criteria

To edit the default criteria:

1. Select a criterion and click **Edit** (on the right side of the **Other Exclusion/Rejection Criteria** list).  
The Reject or Exclude a Host or URL window opens.
2. Select either **Host or URL**.
3. In the **Host/URL** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select either **Reject**, **Exclude**, or both.
5. Click **OK**.

## Adding Criteria

To add exclusion/rejection criteria:

1. Click **Add** (on the right side of the **Excluded or Rejected URLs and Hosts** list).  
The Create Exclusion window opens.
2. Select an item from the **Target** list.
3. If you selected Query Parameter or Post Parameter as the target, enter the **Target Name**.
4. From the **Match Type** list, select the method to be used for matching text in the target:
  - Matches Regex - Matches the regular expression you specify in the **Match String** box.
  - Matches Regex Extension - Matches a syntax available from HP's [regular expression extensions](#) you specify in the **Match String** box.

- Matches - Matches the text string you specify in the **Match String** box.
  - Contains - Contains the text string you specify in the **Match String** box.
5. In the **Match String** box, enter the string or regular expression for which the target will be searched. Alternatively, if you selected a regular expression option in the **Match Type**, you can click the drop-down arrow and select **Create Regex** to launch the Regular Expression Editor.
6. Click  (or press Enter).
7. (Optional) Repeat steps 2-6 to add more conditions. Multiple matches are ANDed.
8. If you are working in Current Settings, you can click **Test** to process the exclusions on the current scan. Any sessions from that scan that would have been filtered by the criteria will appear in the test screen, allowing you to modify your settings if required.
9. Click **OK**.
10. When the exclusion appears in the **Excluded or Rejected URLs or Hosts** list, select either **Reject**, **Exclude**, or both.

### Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following exclusion and select **Reject**.

Target	Target Name	Match Type	Match String
URL	N/A	contains	Microsoft.com

### Example 2

Enter "logout" as the match string. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the "logout" example, WebInspect would exclude or reject URLs such as logout.asp or applogout.jsp.

Target	Target Name	Match Type	Match String
URL	N/A	contains	logout

### Example 3

The following example rejects or excludes a session containing a query where the query parameter "username" equals "John."

Target	Target Name	Match Type	Match String
Query parameter	username	matches	John

**Example 4**

The following example excludes or rejects the following directories:

<http://www.test.com/W3SVC55/>

<http://www.test.com/W3SVC5/>

<http://www.test.com/W3SVC550/>

Target	Target Name	Match Type	Match String
URL	N/A	matches regex	/W3SVC[0-9]*/

**See Also**

- ["Scan Settings: Allowed Hosts" below](#)
- ["Scan Settings: Authentication" on page 315](#)
- ["Scan Settings: Content Analyzers" on page 287](#)
- ["Scan Settings: Cookies/Headers " on page 310](#)
- ["Scan Settings: Custom Parameters" on page 305](#)
- ["Scan Settings: File Not Found " on page 320](#)
- ["Scan Settings: Filters" on page 308](#)
- ["Scan Settings: General" on page 282](#)
- ["Scan Settings: HTTP Parsing " on page 300](#)
- ["Scan Settings: Method " on page 278](#)
- ["Scan Settings: Policy " on page 322](#)
- ["Scan Settings: Proxy " on page 312](#)
- ["Scan Settings: Requestor" on page 289](#)
- ["Scan Settings: Session Storage " on page 292](#)

## Scan Settings: Allowed Hosts

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Allowed Hosts**.

## Using the Allowed Host Setting

Use the Allowed Host setting to add domains to be crawled and audited. If your Web presence uses multiple domains, add those domains here. For example, if you were scanning "Wlexample.com," you

would need to add "Wlexample2.com" and "Wlexample3.com" here if those domains were part of your Web presence and you wanted to include them in the crawl and audit.

You can also use this feature to scan any domain whose name contains the text you specify. For example, suppose you specify www.myco.com as the scan target and you enter "myco" as an allowed host. As WebInspect scans the target site, if it encounters a link to any URL containing "myco," it will pursue that link and scan that site's server, repeating the process until all linked sites are scanned. For this hypothetical example, WebInspect would scan the following domains:

- www.myco.com:80
- contact.myco.com:80
- www1.myco.com
- ethics.myco.com:80
- contact.myco.com:443
- wow.myco.com:80
- mycocorp.com:80
- www.interconnection.myco.com:80

## Adding Allowed Domains

To add allowed domains:

1. Click **Add**.
2. On the Specify Allowed Host window, enter a URL (or a regular expression representing a URL) and click **OK**.

**Note:** When specifying the URL, do not include the protocol designator (such as http:// or https://).

## Editing or Removing Domains

To edit or remove an allowed domain:

1. Select a domain from the **Allowed Hosts** list.
2. Click **Edit** or **Remove**.

### See Also

["Scan Settings: Authentication" on page 315](#)

["Scan Settings: Content Analyzers" on page 287](#)  
["Scan Settings: Cookies/Headers " on page 310](#)  
["Scan Settings: Custom Parameters" on page 305](#)  
["Scan Settings: File Not Found " on page 320](#)  
["Scan Settings: Filters" on page 308](#)  
["Scan Settings: General" on page 282](#)  
["Scan Settings: HTTP Parsing " below](#)  
["Scan Settings: Method " on page 278](#)  
["Scan Settings: Policy " on page 322](#)  
["Scan Settings: Proxy " on page 312](#)  
["Scan Settings: Requestor" on page 289](#)  
["Scan Settings: Session Exclusions" on page 294](#)  
["Scan Settings: Session Storage " on page 292](#)

## Scan Settings: HTTP Parsing

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **HTTP Parsing**.

## Options

The HTTP Parsing options are described in the following table:

Option	Description
HTTP Parameters Used for State	<p>If your application uses URL rewriting or post data techniques to maintain state within a Web site, you must identify which parameters are used. For example, a PHP4 script can create a constant of the session ID named SID, which is available inside a session. By appending this to the end of a URL, the session ID becomes available to the next page. The actual URL might look something like the following:</p> <p style="margin-left: 20px;">.../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01</p> <p>Because session IDs change with each connection, an HTTP request containing this URL would create an error when you tried to replay it. However, if you identify the parameter (PHPSESSID in this example), then WebInspect will replace its assigned value with the new session ID obtained from the server each time the connection is made.</p> <p>Similarly, some state management techniques use post data to pass information. For example, the HTTP message content may include userid=slbhkelvbkI73dhj. In this case, "userid" is the parameter you would identify.</p>
	<p><b>Note:</b> You need to identify parameters only when the application uses URL rewriting or posted data to manage state. It is not necessary when using cookies.</p> <p>WebInspect can identify potential parameters if they occur as posted data or if they exist within the query string of a URL. However, if your application embeds session data in the URL as extended path information, you must provide a regular expression to identify it. In the following example, "1234567" is the session information:</p> <p style="margin-left: 20px;"><a href="http://www.onlinestore.com/bikes/(1234567)/index.html">http://www.onlinestore.com/bikes/(1234567)/index.html</a></p> <p>The regular expression for identifying the parameter would be: <code>\([w d]+\)</code></p>
Enable CSRF	<p>The Enable CSRF option should only be selected if the site you are scanning includes Cross-Site Request Forgery (CSRF) tokens as it adds overhead to the process. For more information, see <a href="#">CSRF</a>.</p>
Determine State from URL Path	<p>If your application determines state from certain components in the URL path, select this check box and add one or more regular expressions that identify those components. Two default regular expressions identify two ASP.NET cookieless session IDs. The third regular expression matches jsessionid cookie.</p>

Option	Description
HTTP Parameters Used for Navigation	<p>Some sites contain only one directly accessible resource, and then rely on query strings to deliver the requested information, as in the following examples:</p> <p>Ex. 1 — http://www.anysite.com?Master.asp?Page=1      Ex. 2 — http://www.anysite.com?Master.asp?Page=2;      Ex. 3 — http://www.anysite.com?Master.asp?Page=13;Subpage=4</p> <p>Ordinarily, WebInspect would assume that these three requests refer to identical resources and would conduct a vulnerability scan on only one of them. Therefore, if your target Web site employs this type of architecture, you must identify the specific resource parameters that are used.</p> <p>Examples 1 and 2 contain one resource parameter: "Page." Example 3 contains two parameters: "Page" and "Subpage."</p> <p>To identify resource parameters:</p> <ol style="list-style-type: none"> <li>1. Click <b>Add</b>.</li> <li>2. On the HTTP Parameter window, enter the parameter name and click <b>OK</b>.</li> </ol> <p>The string you entered appears in the <b>Parameter</b> list.</p> <ol style="list-style-type: none"> <li>3. Repeat this procedure for additional parameters.</li> </ol>
Advanced HTTP Parsing	<p>Most Web pages contain information that tells the browser what character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document.</p> <p>For pages that do not announce their character set, you can specify which language family (and implied character set) WebInspect should use.</p>

Option	Description
<p>Treat query parameter value as parameter name when only value is present</p>	<p>This setting defines how WebInspect interprets query parameters without values. For example:</p> <p><code>http://somehost?param</code></p> <p>If this checkbox is selected, WebInspect will interpret “param” to be a parameter named “param” with an empty value.</p> <p>If this checkbox is not selected, WebInspect will interpret “param” to be a nameless parameter with the value “param”.</p> <p>This setting can influence the way WebInspect calculates the hit count (see the <a href="#">"Limit maximum single URL hits to " on page 285</a>setting under Scan Settings: General). This setting is useful for scenarios in which a URL contains an anti-caching parameter. These often take the form of a numeric counter or timestamp. For example, the following parameters are numeric counters:</p> <ul style="list-style-type: none"> <li>• <code>http://somehost?1234567</code></li> <li>• <code>http://somehost?1234568</code></li> </ul> <p>In such cases, the value is changing for each request. If the value is treated as the parameter name, and the “Include parameters in hit count” setting is selected, the crawl count may inflate artificially, thus increasing the scan time. In these cases, clearing the “Treat query parameter value as parameter name when only value is present” checkbox will prevent these counters from contributing to the hit count and produce a more reasonable scan time.</p>

## See Also

- ["Scan Settings: Allowed Hosts" on page 298](#)
- ["Scan Settings: Authentication" on page 315](#)
- ["Scan Settings: Content Analyzers" on page 287](#)
- ["Scan Settings: Cookies/Headers " on page 310](#)
- ["Scan Settings: Custom Parameters" on page 305](#)
- ["Scan Settings: File Not Found " on page 320](#)
- ["Scan Settings: Filters" on page 308](#)
- ["Scan Settings: General" on page 282](#)
- ["Scan Settings: Method " on page 278](#)
- ["Scan Settings: Policy " on page 322](#)
- ["Scan Settings: Proxy " on page 312](#)
- ["Scan Settings: Requestor" on page 289](#)

["Scan Settings: Session Exclusions" on page 294](#)

["Scan Settings: Session Storage " on page 292](#)

## CSRF

The Enable CSRF option should only be selected if the site you are scanning includes Cross-Site Request Forgery (CSRF) tokens as it adds overhead to the process.

### About CSRF

Cross-Site Request Forgery (CSRF) is a malicious exploit of a website where unauthorized commands are transmitted from a user's browser that the website trusts. CSRF exploits piggyback on the trust that a site has in a user's browser; using the fact that the user has already been authenticated by the site and the chain of trust is still open.

#### **Example:**

A user visits a bank, is authenticated, and a cookie is placed on the user's machine. After the user completes the banking transaction, he or she switches to another browser tab and continues a conversation on an enthusiast Web site devoted to the user's hobby. On the site, someone has posted a message that includes an HTML image element. The HTML image element includes a request to the user's bank to extract all of the cash from the account and deposit it into another account. Because the user has a cookie on his or her device that has not expired yet, the transaction is honored and all of the money in the account is withdrawn.

CSRF exploits often involve sites that rely on trust in a user's identity, often maintained through the use of a cookie. The user's browser is then tricked into sending HTTP requests to the target site in hopes that a trust between the user's browser and the target site still exists.

### Using CSRF Tokens

To stop Cross-site request forgeries from occurring, common practice is to set up the server to generate requests that include a randomly generated parameter with a common name such as "CSRFToken". The token may be generated once per session or a new one generated for each request. If you have used CSRF tokens in your code and enabled CSRF in WebInspect, we will take this into consideration when crawling your site. Each time WebInspect launches an attack, it will request the form again to acquire a new CSRF token. This adds significantly to the time it takes for WebInspect to complete a scan, so do not enable CSRF if you are not using CSRF tokens on your site.

### Enabling CSRF Awareness in WebInspect

If your site uses CSRF tokens, you can enable CSRF awareness in WebInspect as follows:

1. Select **Default Scan Settings** from the Edit menu.

The Scan Settings window appears.

2. From the Scan Settings column, select **HTTP Parsing**.
3. Select the **Enable CSRF** box.

## Scan Settings: Custom Parameters

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Custom Parameters**.

Custom Parameters are used to accommodate sites that use URL rewriting techniques and/or Representation State Transfer (REST) web services technologies. You can write rules for these custom parameters, or you can import rules from a common configuration file written in Web Application Description Language (WADL).

## URL Rewriting

Many dynamic sites use URL rewriting because static URLs are easier for users to remember and are easier for search engines to index the site. For example, an HTTP request such as

`http://www.pets.com>ShowProduct/7`

is sent to the server's rewrite module, which converts the URL to the following:

`http://www.pets.com>ShowProduct.php?product_id=7`

In this example, the URL causes the server to execute the php script "ShowProduct" and display the information for product number 7.

When WebInspect scans a page, it must be able to determine which elements are variables so that its attack agents can thoroughly check for vulnerabilities. To enable this, you must define rules that identify these elements. You can do so using a proprietary WebInspect syntax.

### Examples:

HTML: `<a href="someDetails/user1/">User 1 details</a>`

Rule: `/someDetails/{username}/`

HTML: `<a href="TwoParameters/Details/user1/Value2">User 1 details</a>`

Rule: `/TwoParameters/Details/{username}/{parameter2}`

HTML: `<a href="/Value2/PreFixParameter/Details/user1">User 1 details</a>`

Rule: `/{parameter2}/PreFixParameter/Details/{username}`

## RESTful Services

A RESTful web service (also called a RESTful web API) is a simple Web service implemented using HTTP and the principles of REST. It has gained widespread acceptance across the Web as a simpler alternative to web services based on SOAP and Web Services Description Language (WSDL).

The following request adds a name to a file using an HTTP query string:

```
GET /adduser?name=Robert HTTP/1.1
```

This same function could be achieved by using the following method with a Web service. Note that the parameter names and values have been moved from the request URI and now appear as XML tags in the request body.

```
POST /users HTTP/1.1 Host: myserver
Content-Type: application/xml
<?xml version="1.0"?>
<user>
<name>Robert</name>
</user>
```

In the case of both URL rewriting and RESTful web services, you must create rules that instruct WebInspect how to create the appropriate requests.

### Creating a Rule

To create a rule:

1. Click **New Rule**.
2. In the Expression column, enter a rule. See [Path Matrix Parameters](#) for guidelines and examples.

The **Enabled** check box is selected by default. WebInspect examines the rule and, if it is valid, removes the red X.

### Deleting a Rule

To delete a rule:

1. Select a rule from the **Custom Parameters Rules** list.
2. Click **Delete**.

### Disabling a Rule

To disable a rule without deleting it:

1. Select a rule.
2. Clear the check mark in the **Enabled** column.

## Importing Rules

To import a file containing rules:

1. Click  Import...
2. Using a standard file-selection dialog, select the type of file (.wadl or .txt) containing the custom rules you want to apply.
3. Locate the file and click Open.

## Enable automatic seeding of rules that were not used during scan

The most reliable rules for custom parameters are those deduced from a WADL file or created by developers of the Web site. If a rule is not invoked during a scan (because the rule doesn't match any URL), then WebInspect can programmatically assume that a valid portion of the site has not been attacked. Therefore, if you select this option, WebInspect will create sessions to exercise these unused rules in an effort to expand the attack surface.

## Double Encode URL Parameters

Double-encoding is an attack technique that encodes user request parameters twice in hexadecimal format in an attempt to bypass security controls or cause unexpected behavior from the application. For example, a cross-site scripting (XSS) attack might normally appear as:

```
<script>alert('FOO')</script>
```

This malicious code could be inserted into a vulnerable application, resulting in an alert window with the message "FOO." However, the web application can have a filter that prohibits characters such as < (less than) > (greater than) and / (forward slash), since they are used to perform Web application attacks. The attacker could attempt to circumvent this safeguard by using a "double encoding" technique to exploit the client's session. The encoding process for this Javascript is:

Char	Hex encode	Encoded % Sign	Double encoded result
<	%3C	%25	%253C
/	%2F	%25	%252F
>	%3E	%25	%253E

Finally, the malicious code, double-encoded, is:

```
%253Cscript%253Ealert('XSS')%253C%252Fscript%253E
```

If you select this option, WebInspect will create double-encoded URL parameters (instead of single-encoded parameters) and submit them as part of the attack sequence. This is recommended when the Web server uses, for example, Apache mod-rewrite plus PHP or Java URL Rewrite Filter 3.2.0.

## See Also

- "Scan Settings: Allowed Hosts" on page 298
- "Scan Settings: Authentication" on page 315
- "Scan Settings: Content Analyzers" on page 287
- "Scan Settings: Cookies/Headers " on page 310
- "Scan Settings: File Not Found " on page 320
- "Scan Settings: Filters" below
- "Scan Settings: General" on page 282
- "Scan Settings: HTTP Parsing " on page 300
- "Scan Settings: Method " on page 278
- "Scan Settings: Policy " on page 322
- "Scan Settings: Proxy " on page 312
- "Scan Settings: Requestor" on page 289
- "Scan Settings: Session Exclusions" on page 294
- "Scan Settings: Session Storage " on page 292

## Scan Settings: Filters

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Filters**.

Use the Filters settings to add search-and-replace rules for HTTP requests and responses. This feature is used most often to avoid the disclosure of sensitive data such as credit card numbers, employee names, or social security numbers. It is a means of disguising information that you do not want to be viewed by persons who use WebInspect or those who have access to the raw data or generated reports.

If the text you specify is found, WebInspect reports it on the Information tab as a "Hidden Reference Found" vulnerability.

## Options

The Filter options are described in the following table:

Option	Description
Filter HTTP Request Content	Use this area to specify search-and-replace rules for HTTP requests.
Filter HTTP Response Content	Use this area to specify search-and-replace rules for HTTP responses.

## Adding Rules for Finding and Replacing Keywords

Follow the steps below to add a regular expression rule for finding or replacing keywords in requests or responses:

1. In either the **Request Content** or the **Response Content** group, click **Add**.  
The Add Request/Response Data Filter Criteria window opens.
2. In the **Search For Text** box, type (or paste) the string you want to locate (or enter a regular expression that describes the string).  
Click  to insert regular expression notations or to launch the Regular Expression Editor (which facilitates the creation and testing of an expression).
3. In the **Search For Text In** box, select an area to search:
  - For Requests: select All, Headers, or Postdata.
  - For Responses: select All, Headers, or Body (that is, the code of the page itself)
4. Type (or paste) the replacement string in the **Replace search text with** box.  
Click  for assistance with regular expressions.
5. For case-sensitive searches, select the **Case-Sensitive Match** check box.
6. Click **OK**.

### See Also

- ["Scan Settings: Allowed Hosts" on page 298](#)
- ["Scan Settings: Authentication" on page 315](#)
- ["Scan Settings: Content Analyzers" on page 287](#)
- ["Scan Settings: Cookies/Headers" on the next page](#)
- ["Scan Settings: Custom Parameters" on page 305](#)
- ["Scan Settings: File Not Found" on page 320](#)
- ["Scan Settings: General" on page 282](#)
- ["Scan Settings: HTTP Parsing" on page 300](#)
- ["Scan Settings: Method" on page 278](#)
- ["Scan Settings: Policy" on page 322](#)
- ["Scan Settings: Proxy" on page 312](#)
- ["Scan Settings: Requestor" on page 289](#)

["Scan Settings: Session Exclusions" on page 294](#)

["Scan Settings: Session Storage " on page 292](#)

## Scan Settings: Cookies/Headers

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Cookies/Headers**.

### Standard Header Parameters

This section includes the following options:

Option	Description
Include 'referer' in HTTP request headers	Select this check box to include referer headers in WebInspect HTTP requests. The Referer request-header field allows the client to specify, for the server's benefit, the address (URI) of the resource from which the Request-URI was obtained.
Include 'host' in HTTP request headers	Select this check box to include host headers with WebInspect HTTP requests. The Host request-header field specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource (generally an HTTP URL).

### Append Custom Headers

Use this section to add, edit, or delete headers that will be included with each audit WebInspect performs. For example, you could add a header such as "Alert: You are being attacked by Consultant ABC" that would be included with every request sent to your company's server when WebInspect is auditing that site. You can add multiple custom headers.

The default custom headers are:

Header	Description
Accept: */*	Any encoding or file type is acceptable to the crawler.
Pragma: no-cache	This forces a fresh response; cached or proxied data is not acceptable.

### Adding a Custom Header

Follow the steps below to add a custom header:

1. Click **Add**.

The Specify Custom Header window opens.

2. In the **Custom Header** box, enter the header using the format <name>: <value>.
3. Click **OK**.

## Append Custom Cookies

Use this section to specify data that will be sent with the Cookie header in HTTP requests sent by WebInspect to the server when conducting a vulnerability scan.

The default custom cookie is

CustomCookie=WebInspect;path=/

which is used simply to flag the scan traffic.

## Adding a Custom Cookie

Follow the steps below to add a custom cookie:

1. Click **Add**.

The Specify Custom Cookie window opens.

2. In the **Custom Cookie** box, enter the cookie using the format <name>=<value>.

For example, if you enter

CustomCookie=ScanEngine

then each HTTP-Request will contain the following header:

Cookie: CustomCookie=ScanEngine

3. Click **OK**.

### See Also

["Scan Settings: Allowed Hosts" on page 298](#)

["Scan Settings: Authentication" on page 315](#)

["Scan Settings: Content Analyzers" on page 287](#)

["Scan Settings: Custom Parameters" on page 305](#)

["Scan Settings: File Not Found " on page 320](#)

["Scan Settings: Filters" on page 308](#)

- "Scan Settings: General" on page 282
- "Scan Settings: HTTP Parsing " on page 300
- "Scan Settings: Method " on page 278
- "Scan Settings: Policy " on page 322
- "Scan Settings: Proxy " below
- "Scan Settings: Requestor" on page 289
- "Scan Settings: Session Exclusions" on page 294
- "Scan Settings: Session Storage " on page 292

## Scan Settings: Proxy

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Proxy**.

## Options

The Proxy options are described in the following table:

Option	Description
Direct Connection (proxy disabled)	Select this option if you are not using a proxy server.
Auto detect proxy settings	Use the Web Proxy Autodiscovery (WPAD) protocol to locate a proxy autoconfig file and configure the browser's Web proxy settings.
Use Internet Explorer proxy settings	Import your proxy server information from Internet Explorer.
Use Firefox proxy settings	Import your proxy server information from Firefox. <b>Note:</b> Electing to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy server will not be used.
Configure proxy using a PAC file URL	Load proxy settings from a Proxy Automatic Configuration (PAC) file in the location you specify in the <b>URL</b> box.

Option	Description
<p>Explicitly configure proxy</p> <p>Configure a proxy by entering the requested information</p> <ol style="list-style-type: none"> <li>1. In the <b>Server</b> box, type the URL or IP address of your proxy server, followed (in the <b>Port</b> box) by the port number (for example, 8080).</li> <li>2. Select a protocol <b>Type</b> for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.</li> <li>3. If authentication is required, select a type from the <b>Authentication</b> list:</li> </ol> <p>Automatic</p> <p>Allow WebInspect to determine the correct authentication type.</p> <p><b>Note:</b> Automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.</p> <p>Digest</p> <p>The Windows Server operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.</p> <p>HTTP Basic</p> <p>A widely used, industry-standard method for collecting user name and password information.</p> <ol style="list-style-type: none"> <li>a. The Web browser displays a window for a user to enter a previously assigned user name and password, also known as credentials.</li> <li>b. The Web browser then attempts to establish a connection to a server using the user's credentials.</li> <li>c. If a user's credentials are rejected, the browser displays an authentication window to re-enter the user's credentials. Internet Explorer allows the user three connection attempts before failing the connection and reporting an error to the user.</li> <li>d. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established.</li> </ol>	

Option	Description
	<p>The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that Web browsers using Basic authentication transmit passwords in an unencrypted form. By monitoring communications on your network, an attacker can easily intercept and decode these passwords using publicly available tools. Therefore, Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.</p> <p><b>NT LAN Manager (NTLM)</b></p> <p>NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.</p> <p>Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and WebInspect has to pass through a proxy server to submit its requests to the Web server, WebInspect may not be able to crawl or audit that Web site. Use <b>caution</b> when configuring WebInspect for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.</p> <p><b>Kerberos</b></p> <p>Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.</p> <p><b>Negotiate</b></p> <p>The Negotiate authentication protocol begins with the option to negotiate for an authentication protocol. When the client requests access to a service, the server replies with a list of authentication protocols that it can support and an authentication challenge based on the protocol that is its first choice.</p> <p>For example, the server might list Kerberos and NTLM, and send a Kerberos challenge. The client examines the contents of the reply and checks to determine whether it supports any of the specified protocols. If the client supports the preferred protocol, authentication proceeds. If the client does not support the preferred protocol, but</p>

Option	Description
	<p>does support one of the other protocols listed by the server, the client lets the server know which authentication protocol it supports, and the authentication proceeds. If the client does not support any of the listed protocols, the authentication exchange fails.</p> <ol style="list-style-type: none"> <li data-bbox="551 460 1367 523">4. If your proxy server requires authentication, enter the qualifying user name and password.</li> <li data-bbox="551 555 1334 677">5. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the <b>Bypass Proxy For</b> box. Use commas to separate entries.</li> </ol>
Specify Alternative Proxy for HTTPS	For proxy servers accepting HTTPS connections, select <b>Specify Alternative Proxy for HTTPS</b> and provide the requested information.

## See Also

- ["Scan Settings: Allowed Hosts" on page 298](#)
- ["Scan Settings: Authentication" below](#)
- ["Scan Settings: Content Analyzers" on page 287](#)
- ["Scan Settings: Cookies/Headers" on page 310](#)
- ["Scan Settings: Custom Parameters" on page 305](#)
- ["Scan Settings: File Not Found" on page 320](#)
- ["Scan Settings: Filters" on page 308](#)
- ["Scan Settings: General" on page 282](#)
- ["Scan Settings: HTTP Parsing" on page 300](#)
- ["Scan Settings: Method" on page 278](#)
- ["Scan Settings: Policy" on page 322](#)
- ["Scan Settings: Requestor" on page 289](#)
- ["Scan Settings: Session Exclusions" on page 294](#)
- ["Scan Settings: Session Storage" on page 292](#)

## Scan Settings: Authentication

To access this feature in a Basic Scan, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Authentication**.

Authentication is the verification of identity as a security measure. Passwords and digital signatures are forms of authentication. You can configure automatic authentication so that a user name and password will be entered whenever WebInspect encounters a server or form that requires authentication. Otherwise, a crawl might be prematurely halted for lack of logon information.

## Scan Requires Network Authentication

Select this check box if users must log on to your Web site or application.

## Authentication Method

If authentication is required, select the authentication method as described in the following table:

Authentication Method	Description
Automatic	<p>Allow WebInspect to determine the correct authentication type. Automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.</p>
HTTP Basic	<p>A widely used, industry-standard method for collecting user name and password information.</p> <ol style="list-style-type: none"><li data-bbox="551 1136 1367 1199">1. The Web browser displays a window for a user to enter a previously assigned user name and password, also known as credentials.</li><li data-bbox="551 1231 1367 1294">2. The Web browser then attempts to establish a connection to a server using the user's credentials.</li><li data-bbox="551 1326 1367 1474">3. If a user's credentials are rejected, the browser displays an authentication window to re-enter the user's credentials. Internet Explorer allows the user three connection attempts before failing the connection and reporting an error to the user.</li><li data-bbox="551 1505 1269 1569">4. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established.</li></ol> <p>The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that Web browsers using Basic authentication transmit passwords in an unencrypted form. By monitoring communications on your network, an attacker can easily intercept and decode these passwords using publicly available tools. Therefore, Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.</p>

Authentication Method	Description
NT LAN Manager (NTLM)	<p>NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.</p> <p>Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and WebInspect has to pass through a proxy server to submit its requests to the Web server, WebInspect may not be able to crawl or audit that Web site. Use caution when configuring WebInspect for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.</p>
Digest	<p>The Windows Server operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.</p>
Kerberos	<p>Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.</p>

## Authentication Credentials

Type a user ID in the **User name** box and the user's password in the **Password** box. To guard against mistyping, repeat the password in the **Confirm Password** box.

**Caution:** WebInspect will crawl all servers granted access by this password (if the sites/servers are included in the "allowed hosts" setting). To avoid potential damage to your administrative systems, do not use a user name and password that has administrative rights. If you are unsure about your access rights, contact your System Administrator or internal security professional, or contact Hewlett-Packard technical support.

## Client Certificates

Client certificate authentication allows users to present client certificates rather than entering a user name and password. You can select a certificate from the local machine or a certificate assigned to a

current user. Follow the steps below to use client certificates.

1. In the right pane, select **Client Certificate**.
2. To use a certificate on the computer, select **Local Machine**.
3. Current User.
4. Click **Select** to open the Client Certificates window.
5. Choose a certificate.

When using tools that incorporate a proxy (specifically Web Macro Recorder, Web Proxy, Web Brute, and Web Form Editor), you may encounter servers that do not ask for a client certificate even though a certificate is required. To accommodate this situation, you must edit the SPI.Net.Proxy.Config file using the following procedure.

## Task 1: Find your certificate's serial number

1. Open Microsoft Internet Explorer.
2. From the **Tools** menu, click **Internet Options**.
3. On the Internet Options window, select the **Content** tab and click **Certificates**.
4. On the Certificates window, select a certificate and click **View**.
5. On the Certificate window, click the **Details** tab.
6. Click the **Serial Number** field and copy the serial number that appears in the lower pane (highlight the number and press Ctrl + C).
7. Close all windows.

## Task 2: Create an entry in the SPI.Net.Proxy.Config file

1. Open the SPI.Net.Proxy.Config file for editing. The default location is C:\Program Files\HP\HP WebInspect.
2. In the ClientCertificateOverrides section, add the following entry:

```
<ClientCertificateOverride HostRegex="RegularExpression" CertificateSerialNumber="Number">
```

where:

RegularExpression is a regular expression matching the host URL (example: .\*austin\.hp\.com).

Number is the serial number obtained in Task 1.

3. Save the edited file.

## Use a login macro for forms authentication

This type of macro is used primarily for Web form authentication. It incorporates logic that will prevent WebInspect from terminating prematurely if it inadvertently logs out of your application. When recording this type of macro, be sure to specify the application's log-out signature. Click the ellipsis button  to locate the macro. Click **Record** to record a macro.

**Note:** The Record button is not available for Guided Scan, because Guided Scan includes a separate stage for recording a login macro.

## Login Macro Parameters

This section appears only if you have selected **Use a login macro for forms authentication** and the macro you have chosen or created contains fields that are designated as Smart Credentials (if you used the session-based or event-based Web Macro Recorder) or username and password parameters (if you used the HP WebInspect Web Macro Recorder).

If you start a scan using a macro that includes Smart Credentials (or parameters for user name and password), then when you scan the page containing the input elements associated with these entries, WebInspect substitutes the user name and password specified here. This allows you to create the macro using your own user name and password, yet when other persons run the scan using this macro, they can substitute their own user name and password.

Click [here](#) for information about creating parameters using the HP WebInspect Web Macro Recorder.

Click [here](#) for information about Smart Credentials using the event-based Web Macro Recorder.

## Use a startup macro

This type of macro is used most often to focus on a particular subsection of the application. It specifies URLs that WebInspect will use to navigate to that area. It may also include login information, but does not contain logic that will prevent WebInspect from logging out of your application. WebInspect visits all URLs in the macro, collecting hyperlinks and mapping the data hierarchy. It then calls the Start URL and begins a normal crawl (and, optionally, audit). Click the ellipsis button  to locate the macro. Click **Record** to record a macro.

### See Also

["Scan Settings: Allowed Hosts" on page 298](#)

["Scan Settings: Content Analyzers" on page 287](#)

["Scan Settings: Cookies/Headers " on page 310](#)

["Scan Settings: Custom Parameters" on page 305](#)

["Scan Settings: File Not Found " on the next page](#)

- "Scan Settings: Filters" on page 308
- "Scan Settings: General" on page 282
- "Scan Settings: HTTP Parsing " on page 300
- "Scan Settings: Method " on page 278
- "Scan Settings: Policy " on page 322
- "Scan Settings: Proxy " on page 312
- "Scan Settings: Requestor" on page 289
- "Scan Settings: Session Exclusions" on page 294
- "Scan Settings: Session Storage " on page 292

## Scan Settings: File Not Found

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **File Not Found**.

## Options

The File Not Found options are described in the following table:

Option	Description
Determine "file not found" (FNF) using HTTP response codes	<p>Select this option to rely on HTTP response codes to detect a file-not-found response from the server. You can then identify the codes that fit the following two categories.</p> <ul style="list-style-type: none"><li>• <b>Forced Valid Response Codes (Never an FNF):</b> You can specify HTTP response codes that should never be treated as a file-not-found response.</li><li>• <b>Forced FNF Response Codes (Always an FNF):</b> Specify those HTTP response codes that will always be treated as a file-not-found response. WebInspect will not process the response contents.</li></ul> <p>Enter a single response code or a range of response codes. For ranges, use a dash or hyphen to separate the first and last code in the list (for example, 400-404). You can specify multiple codes or ranges by separating each entry with a comma.</p>

Option	Description
Determine "file not found" from custom supplied signature	Use this area to add information about any custom 404 page notifications that your company uses. If your company has configured a different page to display when a 404 error occurs, add the information here. False positives can result in WebInspect from 404 pages that are unique to your site.
Auto detect "file not found" page	<p>Some Web sites do not return a status "404 Not Found" when a client requests a resource that does not exist. Instead, they may return a status "200 OK" but the response contains a message that the file cannot be found, or they might redirect to a home page or login page. Select this check box if you want WebInspect to detect these "custom" file-not-found pages.</p> <p>WebInspect attempts to detect custom file-not-found pages by sending requests for resources that cannot possibly exist on the server. It then compares each response and measures the amount of text that differs between the responses. For example, most messages of this type have the same content (such as "Sorry, the page you requested was not found"), with the possible exception being the name of the requested resource. If you select the <b>Auto detect</b> check box, you can specify what percentage of the response content must be the same. The default is 90 percent.</p>

## See Also

- ["Scan Settings: Allowed Hosts" on page 298](#)
- ["Scan Settings: Authentication" on page 315](#)
- ["Scan Settings: Content Analyzers" on page 287](#)
- ["Scan Settings: Cookies/Headers" on page 310](#)
- ["Scan Settings: Custom Parameters" on page 305](#)
- ["Scan Settings: Filters" on page 308](#)
- ["Scan Settings: General" on page 282](#)
- ["Scan Settings: HTTP Parsing" on page 300](#)
- ["Scan Settings: Method" on page 278](#)
- ["Scan Settings: Policy" on the next page](#)
- ["Scan Settings: Proxy" on page 312](#)
- ["Scan Settings: Requestor" on page 289](#)
- ["Scan Settings: Session Exclusions" on page 294](#)
- ["Scan Settings: Session Storage" on page 292](#)

## Scan Settings: Policy

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Scan Settings** category, select **Policy**.

You can change to a different policy when starting a scan through the Scan Wizard, but the policy you select here will be used if you do not select an alternate.

You can also create, import, or delete policies.

## Creating a Policy

To create a policy:

1. Click **Create**.
2. The Policy Manager tool opens.
3. Select **New** from the **File** menu (or click the New Policy icon).
4. Select the policy on which you will model a new one.
5. Refer to the Policy Manager on-line Help for additional instructions.

## Editing a Policy

To edit a policy:

1. Select a custom policy.
2. Only custom policies may be edited.
3. Click **Edit**.
4. The Policy Manager tool opens.
5. Refer to the on-line Help for additional instructions.

## Importing a Policy

To import a policy:

1. Click **Import**.
2. On the Import Custom Policy window, click the ellipses button .

3. Using the **Files of type** list on the standard file-selection window, choose a policy type:
  - Policy Files (\*.policy): Policy files designed and created for versions of WebInspect beginning with release 7.0.
  - Old Policy Files (\*.apc): Policy files designed and created for versions of WebInspect prior to release 7.0.
  - All Files (\*.\*): Files of any type, including non-policy files.

4. Click **OK**.

A copy of the policy is created in the Policies folder (the default location is C:\Documents and Settings\All Users\Application Data\HP\HP WebInspect\Policies\). The policy and all of its enabled checks are imported into SecureBase using the specified policy name. Custom agents are not imported.

**Note:** When importing policy files created for earlier versions of WebInspect, any custom check associated with that policy will be imported only if it can be found in the CustomAgents.xml file used by WebInspect 6.5 or earlier.

## Deleting a Policy

To delete a policy:

1. Select a custom policy.

Only custom policies may be deleted.
2. Click **Delete**.

### See Also

- ["Scan Settings: Allowed Hosts" on page 298](#)
- ["Scan Settings: Authentication" on page 315](#)
- ["Scan Settings: Content Analyzers" on page 287](#)
- ["Scan Settings: Cookies/Headers " on page 310](#)
- ["Scan Settings: Custom Parameters" on page 305](#)
- ["Scan Settings: File Not Found " on page 320](#)
- ["Scan Settings: Filters" on page 308](#)
- ["Scan Settings: General" on page 282](#)
- ["Scan Settings: HTTP Parsing " on page 300](#)
- ["Scan Settings: Method " on page 278](#)

- "Scan Settings: Proxy " on page 312
- "Scan Settings: Requestor" on page 289
- "Scan Settings: Session Exclusions" on page 294
- "Scan Settings: Session Storage " on page 292

# Crawl Settings

The WebInspect crawler is a software program designed to follow hyperlinks throughout a Web site, retrieving and indexing pages to document the hierarchical structure of the site. The parameters that control the manner in which WebInspect crawls a site are available from the Crawl Settings list.

## See Also

["Crawl Settings: Link Parsing" below](#)

["Crawl Settings: Session Exclusions" on the next page](#)

## Crawl Settings: Link Parsing

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Crawl Settings** category, select **Link Parsing**.

WebInspect follows all hyperlinks defined by HTML (using the <a href> tag) and those defined by scripts (JavaScript and VBScript). However, you may encounter other communications protocols that use a different syntax for specifying links. To accommodate this possibility, you can use the Custom Links feature and regular expressions to identify links that you want WebInspect to follow. These are called special link identifiers.

## Adding a Specialized Link Identifier

Follow the steps below to add a specialized link identifier:

1. Click **Add**.

The Specialized Link Entry window opens.

2. In the **Specialized Link Pattern** box, enter a regular expression designed to identify the link.
3. (Optional) Enter a description of the link in the **Comment** box.
4. Click **OK**.

## See Also

["Crawl Settings: Session Exclusions" on the next page](#)

## Crawl Settings: Session Exclusions

All items specified in the **Scan Settings - Session Exclusions** are automatically replicated in the **Session Exclusions** for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the crawl, you must remove them from the **Scan Settings - Session Exclusions** panel.

This panel (**Crawl Settings - Session Exclusions**) allows you to specify additional objects to be excluded from the crawl.

## Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested.

If you select **Exclude**, files having the specified extension will be requested, but will not be audited.

### Adding a File Extension to Exclude/Reject

Follow the steps below to add a file extension:

1. Click **Add**.

The Exclusion Extension window opens.

2. In the **File Extension** box, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **OK**.

## Excluded MIME Types

Files associated with the MIME types you specify will not be audited.

### Adding a MIME Type to Exclude

Follow the steps below to add a MIME Type:

1. Click **Add**.

The Provide a Mime-type to Exclude window opens.

2. In the **Exclude Mime-type** box, enter a MIME type.
3. Click **OK**.

## Other Exclusion/Rejection Criteria

You can identify various components of an HTTP message and then specify whether you want to exclude or reject a session that contains that component.

- **Reject** - WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude** - During a crawl, WebInspect will not examine the specified URL or host for links to other resources. During the audit portion of the scan, WebInspect will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

## Editing the Default Criteria

To edit the default criteria:

1. Select a criterion and click **Edit** (on the right side of the **Other Exclusion/Rejection Criteria** list).  
The Reject or Exclude a Host or URL window opens.
2. Select either **Host** or **URL**.
3. In the **Host/URL** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select either **Reject**, **Exclude**, or both.
5. Click **OK**.

## Adding Exclusion/Rejection Criteria

To add exclusion/rejection criteria:

1. Click **Add** (on the right side of the **Excluded or Rejected URLs and Hosts** list).  
The Create Exclusion window opens.
2. Select an item from the **Target** list.

3. If you selected Query Parameter or Post Parameter as the target, enter the **Target Name**.
4. From the **Match Type** list, select the method to be used for matching text in the target:
  - Matches Regex - Matches the regular expression you specify in the **Match String** box.
  - Matches Regex Extension - Matches a syntax available from HP's [regular expression extensions](#) you specify in the **Match String** box.
  - Matches - Matches the text string you specify in the **Match String** box.
  - Contains - Contains the text string you specify in the **Match String** box.
5. In the **Match String** box, enter the string or regular expression for which the target will be searched. Alternatively, if you selected a regular expression option in the **Match Type**, you can click the drop-down arrow and select **Create Regex** to launch the Regular Expression Editor.
6. Click  (or press **Enter**).
7. (Optional) Repeat steps 2-6 to add more conditions. Multiple matches are ANDed.
8. If you are working in Current Settings, you can click **Test** to process the exclusions on the current scan. Any sessions from that scan that would have been filtered by the criteria will appear in the test screen, allowing you to modify your settings if required.
9. Click **OK**.
10. When the exclusion appears in the **Excluded or Rejected URLs or Hosts** list, select either **Reject**, **Exclude**, or both.

#### Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following exclusion and select **Reject**.

Target	Target Name	Match Type	Match String
URL	N/A	contains	Microsoft.com

#### Example 2

Enter "logout" as the match string. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the "logout" example, WebInspect would exclude or reject URLs such as logout.asp or applogout.jsp.

Target	Target Name	Match Type	Match String
URL	N/A	contains	logout

**Example 3**

The following example rejects or excludes a session containing a query where the query parameter "username" equals "John."

Target	Target Name	Match Type	Match String
Query parameter	username	matches	John

**Example 4**

The following example excludes or rejects the following directories:

`http://www.test.com/W3SVC55/`

`http://www.test.com/W3SVC5/`

`http://www.test.com/W3SVC550/`

Target	Target Name	Match Type	Match String
URL	N/A	matches regex	<code>/W3SVC[0-9]*/</code>

**See Also**

["Crawl Settings: Link Parsing" on page 325](#)

# Audit Settings

An audit is the probe or attack conducted by WebInspect which is designed to detect vulnerabilities. The parameters that control the manner in which WebInspect conducts that probe are available from the Audit Settings list.

## See Also

["Audit Settings: Attack Exclusions" on page 334](#)

["Audit Settings: Attack Expressions" on page 337](#)

["Audit Settings: Session Exclusions" below](#)

["Audit Settings: Smart Scan" on page 339](#)

["Audit Settings: Vulnerability Filtering" on page 337](#)

## Audit Settings: Session Exclusions

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Audit Settings** category, select **Session Exclusions**.

All items specified in the **Scan Settings - Session Exclusions** are automatically replicated in the **Session Exclusions** for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the audit, you must remove them from the **Scan Settings - Session Exclusions** panel.

This panel (**Audit Settings - Session Exclusions**) allows you to specify additional objects to be excluded from the audit.

## Excluded or Rejected File Extensions

If you select **Reject**, WebInspect will not request files having the specified extension.

If you select **Exclude**, WebInspect will request files having the specified extension, but will not audit them.

## Adding a File Extension to Exclude/Reject

Follow the steps below to add a file extension:

1. Click **Add**.

The Exclusion Extension window opens.

2. In the **File Extension** box, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **OK**.

## Excluded MIME Types

WebInspect will not audit files associated with the MIME types you specify.

### Adding a MIME Type to Exclude

Follow the steps below to add a MIME type:

1. Click **Add**.  
The Provide a Mime-type to Exclude window opens.
2. In the **Exclude Mime-type** box, enter a MIME type.
3. Click **OK**.

## Other Exclusion/Rejection Criteria

You can identify various components of an HTTP message and then specify whether you want to exclude or reject a session that contains that component.

- **Reject** - WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude** - During a crawl, WebInspect will not examine the specified URL or host for links to other resources. During the audit portion of the scan, WebInspect will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

### Editing the Default Criteria

To edit the default criteria:

1. Select a criterion and click **Edit** (on the right side of the **Other Exclusion/Rejection Criteria** list).

The Reject or Exclude a Host or URL window opens.

2. Select either **Host** or **URL**.
3. In the **Host/URL** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select either **Reject**, **Exclude**, or both.
5. Click **OK**.

## Adding Exclusion/Rejection Criteria

To add exclusion/rejection criteria:

1. Click **Add** (on the right side of the **Excluded or Rejected URLs and Hosts** list).

The Create Exclusion window opens.
2. Select an item from the **Target** list.
3. If you selected Query Parameter or Post Parameter as the target, enter the **Target Name**.
4. From the **Match Type** list, select the method to be used for matching text in the target:
  - Matches Regex - Matches the regular expression you specify in the **Match String** box.
  - Matches Regex Extension - Matches a syntax available from HP's [regular expression extensions](#) you specify in the **Match String** box.
  - Matches - Matches the text string you specify in the **Match String** box.
  - Contains - Contains the text string you specify in the **Match String** box.
5. In the **Match String** box, enter the string or regular expression for which the target will be searched. Alternatively, if you selected a regular expression option in the **Match Type**, you can click the drop-down arrow and select **Create Regex** to launch the Regular Expression Editor.
6. Click  (or press Enter).
7. (Optional) Repeat steps 2-6 to add more conditions. Multiple matches are ANDed.
8. If you are working in Current Settings, you can click **Test** to process the exclusions on the current scan. Any sessions from that scan that would have been filtered by the criteria will appear in the test screen, allowing you to modify your settings if required.
9. Click **OK**.
10. When the exclusion appears in the **Excluded or Rejected URLs or Hosts** list, select either **Reject**, **Exclude**, or both.

**Example 1**

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following exclusion and select **Reject**.

Target	Target Name	Match Type	Match String
URL	N/A	contains	Microsoft.com

**Example 2**

Enter "logout" as the match string. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the "logout" example, WebInspect would exclude or reject URLs such as logout.asp or applogout.jsp.

Target	Target Name	Match Type	Match String
URL	N/A	contains	logout

**Example 3**

The following example rejects or excludes a session containing a query where the query parameter "username" equals "John."

Target	Target Name	Match Type	Match String
Query parameter	username	matches	John

**Example 4**

The following example excludes or rejects the following directories:

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

Target	Target Name	Match Type	Match String
URL	N/A	matches regex	/W3SVC[0-9]*/

**See Also**

["Audit Settings: Attack Exclusions" on the next page](#)

["Audit Settings: Attack Expressions" on page 337](#)

["Audit Settings: Smart Scan" on page 339](#)

["Audit Settings: Vulnerability Filtering" on page 337](#)

## Audit Settings: Attack Exclusions

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Audit Settings** category, select **Attack Exclusions**.

### Excluded Parameters

Use this feature to prevent WebInspect from using certain parameters in the HTTP request to attack the Web site. This feature is used most often to avoid corrupting query and POSTDATA parameters.

#### Adding Parameters to Exclude

To prevent certain parameters from being modified:

1. In the **Excluded Parameters** group, click **Add**.

The Specify HTTP Exclusions window opens.

2. In the **HTTP Parameter** box, enter the name of the parameter you want to exclude.

Click to insert regular expression notations.

3. Choose the area in which the parameter may be found: HTTP query data or HTTP POST data. You can select both areas, if necessary.

4. Click **OK**.

### Excluded Cookies

Use this feature to prevent WebInspect from using certain cookies in the HTTP request to attack the Web site. This feature is used to avoid corrupting cookie values.

This setting requires you to enter the name of a cookie. In the following example HTTP response ...

Set-Cookie: FirstCookie=Chocolate+Chip; path=/

... the name of the cookie is "FirstCookie."

### Excluding Certain Cookies

Follow the steps below to exclude certain cookies.

1. In the **Excluded Headers** group, click **Add**.

The Regular Expression Editor appears.

**Note:** You can specify a cookie using either a text string or a regular expression.

2. To enter a text string:
  - a. In the **Expression** box, type a cookie name.
  - b. Click **OK**.
3. To enter a regular expression:
  - a. In the **Expression** box, type or paste a regular expression that you believe will match the text for which you are searching.  
Click  to insert regular expression notations.
  - b. In the **Comparison Text** box, type or paste the text that is known to contain the string you want to find (as specified in the **Expression** box).
  - c. To find only those occurrences matching the case of the expression, select the **Match Case** check box.
  - d. If you want to replace the string identified by the regular expression, select the **Replace** check box and then type or select a string from the **Replace** box.
  - e. Click **Test** to search the comparison text for strings that match the regular expression.  
Matches will be highlighted in red.
  - f. Did your regular expression identify the string?
    - If yes, click **OK**.
    - If no, verify that the Comparison Text contains the string you want to identify or modify the regular expression.

## Excluded Headers

Use this feature to prevent WebInspect from using certain headers in the HTTP request to attack the Web site. This feature is used to avoid corrupting header values.

### Excluding Certain Headers

To prevent certain headers from being modified, create a regular expression using the procedure described below.

1. In the **Excluded Headers** group, click **Add**.

The Regular Expression Editor appears.

**Note:** You can specify a header using either a text string or a regular expression.

2. To enter a text string:
  - a. In the **Expression** box, type a header name.
  - b. Click **OK**.
3. To enter a regular expression:
  - a. In the **Expression** box, type or paste a regular expression that you believe will match the text for which you are searching.  
Click  to insert regular expression notations.
  - b. In the **Comparison Text** box, type or paste the text that is known to contain the string you want to find (as specified in the **Expression** box).
  - c. To find only those occurrences matching the case of the expression, select the **Match Case** check box.
  - d. If you want to replace the string identified by the regular expression, select the **Replace** check box and then type or select a string from the **Replace** box.
  - e. Click **Test** to search the comparison text for strings that match the regular expression.  
Matches will be highlighted in red.
  - f. Did your regular expression identify the string?
    - o If yes, click **OK**.
    - o If no, verify that the Comparison Text contains the string you want to identify or modify the regular expression.

## Audit Inputs Editor

Using the Audit Inputs Editor, you can create or modify parameters for audit engines and checks that require inputs.

- To launch the tool, click **Audit Inputs Editor**.
- To load inputs that you previously created using the editor, click **Import Audit Inputs**.

### See Also

["Audit Settings: Attack Expressions" below](#)

["Audit Settings: Session Exclusions" on page 330](#)

["Audit Settings: Smart Scan" on page 339](#)

["Audit Settings: Vulnerability Filtering" below](#)

## Audit Settings: Attack Expressions

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Audit Settings** category, select **Attack Expressions**.

## Additional Regular Expression Languages

You may select one of the following language code-country code combinations (as used by the `CultureInfo` class in the .NET Framework Class Library):

- zh-cn: Chinese - China
- zh-tw: Chinese - Taiwan
- ja-jp: Japanese - Japan
- ko-kr: Korean - Korea
- es-mx: Spanish - Mexico

The `CultureInfo` class holds culture-specific information, such as the associated language, sublanguage, country/region, calendar, and cultural conventions. This class also provides access to culture-specific instances of `DateTimeFormatInfo`, `NumberFormatInfo`, `CompareInfo`, and `TextInfo`. These objects contain the information required for culture-specific operations, such as casing, formatting dates and numbers, and comparing strings.

### See Also

["Audit Settings: Attack Exclusions" on page 334](#)

["Audit Settings: Session Exclusions" on page 330](#)

["Audit Settings: Smart Scan" on page 339](#)

["Audit Settings: Vulnerability Filtering" below](#)

## Audit Settings: Vulnerability Filtering

To access this feature, click the **Edit** menu and select **Default Settings** or **Current Settings**. Then, in the **Audit Settings** category, select **Vulnerability Filtering**.

By applying certain filters, you can limit the display of certain vulnerabilities reported during a scan. The options are:

- **Standard Vulnerability Definition** - This filter sorts parameter names for determining equivalency between similar requests. For example, if a SQL injection vulnerability is found in parameter "a" in both `http://x.y?a=x;b=y` and `http://x.y?b=y;a=x`, it would be considered equivalent.
- **Parameter Vulnerability Roll-Up** - This filter consolidates multiple parameter manipulation and parameter injection vulnerabilities discovered during a single session into one vulnerability.
- **403 Blocker** - This filter revokes vulnerabilities when the status code of the vulnerable session is 403 (Forbidden).
- **Response Inspection DOM Event Parent-Child** - This filter disregards a keyword search vulnerability found in JavaScript if the same vulnerability has already been detected in the parent session.

## Adding a Vulnerability Filter

To add a filter to your default settings:

1. Click the **Edit** menu and select **Default Scan Settings**.
2. In the **Audit Settings** panel in the left column, select **Vulnerability Filtering**.

All available filters are listed in either the **Disabled Filters** list or the **Enabled Filters** list.

3. To enable a filter, select a filter in the **Disabled Filters** list and click **Add**.

The filter is removed from the **Disabled Filters** list and added to the **Enabled Filters** list.

4. To disable a filter, select a filter in the **Enabled Filters** list and click **Remove**.

The filter is removed from the **Enabled Filters** list and added to the **Disabled Filters** list.

You can also modify the settings for a specific scan by clicking the **Settings** button at the bottom of the Start an Advanced Scan window or the Perform a Web Service Scan window.

### See Also

["Audit Settings: Attack Exclusions" on page 334](#)

["Audit Settings: Attack Expressions" on the previous page](#)

["Audit Settings: Session Exclusions" on page 330](#)

["Audit Settings: Smart Scan" on the next page](#)

## Audit Settings: Smart Scan

To access this feature, click the **Edit** menu and select **Default Scan Settings** or **Current Scan Settings**. Then, in the **Audit Settings** category, select **Smart Scan**.

### Enable Smart Scan

Smart Scan is an "intelligent" feature that discovers the type of server that is hosting the Web site and checks for known vulnerabilities against that specific server type. For example, if you are scanning a site hosted on an IIS server, WebInspect will probe only for those vulnerabilities to which IIS is susceptible. It would not check for vulnerabilities that affect other servers, such as Apache or iPlanet.

If you select this option, you can choose one or more of the identification methods described below.

### Use regular expressions on HTTP responses

This method, employed by previous releases of WebInspect, searches the server response for strings that match predefined regular expressions designed to identify specific servers.

### Use server analyzer fingerprinting and request sampling

This advanced method sends a series of HTTP requests and then analyzes the responses to determine the server/application type.

### Custom server/application type definitions

If you know the server type for a target domain, you can select it using the **Custom server/application type definitions** section. This identification method overrides any other selected method for the server you specify.

1. Click **Add**.

The Server/Application Type Entry window opens.

2. In the **Host** box, enter the domain name or host, or the server's IP address.
3. (Optional) Click **Identify**.  
WebInspect contacts the server and uses the server analyzer fingerprinting method to determine the server type. If successful, it selects the corresponding check box in the **Server/Application Type** list.

**Note:** Alternatively, if you select the **Use Regular Expressions** option, enter a regular expression designed to identify a server. Click  to insert regular expression notations or to launch the Regular Expression Editor (which facilitates the creation and testing of an expression).

4. Select one or more entries from the **Server/Application Type** list.
5. Click **OK**.

#### See Also

- ["Audit Settings: Attack Exclusions" on page 334](#)
- ["Audit Settings: Attack Expressions" on page 337](#)
- ["Audit Settings: Session Exclusions" on page 330](#)
- ["Audit Settings: Vulnerability Filtering" on page 337](#)

# Application Settings: General

To access this feature, click **Edit > Application Settings** and then select **General**.

## General

The General options are described in the following table:

Option	Description
Enable Active Content in Browser Views	<p>Select this option to allow execution of JavaScript and other dynamic content in all browser windows within WebInspect.</p> <p>For example, one WebInspect attack tests for cross-site scripting by attempting to embed a script in a dynamically generated Web page. That script instructs the server to display an alert containing the number "76712." If active content is enabled and if the attack is successful (i.e., cross-site scripting is possible), then selecting the vulnerable session and clicking on <b>Web Browser</b> in the Session Info panel will execute the script and display the following:</p>  <p><b>Note:</b> If you initiate or open a scan while this option is disabled, and you then enable this option, the browser will not execute the active content until you close and then reopen the scan.</p>
Enable Diagnostic File Creation	<p>If the WebInspect application should ever fail, this option forces WebInspect to create a file containing data that was stored in main memory at the time of failure. The file can be transferred to HP support personnel using the HP Support Tool.</p> <p>If you select this option, you may also specify how many diagnostic files should be retained. When the number of files exceeds this limit, the oldest file will be deleted.</p>

Option	Description
Reset "Don't Show Me Again" messages	By default, WebInspect displays various prompts and dialogs to remind you of certain consequences that may occur as a result of an action you take. These dialogs contain a check box labeled "Don't show me again." If you select that option, WebInspect discontinues displaying those messages. You can force WebInspect to resume displaying those messages if you click <b>Reset "Don't Show Me Again" messages</b> .

Option	Description
Use Seven Pernicious Kingdom Taxonomy	<p>This option allows you to select The Seven Pernicious Kingdoms taxonomy for ordering and organizing the reported vulnerabilities.</p> <p>Seven Pernicious Kingdoms (7PK) is a taxonomy of software security errors developed by the Fortify Software Security Research Group together with Dr. Gary McGraw. Each vulnerability category is accompanied by a detailed description of the issue with references to original sources and code excerpts, where applicable, to better illustrate the problem.</p> <p>The organization of the classification scheme is described with the help of terminology borrowed from biology: vulnerability categories are referred to as phyla, while collections of vulnerability categories that share the same theme are referred to as kingdoms. Vulnerability phyla are classified into pernicious kingdoms presented in the order of importance to software security:</p> <p>The seven kingdoms are:</p> <ol style="list-style-type: none"> <li>1. Input Validation and Representation</li> <li>2. API Abuse</li> <li>3. Security Features</li> <li>4. Time and State</li> <li>5. Errors</li> <li>6. Code Quality</li> <li>7. Encapsulation</li> </ol> <p>The primary goal of defining this taxonomy is to organize sets of security rules that can be used to help software developers understand the kinds of errors that have an impact on security. By better understanding how systems fail, developers will better analyze the systems they create, more readily identify and address security problems when they see them, and generally avoid repeating the same mistakes in the future. For more information, see <a href="http://www.hpentersesecurity.com/vulncat/en/vulncat/index.html">http://www.hpentersesecurity.com/vulncat/en/vulncat/index.html</a>.</p> <p>You may want to use the Seven Pernicious Kingdoms taxonomy if you are integrating WebInspect with other HP Fortify products as it provides for a unified taxonomy.</p>

## WebInspect Agent

The WebInspect Agent options are described in the following table:

Option	Description
Use WebInspect Agent information when encountered on target site	<p>If this option is selected and WebInspect detects that HP WebInspect Agent is installed on a target server, it will incorporate WebInspect Agent information to improve overall scan efficiency.</p> <p>A notation on the WebInspect dashboard indicates whether or not WebInspect Agent has been detected.</p>
Automatically group by duplicate vulnerabilities in Vulnerability window	<p>If this option is selected and HP WebInspect Agent information is used (above setting), then vulnerabilities listed on the <b>Vulnerability</b> tab in the Summary pane will be grouped by check and then by equivalent vulnerabilities.</p>
Allow WebInspect Agent to Suggest Attack Strategy	<p>If this option is selected and HP WebInspect information is used (see <i>Use WebInspect Agent Information When Encountered on Target Site</i> above), the agent operates in an active mode and can suggest attack strategies to WebInspect to improve accuracy and performance. This feature requires version 4.1 or above of the WebInspect Agent and you must be using the <a href="#">Seven Pernicious Kingdoms</a> taxonomy.</p>

## See Also

- ["Application Settings: Database" below](#)
- ["Application Settings: Directories" on page 346](#)
- ["Application Settings: HP Quality Center" on page 364](#)
- ["Application Settings: IBM Rational ClearQuest" on page 366](#)
- ["Application Settings: License" on page 347](#)
- ["Application Settings: Logging" on page 352](#)
- ["Application Settings: Override SQL Database Settings" on page 361](#)
- ["Application Settings: Proxy" on page 353](#)
- ["Application Settings: Reports" on page 357](#)
- ["Application Settings: Run as a Sensor" on page 359](#)
- ["Application Settings: Server Profiler" on page 349](#)
- ["Application Settings: Smart Update" on page 362](#)
- ["Application Settings: Step Mode" on page 351](#)
- ["Application Settings: Support Channel" on page 363](#)

## Application Settings: Database

To access this feature, click **Edit > Application Settings** and then select **Database**.

## Connection Settings for Scan/Report Storage

Select the device that will store WebInspect scan and report data. The choices are:

- **Use SQL Server Express** (for SQL Server Express Edition). Data for each scan will be stored in a separate database. The maximum size is 4 GB (unless you are using SQL Server 2008 R2 Express, which has a maximum database storage of 10GB).
- **Use SQL Server** (for SQL Server Standard Edition). Data for multiple scans will be stored in a single database. You can configure multiple database settings and assign a "profile name" to each collection of settings, allowing you to switch easily from one configuration to another.

## Configuring SQL Server Standard Edition

To configure a profile for SQL Server Standard Edition:

1. Click **Configure** (to the right of the drop-down list).
2. On the Manage Database Settings window, click **Add**.
3. Enter a name for this database profile.
4. Select a server from the **Server Name** list.
5. In the **Log on to the server** group, specify the type of authentication used for the selected server:
  - **Use Windows Authentication** - Log on by submitting the user's Windows account name and password.
  - **Use SQL Server Authentication** - Use SQL Server authentication, which relies on the internal user list maintained by the SQL Server computer. Enter the user name and password.
6. Enter or select a specific database, or click **New** to create a database.
7. Click **OK** to close the Add Database window.
8. Click **OK** to close the Manage Database Settings window.

## Connection Settings for Scan Viewing

When displaying a list of scans (using either the Manage Scans view or the Report Generator wizard), WebInspect can access scan data stored in SQL Server Standard Edition and/or SQL Server Express Edition. You can select either or both options.

- **Show Scans Stored in SQL Server Express:** Select this option if you want to access scan data stored in a local SQL Server Express Edition.
- **Show Scans Stored in SQL Server Standard:** Select this option if you want to access data in SQL Server Standard Edition. See [Configuring SQL Server Standard Edition](#) (above) for instructions.

#### See Also

- "Application Settings: Directories" below
- "Application Settings: General" on page 341
- "Application Settings: HP Quality Center" on page 364
- "Application Settings: IBM Rational ClearQuest" on page 366
- "Application Settings: License" on the next page
- "Application Settings: Logging" on page 352
- "Application Settings: Override SQL Database Settings" on page 361
- "Application Settings: Proxy" on page 353
- "Application Settings: Reports" on page 357
- "Application Settings: Run as a Sensor" on page 359
- "Application Settings: Server Profiler" on page 349
- "Application Settings: Smart Update" on page 362
- "Application Settings: Step Mode" on page 351
- "Application Settings: Support Channel" on page 363

## Application Settings: Directories

To access this feature, click **Edit > Application Settings** and then select **Directories**.

## Changing Where WebInspect Files Are Saved

You can change the locations in which WebInspect files are saved.

1. Click the ellipsis button  next to a category of information.
2. Use the Browse For Folder window to select or create a directory.
3. Click **OK**.

#### See Also

- "Application Settings: Database" on page 344
- "Application Settings: General" on page 341
- "Application Settings: HP Quality Center" on page 364
- "Application Settings: IBM Rational ClearQuest" on page 366
- "Application Settings: License" below
- "Application Settings: Logging" on page 352
- "Application Settings: Override SQL Database Settings" on page 361
- "Application Settings: Proxy" on page 353
- "Application Settings: Reports" on page 357
- "Application Settings: Run as a Sensor" on page 359
- "Application Settings: Server Profiler" on page 349
- "Application Settings: Smart Update" on page 362
- "Application Settings: Step Mode" on page 351
- "Application Settings: Support Channel" on page 363

## Application Settings: License

To access this feature, click **Edit > Application Settings** and then select **License**.

### License Details

This section provides pertinent information about the WebInspect license. If you want to change certain provisions of the license, click **Configure Licensing**, which will invoke the HP License Wizard.

The contents of the lower section of the window depend on the type of license management currently employed:

- Connected directly to the HP license server
- Connected to a local License and Infrastructure Manager (LIM).

### Direct Connection to HP

Options are described in the following table:

Option	Description
Update	If you upgrade from a trial version or if you otherwise modify the conditions of your license, click <b>Update</b> . The application will contact the license server and update the information stored locally on your machine.
Deactivate	WebInspect licenses are assigned to specific computers. If you would like to transfer this license to a different computer: <ol style="list-style-type: none"> <li>1. Copy the activation token. Take care not to lose or misplace this number. Write it or print it, and keep it in a safe place.</li> <li>2. Click <b>Deactivate</b>. The application will contact the license server and release your license, allowing you to install WebInspect on another computer.</li> <li>3. At the new computer, access the WebInspect application settings for licensing and enter the activation token.</li> </ol>

## Connection to LIM

Select the manner in which you want the License and Infrastructure Manager to handle the WebInspect license assigned to this computer. Options are described in the following table:

Option	Description
Connected License	The computer can run the HP product only when the computer is able to contact the LIM. Each time you start the HP software, the LIM allocates a seat from the license pool to this installation. When you close the software, the seat is released from the computer and allocated back to the pool, allowing another user to consume the license.
Detached License	The computer can run the HP product anywhere, even when disconnected from your corporate intranet (on which the LIM is normally located), but only until the expiration date you specify. This allows you to take your laptop to a remote site and run the HP software. When you reconnect to the corporate intranet, you can access the Application License settings and reconfigure from Detached to Connected.

### See Also

- "Application Settings: Database" on page 344
- "Application Settings: Directories" on page 346
- "Application Settings: General" on page 341
- "Application Settings: HP Quality Center" on page 364

- "Application Settings: IBM Rational ClearQuest" on page 366
- "Application Settings: Logging" on page 352
- "Application Settings: Override SQL Database Settings" on page 361
- "Application Settings: Proxy" on page 353
- "Application Settings: Reports" on page 357
- "Application Settings: Run as a Sensor" on page 359
- "Application Settings: Server Profiler" below
- "Application Settings: Smart Update" on page 362
- "Application Settings: Step Mode" on page 351
- "Application Settings: Support Channel" on page 363

## Application Settings: Server Profiler

To access this feature, click **Edit > Application Settings** and then select **Server Profiler**.

Before starting a scan, WebInspect can invoke the Server Profiler to conduct a preliminary examination of the target Web site to determine if certain scan settings should be modified. If changes appear to be required, the Server Profiler returns a list of suggestions, which you may accept or reject.

To enable this preliminary examination, click **Profile** (or select **Run Profiler Automatically**) on Step 4.

By default, 10 specific modules are enabled. To exclude a module, clear its associated check box.

## Modules

The Server Profiler modules are described in the following table:

Module	Description
Check for case-sensitive servers	This module determines if the host server is case-sensitive when discriminating among URLs. For example, some servers (such as IIS) do not differentiate between www.mycompany.com/samplepage.htm and www.mycompany.com/SamplePage.htm. If the profiler determines that the server is not case-sensitive, you can disable WebInspect's case-sensitive feature, which would improve the speed and accuracy of the crawl.

Module	Description
Check 'Maximum Folder Depth' setting	The maximum folder depth setting is intended primarily for sites that programmatically append subfolders to URLs. Without such a limit, WebInspect would endlessly crawl these dynamic folders. This module determines if the site contains valid URLs that extend beyond that limit and, if so, allows you to increase the setting.
Verify client authentication protocol	This module determines which authentication (sign-in) protocol, if any, is required. WebInspect supports HTTP Basic, NTLM, Digest, Kerberos.
Check for additional hosts	This module searches the target site for references to additional host servers and allows you to include them as allowed hosts.
Reveal navigation parameters	This module determines if the target site uses query parameters in URLs to specify the content of the page and, if so, displays a list of parameters and values that were encountered during the analysis. You can select one or more parameters for WebInspect to use during the scan.
Check for non-standard 'file not found' responses	This module determines if a site returns a response code other than 404 when the client requests a non-existent resource. Recognizing this will prevent WebInspect from auditing non-essential responses.
Check for session state embedded in URLs	Instead of using cookies, some servers embed session state in URLs. WebInspect detects this practice by analyzing the URL with regular expressions. This module attempts to determine if changes to the regular expressions are required.
Analyze thread count	This module determines if the thread count should be lowered. Relatively high thread counts, while enabling a faster scan, can sometimes exhaust server resources.
Check for invalid audit exclusions	WebInspect settings prevent pages with certain file extensions from being audited (see <a href="#">Audit Settings: Session Exclusions</a> ). The specified extensions are for pages that ordinarily do not have query parameters in the URL of the request. If the settings are incorrect, the audit will not be as thorough. The profiler can detect when pages having audit-excluded extensions actually contain query parameters and will recommend removing those exclusions.
Verify maximum response size	A WebInspect scan setting specifies the maximum response size allowed; the default is 1,000 kilobytes. This module attempts to detect responses larger than the maximum and, if found, recommends that you increase the limit.
Optimize settings for specific applications	This module determines if you are scanning a well-known test site (such as WebGoat, Hacme Bank, etc.) and determines if WebInspect has a prepopulated settings file (a template) designed specifically for that site. These templates are configured to optimize the crawl, audit, and performance of your scans.

Module	Description
Add/Remove Trailing Slash	This module determines if the target site requires or prohibits a trailing slash on the start URL.
Check for cross-site request forgery	Cross-site request forgery, also known as a one-click attack or session riding, is often abbreviated as CSRF. CSRF is a type of website exploit where unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting, which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser. For more on CSRF, see <a href="#">CSRF</a> .
Check for WebSphere servers	WebSphere servers require additional settings changes; enables the Profiler to detect these changes are required.

## See Also

- ["Application Settings: Database" on page 344](#)
- ["Application Settings: Directories" on page 346](#)
- ["Application Settings: General" on page 341](#)
- ["Application Settings: HP Quality Center" on page 364](#)
- ["Application Settings: IBM Rational ClearQuest" on page 366](#)
- ["Application Settings: License" on page 347](#)
- ["Application Settings: Logging" on the next page](#)
- ["Application Settings: Override SQL Database Settings" on page 361](#)
- ["Application Settings: Proxy" on page 353](#)
- ["Application Settings: Reports" on page 357](#)
- ["Application Settings: Run as a Sensor" on page 359](#)
- ["Application Settings: Smart Update" on page 362](#)
- ["Application Settings: Step Mode" below](#)
- ["Application Settings: Support Channel" on page 363](#)

## Application Settings: Step Mode

To access this feature, click **Edit > Application Settings** and then select **Step Mode**.

Options for Step Mode are described in the following table:

Option	Description
Default Audit Mode	<p>Select one of the following choices:</p> <ul style="list-style-type: none"> <li>• <b>Audit as you browse:</b> While you are navigating a target Web site, WebInspect concurrently audits the pages you visit.</li> <li>• <b>Manual Audit:</b> This option allows you to pause the Step Mode scan and return to WebInspect, where you can select a specific session and audit it.</li> </ul>
Proxy Listener	<p>Select the following options:</p> <ul style="list-style-type: none"> <li>• <b>Local IP Address:</b> Step Mode requires a proxy. Specify the IP address that the proxy should use.</li> <li>• <b>Port:</b> Specify the port that the proxy should use, or select <b>Automatically Assign Port</b>.</li> </ul>

## See Also

- ["Application Settings: Database" on page 344](#)
- ["Application Settings: Directories" on page 346](#)
- ["Application Settings: General" on page 341](#)
- ["Application Settings: HP Quality Center" on page 364](#)
- ["Application Settings: IBM Rational ClearQuest" on page 366](#)
- ["Application Settings: License" on page 347](#)
- ["Application Settings: Logging" below](#)
- ["Application Settings: Override SQL Database Settings" on page 361](#)
- ["Application Settings: Proxy" on the next page](#)
- ["Application Settings: Reports" on page 357](#)
- ["Application Settings: Run as a Sensor" on page 359](#)
- ["Application Settings: Server Profiler" on page 349](#)
- ["Application Settings: Smart Update" on page 362](#)
- ["Application Settings: Support Channel" on page 363](#)

## Application Settings: Logging

To access this feature, click **Edit > Application Settings** and then select **Logging**.

The Logging options are described in the following table:

Option	Description
Clear Logs	Click this button to clear all logs.
Minimum Logging Level	Specify how WebInspect should log different functions and events that occur within the application. The choices are (from most verbose to least verbose) Debug, Info, Warn, Error, and Fatal.
Threshold for Log Purging	If you do not select <b>Never Purge</b> , WebInspect deletes all logs when either the total amount of disk space used by all logs exceeds the size you specify or the number of logs exceeds the number you specify. Alternatively, you can elect to <b>Never Purge</b> log files.
Rolling Log File Maximum Size	Specify the maximum size (in kilobytes) that any log file may attain. When a file reaches this limit, WebInspect simply stops writing to it.

## See Also

- ["Application Settings: Database" on page 344](#)
- ["Application Settings: Directories" on page 346](#)
- ["Application Settings: General" on page 341](#)
- ["Application Settings: HP Quality Center" on page 364](#)
- ["Application Settings: IBM Rational ClearQuest" on page 366](#)
- ["Application Settings: License" on page 347](#)
- ["Application Settings: Override SQL Database Settings" on page 361](#)
- ["Application Settings: Proxy" below](#)
- ["Application Settings: Reports" on page 357](#)
- ["Application Settings: Run as a Sensor" on page 359](#)
- ["Application Settings: Server Profiler" on page 349](#)
- ["Application Settings: Smart Update" on page 362](#)
- ["Application Settings: Step Mode" on page 351](#)
- ["Application Settings: Support Channel" on page 363](#)

## Application Settings: Proxy

To access this feature, click **Edit > Application Settings** and then select **Proxy Settings**.

WebInspect Web services are used for update and support communications. Configure how these services are accessed in the Proxy Settings.

## Not Using a Proxy Server

If you are not using a proxy server to access these services, select **Direct Connection (proxy disabled)**.

## Using a Proxy Server

If you are required to use a proxy server to access these services, select an option as described in the following table.

Option	Description
Auto detect proxy settings	Use the Web Proxy Autodiscovery (WPAD) protocol to locate a proxy autoconfig file and configure the browser's Web proxy settings.
Use Internet Explorer proxy settings	Import your proxy server information from Internet Explorer. Electing to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy will not be used. To access browser proxy settings in Internet Explorer, go to <b>Tools &gt; Internet Options &gt; Connections &gt; LAN Settings</b> .
Use Firefox proxy settings	Import your proxy server information from Firefox. Electing to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," then a proxy will not be used. To access browser proxy settings in Firefox, go to <b>Tools &gt; Options &gt; Advanced &gt; Network &gt; Settings</b> .
Configure a proxy using a PAC file	Load proxy settings from a Proxy Automatic Configuration (PAC) file in the location you specify in the <b>URL</b> box.
Explicitly configure proxy	Configure a proxy by entering the requested information. See " <a href="#">Configuring a Proxy</a> " below in this topic.

## Configuring a Proxy

To configure a proxy:

1. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080).
2. From the **Type** list, select a protocol for handling TCP traffic through a proxy server: SOCKS4,

SOCKS5, or standard.

**Important:** Smart Update is not available if you use a SOCKS4 or SOCKS5 proxy server configuration. Smart Update is available only when using a standard proxy server.

3. If authentication is required, select a type from the **Authentication** list:

Automatic

Allow WebInspect to determine the correct authentication type.

**Note:** Automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.

Digest

The Windows Server operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.

HTTP Basic

A widely used, industry-standard method for collecting user name and password information.

- a. The Web browser displays a window for a user to enter a previously assigned user name and password, also known as credentials.
- b. The Web browser then attempts to establish a connection to a server using the user's credentials.
- c. If a user's credentials are rejected, the browser displays an authentication window to re-enter the user's credentials. Internet Explorer allows the user three connection attempts before failing the connection and reporting an error to the user.
- d. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established.

The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that Web browsers using Basic authentication transmit passwords in an unencrypted form. By monitoring communications on your network, an attacker can easily intercept and decode these passwords using publicly available tools. Therefore, Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.

NT LAN Manager (NTLM)

NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT

family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and WebInspect has to pass through a proxy server to submit its requests to the Web server, WebInspect may not be able to crawl or audit that Web site. Use **caution** when configuring WebInspect for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

#### Kerberos

Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.

#### Negotiate

The Negotiate authentication protocol begins with the option to negotiate for an authentication protocol. When the client requests access to a service, the server replies with a list of authentication protocols that it can support and an authentication challenge based on the protocol that is its first choice.

For example, the server might list Kerberos and NTLM, and send a Kerberos challenge. The client examines the contents of the reply and checks to determine whether it supports any of the specified protocols. If the client supports the preferred protocol, authentication proceeds. If the client does not support the preferred protocol, but does support one of the other protocols listed by the server, the client lets the server know which authentication protocol it supports, and the authentication proceeds. If the client does not support any of the listed protocols, the authentication exchange fails.

4. If your proxy server requires authentication, enter the qualifying user name and password.

#### See Also

- ["Application Settings: Database" on page 344](#)
- ["Application Settings: Directories" on page 346](#)
- ["Application Settings: General" on page 341](#)
- ["Application Settings: HP Quality Center" on page 364](#)
- ["Application Settings: IBM Rational ClearQuest" on page 366](#)
- ["Application Settings: License" on page 347](#)
- ["Application Settings: Logging" on page 352](#)
- ["Application Settings: Override SQL Database Settings" on page 361](#)
- ["Application Settings: Reports" on the next page](#)
- ["Application Settings: Run as a Sensor" on page 359](#)

"Application Settings: Server Profiler" on page 349

"Application Settings: Smart Update" on page 362

"Application Settings: Step Mode" on page 351

"Application Settings: Support Channel" on page 363

## Application Settings: Reports

To access this feature, click **Edit > Application Settings** and then select **Reports**.

### Options

The Reports options are described in the following table:

Option	Description
Always prompt to save favorites	A "favorite" is simply a named collection of one or more reports and their associated parameters. When using the Report Generator, you can select reports and parameters, and then select <b>Favorites &gt; Add to favorites</b> to create the combination. If you select this option, then WebInspect will prompt you to save the favorite whenever you modify it by adding or removing a report.

Option	Description
	<p>Smart truncate vulnerability text</p> <p>Generated reports can contain very lengthy HTTP request and response messages. To save space and help focus on the pertinent data related to a vulnerability, you can exclude message content that precedes and follows the data that identifies or confirms the vulnerability (identified by red highlighting).</p> <p>The following example illustrates the report of a cross-site scripting vulnerability using "smart" truncation and a padding size of 20 characters. The complete header is always reported. The remaining message text is deleted, except for the vulnerability and the 20 characters preceding it and the 20 characters following it. The retained text is then bracketed by the notation "...TRUNCATED..." to indicate that truncation has occurred. Note that the length of the original message was 2,377 characters (Content-Length: 2377).</p> <p><b>Response:</b></p> <pre>HTTP/1.1 200 OK Date: Tue, 04 Aug 2009 17:35:10 GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET Content-Length: 2377 Content-Type: text/html Cache-control: private  ...TRUNCATED...1&gt;Household Checking&lt;script&gt;alert(53316)&lt;/script&gt;&lt;/td&gt; &lt;/tr&gt;  &lt;tr&gt;...TRUNCATED...</pre> <p>To use smart truncation in reports, select <b>Smart truncate vulnerability text</b> and then specify the number of characters to retain preceding and following the data that identifies or confirms the vulnerability. A maximum of 10 vulnerabilities can be reported in a single request or response.</p> <p><b>Note:</b> This feature functions as described only if the report controls containing the RequestText and ResponseText data fields have the TruncateVulnerability property set to True and the MaxLength property set to zero. If TruncateVulnerability is set to True and the MaxLength property is nonzero, then the application setting for padding size is overridden by the MaxLength value.</p>

## Headers and Footers

Select a template containing the headers and footers to be used by default on all reports. Also, if necessary, enter the requested parameters.

The WebInspect Master Report uses three images to create a report.

- The cover page image appears in the center of the cover page, with the top of the image approximately 3.5 inches from the top.
- The header logo image appears on the left side of the header on every page.

## See Also

- ["Application Settings: Database" on page 344](#)
- ["Application Settings: Directories" on page 346](#)
- ["Application Settings: General" on page 341](#)
- ["Application Settings: HP Quality Center" on page 364](#)
- ["Application Settings: IBM Rational ClearQuest" on page 366](#)
- ["Application Settings: License" on page 347](#)
- ["Application Settings: Logging" on page 352](#)
- ["Application Settings: Override SQL Database Settings" on page 361](#)
- ["Application Settings: Proxy" on page 353](#)
- ["Application Settings: Run as a Sensor" below](#)
- ["Application Settings: Server Profiler" on page 349](#)
- ["Application Settings: Smart Update" on page 362](#)
- ["Application Settings: Step Mode" on page 351](#)
- ["Application Settings: Support Channel" on page 363](#)

## Application Settings: Run as a Sensor

To access this feature, click **Edit > Application Settings** and then select **Run as a Sensor**.

### Sensor

This configuration information is used for integrating WebInspect into WebInspect Enterprise as a sensor. After providing the information and starting the sensor service, you should conduct scans using the WebInspect Enterprise console, not the WebInspect graphical user interface.

The following table describes the options:

Option	Description
Manager URL	Enter the URL or IP address of the WebInspect Enterprise Manager.

Option	Description
Sensor Authentication	Enter a user name (formatted as domain\username) and password, then click <b>Test</b> to verify the entry.
Enable Proxy	If WebInspect must go through a proxy server to reach the WebInspect Enterprise manager, select <b>Enable Proxy</b> and then provide the IP address and port number of the server. If authentication is required, enter a valid user name and password.
Override Database Settings	WebInspect normally stores scan data in the device you specify in the <a href="#">Application Settings for Database Connectivity</a> . However, if WebInspect is connected to WebInspect Enterprise as a sensor, you can select this option and then click <b>Configure</b> to specify an alternative device.
Service Account	<p>Select one of the following options to specify the account under which the service should run:</p> <ul style="list-style-type: none"> <li>• <b>Local system account:</b> The LocalSystem account is a predefined local account used by the service control manager. The service has complete unrestricted access to local resources.</li> <li>• <b>This account:</b> Identify the account and provide the password.</li> </ul>
Sensor Status	<p>This area displays the current status of the Sensor Service and provides buttons allowing you to start or stop the service.</p> <p>After configuring WebInspect as a sensor, click <b>Start</b>.</p> <p><b>Note:</b> Normally, when WebInspect is configured as a sensor, launching WebInspect as a standalone application halts the Sensor Service. When you subsequently close WebInspect, the service restarts, placing WebInspect once again under the control of the WebInspect Enterprise manager. However, if you conduct a Smart Update while WebInspect is running as a standalone application, the service will not restart automatically. You must click the <b>Start</b> button (or right-click the HP Fortify icon in the notification area of the taskbar and select <b>Start Sensor</b>).</p>

## See Also

- ["Application Settings: Database" on page 344](#)
- ["Application Settings: Directories" on page 346](#)
- ["Application Settings: General" on page 341](#)
- ["Application Settings: HP Quality Center" on page 364](#)
- ["Application Settings: IBM Rational ClearQuest" on page 366](#)
- ["Application Settings: License" on page 347](#)
- ["Application Settings: Logging" on page 352](#)

"Application Settings: Override SQL Database Settings" below

"Application Settings: Proxy" on page 353

"Application Settings: Reports" on page 357

"Application Settings: Server Profiler" on page 349

"Application Settings: Smart Update" on the next page

"Application Settings: Step Mode" on page 351

"Application Settings: Support Channel" on page 363

## Application Settings: Override SQL Database Settings

To access this feature, click **Edit > Application Settings > Run as a Sensor > Configure**.

### Override Database Settings

WebInspect normally stores scan data in the device you specify in the [Application Settings for Database Connectivity](#). However, if WebInspect is connected to WebInspect Enterprise as a sensor, you can select this option and then click **Configure** to specify an alternative device.

### Configure SQL Database

To configure SQL Database settings for WebInspect as a sensor:

1. On the Application Settings page, select **Override Database Settings**, and then click **Configure**.
2. In the SQL Settings dialogue that appears, select one of the following options:
  - **Use SQL Server Express**
  - **Use SQL Server**
3. If you selected **Use SQL Server Express**, click **OK** to complete the task and return to the Application Settings screen.
4. If you selected **Use SQL Server**, then type the **Server Name** or select a Server Name from the list.
5. To update the server name, click **Refresh**.
6. In the Log on to the server area, select one of the following authentication options:

- **Use Windows Authentication**
  - **Use SQL Server Authentication**
7. Type the **User name** and **Password** to log on to the server. In the Connect to a Database area, **Select or enter a database name** from the list, or click **New** to browse to a database.
  8. Click **OK**.

#### See Also

- ["Application Settings: Database" on page 344](#)
- ["Application Settings: Directories" on page 346](#)
- ["Application Settings: General" on page 341](#)
- ["Application Settings: HP Quality Center" on page 364](#)
- ["Application Settings: IBM Rational ClearQuest" on page 366](#)
- ["Application Settings: License" on page 347](#)
- ["Application Settings: Logging" on page 352](#)
- ["Application Settings: Proxy" on page 353](#)
- ["Application Settings: Reports" on page 357](#)
- ["Application Settings: Run as a Sensor" on page 359](#)
- ["Application Settings: Server Profiler" on page 349](#)
- ["Application Settings: Smart Update" below](#)
- ["Application Settings: Step Mode" on page 351](#)
- ["Application Settings: Support Channel" on the next page](#)

## Application Settings: Smart Update

To access this feature, click **Edit > Application Settings** and then select **Smart Update**.

## Options

The Smart Update Options are described in the following table:

Option	Description
Service	Enter the URL for the WebInspect Smart Update service. The default is: <a href="https://smartupdate.hpsmartupdate.com/">https://smartupdate.hpsmartupdate.com/</a>
Enable Smart Update on Startup	Select this option to check for updates automatically when starting WebInspect.

## See Also

- ["Application Settings: Database" on page 344](#)
- ["Application Settings: Directories" on page 346](#)
- ["Application Settings: General" on page 341](#)
- ["Application Settings: HP Quality Center" on the next page](#)
- ["Application Settings: IBM Rational ClearQuest" on page 366](#)
- ["Application Settings: License" on page 347](#)
- ["Application Settings: Logging" on page 352](#)
- ["Application Settings: Override SQL Database Settings" on page 361](#)
- ["Application Settings: Proxy" on page 353](#)
- ["Application Settings: Reports" on page 357](#)
- ["Application Settings: Run as a Sensor" on page 359](#)
- ["Application Settings: Server Profiler" on page 349](#)
- ["Application Settings: Step Mode" on page 351](#)
- ["Application Settings: Support Channel" below](#)

## Application Settings: Support Channel

To access this feature, click **Edit > Application Settings** and then select **Support Channel**.

The WebInspect support channel allows WebInspect to send data to and download messages from Hewlett-Packard. It is used primarily for sending logs and "false positive" reports and for receiving "What's New" notices.

## Opening the Support Channel

Select the **Allow connection to Hewlett-Packard** option to open the WebInspect support channel. You may then specify the following:

- Support Channel URL - The default is:

`https://SupportChannel.HPSmartUpdate.com/SupportChannel/service.asmx`

- Upload Directory - The default is:

`C:\ProgramData\HP\HP WebInspect\SupportChannel\Upload\`

- Download Directory - The default is:

`C:\ProgramData\HP\HP WebInspect\SupportChannel\Download\`

## See Also

["Application Settings: Database" on page 344](#)

["Application Settings: Directories" on page 346](#)

["Application Settings: General" on page 341](#)

["Application Settings: HP Quality Center" below](#)

["Application Settings: IBM Rational ClearQuest" on page 366](#)

["Application Settings: License" on page 347](#)

["Application Settings: Logging" on page 352](#)

["Application Settings: Override SQL Database Settings" on page 361](#)

["Application Settings: Proxy" on page 353](#)

["Application Settings: Reports" on page 357](#)

["Application Settings: Run as a Sensor" on page 359](#)

["Application Settings: Server Profiler" on page 349](#)

["Application Settings: Smart Update" on page 362](#)

["Application Settings: Step Mode" on page 351](#)

# Application Settings: HP Quality Center

To access this feature, click **Edit > Application Settings** and then select **HP Quality Center**.

To integrate WebInspect with HP Quality Center, you must create one or more profiles that describe the Quality Center server, project, defect priority, and other attributes. You can then convert a WebInspect vulnerability to a Quality Center defect and add it to the Quality Center database.

## Running HP Quality Center and WebInspect on the Same Machine

If you intend to run HP Quality Center and WebInspect on the same machine, then before creating a profile, you must download the HP Quality Center client application. To do so, simply open your Web browser and enter the Quality Center URL in the Address bar; then click the Quality Center link and log in. This prerequisite does not apply if you are connecting to Quality Center version 11, also known as Application Lifecycle Management (ALM).

## Quality Center License Usage

Creating or editing a profile consumes a license issued to Quality Center. The license is released, however, when the HP Quality Center application settings are closed. Similarly, sending a vulnerability to Quality Center consumes a license, but it is released after the vulnerability is sent.

## Before You Begin

Make sure that the HP ALM Client Registration Add-in is installed on the same machine as WebInspect before creating a profile. Refer to your HP ALM documentation for more details.

## Creating a Profile

Follow the steps below to add a profile.

1. Click **Add**, and then enter a profile name in the Add Profile window.
2. Enter or select the URL of a Quality Center server. If you haven't previously visited a Quality Center site, the list is empty. To enter a URL, use the format `http://<qc-server>/qcbin/`. Do not append "start\_a.htm" (or other file name) to the URL.
3. Enter the user name and password that will allow you to access the server, and then click **Authenticate**.

If the authentication credentials are accepted, the server populates the **Domain** and **Project** lists.

4. Click **Connect**, and then select a subject in the **Defect Reporting** group.
5. From the **Defect priority** list, select a priority that will be assigned to all WebInspect vulnerabilities reported to Quality Center using this profile.
6. Use the **Assign defects to** list to select the person to whom the defect will be assigned, and then

select an entry from the **Project found in** list.

7. Use the remaining lists to map the WebInspect vulnerability rating to an HP Quality Center defect rating. If you select **Do Not Publish**, the vulnerability will not be exported. You must select at least one of the file mappings.
8. To export notes and screenshots associated with a WebInspect vulnerability, select **Upload vulnerability attachments to defect**.
9. In the **Required/Optional Fields** group, double-click an entry and enter or select the requested information. If you try to save your work without supplying a required field, WebInspect prompts you to enter it.

#### See Also

- ["Application Settings: Database" on page 344](#)
- ["Application Settings: Directories" on page 346](#)
- ["Application Settings: General" on page 341](#)
- ["Application Settings: IBM Rational ClearQuest" below](#)
- ["Application Settings: License" on page 347](#)
- ["Application Settings: Logging" on page 352](#)
- ["Application Settings: Override SQL Database Settings" on page 361](#)
- ["Application Settings: Proxy" on page 353](#)
- ["Application Settings: Reports" on page 357](#)
- ["Application Settings: Run as a Sensor" on page 359](#)
- ["Application Settings: Server Profiler" on page 349](#)
- ["Application Settings: Smart Update" on page 362](#)
- ["Application Settings: Step Mode" on page 351](#)
- ["Application Settings: Support Channel" on page 363](#)

## Application Settings: IBM Rational ClearQuest

To access this feature, click **Edit > Application Settings** and then select **IBM Rational ClearQuest**.

To integrate WebInspect with IBM Rational ClearQuest, you must create one or more profiles that describe the server, project, defect priority, and other attributes. IBM Rational ClearQuest must be installed before you can complete this form.

## Creating a Profile

1. Click **Add**.
2. Enter a profile name and click **OK**. Enter a database set (or accept the default).
3. Select a database set from the list (or accept the default).
4. Select a database from the **Database** list (or accept the default).
5. Enter your credentials in the **User Name** and **Password** boxes.
6. Click **Authenticate**.

If successful, the Defect Reporting section becomes enabled.

7. Complete the fields in the Defect Reporting section. You must select at least one of the five "map to" categories.
  - a. In the **Headline Prefix** box, enter a text string that will be prepended to the title of each WebInspect vulnerability.
  - b. From the **Owner** list, select the person to whom the defect will be assigned.
  - c. Select a project from the **Project** list.
  - d. From the **Priority** list, select a priority that will be assigned to all WebInspect vulnerabilities reported to Rational ClearQuest using this profile.
  - e. WebInspect ranks vulnerabilities as either critical, high, medium, low, or informational. Use the **Map <severity> Risks to** lists to specify how these ratings should be equated to those used by Rational ClearQuest. The default selection is "Do Not Publish."
  - f. Edit the Mandatory/Optional fields. Click an entry in the **Value** column to open the appropriate editor. Any field that contains "Mandatory" in the **Requiredness** column must have a value specified. If you try to save your work without supplying a mandatory field, WebInspect prompts you to enter it.

**Note:** For lists that are not limited, the editor displays a checked list box; you can add items to the list by checking **Add New Item** (at the bottom). For the Date/Time editor, both date and time are displayed, regardless of the actual IBM Rational ClearQuest usage (which could be date, time, or date/time).

### See Also

["Application Settings: Database" on page 344](#)

["Application Settings: Directories" on page 346](#)

- "Application Settings: General" on page 341
- "Application Settings: HP Quality Center" on page 364
- "Application Settings: License" on page 347
- "Application Settings: Logging" on page 352
- "Application Settings: Override SQL Database Settings" on page 361
- "Application Settings: Proxy" on page 353
- "Application Settings: Reports" on page 357
- "Application Settings: Run as a Sensor" on page 359
- "Application Settings: Server Profiler" on page 349
- "Application Settings: Smart Update" on page 362
- "Application Settings: Step Mode" on page 351
- "Application Settings: Support Channel" on page 363

# Scan Log Messages

This topic describes the message that appear in the scan log. Messages are arranged alphabetically.

Audit Engine Initialization Error

## Full Message

Audit Engine initialization error, engine:%engine%, error:%error%"

## Description

An unrecoverable error occurred while attempting to initialize an audit engine. Contact HP Support.

## Argument Descriptions

Engine: The engine that was attempting to initialize.

Error: The actual error that occurred.

## Possible Fixes

Not Applicable

## External Links

Not Applicable

Auditor Error

## Full Message

Error: Auditor error, session: <session ID> engine:<engine>, error:<error>

## Description

An error occurred during an audit.

## Argument Descriptions

Session: The session being audited when the error occurred.

Engine: The engine being run when the error occurred.

Error: The actual error that occurred.

## Possible Fixes

Not Applicable

## External Links

Not Applicable

Auditor Skipping Session

## Full Message

Warn:Auditor skipping Session: 8BE3AFEC5051507168B66AEC59C8915B

### Description

A session was skipped due to the **Skip** button.

### Argument Descriptions

Session: Session ID of the session being skipped.

### Possible Fixes

Not Applicable

### External Links

Not Applicable

Check Error

### Full Message

Error: Check error, session:8BE3AFEC5051507168B66AEC59C8915B, Check:10346, engine: SPI.Scanners.Web.Audit.Engines.RequestModify

### Description

An error occurred while processing a check.

### Argument Descriptions

Session: Session where the check error occurred.

Check: The check that encountered the problem.

Engine: The engine being run when the error occurred.

Error: The error.

### Possible Fixes

Install the latest version of SmartUpdate.

### External Links

Not Applicable

Completed Post-Scan Analysis Module

### Full Message

Completed Post-Scan Analysis Module: %module%

### Description

One of the post-scan analysis modules has ended.

### Argument Descriptions

module: the name of the post-scan analysis module.

### Possible Fixes

Not Applicable

**External Links**

Not Applicable

Concurrent Crawl and Audit Start

**Full Message**

Info:Concurrent Crawl and Audit Start

**Description**

This message indicates that Concurrent Crawl and Audit has started.

**Argument Descriptions**

Not applicable

**Possible Fixes**

Not Applicable

**External Links:**

Not Applicable

Concurrent Crawl and Audit Stop

**Full Message**

Info:Concurrent Crawl and Audit Stop

**Description**

This message indicates that Concurrent Crawl and Audit has stopped.

**Argument Descriptions**

Not applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Concurrent Crawl Start

**Full Message**

Info:Concurrent Crawl Start:

**Description**

This message indicates that Concurrent Crawl has started.

**Argument Descriptions**

Not applicable

### Possible Fixes

Not Applicable

### External Links

Not Applicable

Concurrent Crawl Stop

### Full Message

Info:Concurrent Crawl Stop

### Description

This message indicates that Concurrent Crawl has stopped.

### Argument Descriptions

Not applicable

### Possible Fixes

Not Applicable

### External Links

Not Applicable

Connectivity Issue, Reason

### Full Message

Connectivity issue, Reason: FirstRequestFailed, HTTP Status:404,

**Description** This message indicates a network connectivity issue. WebInspect was unable to communicate with the remote host.

### Argument Descriptions

Reason: FirstRequestFailed - a requested has failed.

HTTP Status: 404 - The status returned for the failed request.

### Possible Fixes

- Power cycle your network hardware

If the issue persists, unplug your modem and router, wait a few seconds, then plug them back in. Sometimes, these devices simply need to be refreshed. This could be due to a network outage or improperly configured network settings.

- Use Microsoft's network diagnostic tools

Open Network Diagnostics by right-clicking the network icon in the notification area, and then clicking Diagnose and repair.

- Check wiring

Make sure that all wires are connected properly.

- Check host's power

If you're trying to connect to another computer, make sure that computer is powered on.

- Check connection settings

If the problem began after you installed new software, check your connection settings to see if they have been changed. Open Network Connections by clicking the Start button , clicking Control Panel, clicking Network and Internet, clicking Network and Sharing Center, and then clicking Manage network connections. Right-click the connection, and then click Properties. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

- Troubleshoot all Firewalls

#### **External Links:**

[Troubleshoot network connection problems](#)

[Internet Connectivity Evaluation Tool](#)

[Connectivity Issue, Reason, Error](#)

#### **Full Message**

Connectivity issue, Reason:FirstRequestFailed, Error:Server:zero.webappsecurity.com:80, Error: (11001)Unable to connect to remote host : No such host is known:

#### **Description**

This message indicates a network connectivity issue. WebInspect was unable to communicate with the remote host.

#### **Argument Descriptions**

Reason: FirstRequestFailed - a request has failed.

Server: The server to which the request was sent.

Error: (11001)Unable to connect to remote host : No such host is known: - Communication to the remote host failed due to connectivity issues.

#### **Possible Fixes**

- Power cycle your network hardware

If the issue persists, unplug your modem and router, wait a few seconds, then plug them back in. Sometimes, these devices simply need to be refreshed. This could be due to a network outage or improperly configured network settings.

- Use Microsoft's network diagnostic tools

Open Network Diagnostics by right-clicking the network icon in the notification area, and then clicking Diagnose and repair.

- Check wiring

Make sure that all wires are connected properly.

- Check host's power

If you're trying to connect to another computer, make sure that computer is powered on.

- Check connection settings

If the problem began after you installed new software, check your connection settings to see if they have been changed. Open Network Connections by clicking the Start button , clicking Control Panel, clicking Network and Internet, clicking Network and Sharing Center, and then clicking Manage network connections. Right-click the connection, and then click Properties. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

- Troubleshoot all firewalls
- External Links

[Troubleshoot network connection problems](#)  
[Internet Connectivity Evaluation Tool](#)

Crawler Error

### **Full Message**

Error: Crawler error, session: <session ID> error:<error>

### **Description**

The crawler failed to process the session. Not user-correctable. Contact HP.

### **Argument Descriptions**

Session: The session in which the error occurred.

Error: The actual error.

### **Possible Fixes**

Not Applicable

### **External Links:**

Not Applicable

[Database Connectivity Issue](#)

### **Full Message**

Error: SPI.Scanners.Web.Framework.Session in updateExisting,retries failed, giving up calling IDbConnetivityHandler.OnConnectivityIssueDetected

**Description**

This message indicates that the database stopped responding.

**Argument Descriptions**

Error Text: Contains a description of the error that triggered the message

**Possible Fixes**

Make sure the database server is running and responding.

**External Links**

Not Applicable

Engine Driven Audit Start

**Full Message**

Info:Engine Driven Audit Start

**Description**

This message indicates Engine Driven Audit has started.

**Argument Descriptions**

Not applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Engine Driven Audit Stop

**Full Message**

Info:Engine Driven Audit Stop

**Description**

This message indicates Engine Driven Audit has stopped.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Engine Driven Engine Skip

**Full Message**

Info:Engine Driven Engine Start, Engine: LFI Agent

**Description**

Engine driven audit skipped for the engine due to the **Skip** button.

**Argument Descriptions**

Engine: The Engine that is being skipped.

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Engine Driven Engine Start

**Full Message**

Info:Engine Driven Engine Start, Engine: LFI Agent

**Description**

This message indicates the engine indicated has started execution.

**Argument Descriptions**

Engine: The Engine that is starting.

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Engine Driven Engine Stop

**Full Message**

Info:Engine Driven Engine Stop, Engine: LFI Agent Sessions Processed:406

**Description**

Engine driven audit completed for the specified engine.

**Argument Descriptions**

Engine: The Engine that has been stopped.

Sessions processed: Number of sessions processed by the engine.

**Possible Fixes**

Not Applicable

### **External Links**

Not Applicable

License Issue

### **Full Message**

Error: License issue: License Deactivated

### **Description**

A problem has occurred with the license.

### **Argument Descriptions**

Issue: The issue that occurred.

### **Possible Fixes**

Make sure WebInspect is properly licensed.

### **External Links**

Not Applicable

Log Message Occurred

### **Full Message :**

<Level>: <ScanID> , <Logger>: <Exception>

### **Description:**

Generic message for exceptions

### **Argument Descriptions**

ScanID: Scan ID.

Logger: Name of logger.

Exception: The exception thrown.

### **Possible Fixes**

Not Applicable

### **External Links**

Not Applicable

Memory Limit Reached

### **Full Message**

Warn: Memory limit reached: level:1,limit:1073610752, actual:1076625408.

Error: Memory limit reached: level:0,limit:1073610752, actual:1076625408.

### **Description**

The memory limits of the WI process have been reached.

### **Argument Descriptions**

Level: The severity of the problem.

Limit: The memory limit of the process.

Actual: The actual memory allocated to the process.

### **Possible Fixes**

Close other scans that are not running.

Run only one scan at a time in a given WebInspect instance.

### **External Links**

Not Applicable

Missing Session for Vulnerability

### **Full Message**

Info: Missing Session for Vulnerability

### **Description**

Cannot find session that is associated with a vulnerability.

### **Argument Descriptions**

Not Applicable

### **Possible Fixes**

Not Applicable

### **External Links**

Not Applicable

New Blind SQL Check Not Enabled

### **Full Message**

New Blind SQL check (checkid newcheckid%) is not enabled. A policy with both check %newcheckid% and check %oldcheckid% enabled is recommended.

### **Description**

The newer check for blind SQL injection is not included in the scan policy.

### **Argument Descriptions**

newcheckid: The identifier of the newer SQL injection check (10962)

oldcheckid: The identifier of the older SQL injection check (5659)

### **Possible Fixes**

Add the newer check (10962) to the scan policy.

**External Links**

Not Applicable

Persistent Cross-Site Scripting Audit Start

**Full Message**

Info:Persistent Cross-Site Scripting Audit Start

**Description**

Persistent Cross-Site Scripting Audit has started.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Persistent Cross-Site Scripting Audit Stop

**Full Message**

Info:Persistent Cross-Site Scripting Audit Stop

**Description**

Persistent Cross-Site Scripting Audit has stopped.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Post-Scan Analysis Started

**Full Message**

Post-Scan Analysis started.

**Description**

Post-scan analysis has begun. Additional messages will be displayed for each module used (authentication, macro, file not found, etc.).

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Post-Scan Analysis Completed

**Full Message**

Post-Scan Analysis completed.

**Description**

Post-scan analysis has ended. Additional messages will be displayed for each module used (authentication, macro, file not found, etc.).

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Reflect Audit Start

**Full Message**

Info:Reflect Audit Start

**Description**

Reflection phase started.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Reflect Audit Stop

**Full Message**

Info:Reflect Audit Stop

**Description**

Reflection phase completed.

### **Argument Descriptions**

Not Applicable

### **Possible Fixes**

Not Applicable

### **External Links**

Not Applicable

Scan Complete

### **Full Message**

Info:Scan Complete, ScanID:<id-number>

### **Description**

This message indicates that the scan has completed successfully.

### **Argument Descriptions**

ScanID: Unique identifier of a scan

### **Possible Fixes**

Not Applicable

### **External Links**

Not Applicable

Scan Failed

### **Full Message**

Info:Scan Failed, ScanID::<id-number>

### **Description**

This message indicates that the scan has failed.

### **Argument Descriptions**

ScanID: Unique identifier of a scan

### **Possible Fixes**

Depends upon the reason the scan failed, which is specified in a different message.

### **External Links**

Not Applicable

Scan Start

### **Full Message**

Info:Scan Start, ScanID:<id-number> Version:X.X.X.X, Location:C:\Program Files\HP\HP WebInspect\WebInspect.exe

### Description

This message indicates the start of a scan.

### Argument Descriptions

ScanID: Unique identifier of a scan.

Version: Version of WebInspect running the scan.

Location: The physical location of the WebInspect executable.

### Possible Fixes

Not Applicable

### External Links

Not Applicable

Scan Start Error

### Full Message

Scan start error: %error%

### Description

An unrecoverable error occurred while starting the scan. Contact HP Support.

### Argument Descriptions

error: description of the problem.

### Possible Fixes

Not Applicable

### External Links:

Not Applicable

Scan Stop

### Full Message

Info:Scan Stop, ScanID:<id-number>

### Description

This message indicates that the scan has been stopped.

### Argument Descriptions

ScanID: Unique identifier of a scan.

### Possible Fixes

Not Applicable

### External Links:

Not Applicable

Scanner Retry Start

**Full Message**

Info:Scanner Retry Start

**Description**

Retry phase started.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Scanner Retry Stop

**Full Message**

Info:Scanner Retry Start

**Description**

Retry phase stopped.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Sequential Audit Start

**Full Message**

Info:Sequential Audit Start

**Description**

This message indicates that the Sequential Audit has started.

**Argument Descriptions**

Not applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Sequential Audit Stop

**Full Message**

Info:Sequential Audit Stop

**Description**

This message indicates that the Sequential Audit has stopped.

**Argument Descriptions**

Not applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Sequential Crawl Start

**Full Message**

Info:Sequential Crawl Start

**Description**

This message indicates that Sequential Crawl has started.

**Argument Descriptions**

Not applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Sequential Crawl Stop

**Full Message**

Info:Sequential Crawl Stop

**Description**

This message indicates that the Sequential Crawl has stopped.

**Argument Descriptions**

Not applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Settings Override

**Full Message**

Settings Override, Setting:<setting>, Original Value:<original>, New Value:<newValue>, Reason:<reason>

**Description**

A setting was changed by the product. This may indicate a setting upgrade issue.

**Argument Descriptions**

Setting: The setting that is being overridden.

Original Value: The original value of the setting.

New Value: The value to which the setting is being changed.

Reason: The reason for the override.

**Possible Fixes**

Restore factory defaults and reapply custom settings.

**External Links**

Not Applicable

Skipping Auditor Retry

**Full Message**

Info: Skipping Auditor Retry

**Description**

The retry phase was skipped due to the **Skip** button.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Skiping Crawl

**Full Message**

Warn: Skiping Crawl

**Description**

The crawl was skipped due to the skip button.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

[Skipping Persistent Cross-Site Scripting Audit](#)

**Full Message**

Warn: Skipping Persistent Cross-Site Scripting Audit

**Description**

The Persistent Cross-Site Scripting phase was skipped due to the **Skip** button.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

[Skipping Reflect Audit](#)

**Full Message**

Warn: Skipping Reflect Audit

**Description**

The reflection phase was skipped due to the **Skip** button.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Skipping Verify Audit

**Full Message**

Warn: Skipping Verify Audit

**Description**

The verify phase was skipped due to the **Skip** button.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Start URL Error

**Full Message**

Start Url Error:%url%, error:%error%

**Description**

An unrecoverable error occurred processing the start URL. Check url syntax; if correct, contact HP Support.

**Argument Descriptions**

url: The URL that caused the error.

error: Description of the error.

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Start URL Rejected

**Full Message**

Start Url Rejected:%url%, reason:%reasons%, session:%session%

**Description**

The URL was rejected due to request rejection settings; settings should be modified or a different start URL used.

**Argument Descriptions**

url: the start URL

reason: Reason for the rejection.

session: The session during which the error occurred.

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Starting Post-Scan Analysis Module

**Full Message**

Starting Post-Scan Analysis Module: %module%

**Description**

One of the post-scan analysis modules has begun.

**Argument Descriptions**

module: the name of the post-scan analysis module.

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Stop Requested

**Full Message**

Info:Stop Requested, reason=Pause button pushed

**Description**

Scan is entering suspended state.

**Argument Descriptions**

Reason: Reason for the stop.

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Verify Audit Start

**Full Message**

Info:Verify Audit Start

**Description**

Verify phase started.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Verify Audit Stop

**Full Message**

Info:Verify Audit Stop

**Description**

Verify phase completed.

**Argument Descriptions**

Not Applicable

**Possible Fixes**

Not Applicable

**External Links**

Not Applicable

Web Macro Error

**Full Message**

Error: Web Macro Error, Name: Login webmacro Error: RequestAborted

**Description**

An error occurred during playback of a web macro.

**Argument Descriptions**

Name: Name of the macro being played when the error occurred.

Error: The error that occurred.

**Possible Fixes**

Depends on the error encountered. For RequestAborted error, the server did not respond during macro playback. If this occurs frequently, the value of Request timeout should be increased. See Connectivity issue for other potential solutions.

## **External Links**

Not Applicable

Web Macro Status

## **Full Message**

Error: Web Macro Status, Name: login.webmacro Expected:302, Actual:200, Url:<URL>

## **Description**

WebInspect received a response during macro playback that did not match the response obtained during the recording of the macro.

## **Argument Descriptions**

Name: Name of the web macro.

Expected: The status code expected to be returned.

Actual: The status code that was actually returned.

URL: The target URL of the request.

## **Possible Fixes**

This could indicate that we WebInspect is attempting to log in when it is already logged in or that WebInspect is failing to log in. Check to see if WebInspect is successfully logged in during a scan. If not, record the login macro again.

## **External Links**

Not Applicable

# Contact Technical Support

You can open a support case for Fortify products via email, by telephone, or online, using our customer support system. This streamlined procedure is designed to provide easier access and improved customer satisfaction.

## **E-Mail (Preferred Method)**

Send an email to [fortifytechsupport@HP.com](mailto:fortifytechsupport@HP.com) describing your issue. Be sure to include the product name. A customer support representative will contact you.

## **Telephone**

Call our automated processing service at (650) 735-2215. Please provide your name, phone number, the name of the product, and a brief description of your problem. A customer support representative will contact you.

## Online

Access your account at the Fortify Support Portal at [support.fortify.com](http://support.fortify.com). If you do not have an account, you forgot your user name or password, or you need any assistance regarding your account, please contact us at [fortifytechsupport@hp.com](mailto:fortifytechsupport@hp.com) or (650) 735-2215.

Version: 10.30

Date: September 2014

### See Also

["WebInspect Overview " on page 20](#)

## Suggest Enhancement

We value the opinions of our users and would greatly appreciate any suggestions you may have for improving the quality and usefulness of our products.

1. Click **Help > Support > Request an Enhancement**.
2. Select **Suggestion** or **Enhancement** from the **Type** list.
3. Select a category that most closely matches your area of interest. Select **General** if no category appears suitable.
4. In the **Synopsis** box, enter a brief topic summary.
5. In the **Description** area, tell us how we can improve WebInspect.
6. Click **Submit**.

## Purchases and Renewals

This topic describes how to purchase HP products and renew product licenses.

## New Purchases

Visit [Contact HP](#) to obtain the telephone number of the HP sales office nearest you, or to send an e-mail inquiring about HP products.

## Renew Your Product License

You can obtain a quote and renew your maintenance contract online at HP's [Support Agreement Manager](#). Simply select the region where your company is headquartered, and complete the enrollment. Registration takes only a few minutes and is typically confirmed in one business day.

Use the online chat feature to speak with an HP representative from your region or visit [Contact HP](#) to obtain the telephone number of the HP sales office nearest you, or to send an e-mail inquiring about HP products.

## HTTP Status Codes

The following list of status codes was extracted from the Hypertext Transfer Protocol version 1.1 standard (rfc 2616). You can find more information at <http://www.w3.org/Protocols/>.

Code	Definition
100	Continue
101	Switching Protocols
200 OK	Request has succeeded
201 Created	Request fulfilled and new resource being created
202 Accepted	Request accepted for processing, but processing not completed.
203 Non-Authoritative Information	The returned metainformation in the entity-header is not the definitive set as available from the origin server, but is gathered from a local or a third-party copy.
204 No Content	The server has fulfilled the request but does not need to return an entity-body, and might want to return updated metainformation.
205 Reset Content	The server has fulfilled the request and the user agent should reset the document view which caused the request to be sent.
206 Partial Content	The server has fulfilled the partial GET request for the resource.
300 Multiple Choices	The requested resource corresponds to any one of a set of representations, each with its own specific location, and agent-driven negotiation information (section 12) is being provided so that the user (or user agent) can select a preferred representation and redirect its request to that location.
301 Moved Permanently	The requested resource has been assigned a new permanent URI and any future references to this resource should use one of the returned URIs.

<b>Code</b>	<b>Definition</b>
302 Found	The requested resource resides temporarily under a different URI.
303 See Other	The response to the request can be found under a different URI and should be retrieved using a GET method on that resource.
304 Not Modified	If the client has performed a conditional GET request and access is allowed, but the document has not been modified, the server should respond with this status code.
305 Use Proxy	The requested resource MUST be accessed through the proxy given by the Location field.
306 Unused	Unused.
307 Temporary Redirect	The requested resource resides temporarily under a different URI.
400 Bad Request	The request could not be understood by the server due to malformed syntax.
401 Unauthorized	The request requires user authentication. The response MUST include a WWW-Authenticate header field (section 14.47) containing a challenge applicable to the requested resource.
402 Payment Required	This code is reserved for future use.
403 Forbidden	The server understood the request, but is refusing to fulfill it.
404 Not Found	The server has not found anything matching the Request-URI.
405 Method Not Allowed	The method specified in the Request-Line is not allowed for the resource identified by the Request-URI.
406 Not Acceptable	The resource identified by the request is only capable of generating response entities which have content characteristics not acceptable according to the accept headers sent in the request.
407 Proxy Authentication Required	This code is similar to 401 (Unauthorized), but indicates that the client must first authenticate itself with the proxy.
408 Request Timeout	The client did not produce a request within the time that the server was prepared to wait.
409 Conflict	The request could not be completed due to a conflict with the current state of the resource.
410 Gone	The requested resource is no longer available at the server and no forwarding address is known.
411 Length Required	The server refuses to accept the request without a defined Content-Length.

<b>Code</b>	<b>Definition</b>
412 Precondition Failed	The precondition given in one or more of the request-header fields evaluated to false when it was tested on the server.
413 Request Entity Too Large	The server is refusing to process a request because the request entity is larger than the server is willing or able to process.
414 Request-URI Too Long	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415 Unsupported Media Type	The server is refusing to service the request because the entity of the request is in a format not supported by the requested resource for the requested method.
416 Requested Range Not Satisfiable	A server should return a response with this status code if a request included a Range request-header field (section 14.35), and none of the range-specifier values in this field overlap the current extent of the selected resource, and the request did not include an If-Range request-header field.
417 Expectation Failed	The expectation given in an Expect request-header field (see section 14.20) could not be met by this server, or, if the server is a proxy, the server has unambiguous evidence that the request could not be met by the next-hop server.
500 Internal Server Error	The server encountered an unexpected condition which prevented it from fulfilling the request.
501 Not Implemented	The server does not support the functionality required to fulfill the request. This is the appropriate response when the server does not recognize the request method and is not capable of supporting it for any resource.
502 Bad Gateway	The server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed in attempting to fulfill the request.
503 Service Unavailable	The server is currently unable to handle the request due to a temporary overloading or maintenance of the server.
504 Gateway Timeout	The server, while acting as a gateway or proxy, did not receive a timely response from the upstream server specified by the URI (e.g., HTTP, FTP, LDAP) or some other auxiliary server (e.g., DNS) it needed to access in attempting to complete the request.
505 HTTP Version Not Supported	The server does not support, or refuses to support, the HTTP protocol version that was used in the request message.

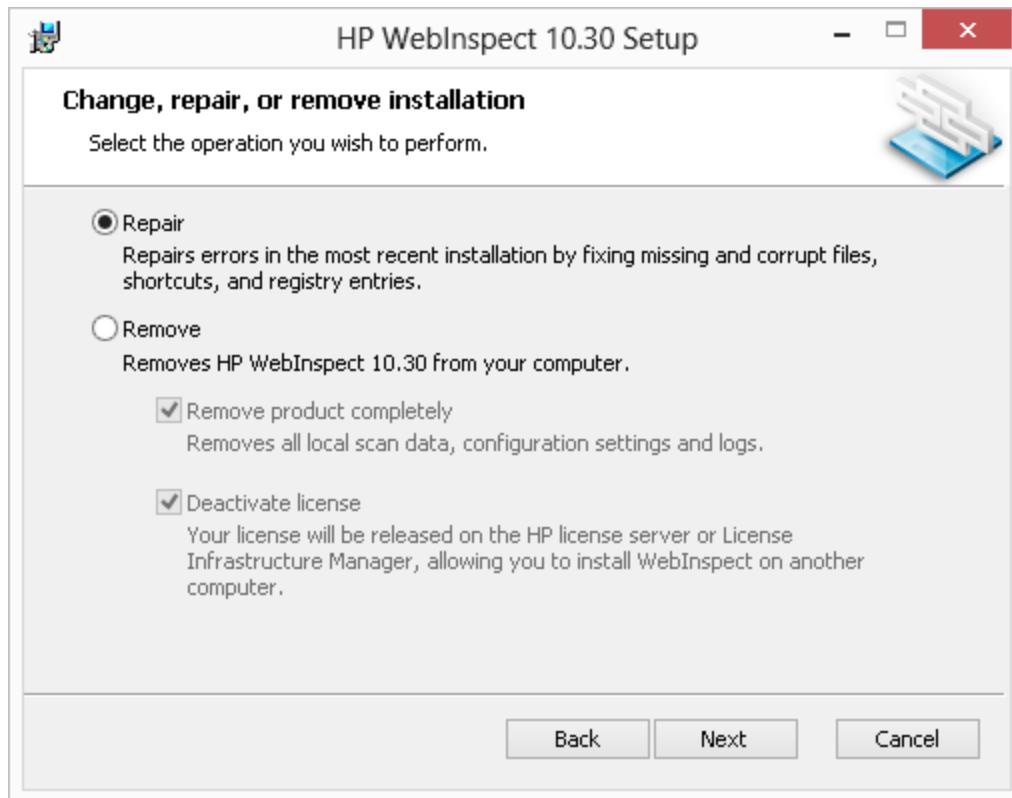
## Uninstalling WebInspect

When uninstalling, you can choose to repair WebInspect or remove it from your computer.

## Options for Removing

If you select **Remove**, you may choose one or both of the following options:

- Remove product completely - Deletes the WebInspect application and all related files, including scan data stored on a local (non-shared) SQL server, settings files and logs.
- Deactivate license - Releases your WebInspect license, which allows you to install WebInspect on a different computer. Application data and files are not deleted.



## About WebInspect

Use the About WebInspect window to view the application version number and display information about the WebInspect license.

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

## **Feedback on WebInspect (WebInspect 10.30)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [HPFortifyTechPubs@hp.com](mailto:HPFortifyTechPubs@hp.com).

We appreciate your feedback!