
Acunetix Web Vulnerability Scanner

User Manual

V7

By Acunetix Ltd.

Acunetix Ltd.

<http://www.acunetix.com>

E-mail: info@acunetix.com

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Acunetix Ltd.

Acunetix WVS is copyright of Acunetix Ltd. 2004–2010.

Acunetix Ltd. All rights reserved.

Document version 7

Last updated 10th August 2010.

Contents

| | |
|--------------------------------------------------------------------|-----------|
| Acunetix Web Vulnerability Scanner..... | i |
| 1. Introduction to Acunetix Web Vulnerability Scanner | 5 |
| <i>Why You Need To Secure Your Web Applications</i> | <i>5</i> |
| The need for automated web application security scanning..... | 6 |
| <i>Acunetix Web Vulnerability Scanner</i> | <i>6</i> |
| How Acunetix WVS Works..... | 6 |
| <i>Acunetix AcuSensor Technology</i> | <i>7</i> |
| Advantages of using AcuSensor Technology | 7 |
| AcuSensor Technology Vulnerability Reporting..... | 8 |
| <i>Acunetix WVS Program Overview.....</i> | <i>8</i> |
| Web Scanner..... | 9 |
| AcuSensor Technology | 9 |
| Port Scanner and Network Alerts | 9 |
| Target Finder..... | 10 |
| Subdomain Scanner..... | 10 |
| Blind SQL Injector..... | 10 |
| HTTP Editor..... | 10 |
| HTTP Sniffer..... | 10 |
| HTTP Fuzzer | 10 |
| Authentication Tester | 11 |
| Web Services Scanner..... | 11 |
| Web Services Editor..... | 11 |
| WVS Scripting tool and Acunetix SDK..... | 11 |
| Vulnerability Editor | 12 |
| Reporter..... | 12 |
| <i>What's new in Acunetix WVS Version 7</i> | <i>13</i> |
| New features | 13 |
| Major Improvements | 13 |
| <i>Acunetix training and Support.....</i> | <i>14</i> |
| <i>License Scheme.....</i> | <i>14</i> |
| Perpetual or Time Based Licenses..... | 14 |
| Small Business Edition 1 Site/Server..... | 14 |
| Enterprise Edition Unlimited Sites/Servers..... | 14 |
| Consultant Edition..... | 15 |
| Upgrading from an Evaluation to a Purchased Edition | 15 |
| Extending a Purchased Edition | 15 |
| Limitations of Evaluation Edition..... | 15 |
| Purchasing Acunetix WVS..... | 15 |
| 2. Installing Acunetix WVS..... | 17 |
| <i>System Minimum Requirements</i> | <i>17</i> |
| <i>Installation Procedure</i> | <i>17</i> |
| <i>Upgrade Procedure</i> | <i>17</i> |
| <i>Configuring an HTTP Proxy or SOCKS proxy Server</i> | <i>18</i> |
| HTTP Proxy Settings..... | 18 |
| SOCKS Proxy Settings..... | 19 |
| HTTP Proxy Settings (For program updates) | 19 |

| | |
|-----------------------------------------------------------|-----------|
| <i>Configuring AcuSensor Technology</i> | 19 |
| Step 1: Configure the Sensor..... | 19 |
| Step 2: Installing the Sensor..... | 20 |
| Step 3: Enabling the Sensor..... | 20 |
| Disabling and uninstalling the Sensor..... | 21 |
| 3. Scanning Your Website | 23 |
| <i>Starting a Scan</i> | 23 |
| Step 1: Select Target(s) to Scan..... | 23 |
| Step 2: Confirm Targets and Technologies Detected..... | 24 |
| Step 3: Specify Crawler Options..... | 25 |
| Crawling Options..... | 25 |
| Step 4: Specify Scanning Profile and Mode..... | 25 |
| Scanning Profile..... | 26 |
| Scan Options..... | 26 |
| Step 5: Configure Login for Password Protected Areas..... | 26 |
| Scanning a HTTP password protected area:..... | 27 |
| Scanning a form based password protected area:..... | 28 |
| Step 6: Configure Custom 404 Error Pages..... | 30 |
| Step 7: Select the Files and directories to Scan..... | 31 |
| Step 8: Completing the scan..... | 31 |
| 4. Analyzing the Scan Results | 33 |
| Introduction..... | 33 |
| Web Alerts node..... | 33 |
| Network Alerts Node..... | 34 |
| Port Scanner Node..... | 34 |
| Knowledge Base Node..... | 34 |
| Site Structure Node..... | 35 |
| Grouping of Vulnerabilities..... | 36 |
| Saving a Scan Result..... | 36 |
| 5. Generating a Report from the results | 37 |
| Introduction to the Reporter..... | 37 |
| Generating a Report from the Scan Results..... | 37 |
| Developer Report..... | 39 |
| Executive Report..... | 39 |
| Vulnerability Report..... | 40 |
| Scan Comparison Report..... | 40 |
| Statistical Reports..... | 41 |
| Compliance Reports..... | 41 |
| Customizing the Report Layout..... | 42 |
| Report Options..... | 42 |
| Page Settings..... | 42 |
| The Report Viewer..... | 42 |
| Using Microsoft SQL..... | 42 |
| 6. Site Crawler Options | 45 |
| Introduction..... | 45 |

| | |
|-------------------------------------------------------------|-----------|
| Starting a Website Crawl..... | 46 |
| Analyzing the Site Crawler results..... | 46 |
| Configuring the Crawler | 48 |
| Site Crawler Settings..... | 48 |
| Site Crawler Settings > File Extension Filters | 49 |
| Site Crawler Settings > Directory and File Filters..... | 49 |
| Site Crawler Settings > URL Rewrite | 50 |
| Site Crawler Settings > Custom Cookies | 51 |
| 7. Manual crawling with the HTTP Sniffer Tool | 53 |
| Introduction..... | 53 |
| Configuring and using the HTTP Sniffer..... | 54 |
| Mozilla Firefox | 54 |
| Internet Explorer | 54 |
| Google Chrome | 54 |
| Capturing HTTP traffic..... | 54 |
| Configuration Options..... | 54 |
| HTTP Sniffer Trap Filters | 55 |
| Creating a HTTP Sniffer Trap Filter | 55 |
| The Trap Form..... | 56 |
| Editing a HTTP Request without a Trap | 56 |
| 8. Compare Results Tool..... | 57 |
| Introduction..... | 57 |
| Comparing Results | 57 |
| Analyzing the Results Comparison | 57 |
| 9. Scanning Web Services | 59 |
| Introduction..... | 59 |
| Starting a Web Service Scan..... | 59 |
| Web Services Editor | 60 |
| Importing WSDL and Sending Request | 60 |
| Response Tab | 60 |
| Structured Data Tab | 60 |
| WSDL Structure Tab | 60 |
| WSDL Tab..... | 61 |
| HTTP Editor Export | 61 |
| 10. Command Line Operation | 63 |
| Introduction..... | 63 |
| WVS Console Scanner Command Line Parameters..... | 63 |
| WVS Console Scanner Command Line Options | 65 |
| The Acunetix WVS console Reporter | 67 |
| The Acunetix WVS console Reporter command line options..... | 67 |
| 11. The Scheduler..... | 69 |
| Introduction..... | 71 |
| Creating a Scheduled scan | 71 |
| Creating a queue and a schedule..... | 71 |
| Advanced Options tab | 72 |

| | |
|-----------------------------------------------------|-----------|
| <i>Scheduler Settings</i> | 73 |
| General settings tab | 73 |
| Email notifications settings tab | 73 |
| <i>Scheduled Scans controls</i> | 73 |
| 12. Other Acunetix WVS tools | 75 |
| <i>The Target Finder</i> | 75 |
| <i>The Subdomain scanner</i> | 75 |
| <i>The Authentication tester</i> | 75 |
| <i>Login Sequence Recorder</i> | 75 |
| Creating or editing login sequences | 75 |
| <i>Traversing Web Form pages</i> | 77 |
| <i>The HTTP Fuzzer tool</i> | 78 |
| <i>The HTTP editor tool</i> | 79 |
| <i>The SQL injector tool</i> | 79 |
| 13. Advanced Configuration Options | 81 |
| <i>Introduction</i> | 81 |
| <i>General</i> | 81 |
| <i>Client Certifications</i> | 82 |
| <i>Logging</i> | 82 |
| <i>Scanner Settings</i> | 82 |
| <i>Headers and Cookies</i> | 84 |
| <i>Parameter Exclusions</i> | 84 |
| Settings > Scanner Settings > GHDB | 84 |
| Settings > Scanner Settings > Port Scanner | 85 |
| Settings > Scanner Settings > False Positives | 85 |
| <i>Scanning Profiles</i> | 85 |
| Default Scanning Profiles | 85 |
| Creating/Modifying Scanning Profiles | 86 |
| <i>Creating custom vulnerability checks</i> | 87 |
| 14. Troubleshooting | 89 |
| <i>Obtaining support</i> | 89 |
| <i>Request Support via E-Mail</i> | 89 |

1. Introduction to Acunetix Web Vulnerability Scanner

Why You Need To Secure Your Web Applications

Website security is possibly today's most overlooked aspect of securing the enterprise and should be a priority in any organization.

Increasingly, hackers are concentrating their efforts on web-based applications – shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases and also allow hackers to perform illegal activities using the attacked sites. A victim's website can be used to launch criminal activities such as hosting phishing sites or to transfer illicit content, while abusing the website's bandwidth and making its owner liable for these unlawful acts.

Hackers already have a wide repertoire of attacks that they regularly launch against organizations including SQL Injection, Cross Site Scripting, Directory Traversal Attacks, Parameter Manipulation (e.g., URL, Cookie, HTTP headers, web forms), Authentication Attacks, Directory Enumeration and other exploits. Moreover, the hacker community is very close-knit; newly discovered web application intrusions are posted on a number of forums and websites known only to members of that exclusive group. These are called Zero Day exploits. Postings are updated daily and are used to propagate and facilitate further hacking.

Web applications – shopping carts, forms, login pages, dynamic content, and other bespoke applications – are designed to allow your website visitors to retrieve and submit dynamic content including varying levels of personal and sensitive data.

If these web applications are not secure, then your entire database of sensitive information is at serious risk. A Gartner Group study reveals that 75% of cyber attacks are done at the web application level.

Why does this happen?

- Websites and related web applications must be available 24 hours a day, 7 days a week to provide the required service to customers, employees, suppliers and other stakeholders.
- Firewalls and SSL provide no protection against web application hacking, simply because access to the website has to be made public.
- Web applications often have direct access to backend data such as customer databases and, hence, control valuable data and are much more difficult to secure.
- Corporate web applications have large amounts of bandwidth available. Since bandwidth is expensive, for a hacker to transfer huge amounts of illegal content, they revert to steal bandwidth from others.
- Most web applications are custom-made and, therefore, involve a lesser degree of testing than off-the-shelf software. Consequently, custom applications are more susceptible to attack.

Various high-profile hacking attacks have proven that web application security remains the most critical. If your web applications are compromised,

hackers will have complete access to your backend data even though your firewall is configured correctly and your operating system and applications are patched repeatedly.

Network security defense provides no protection against web application attacks since these are launched on port 80 (default for websites) which has to remain open to allow regular operation of the business.

For the most comprehensive security strategy, it is therefore imperative that you regularly and consistently audit your web applications for exploitable vulnerabilities.

The need for automated web application security scanning

Manual vulnerability auditing of all your web applications is complex and time-consuming. It also demands a high-level of expertise and the ability to keep track of considerable volumes of code and of all the latest tricks of the hacker's 'trade'.

Automated vulnerability scanning allows you to focus on the more challenging issue of securing your web applications from any exploitable vulnerability that jeopardizes your data.

Acunetix Web Vulnerability Scanner

Acunetix Web Vulnerability Scanner (WVS) broadens the scope of vulnerability scanning by introducing highly advanced heuristic and rigorous technologies designed to tackle the complexities of today's web-based environments.

WVS is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injections, Cross site scripting and other exploitable hacking vulnerabilities. In general, Acunetix WVS scans any website or web application that is accessible via a web browser and that respects HTTP/HTTPS protocol.

Besides automatically scanning for exploitable vulnerabilities, WVS offers a strong and unique solution for analyzing off-the-shelf and custom web applications including those relying on client scripts such as JavaScript, AJAX and Web 2.0 web applications.

Acunetix WVS is suitable for any small, medium sized and large organizations with intranets, extranets, and websites aimed at exchanging and/or delivering information with/to customers, vendors, employees and other stakeholders.

How Acunetix WVS Works

Acunetix WVS has a vast array of automated features and manual testing tools and, in general, the automated scan works in the following manner:

1. The crawler crawls the entire website by following all the links on the site and in the robots.txt file and sitemap.xml (if available). WVS will then map out the website structure and display detailed information about every file. If Acunetix **AcuSensor Technology** is enabled, the sensor will retrieve a listing of all the files present in the web application directory and adds the files not found by the crawler to the crawler output. Such files usually are not discovered by the crawler as they are not accessible from the web server, or not linked through the website or even hidden application files, such as web.config.

2. After the crawling process, WVS automatically launches a series of vulnerability attacks on each page found, in essence emulating a hacker. Also, WVS analyzes each page for places where it can input data, and subsequently attempts all the different input combinations. This is the

Automated Scan Stage. If the **AcuSensor Technology** is enabled, a series of vulnerability checks which cannot be done when using a typical black box application scanner are launched against the website. For more information about **AcuSensor Technology** refer to the paragraph below.

3. During the scan process, a port scan is also launched against the web server hosting the website (the port scanner can be switched off from the configuration settings). If open ports are found, Acunetix WVS will perform a range of network security checks against the network service running on that port.

4. As vulnerabilities are found, Acunetix WVS reports these in the 'Alerts' node. Each alert contains information about the vulnerability such as POST variable name, affected item, http response of the server and more. If **AcuSensor Technology** is used details such as source code line, stack trace, SQL query which lead to the vulnerability are listed. Recommendations on how to fix the vulnerability are also listed.

5. If open ports are found, they will be reported in the 'Knowledge Base' node. The list of open ports contains information such as the banner returned from the port and if a security test failed.

6. After a scan has been completed, it can be saved to file for later analysis and for comparison to previous scans. Using the Acunetix reporter a professional report can be created summarizing the scan.

Acunetix AcuSensor Technology

Acunetix' unique AcuSensor Technology is a security technology that allows you to identify more vulnerabilities than a traditional Web Application Scanner, whilst generating less false positives. In addition, it indicates exactly where in your code the vulnerability is and reports debug information.

The increased accuracy is achieved by combining black box scanning techniques with feedback from sensors placed inside the source code while the source code is executed. Black box scanning does not know how the application reacts and source code analyzers do not understand how the application will behave while it is being attacked. Therefore combining these techniques together achieves more relevant results than using source code analyzers and black box scanning independently.

The AcuSensor Technology does not require .NET source code; it can be injected in already compiled .NET applications! Thus there is no need to install a compiler or obtain the web applications' source code, which is a big advantage when using a third party .NET application. In case of PHP web applications, the source is already available.

To date, Acunetix is the only Web Vulnerability Scanner to implement this technology.

Advantages of using AcuSensor Technology

- Ability to provide more information about the vulnerability, such as source code line number, stack trace, affected SQL query.
- Allows you to locate and fix the vulnerability faster because of the ability to provide more information about the vulnerability, such as source code line number, stack trace, affected SQL query, etc.
- Significantly reduces false positives when scanning a website because it understands the behaviour of the web application better.
- Can alert you of web application configuration problems which could result in a vulnerable application or expose sensitive information. E.g. If

'custom errors' are enabled in .NET, this could expose sensitive application details to a malicious user.

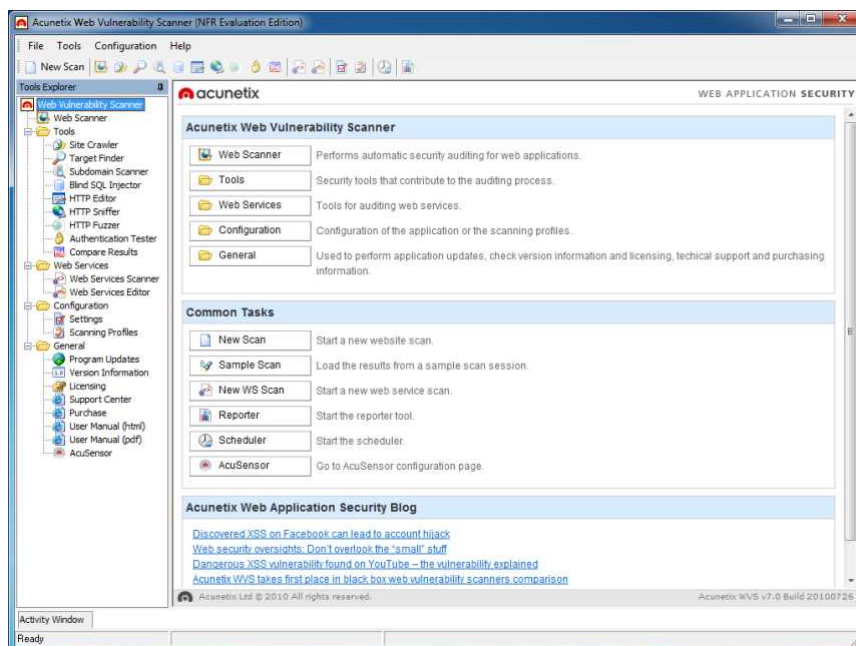
- It can advise you how to better secure your web application and web server settings, e.g. if write access is enabled on the web server.
- Detects many more SQL injection vulnerabilities. Previously SQL injection vulnerabilities could only be found if database errors were reported or via other common techniques.
- Ability to detect SQL Injection vulnerabilities in all SQL statements, including in SQL INSERT statements. With a black box scanner such SQL injection vulnerabilities cannot be found.
- Ability to know about all the files present and accessible through the web server. If an attacker will gain access to the website and create a backdoor file in the application directory, the file will be found and scanned when using the AcuSensor Technology and you will be alerted.
- AcuSensor Technology is able to intercept all web application inputs and build a comprehensive list with all possible inputs in the website and tests them.
- No need to write URL rewrite rules when scanning web applications which use search engine friendly URL's! Using the AcuSensor Technology the scanner is able to rewrite SEO URL's on the fly.
- Ability to test for arbitrary file creating and deletion vulnerabilities. E.g. Through a vulnerable script a malicious user can create a file in the web application directory and execute it to have privileged access, or delete sensitive web application files.
- Ability to test for email injection. E.g. A malicious user may append additional information such as a list of recipients or additional information to the message body to a vulnerable web form, to spam a large number of recipients anonymously.
- Ability to test for file upload forms vulnerabilities. E.g. A malicious user can easily bypass file upload form validation checks and upload a malicious file and execute it.

AcuSensor Technology Vulnerability Reporting

Unlike other vulnerabilities reported in typical scans, a vulnerability reported by the AcuSensor Technology contains much more detailed information. It can contain details such as source code line number, POST variable value, stack trace, affected SQL query etc. A vulnerability reported by the AcuSensor Technology, will be marked with '(AS)' in the title.

Acunetix WVS Program Overview

The following pages briefly explain the main WVS tools and features:



Screenshot 1 - Acunetix Web Vulnerability Scanner

Web Scanner

The Web Scanner is the most important component; it launches an automatic security audit of a website. A website security scan typically consists of two phases:

1. Crawling – In this phase, the crawler will automatically crawl and analyze the website and then build a site structure.
2. Scanning – In this phase, Acunetix WVS launches a series of attacks (web vulnerabilities checks) against the website or web application, in effect, emulating a hacker.

The results of a scan are displayed in an Alert Node tree with details on all the vulnerabilities found within the website.

AcuSensor Technology

Acunetix AcuSensor Technology is a unique technology that allows you to identify more vulnerabilities than a traditional black box web security scanner, whilst generating less false positives. In addition it also indicates exactly where in your code the vulnerability is. The increased accuracy is achieved by combining black box scanning techniques with dynamic code analysis whilst the source code is being executed.

Port Scanner and Network Alerts

The Port Scanner and network alerts give you the option to perform a port scan (optional) against the web server where the scanned website is hosted. When open ports are found, Acunetix WVS will perform complex network level security checks against the network service running on that port, such as DNS Open recursion tests, badly configured proxy server tests, weak SNMP community strings and many other network level security checks.

You can also write your own network services security checks. A scripting reference is also available from the following URL; <http://www.acunetix.com/vulnerability-scanner/scriptingreference/index.html>.

Target Finder

The Target Finder is a port scanner that allows you to locate web servers (port 80, 443) within a given range of IP addresses. If a web server is found, the scanner will also display the response header of the server and the web server software. The port numbers to scan are configurable.

Subdomain Scanner

Using various techniques and guessing of common sub domain names, the Subdomain scanner allows fast and easy identification of active sub domains in a DNS zone. The Subdomain Scanner can be configured to use the target's DNS server or a user specified one.

Blind SQL Injector

Ideal for penetration testers, the Blind SQL injector is an automated database data extraction tool with which you can make manual tests to further analyze reported SQL injections. The tool is also able to enumerate databases, tables, dump data and also read specific files on the file system of the web server if an exploitable SQL injection is discovered.

HTTP Editor

The HTTP Editor allows you to create custom HTTP requests and debug HTTP requests and responses. It also includes an encoding and decoding tool to encode / decode text and URL's to MD5 hashes, UTF-7 formats and many other formats.

HTTP Sniffer

The HTTP Sniffer acts as a proxy and allows you to capture, examine and modify HTTP traffic between an HTTP client and a web server. You can also enable, add or edit traps to trap traffic before it is sent to the web server or back to the web client. This tool is useful to:

- Analyze how Session IDs are stored and how inputs are sent to the server.
- Alter any HTTP request being sent back to the server before it gets sent.
- Navigate through parts of the website which cannot be crawled automatically. You can then import the results to the scanner afterwards.

To use this tool, all http requests must pass through Acunetix WVS. To achieve this, you must set Acunetix WVS as your proxy in your browser. You can read more about HTTP Sniffer and it's configuration on page 53 of this manual.

HTTP Fuzzer

With the HTTP Fuzzer you can launch a series of sophisticated fuzzing tests, to test the web application's handling of invalid and unexpected random data. With this tool you can easily create input rules for Acunetix WVS to test.

An example would be the following URL:

```
http://testphp.acunetix.com/listproducts.php?cat=1
```

Using the HTTP Fuzzer you can create a rule which would automatically replace the last part of the URL '1' with numbers between 1 and 999. Only valid results will be reported. This degree of automation allows you to quickly test the results of a 1000 queries without having to perform them one by one.

Authentication Tester

With the Authentication Tester you can perform a dictionary attack against login pages which use both HTTP (NTLM v1, NTLM v2, digest) or form based authentication. This tool uses two predefined text files (dictionaries) which contain a list of common usernames and passwords. You can add your own combinations to these text files.

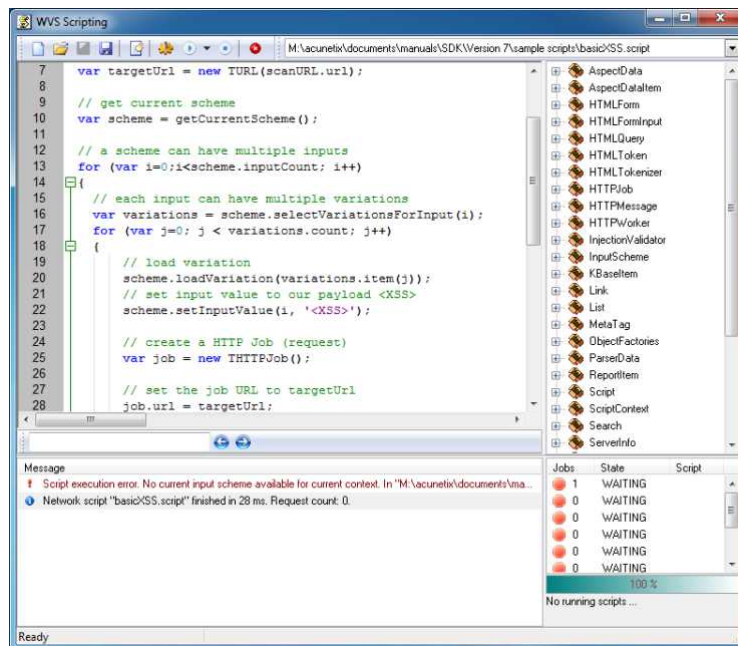
Web Services Scanner

The Web Services Scanner allows you to launch automated vulnerability scans against WSDL based Web Services.

Web Services Editor

The Web Services Editor allows you to import an online or local WSDL for custom editing and execution of various web service operations over different port types for an in depth analyses of WSDL requests and responses. The editor also features syntax highlighting for all languages to easily edit SOAP headers and customize your own manual attacks.

WVS Scripting tool and Acunetix SDK



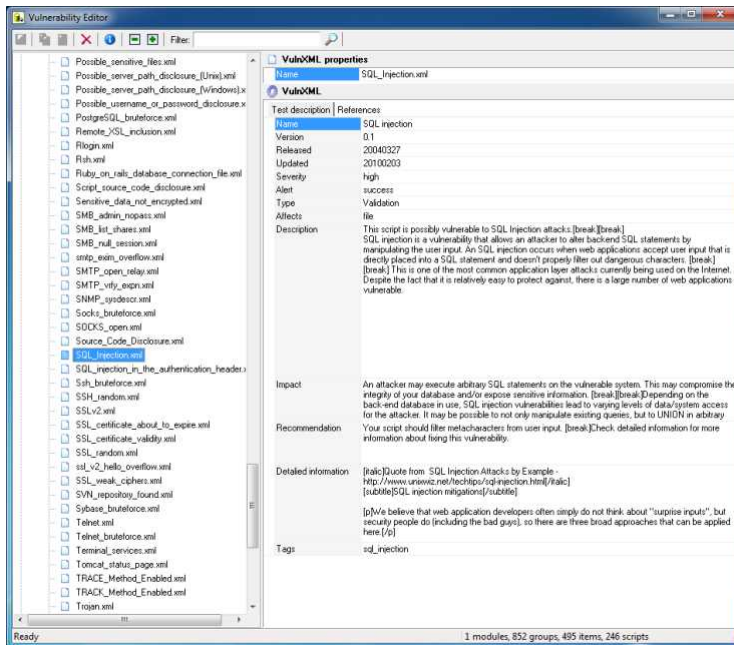
Screenshot 2 – WVS Scripting tool

The WVS Scripting tool allows you to create new custom web vulnerability checks. Acunetix WVS web vulnerability checks scripts are developed in JavaScript. You can download an SDK to create scripts from here:

http://www.acunetix.com/download/tools/Acunetix_SDK.zip

Note: The WVS Scripting tool is not included in the main download but in the Acunetix SDK.

Vulnerability Editor

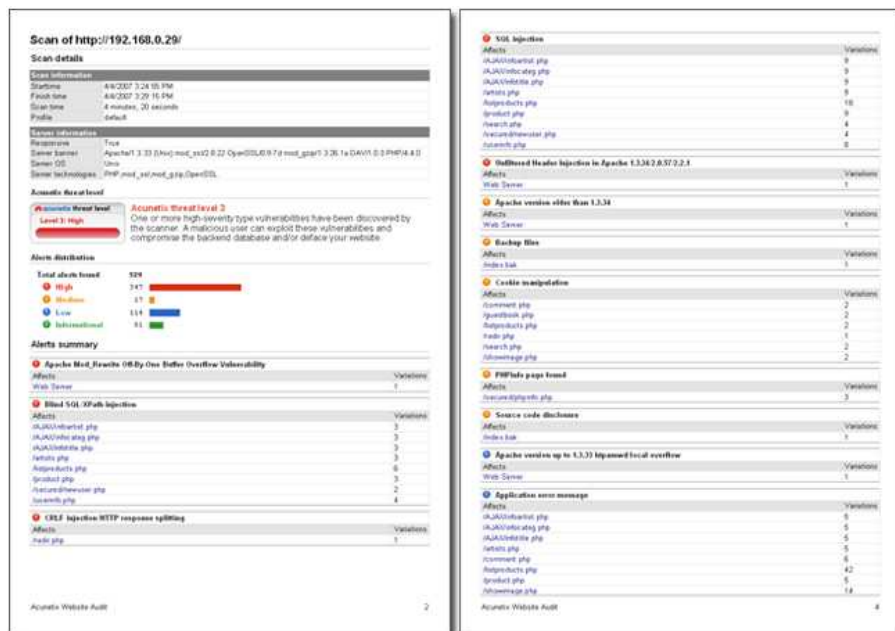


Screenshot 3 – The Vulnerability Editor

The Vulnerability Editor allows you to edit all documentation related to vulnerability description. It also allows you to change the severity level of vulnerability and more.

Reporter

The Reporter allows you to generate reports of scan results in a printable format. Various report templates are available, including summary, detailed reports and compliance reporting. The Consultant Version of the WVS allows customization of the generated report.



Screenshot 4 - Typical WVS Report including Chart of alerts

What's new in Acunetix WVS Version 7

New features

- Revamped scanning engine which avoids checks being launched in 'brute force' style. Web application inputs are thoroughly analyzed by the scanner to understand their purpose.
- Consolidation of discovered vulnerabilities and reported information to facilitate prioritization and coordination of vulnerability remediation.
- Advanced analyses of website presentation layer which help the scanner understand the scope of an input of the website. This helps the scanner in targeting more appropriate attacks and produces less load on the website during a web security scan.
- A whole variety of new vulnerability checks such as stored SQL Injection, Stored File Inclusion, form based authentication auditing, SQL injection in URI etc.
- Saved HTTP Authentication credentials are now shared between all penetration testing tools in Acunetix WVS.
- Support for scriptable vulnerabilities make it easier for you to write new and more advanced vulnerabilities.
- Support for a wider variety of content-types.
- Scan status interface now presents the user with more real time information of the scan. The presentation is presented in a more granular way and allows you to view more information at a glance.
- Re-scan for existing vulnerabilities, to help minimize auditing time when a vulnerability is fixed and website needs to be re-scanned.
- AcuSensor Test button to verify whether AcuSensor is installed correctly.
- Ability to specify a label or tag instead of the actual input parameter name in the Input fields settings node. This provides more flexibility and reduces manual input.
- Ability to specify automated randomization of fields declared in 'Input Fields' settings.
- Well known web applications (e.g. Wordpress) finger printing module to automatically detect and launch a number of targeted security checks against such web applications.

Major Improvements

- Scan engine is 70% faster and more efficient and reduces stress on the server connection.
- Drastically improved Web 2.0 application support by implementing better handling and parsing of JSON, XML and other web 2.0 requests and responses.
- Improved detection rate of web vulnerabilities such as XSS and SQL injections.
- Improved security auditing checks for WebDav and file upload forms.
- Improved web server security auditing techniques, such as source code disclosure checks, directory listing and directory traversal security checks.
- Crawler now supports a wider variety of communication mechanisms between servers and clients which result in better and more precise

handling and detection of links, input variables and parameters. Crawler speed has also been increased drastically.

- Improved network traffic handling. Support for HTTP Keep-alive, DNS caching to help reduce DNS requests and the ability to control delay between requests. This improves performance.
- Improved HTTP Sniffer and manual crawling process by supporting much more content. Now we also have the ability to easily extend support for newer web technologies.
- HTTP authentication module now supports Digest HTTP authentication mechanism. Now Acunetix WVS also supports granular specification of credentials, i.e. per server, per directory and even per file or URL. Therefore one can use more than one pair of credentials in a single website crawl or scan.

Acunetix training and Support

Acunetix publishes a number of web security and Acunetix 'how to' technical documents on the Acunetix Web Application Security Blog; <http://www.acunetix.com/blog>.

You can also find a number of support related documents, such as FAQ's in the Acunetix WVS support page; <http://www.acunetix.com/support>.

License Scheme

Acunetix Web Vulnerability Scanner (WVS) is available in 3 editions: Small Business, Enterprise and Consultant.

Perpetual or Time Based Licenses

Acunetix WVS is sold as a one-year or perpetual license. The 1 year license expires 1 year from the date of activation. The perpetual license does not expire.

The Enterprise and Consultant editions are available as both a one-year and perpetual license. The Small Business version is available as a perpetual license only.

If you purchase the perpetual license, you must buy a maintenance agreement to get free support and upgrades beyond the first month after purchase. The maintenance agreement entitles you to free version upgrades and support for the duration of the agreement.

Small Business Edition 1 Site/Server

The Small Business edition license allows you to install one copy of Acunetix WVS on one computer, and scan one nominated site; this site must be owned by yourself (or your company) and not by third parties. Acunetix Small Business edition will leave a trail in the log files of the scanned server and scanning of third party sites is prohibited with this license. To scan multiple websites you need an Enterprise unlimited license.

To install copies on several computers, you must buy additional licenses.

Enterprise Edition Unlimited Sites/Servers

The Enterprise edition license allows you to install one copy of Acunetix WVS on one computer, and scan an unlimited number of sites or servers. The sites or servers must be owned by yourself (or your company) and not by third parties. Acunetix Enterprise edition will leave a trail in the log files of the scanned server and scanning of third party sites is prohibited with this

license. To install copies on several computers, you must buy additional licenses.

Consultant Edition

The Consultant edition license allows you to install one copy of Acunetix on one computer, and scan an unlimited number of sites or servers including 3rd party sites, provided that you have obtained permission from the respective site owners. This is the correct edition to use if you are a consultant who provides web security testing services, or an ISP. The consultant edition also includes the capability of modifying the reports to include your own company logo. This edition does not leave any trail in the log files of the scanned server. To install copies on several computers, you must buy additional licenses.

Upgrading from an Evaluation to a Purchased Edition

If you decide to purchase Acunetix WVS, you will need to un-install the evaluation edition and install the purchased edition. You will receive a new download location to obtain the unlocked and full version.

After download, simply launch the setup file. Setup will ask whether it can remove the evaluation edition and install the full edition. Any settings you have already made will be retained.

You will be able to enter the License key you received, after which setup will install the full edition and scan your website.

Extending a Purchased Edition

If you have already installed the full edition, but only want to extend the license key, you can enter your new license key in the 'Licensing' node under the 'General' section. Right-click on the General/Licensing Node, select 'License Product' and enter your new license key.

Limitations of Evaluation Edition

The evaluation version of WVS, which is downloadable from the Acunetix main website, is practically identical to the full version in functionality and in the set of tools that it presents – with the following limitations:

- Websites will be scanned only for Cross Site Scripting (XSS) vulnerabilities: only the Acunetix test websites will be scanned for all types of vulnerabilities.
- Only the default report can be generated and it cannot be printed or exported.
- Scan Results cannot be saved.

Purchasing Acunetix WVS

To purchase any of these licenses please visit:

<http://www.acunetix.com/ordering/>

Pricing can be found here:

<http://www.acunetix.com/ordering/pricing.htm>

2. Installing Acunetix WVS

System Minimum Requirements

- Microsoft Windows XP Professional or Home Edition, Windows 2000, Windows Server 2003, Windows Vista, Windows 2008 and Windows 7.
- 32 bit or 64 bit processor.
- 1 GB of RAM.
- 200 MB of available hard-disk space.
- Microsoft Internet Explorer 6 (or higher).
- Microsoft SQL Server / Microsoft Access support – if you intend to use the reporting database (optional).

Installation Procedure

1. Download the latest version of Acunetix Web Vulnerability Scanner from the download location provided to you when you purchased the license. Double click on the webvulnscan7.exe file to launch the Acunetix WVS installation wizard and click 'Next'.
2. You will be asked to review and approve the License agreement and to enter your Name, Company Name and License key. If you are evaluating the product, leave the license key edit box blank.
3. Select the folder location where you want to install Acunetix Web Vulnerability Scanner. You also have to choose whether to install the Acunetix Firefox toolbar and choose whether a program shortcut icon is to be created on the desktop.
4. Click Install to start the installation. Setup will now copy all files and install the necessary Windows Service. Click 'Finish' when ready and the Acunetix WVS main window will launch, unless the option is un-ticked.

Note: If using the evaluation edition, you will only be able to scan one of the Acunetix test websites:

http://testphp.vulnweb.com - A test website with PHP technology
http://testasp.vulnweb.com - A test website with ASP technology
http://testaspnet.vulnweb.com - A test website with ASP.NET technology

Furthermore, you will not be able to save the scan results

Upgrade Procedure

Note: Acunetix WVS Version 7 will be installed alongside your current Acunetix WVS Version 6.5 install. If you would like to remove Acunetix WVS Version 6.5, run the uninstall from the Acunetix WVS program group.

1. Double click on webvulnscan7.exe file to launch Acunetix WVS installation wizard. The installer automatically detects any builds of the same version and will display a dialog which gives you a choice to continue or not.
2. Click on 'Yes' to proceed with the upgrade.

3. At this point the uninstaller is automatically launched and it will verify that you want to uninstall the previous version of Acunetix WVS. Click on 'Yes' to proceed with the upgrade.

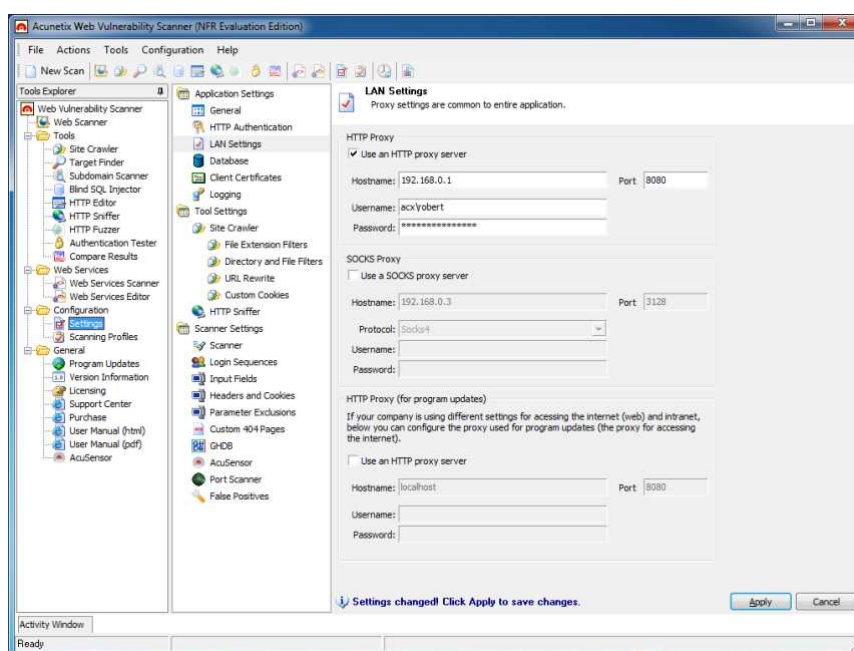
4. To keep your past scan results and use them in the new version of Acunetix WVS, select 'No' when asked to remove the current database.

5. The rest of the installation procedure will be identical to a new.

6. Once the installation is finished, run Acunetix WVS. The application will present a dialog to import any previous settings from the previous build or version that was installed. Click on 'Yes' to restore any previous configurations to the new version or build just installed.

Note: Due to major changes saved scan results from Version 6.5 are not compatible with Version 7, hence why you can run Acunetix WVS Version 6.5 and 7 on the same machine.

Configuring an HTTP Proxy or SOCKS proxy Server



Screenshot 5 - LAN HTTP Proxy Settings

If your machine is located behind a proxy server, you need to configure the Proxy server settings in Acunetix WVS. To do this:

Navigate to the Configuration > Settings > Application Settings > LAN Settings node to access the HTTP Proxy and SOCKS proxy settings page shown in the above screenshot.

HTTP Proxy Settings

- **Use an HTTP proxy server** - Tick the check box to configure Acunetix WVS to use a HTTP proxy server.
- **Hostname and Port** - Hostname (or IP address) and port number of the HTTP proxy server.
- **Username and Password** - Credentials used to access the proxy. If no authentication is required, leave these options empty.

SOCKS Proxy Settings

- **Use a SOCKS proxy server** - Tick the check box to configure Acunetix WVS to use a SOCKS proxy server.
- **Hostname and Port** - Hostname (or IP address) and port number for the SOCKS proxy server.
- **Protocol** - Select which SOCKS protocol to use. Both Socks v4 or v5 protocols are supported by Acunetix WVS.
- **Username and Password** - The credentials used to access this proxy. If no authentication is required, leave these options empty.

HTTP Proxy Settings (For program updates)

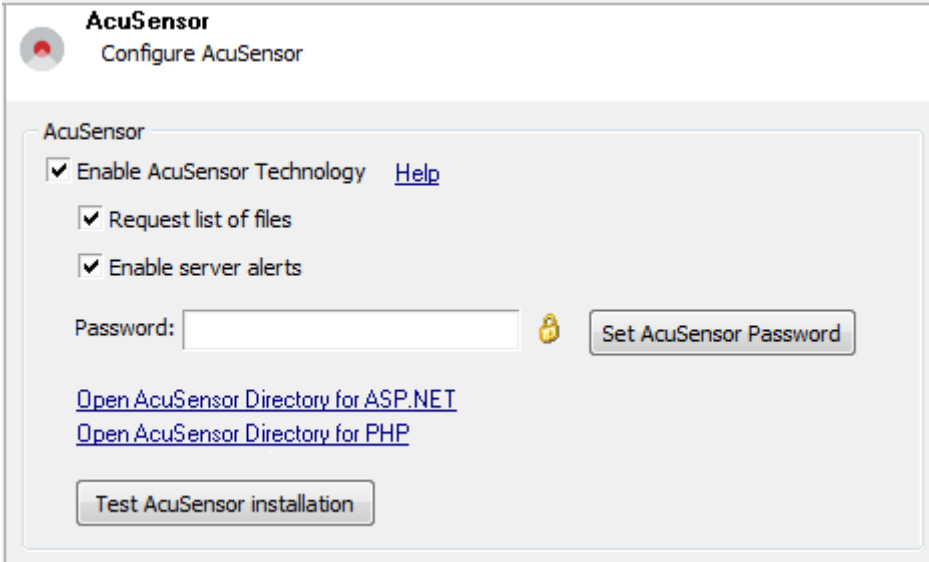
If you are using different Proxy servers for accessing the internet (web) and intranet (internal network), you can configure a different Proxy server for program updates.

Configuring AcuSensor Technology

Acunetix' unique AcuSensor Technology is a security technology that allows you to identify more vulnerabilities than a traditional Web Application Scanner, whilst generating less false positives. In addition, it indicates exactly where in your code the vulnerability is and reports debug information.

It is not required to install and use AcuSensor technology, Acunetix can be used as a 'pure' black-box scanner too, but it is recommended as it improves the results significantly. To install Acunetix' AcuSensor Technology;

Step 1: Configure the Sensor



The screenshot shows the 'Configure AcuSensor' window. At the top left is the AcuSensor logo and the title 'Configure AcuSensor'. Below this is a section titled 'AcuSensor' containing several options: a checked checkbox for 'Enable AcuSensor Technology' with a 'Help' link; a checked checkbox for 'Request list of files'; and a checked checkbox for 'Enable server alerts'. There is a 'Password:' label followed by an empty text input field, a lock icon, and a 'Set AcuSensor Password' button. Below these are two links: 'Open AcuSensor Directory for ASP.NET' and 'Open AcuSensor Directory for PHP'. At the bottom is a 'Test AcuSensor installation' button.

Screenshot 6 – AcuSensor Technology Settings

Run the Acunetix WVS scanner and go to the 'Configuration > Settings' node in the Tools Explorer. Click on 'AcuSensor Technology' under 'Scanner Settings' node and configure the following options:

- **Enable AcuSensor Technology** – Select this option to enable Acunetix AcuSensor Technology during a scan.
- **Request List of files** – Select this option to use the Acunetix AcuSensor Technology to retrieve a list of all files present in the website directory and scan them.

- **Enable Server Alerts** – Select this option so the Acunetix AcuSensor Technology will report back server and platform configuration problems.
- **Password** – Click on the Padlock Icon to generate a random password unless you want to specify one yourself. Once a new password is specified, click on 'Set AcuSensor Password' to generate the Acunetix AcuSensor Technology agent files with the new specified password.
- **Test AcuSensor Installation** – Use this button to check if AcuSensor Technology is installed correctly on a remote website. Click on the button, enter a URL of a file and click 'OK' to check if AcuSensor is installed correctly or not.

Note: Each time the password is changed and AcuSensor Technology agent files are generated, the AcuSensor Technology agent files on the server must be updated. In a .NET scenario, you must un-inject the files and uninstall the Acunetix AcuSensor Injector' from the target server, copy the new setup.exe on the target system and install it again. Re-inject the files for .NET. For PHP simply overwrite the old 'acu_phpaspect.php' with the new one.

Step 2: Installing the Sensor

.NET

1. From the Acunetix AcuSensor Technology page, click on 'Open AcuSensor Technology directory for ASP.NET' and copy 'Setup.exe' to the remote server where the target website is hosted. The application requires Microsoft .NET Framework 3.5 to install.
2. Click on Setup.exe to start the Acunetix .NET AcuSensor Technology Injector installation and specify the installation path. The application will start automatically once the installation is ready, unless the option 'Start application after installation is finished' is uticked. If the application is not set to start automatically, click on 'Acunetix .NET AcuSensor Technology Injector' from the program group menu.

Note: On Windows 2008, install IIS 6 Metabase Compatibility from 'Control Panel > Turn Windows features On or Off > Roles > Web Server (IIS) > Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility' to be able to list all .NET applications running on server.

PHP

1. From the Acunetix AcuSensor Technology settings page:
 - a. click on 'Open AcuSensor Technology directory for PHP'
 - b. copy the file 'acu_phpaspect.php' to the remote server (where the target website is hosted) to a location where it can be accessed from the web server software.

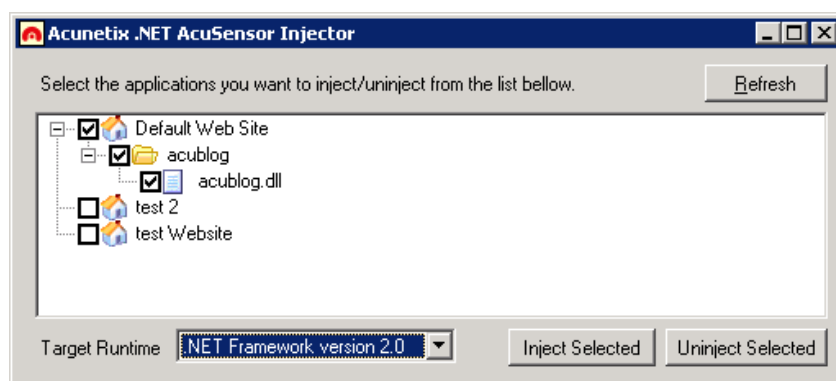
Note: For PHP there is no installation procedure. As explained below, in PHP the AcuSensor Technology file is appended to any PHP file via a configuration in the web server. Acunetix AcuSensor Technology works on PHP 5 and onwards. Previous PHP versions are not supported.

Step 3: Enabling the Sensor

.NET

1. On starting up, the Acunetix .NET AcuSensor Technology Injector will retrieve a list of .NET applications installed on your server. Select which applications you would like to inject with AcuSensor Technology and select the Framework version from the drop down menu.

2. Click on 'Inject Selected' to inject the AcuSensor Technology code in the selected .NET applications. Once files are injected, close the confirmation window and also the AcuSensor Technology Injector.



Screenshot 7 – Acunetix .NET AcuSensor Technology Injector

PHP

In PHP there are two methods to install the sensor. Method one can be used to install the Acunetix AcuSensor Technology on Apache only and Method 2 can be used to install the Acunetix AcuSensor Technology both on Apache and IIS.

Method 1: .htaccess file (Apache)

1. Create a .htaccess file in the website directory and add the following directive: **php_value auto_prepend_file '[path to acu_phpaspect.php file]'**.

Note: For Windows use 'C:\sensor\acu_phpaspect.php' and for Linux use '/Sensor/acu_phpaspect.php' path declaration formats. If Apache does not execute .htaccess files, it must be configured to do so. Refer to the following configuration guide: <http://httpd.apache.org/docs/2.0/howto/htaccess.html>. The above directive can also be configured in the httpd.conf file.

Method 2: php.ini (IIS and Apache)

1. Locate the file 'php.ini' on the server by using phpinfo() function. Click here for more information about phpinfo() function.
2. Search for the directive **auto_prepend_file**, and specify the path to the acu_phpaspect.php file. If the directive does not exist, add it in the php.ini file: **auto_prepend_file="[path to acu_phpaspect.php file]"**.
3. Save all changes and restart the web server for the above changes to take effect.

Disabling and uninstalling the Sensor

.NET

1. Run the Acunetix .NET AcuSensor Technology Injector from the program group and select the already injected code. Click on 'Uninject Selected' to remove the AcuSensor Technology code from the .NET applications. On success confirmation, close the confirmation window and the Acunetix .NET AcuSensor Technology Injector.
2. Run uninstall.exe from the application's installation directory.

Note: If you uninstall the Acunetix .NET AcuSensor Technology Injector without un-injecting the .NET application, then the AcuSensor Technology code will not be removed from your .NET application.

PHP

1. Delete the directive: **php_value auto_prepend_file="[path to acu_phpaspect.php file]"** from the .htaccess file or from the 'httpd.conf' configuration if method 1 is being used. If method 2 is being used, delete the directive: **auto_prepend_file="[path to acu_phpaspect.php file]"** from the php.ini file.

2. Delete the Acunetix AcuSensor Technology php file; acu_phpaspect.php.

Note: Although the Acunetix AcuSensor Technology requires authentication, uninstall / remove the AcuSensor Technology client files if they are not being used anymore.

3. Scanning Your Website

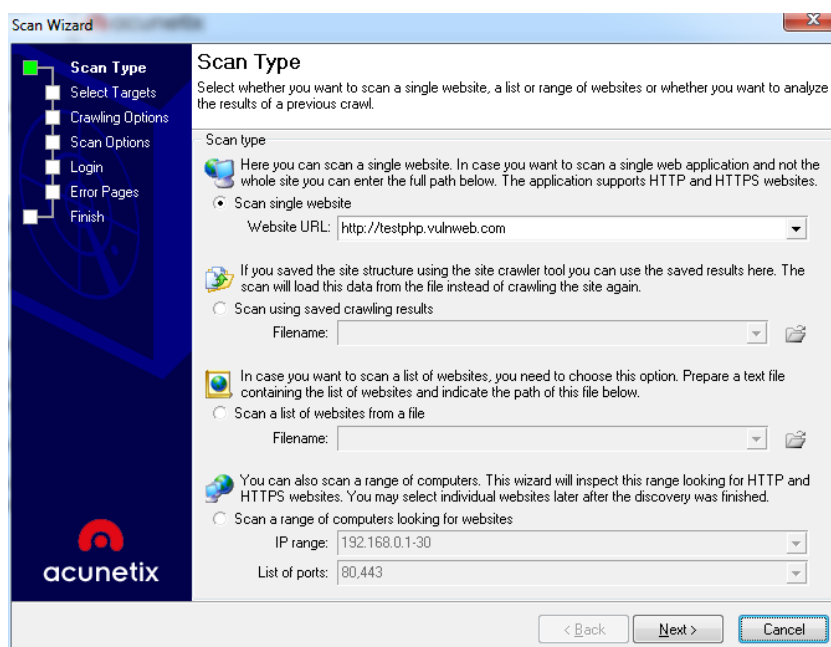
Starting a Scan

The Scan Wizard allows you to quickly scan your website and provides a comprehensive overview of the security of your website. This chapter explains the process of launching a security audit of your website.

NOTE: DO NOT SCAN A WEBSITE WITHOUT PROPER AUTHORISATION! The web server logs will show the scans and any attacks made by Acunetix WVS. If you are not the sole administrator of the website please make sure to warn other administrators before performing a scan. Some scans might cause a website to crash requiring a restart of the website.

Step 1: Select Target(s) to Scan

1. Click on 'File > New > New Website Scan' to start the Scan Wizard or click on 'New Scan' button on the top right hand of the Acunetix WVS user interface.



Screenshot 8 – Scan Wizard Select Scan Type

2. Specify the website(s) to be scanned. The scan target options are:

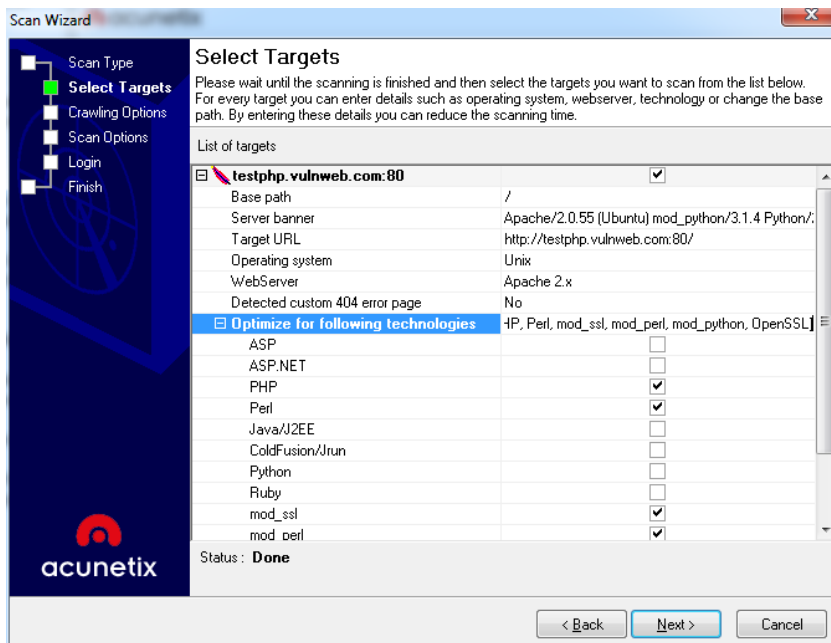
- **Scan single website** - Scans a single website. Enter a URL, e.g. `http://testphp.vulnweb.com`.
- **Scan using saved crawling results** - If you previously performed a crawl on a website and saved the results, you can launch a scan against the saved crawl, instead of having to crawl the website again.
- **Scan List of Websites** - Scans a list of target websites specified in a plain text file (one target per line). Every target in the file is to be specified in the format `<URL>` or `<URL:port>` if the web server is listening on a non default port. The maximum number of websites Acunetix WVS can scan

at one time is between 20 and 30 sites; depending on the size of the websites.

- **Scan Range of Computers** - This will scan a specific range of IP's (e.g. 192.168.0.10-192.168.0.200) and port range (80,443) for available target sites. Port numbers are configurable.

3. Click 'Next' to continue.

Step 2: Confirm Targets and Technologies Detected



Screenshot 9 – Scan Wizard Selecting Targets and Technologies

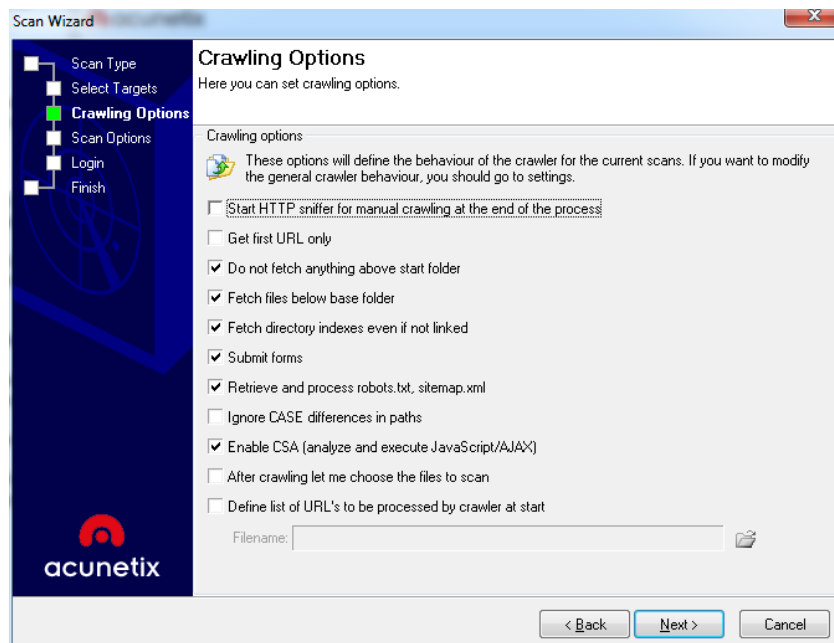
Acunetix WVS will automatically fingerprint the target website(s) for basic details such as operating system, web server, web server technologies and whether a custom 404 error page is being used (For more details on Custom 404 Error Pages refer to page 30 of this manual).

The web vulnerability scanner will optimize the scan for the selected technologies by reducing the number of tests performed. E.g. Acunetix WVS will not launch IIS security checks against a Linux system. This will reduce scanning time.

Click on the relevant field and change the settings from the provided check boxes if you would like to add or remove scans for specific technologies.

Note: if a specific web technology is not listed under 'Optimize for the following technologies', it means that there are no specific tests for it.

Step 3: Specify Crawler Options



Screenshot 10 – Scan Wizard Crawling Options

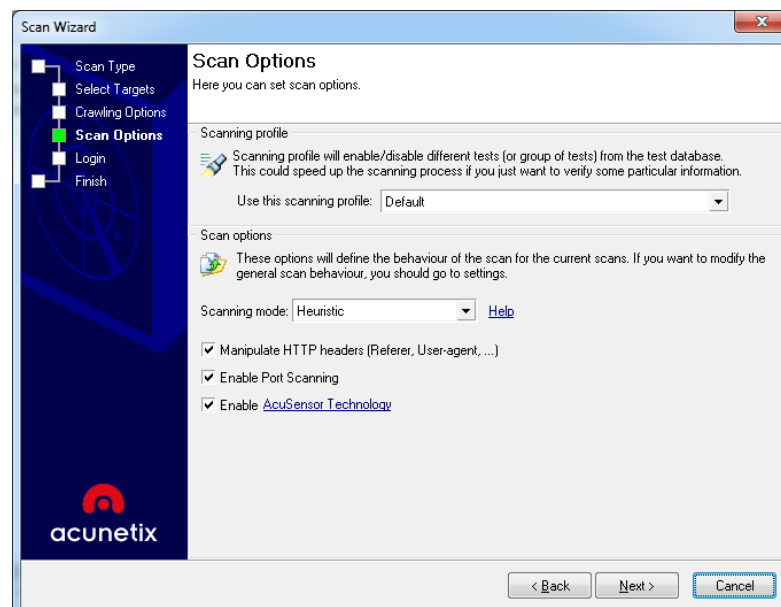
In this dialog you can configure the website crawling options.

Crawling Options

The Crawler traverses the entire website and identifies its structure and parameters. You can configure one or more crawling options, however if the scan is being launched from a saved crawl result, these options will be grayed out because the crawling options used for the original crawl will be retained.

Note: You can use the default crawling options or tweak them. In this case refer to Configuring the Crawler section on page 48.

Step 4: Specify Scanning Profile and Mode



Screenshot 11 – Scanning Profile and Mode Options

In this dialog you can configure the scanning profile and scan options.

Scanning Profile

The **Scanning Profile** will determine which tests are to be launched against the target website. For example, if you only want to test your website(s) for SQL injection, select the profile `sql_injection`. No additional tests will be performed.

Refer to the 'Scanning Profiles' section on page 85 for more information on how to customize existing scanning profiles or create new scanning profiles.

Scan Options

From this section you can select the **Scanning Mode** for the crawling and scanning of the target website. The scan mode will determine how both the crawler and the scanner will treat website parameters (also known as inputs), which will affect the number of security checks launched against the website. The scanning mode options available are the following:

- **Quick** - In this mode, the crawler will only fetch a very limited number of variations of each parameter, because they are not considered to be actions parameters. Action parameters are parameters which are designed to control the execution flow of the server scripts.
- **Heuristic** - In this mode, the crawler will try to make heuristic decisions on which parameters should be considered as action parameters and which should not. It will try to fetch more possible values of each parameter. This will result in a larger number of different variations, and therefore the scanner will launch more security checks against the website.
- **Extensive** - In this mode, the crawler will fetch all possible values and combinations of all parameters. This will lead to a much larger number of variations, and therefore the scanner will take much longer to complete the scan.

The other options which you can select from this step of the wizard are:

- **Manipulate HTTP headers** - With this option enabled, the scanner will try to manipulate the HTTP headers. If HTTP headers are successfully manipulated, a vulnerability such as SQL injection can be discovered.
- **Enable Port Scanning** - Enable this option to run the port scanner against the web server during a website scan. For more details about the Port Scanner and Network Security checks refer to page 85 'Configuring the Port Scanner'.
- **Enable AcuSensor Technology** - Tick this option to enable AcuSensor Technology during the scan. Note that the AcuSensor client has to be installed on the web server which is being scanned. For more details about the AcuSensor Technology refer to page 19.

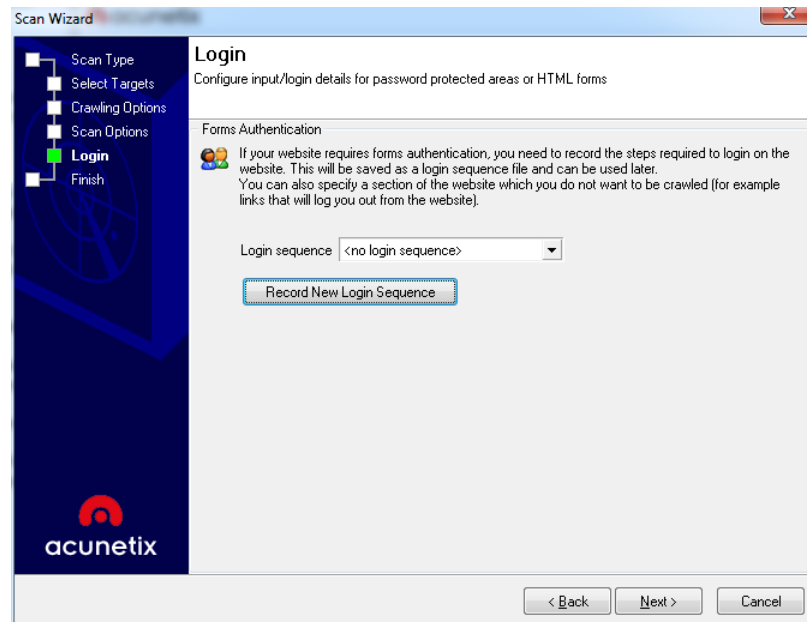
Note: If the scan is being launched from saved crawl results, in the Enable AcuSensor Technology option you can specify to use sensor data from crawling results without revalidation, or to not use sensor data from crawling results only, or else to revalidate sensor data..

Step 5: Configure Login for Password Protected Areas

There are 2 types of Login pages:

- **HTTP Authentication** - This type of authentication is handled by the web server, where the user is prompted with a password dialog.

- **Forms Authentication** - This type of authentication is handled via a web form not via HTTP. The credentials are sent to the server for validation by a custom script.

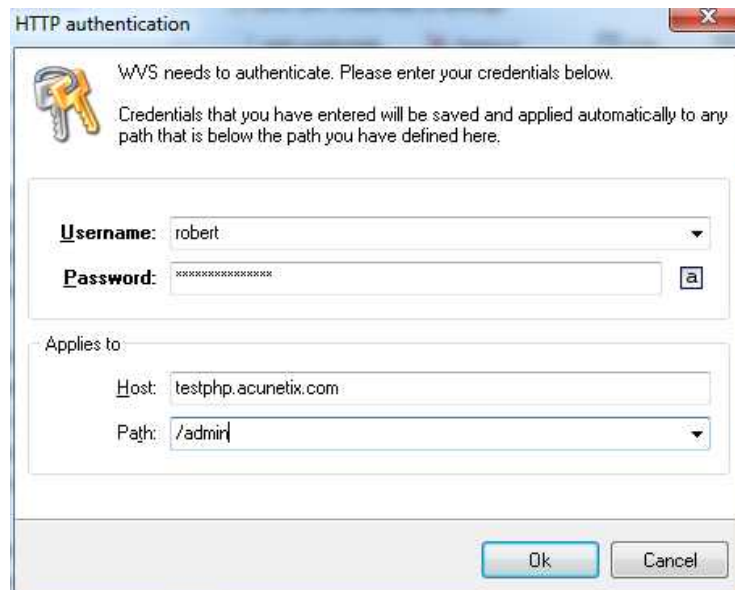


Screenshot 12 - Login Details Options

Scanning a HTTP password protected area:

If you scan an HTTP password protected website, you will be automatically prompted to specify the username and password. Acunetix WVS supports multiple sets of HTTP credential for the same target website. HTTP authentication credentials can be configured to be used for a specific website / host, url or even for a specific file only. To specify HTTP authentication credentials:

1. Go to Settings > Application Settings > HTTP Authentication.
2. Click on the 'Add credentials' button.



Screenshot 13 – HTTP Authentication

3. Enter the Username and Password. In the 'Host' text box field specify the main website URL, e.g. testphp.vulnweb.com. In the 'Path' text box, specify

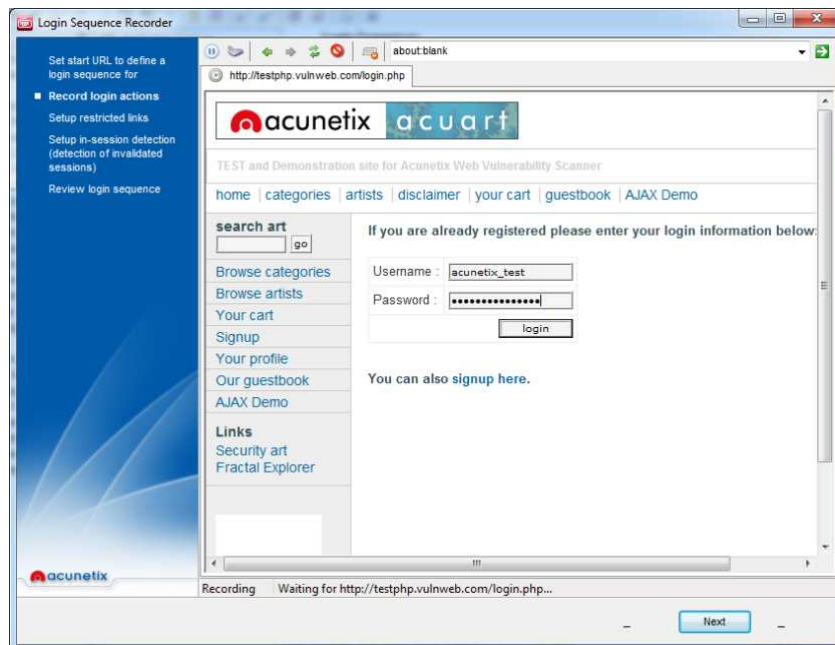
the path for where the credentials should be used, e.g. protected/. Do not specify a path if the credentials are needed site wide.

HTTP authentication options

- **Don't ask for authentication automatically** – By default, when a target website requires HTTP authentication during a crawl and scan, a window will automatically pop up allowing you to enter credentials. If this option is switched off, Acunetix WVS will continue crawling and scanning the website without authenticating, therefore protected website parts will not be crawled and scanned.
- **Save new credentials to settings** – If you specify a set of new credentials during a crawl or scan, if this option is switched on, the credentials and their URL are automatically saved in the Acunetix WVS scanner settings for future use.

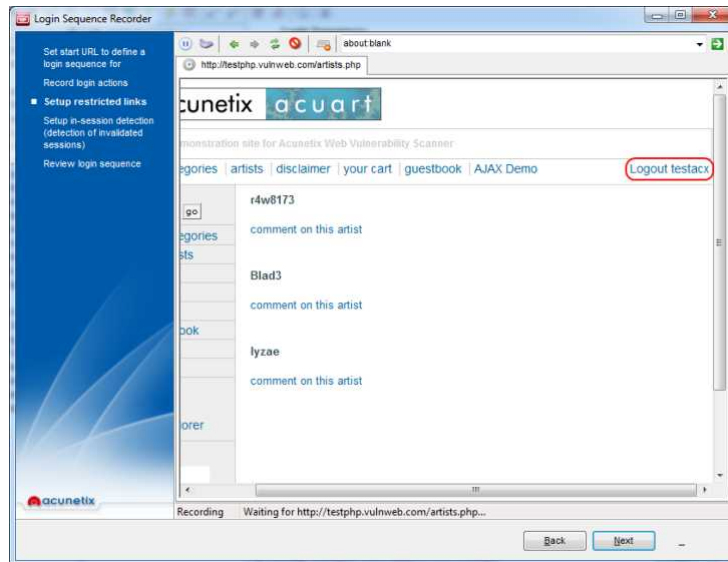
Scanning a form based password protected area:

1. Click on 'Record new login sequence' and enter the URL of the website for which you would like to record a login sequence. By default the URL of the target website is automatically populated. Click 'Next' to proceed.



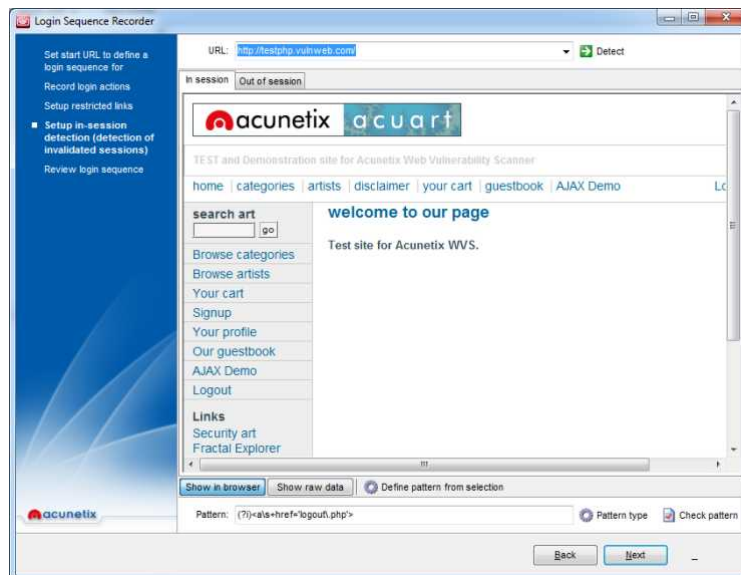
Screenshot 14 – Login Sequence Recorder

2. In the second step of the wizard, browse to the login page, enter the credentials and authenticate. Wait for the page to fully load after logging in and then click 'Next'.



Screenshot 15 – Specify an excluded link

3. Once authenticated, you also need to identify the logout link so the crawler will not access it and log out the session. In the 'Setup restricted links' step of the wizard, click on the logout link. If the logout link is not in the same page, click on 'Pause' in the top menu, navigate to a page where there is the logout link, resume the session and click on the logout link. Click 'Next' to proceed.



Screenshot 16 – Specify an 'In session' or 'Out of session' pattern

4. In this step, you have to specify 'In Session' or 'Out of Session' detection patterns. In the 'In-session detection' specify a pattern which allows the crawler to detect that the session is still valid. If the session for some reason expires during a crawl, the crawler will automatically re-login. Click on 'Detect' so Acunetix WWS will try to automatically detect the pattern.

If the automatic detection does not work, you must specify the pattern manually. The pattern can be plain text or a regular expression, e.g. `(?!<a\s+href='logout.php'>`. One can also highlight specific content and click on 'Define pattern from selection' and a regular expression will be automatically generated.

5. You also have to specify where the pattern can be found from the 'Pattern Type' drop down menu. The options are 'In headers', 'Not in headers', 'In body', 'Not in body', 'Status code is' and 'Status code is not'. Click on 'Check

Pattern' to verify that the crawler is able to recognize the difference between a logged in session and a logged out session. Click 'Next' to proceed with the wizard.

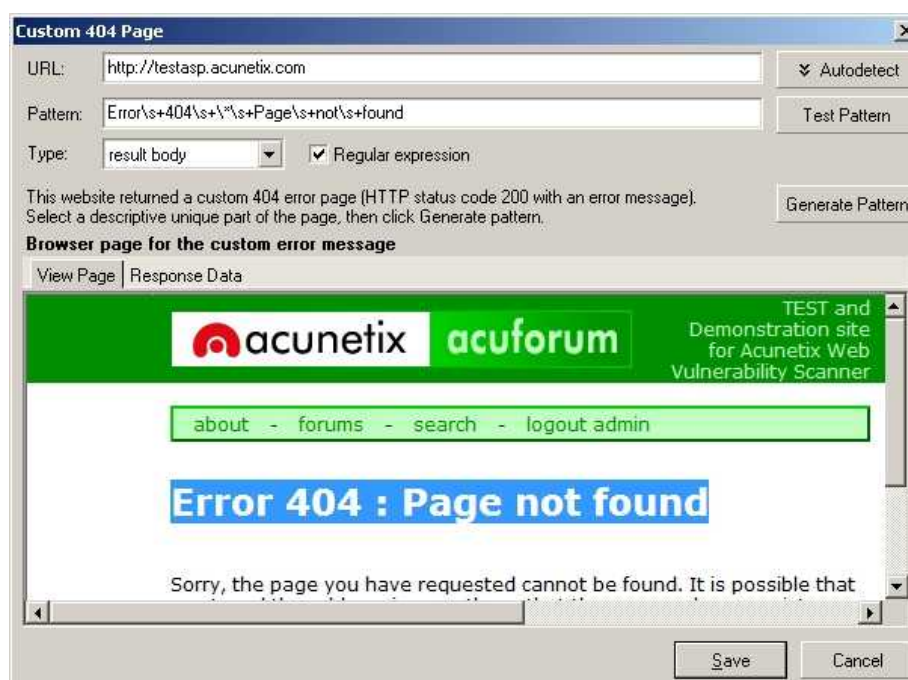
6. In the last step of the wizard, you can review the recorded sequence. One can change priority of url's, edit requests and add or remove requests. Click 'Finish' to finalize the session recording.

Note: Login sequences are saved in the Acunetix installation directory, in the sub directory '\Data\General\LoginSequences'.

Note: The Login Sequence Recorder can also be used to configure Acunetix WVS to crawl a web application in a pre-defined manner, such as a shopping cart or to automatically input data into a web form. For more information on the Login Sequence Recorder and its uses, see the section 'Login Sequence Recorder' on page 7575.

Step 6: Configure Custom 404 Error Pages

A 404 error page is the page which appears when a requested page is not found. In many cases, rather than returning an HTTP Status Code "404 Not Found", websites return an HTTP Status Code of 200 Success and show a page formatted according to the look and feel of the website to inform the user that the page requested does not exist. Custom 404 error pages do not necessarily represent a server 404 error (Page not found), and therefore Acunetix WVS must be able to automatically identify these pages, to detect the difference between a non existing URL and a valid web page.



Screenshot 17 - Custom Error Page Configuration

To configure a custom error page:

1. The scan wizard will automatically try to detect whether the site uses custom error pages.
2. If it does, WVS will display the custom error page and will automatically attempt to locate a unique pattern on the error page. If the string is correct, click 'Save' to continue. You can skip the remaining steps.
3. If the unique pattern is not correct or cannot be detected, highlight the text that is unique to this custom error page (text should not be found on any other page of the website), e.g. "Error 404: Page not found" and click on the

'Generate pattern' button. This will generate a regular expression from the highlighted text which will appear in the 'Pattern' textbox.

4. From the 'Type' drop down menu, select one of the following:

- **Location header** - To look for the defined pattern in the header of the custom error page.
- **Result Body** - To look for the defined pattern in the body of the custom error page.
- **Result** - To look for the defined pattern in both the header and body of the custom error page.

5. Click 'Save' to save this custom error page configuration.

Note: you can edit the custom 404 error page detection later from Settings > Scanner Settings > Custom 404 Pages node.

Step 7: Select the Files and directories to Scan

If the option 'After crawling let me choose the files to scan' was ticked in the crawling options, a window with the crawled site structure will automatically pop up at the end of the crawl, from which you can select which files to scan.

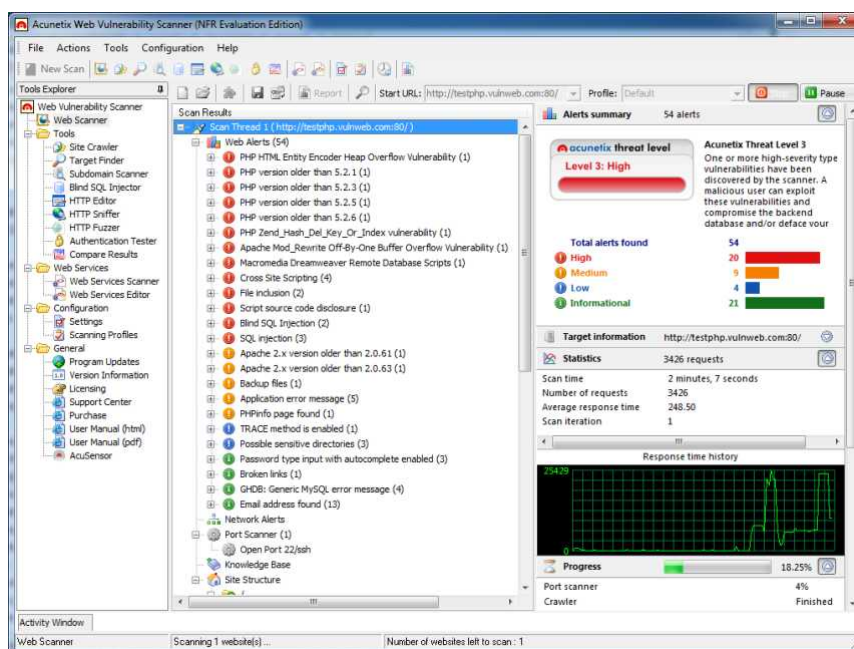
Step 8: Completing the scan

If you want to automatically save the scan results to the reporting database, enable the option 'Save scan results to the database for report generation' in the last step of the scan wizard. Click on the 'Finish' button to start the scan. Depending on the size of the website and the server response time, a scan may take several hours!

4. Analyzing the Scan Results

Introduction

During the scan, security alerts that are discovered on the website are listed in real time under the Alerts node in the 'Scan Results' window. A node 'Site Structure' is also created which lists and folders discovered.



Screenshot 18 - Scan Result and Information window

Web Alerts node

The Web Alerts node displays all vulnerabilities found on the target website. Web Alerts are sorted into four severity levels:

| | |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Severity HIGH | High Risk Alert Level 3 – Vulnerabilities categorized as the most dangerous, which put a site at maximum risk for hacking and data theft. |
| Severity MEDIUM | Medium Risk Alert Level 2 – Vulnerabilities caused by server miss-configuration and site-coding flaws, which facilitate server disruption and intrusion. |
| Severity LOW | Low Risk Alert Level 1 – Vulnerabilities derived from lack of encryption for data traffic, or directory path disclosures. |
| Severity INFO | Informational Alert – Sites which are susceptible to revealing information through GHDB search strings, or email address disclosure. |

The number of vulnerabilities detected is displayed in brackets () next to the alert categories. If a vulnerability is reported by AcuSensor Technology, (AS) is displayed next to the vulnerability group. More information about the vulnerability is shown when you click on an alert category node:

- **Vulnerability description** - A description of the discovered vulnerability.

- **Affected items** - The list of files which are vulnerable to the discovered vulnerability.
- **The impact of this vulnerability** - What impact this vulnerability can have on the website or web server if the reported vulnerability is exploited.
- **Attack details** - Details about the parameters and variables used to test for this vulnerability. E.g. For a Cross Site Scripting alert, the name of the effected input variable and the string it was set to will be displayed. In this node, you can also find the HTTP Request sent to the web server and the Response sent back by the web server, and also the HTML response. The attack can be inspected and re-launched manually by clicking 'Launch the attack with HTTP Editor'. From the attack details section, you can also mark an alert as false positive. For more information about the HTTP Editor, please refer to the 'HTTP Editor' chapter on page 79.
- **How to fix this vulnerability** - This section provides recommendations on how to fix the vulnerability.
- **Detailed information** - This section provides detailed information about the vulnerability.
- **Web references** - A list of web links with more information on the vulnerability and how to fix it.

Note: A vulnerability can be removed from the False Positive list by navigating to 'Configuration > Settings' node in the Tools Explorer and 'Scanner Settings > False Positives' node.

Network Alerts Node

The Network Alerts node displays all vulnerabilities discovered in scanned network services, such as DNS, FTP and SSH servers. Network alerts are sorted into four severity levels (similar to web alerts). The number of vulnerabilities detected is displayed in brackets () next to the alert categories. By clicking on an alert category node more information will be shown (similar to web alerts).

Note: You can switch off network security checks by un-ticking the option 'Enable Port Scanning' in the scan wizard.

Port Scanner Node

The Port Scanner node displays all the discovered open ports on the server. Click on an open port to view the network service banner.

Note: Port Scanning of the target server can be switched off by un-ticking the option 'Enable Port Scanning' in the scan wizard.

Knowledge Base Node

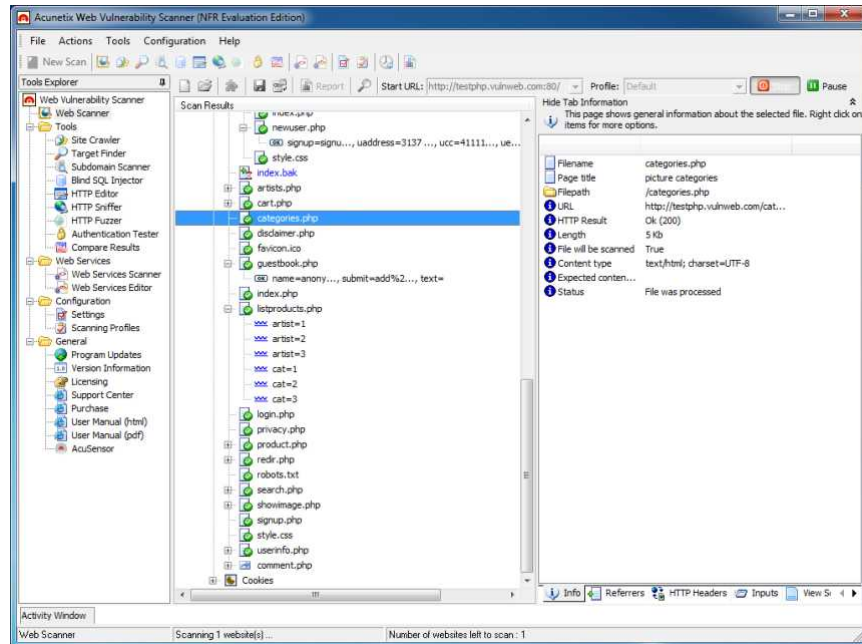
The knowledge base node displays the following items:

- List of open TCP ports found on the server, including the port banner.
- List of Network Services running on the web server and their response.
- List of files with inputs found on the website. It also lists how many inputs each file has.
- List of links to external hosts found on the website. E.g. testphp.vulnweb.com contains a link to www.acunetix.com.

- List of uncommon HTTP responses and the HTTP requests that generated uncommon HTTP Errors, such as Server Internal Error – HTTP 500.

Site Structure Node

The Site Structure Node displays the layout of the target website including all files and directories discovered during the crawling process.



Screenshot 19 - Scan Result and Information window

In the crawling results (Site Structure node), different colors are used to differentiate files. The filename color coding is as follows;

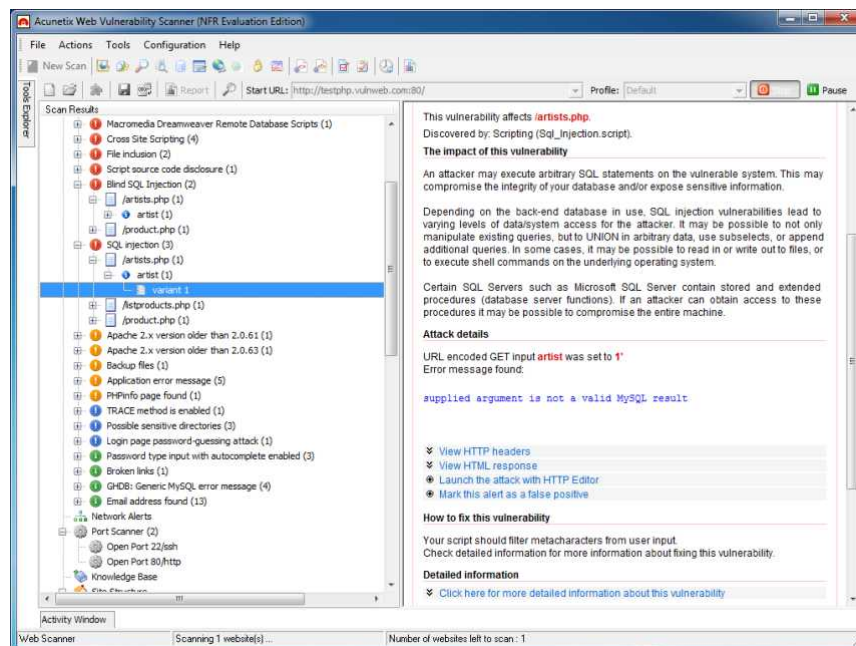
- Green – File returns AcuSensor Technology related data
- Blue – File detected by scanner and not by crawler, e.g. File was not linked from anywhere, therefore it was not found by the crawler, but by a vulnerability tests during the scanning stage
- Black – Files discovered by the crawler

For every discovered item, more detailed information is available in the right Information pane. Summary information for a selected file or directory includes:

- **Info** - Generic information about the highlighted file such as file name, page title, path, URL etc.
- **Referrers** - A list of other files on the website which linked to this selected file.
- **HTTP Headers** - The HTTP request sent to the web server to retrieve the selected file and the HTTP response headers received from the web server when requesting the selected file.
- **Inputs** - A list of detected parameters in the selected file. A list of possible parameter values is also shown.
- **View Source** - The source HTML sent to Acunetix WVS when accessing the selected file.
- **View Page** - The page is displayed as it is shown in a web browser. Most client side scripts are disabled in this tab to avoid launching vulnerabilities against the computer on which Acunetix WVS is running.

- **HTML Structure Analysis** - Specific HTML structure information can be found in the HTML of the selected file. E.g. comments, links, client scripts, input forms, Meta tags etc.
- **AcuSensor Data** – If the highlighted item returned AcuSensor Technology data during a crawl and a scan, this information will be displayed in this tab.
- **Alerts** – A list of alerts this item is vulnerable to can be found in this tab.

Grouping of Vulnerabilities



Screenshot 20 – Grouping of vulnerabilities

When a number of the same vulnerability is detected, on a number of different pages, the scanner will group these variants under one alert node. Upon expanding an alert node, you are presented with the vulnerable pages, and upon expanding further, you are presented with the vulnerable parameters of that page, as can be seen in the above screen shot.

This vulnerability reporting makes it easier to keep track of vulnerable pages and what vulnerabilities need to be fixed. Vulnerability data can also be presented in a report by method of grouping, by selecting the Vulnerability Report template in the reporting application.

Saving a Scan Result

When a scan is completed you can save the scan results to an external file for analysis and comparison at a later stage. The saved file will contain all the scans from the current session including alert information and site structure.

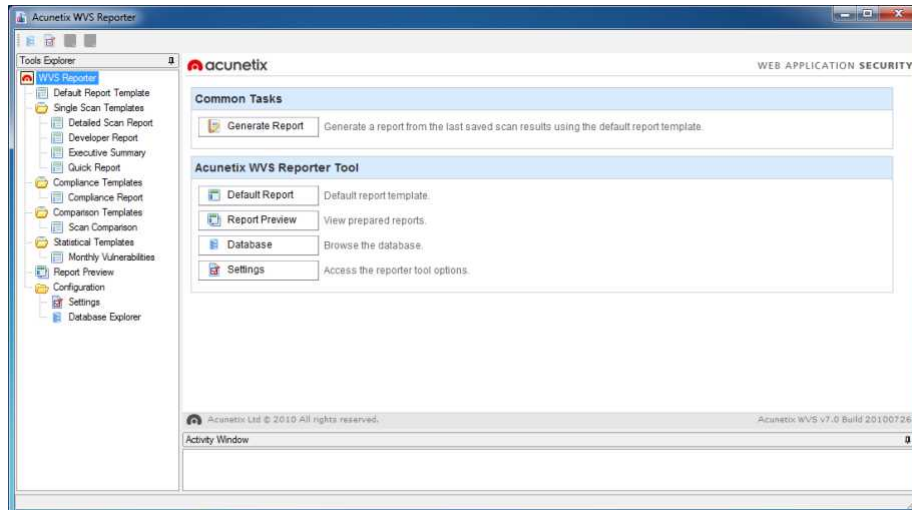
To save the scan results go to 'File' and select 'Save Scan Results'.

To load the scan results go to 'File' and select 'Load Scan Results'.

If the option 'Save scan results to database for report generation' is not ticked in the wizard, where by default it is ticked, no reporting details are saved from the scan. So to generate a report from a saved scan one has to import the scan details to the reporting database. To do so, right click 'Web Scanner' node and select 'Import scan results to database'.

5. Generating a Report from the results

Introduction to the Reporter



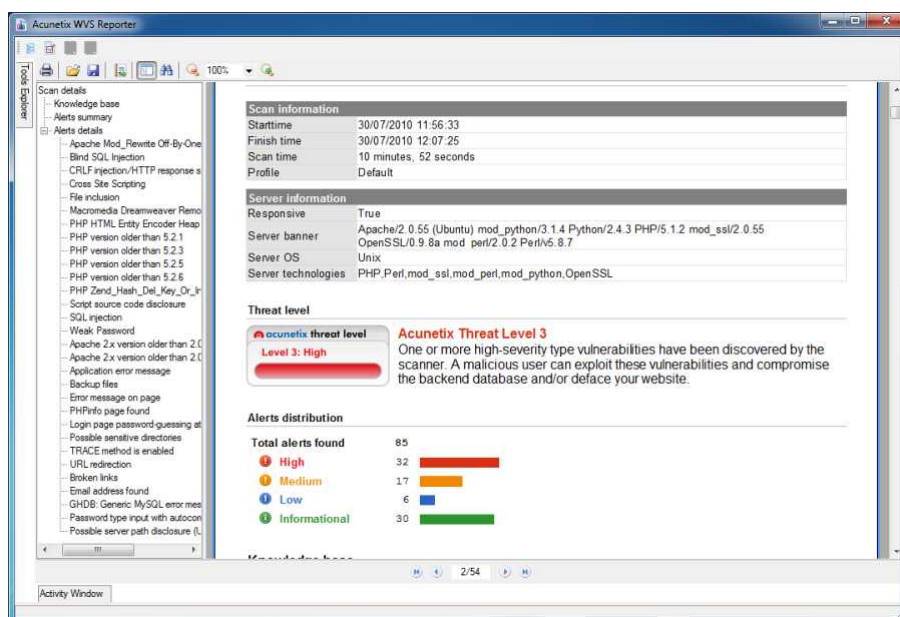
Screenshot 21 – The Reporter Application

The Reporter Application is a separate application which allows you to generate reports on the security scans that you have performed. It can be launched directly from the Acunetix WVS interface from a completed scan or from the Acunetix WVS program group. The following groups of reports are available

- Developer Reports – Shows effected pages and files
- Executive Reports – Summary of security of the website
- Vulnerability Report – List vulnerabilities and their impact
- Comparison Report – compare against previous scans
- Statistical Reports – Compile trend analysis
- Compliance Standard reports – PCI DSS, OWASP, WASC and more

Generating a Report from the Scan Results

To generate a report, click on the  **Report** button on the toolbar at the top. This will start the Acunetix WVS Reporter.

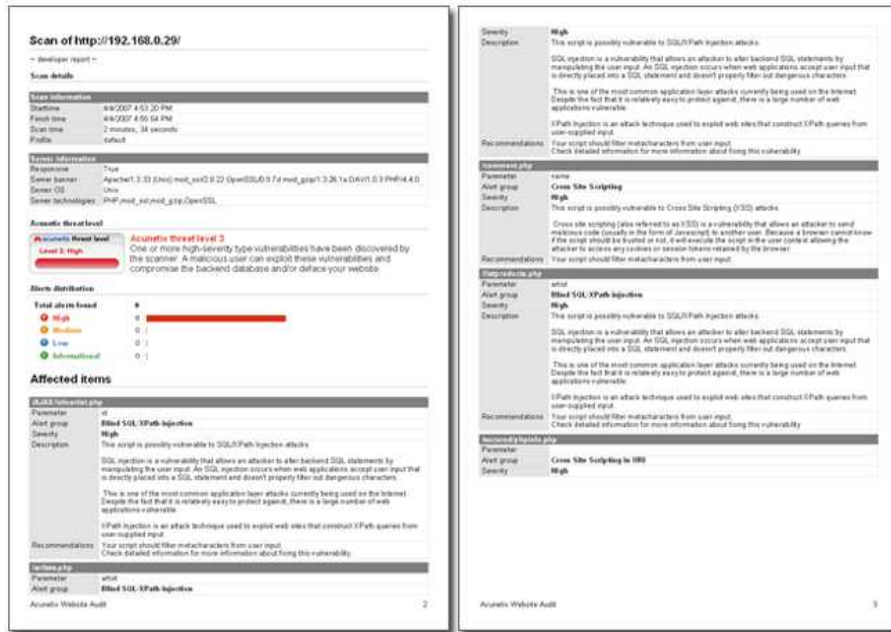


Screenshot 22 – Default Generated Report from Scan Results

From here you can generate a Developer Report, Executive Report, Compliance Report and many other types of reports. Once the report is generated, it can be exported to various formats including PDF and HTML. To generate a report follow the below procedure;

1. Select the type of report you would like to generate and click on 'Report Wizard' to launch a wizard to assist you in generating the report.
2. If you are generating a compliance report, select the type of compliance report. If you are generating a comparison report, select the scans you would like to compare. If you are generating a monthly report, specify the month and year you would like to report. Click 'Next' to proceed to the next step.
3. Configure the scan filter to list a number of specific saved scans, or leave the default selection to display all scan results. Click 'Next' to proceed and select the specific scan for which to generate a report.
4. Select what properties and details should the report include. Click 'Generate' button to finalize the wizard and generate the report.

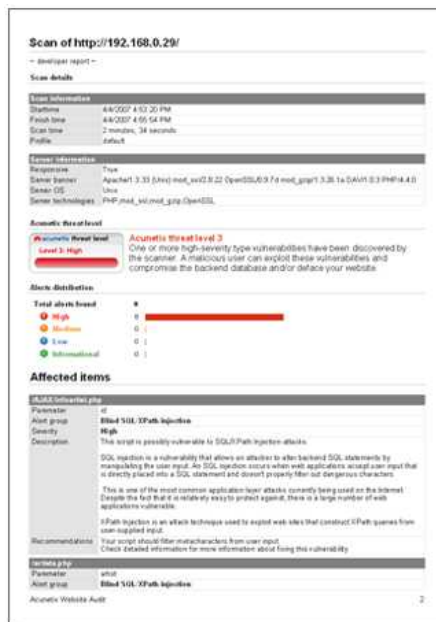
Developer Report



Screenshot 23 – Developer Report

The developer report groups scan results by effected pages and files, allowing developers to quickly identify and resolve vulnerabilities. This report also features detailed remediation examples and best-practice recommendations for fixing the vulnerabilities.

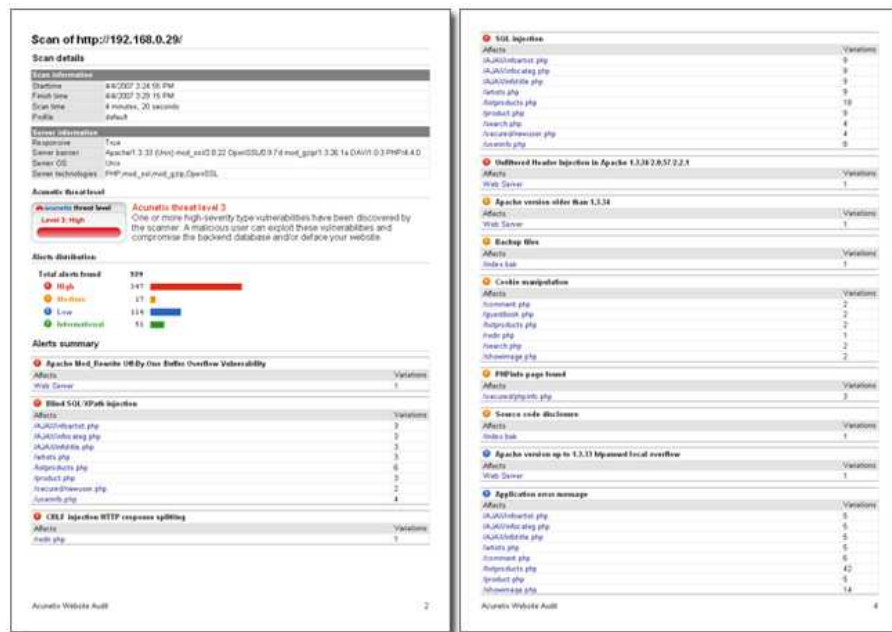
Executive Report



Screenshot 24 – Executive Report

The Executive report creates a summary of the total number of vulnerabilities found in every vulnerability class. This makes it ideal for management to get an overview of the security of the site without needing to review technical details.

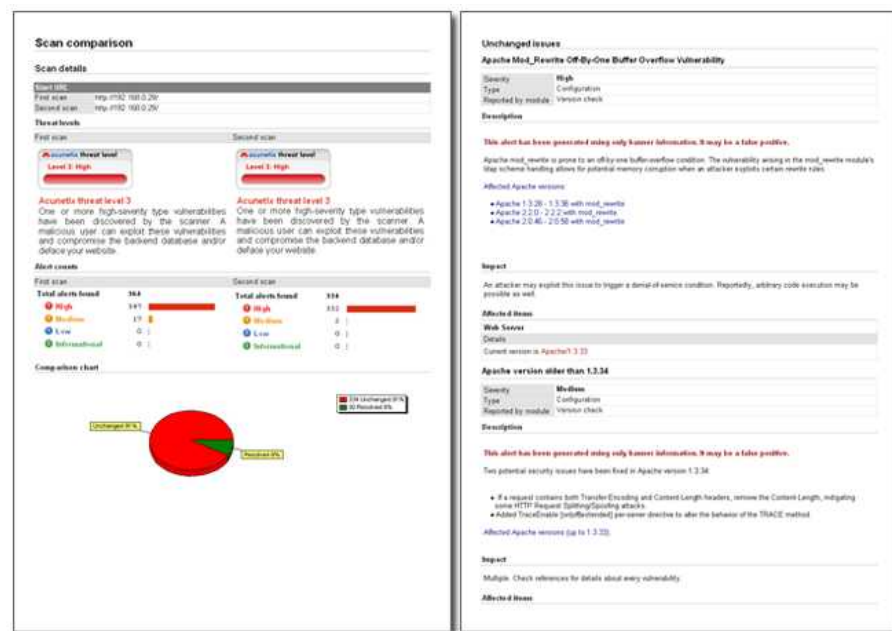
Vulnerability Report



Screenshot 25 – Vulnerability Report

The Vulnerability report style presents a technical summary of the scan results and groups all the vulnerabilities according to their vulnerability class. Each vulnerability class contains information about the exposed pages, the attack headers and the specific test details.

Scan Comparison Report



Screenshot 26 – Comparison Report

The Scan Comparison report allows the user to track the changes between two scan results. This report will document resolved and unchanged vulnerabilities, and new vulnerability details. This report style makes it easy to periodically track development changes for a web application.

Statistical Reports

Vulnerability trends by month and vulnerability group

Year: 2007
Month: April
Number of scans: 12

High Risk Vulnerabilities

| Vulnerability group | Instances |
|---------------------------------------------------------|-----------|
| Cross Site Scripting | 600 |
| SQL injection | 308 |
| Directory traversal (AUI) | 44 |
| Blind SQLi/Path injection for numeric inputs | 18 |
| Cross Site Scripting in URL | 18 |
| PHP code injection | 12 |
| Blind SQLi/Path injection for string inputs | 8 |
| File inclusion | 8 |
| CGI/HTTP/SMTP response splitting | 4 |
| Macromedia Dreamweaver Remote Database Scripts | 4 |
| PHP session idler than 4.3.9 | 4 |
| PHP Send_Mail_Data_Type_Cookies vulnerability | 4 |
| Script source file disclosure | 4 |
| Unbuffered Header Injection in Apache 1.3.362.0.572.2.1 | 4 |

Medium Risk Vulnerabilities

| Vulnerability group | Instances |
|------------------------------------------------------------|-----------|
| Cookie manipulation | 36 |
| PHPinfo page found | 15 |
| Apache Mod_Security One-Byte-Buffer Overflow Vulnerability | 4 |
| Apache version older than 1.3.34 | 4 |
| Backup file | 4 |
| Source code disclosure | 4 |

Low Risk Vulnerabilities

| Vulnerability group | Instances |
|-----------------------------------------------------|-----------|
| Directory listing found | 27 |
| Possible sensitive directories | 20 |
| CVE file found | 12 |
| Possible sensitive files | 8 |
| PHP script location error message | 6 |
| Apache version up to 1.3.33 bypasses local overflow | 4 |
| TRACE Method Enabled | 4 |
| URL redirection | 4 |

Informational Risk Vulnerabilities

| Vulnerability group | Instances |
|---------------------------------------------------------|-----------|
| Email address found | 208 |
| GDCH Apache directory listing which show Apache version | 12 |
| GDCH Default phpinfo page | 8 |

Screenshot 27 – Statistical Report

These reports allow you to gather vulnerability information from the results database and present periodical vulnerability statistics. This report allows developers and management to track security changes and to compile trend analysis reports.

Compliance Reports

OWASP TOP 10 2010

compliance report

Description

The primary aim of the OWASP Top 10 is to educate developers, integrators, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas and also provides guidance on where to go from here.

Disclaimer

This document or any of its content cannot account for or be included in any form of legal advice. The outcome of a vulnerability scan or security evaluation should be utilized to ensure that mitigation measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be sought according to its legal context. All laws and the environments in which they are applied are constantly changing and varied. Therefore no information provided in this document may be used as an alternative to a qualified legal body or legal representative.

A portion of this report is taken from OWASPs "The ten most critical web application security vulnerabilities - 2010" document, that can be found at <http://www.owasp.org>.

Scan

URL: <http://testlab.vulnweb.com:80/>
Scan date: 30/07/2010 17:20:02
Duration: 8 minutes, 2 seconds

[View report with Acunetix WVS evaluation engine \(not for commercial use\)](#)

Compliance at a Glance

This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

- Injection (A1)
 - Total number of alerts in this category: 8
- Cross Site Scripting (A2)
 - Total number of alerts in this category: 4
- Broken Authentication and Session Management (A3)
 - No alerts in this category
 - Insecure Direct Object Reference (A4)
 - No alerts in this category
 - Cross Site Request Forgery (CSRF) (A5)
 - No alerts in this category
 - Security Misconfiguration (A6)
 - Total number of alerts in this category: 10
 - Insecure Configuration Storage (A7)
 - No alerts in this category
 - Failure to Restrict URL Access (A8)
 - No alerts in this category
 - Insufficient Transport Layer Protection (A9)
 - No alerts in this category

Acunetix Website Audit

Screenshot 28 – Compliance Report

These reports allow you to generate a report according to the various compliance standard specifications. An easy to use wizard will prioritize and report specific vulnerabilities according to the standardized format as specified by the following compliance bodies;

- The Health Insurance Portability and Accountability Act (HIPAA)
- OWASP Top10
- Payment Card Industry (PCI) standards

- Sarbanes Oxley Act of 2002
- Web Application Security Consortium (WASC) Threat Classification
- NIST Special Publication 800-53
- DISA STIG Web Security

Customizing the Report Layout

The Reporter settings allow you to configure the layout and style of the generated reports. To access the report settings navigate to the 'Configuration > Settings' node in the Reporter Tools Explorer.

Report Options

This configuration node consists of two sections which can be used to customize the layout, titles and images in the headers of the report.

General Settings - Configure the default report template for generating a report directly from Acunetix WVS.

Report Options - Select custom icons, logos, headers and footers to customize the report.

You can use these settings to change the report layout to suit your needs and also to brand them for your own company. These settings are general default settings and will be used for all the reports generated with the WVS Reporter.

Page Settings

The Page Settings node allows you to configure the default page size, orientation and margin dimensions of your reports. These settings are general default settings and will be used for all the reports generated with the WVS Reporter.

The Report Viewer

The Report Viewer is a standalone application that allows you to view, save, export or print generated reports. The reports can be exported to PDF, HTML, Text, Word Document and BMP. The Acunetix Report Viewer is a free application and can be downloaded from the following location; <http://www.acunetix.com/download/tools/reportviewer.zip>

Using Microsoft SQL

Acunetix reporter needs a database backend to store the scan results and generate reports from. By default it uses the Microsoft Access database engine built into Windows. However you can choose to use Microsoft SQL server as a backend. To do this:

1. Go to 'Configuration > Settings > Database' node in the Acunetix WVS interface. Select MS SQL Server from the 'Database Type' drop down menu.
2. Insert the Server IP or FQDN in the 'Server' text box and the credentials to connect to the server in the 'Username' and 'Password' text box.
3. Specify a database name in the 'Database' text box. If the database does not exist it will be automatically created. If the database specified already exists, the user is prompted with a confirmation to overwrite the current database structure and data.

Note: To create a new database, a user with SQL Administrator privileges must be specified. If an existing database is specified, a user with

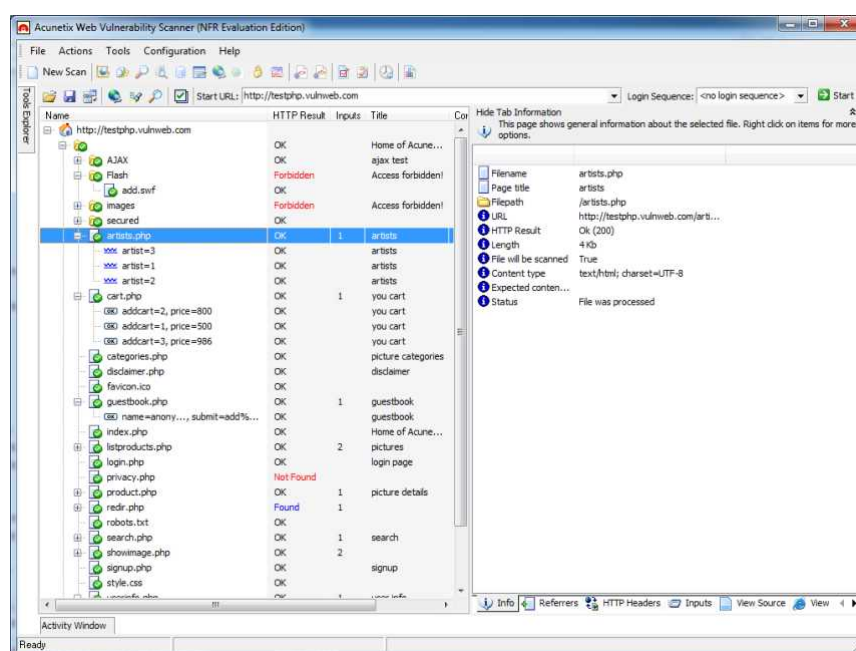
Administrator privileges on the specified database ONLY is required. Once the database is created, a user with read and write access only can be used.

You can also import a database configuration file. Select 'Import Database Configuration' and select a *.dbconfig file generated by the Acunetix Enterprise Reporter to automatically import SQL database settings.

6. Site Crawler Options

Introduction

The Site Crawler crawls through a target website and builds the site layout using the information collected, including the site directories and directories. You can use the site crawler tool to analyze the structure of a website without automatically launching the attacks.



Screenshot 29 – The crawler tool interface

The Crawler tool interface consists of:

- **Toolbar** – Here you can find a number of options and tools to be used along with the site crawler. The options are:
 - **Load Results** – Load a previously saved crawl
 - **Save Results** – Save a completed crawl. If you use the option 'choose files to be scanned' to select / deselect a number of files to be scanned, these changes will also be saved
 - **Export Results** – Export current crawl to XML format
 - **Build structure from HTTP Sniffer logs** – If you used the HTTP sniffer to manually crawl a website, you can import the captured data into the site crawler tool to automatically build a website structure.
 - **Scan this site** – Automatically launch a vulnerability scan against the crawled website.
 - **Filter** – Search functionality to allow you to search for any detail which was recorded during the website crawl
 - **Choose files to be scanned** – Once a crawl is ready, with this feature you can specify which of the crawled files should be scanned or not, in case you are launching the scan. If you select

/ deselect any files to be scanned, upon saving the crawl, such changes will also be saved

- **Start URL** – Specify the URL of the website you would like to crawl
- **Login Sequence** – If the website to be crawled requires a login sequence, you can select a previously recorded login sequence from the drop down menu.
- **Site structure window** (left hand side) – Displays target site information fetched by the crawler, e.g., cookies, robots, files and directories.
- **Details window** (right hand side) – Displays general information about a file selected in the site structure window (e.g., filename, file path etc). At the bottom of the details window, there are also a number of tabs, from where you can find further information about the selected object.

Starting a Website Crawl

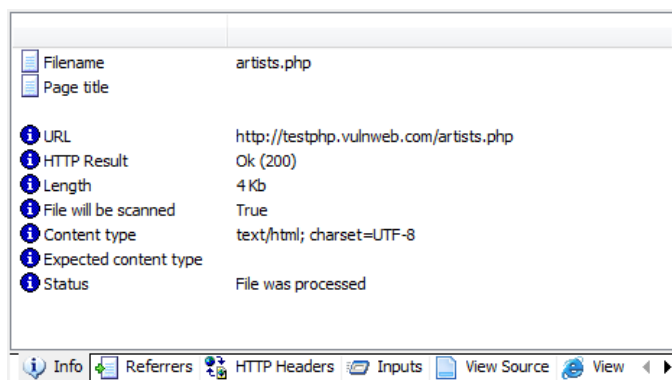
Enter the URL of the target website from where the crawler should start crawling (e.g. <http://testphp.vulnweb.com/>). If you want to use a recorded login sequence during the crawl, select it from the 'Login Sequence' drop down menu. Click on the start button to start the crawling. If the website or any parts of it require HTTP authentication to be accessed, a window will automatically pop up where you can enter the credentials, unless the credentials have already been configured in the HTTP Authentication settings node.

The site structure will be displayed on the left hand side – for each directory found, a node will be created together with sub nodes for each file. The site crawler will also create a Cookies Node, which displays information about the cookies used.

Analyzing the Site Crawler results

Acunetix WVS uses three different colors for filenames;

- Green – File detected by AcuSensor Technology.
- Blue – File was detected during the scanning process instead of the crawling process. This typically happens when a file is not linked from anywhere and has been discovered via a vulnerability.
- Black – Files discovered by the crawling process.



Screenshot 30 – File Details Pane

In addition to the filename the crawler also gathers further technical details about each crawled object. Click on the object to view detailed information in the right hand pane.

The following information about the highlighted object is available:

- **Info** - Generic information such as filename, page title, file path, URL, HTTP Result, Length and more.
- **Referrers** - A list of other objects on the website from where the crawler found links to the selected object.
- **HTTP Headers** - This tab contains the HTTP request header used to access the object and also the HTTP response headers received. Details such as content type, date, whether file is cached or not and any relevant server information are found in this tab. You can also edit the HTTP request in the HTTP Editor by clicking the 'Edit with HTTP Editor' icon located on top of the HTTP request pane. This allows the user to analyze how the application will behave when certain parameters are altered.
- **Inputs** - Lists the parameters (inputs) discovered in the selected object. The parameter name and a list of possible values accepted by each parameter are also shown.
- **View Source** – Shows the source HTML code sent to the scanner when accessing the selected file. You can also use the search utility to search for specific information through the HTML code. The search utility also accepts regular expressions.
- **View Page** – Shows the page as it is displayed in a web browser. Any formatting data such as CSS files, images and client side scripts are disabled as a security precaution.
- **HTML Structure Analysis** – This tab displays the following HTML information:
 - **Simple URLs Sub-Tab** – A list of links discovered in the selected object.
 - **Comments Sub-Tab** – A list of comments discovered in the selected object. The information contained in the comments cannot be automatically analyzed but may reveal interesting information about the construction and coding of the website.
 - **Client Script Sub-Tab** – A list of client side scripts (JavaScript, VBscript etc.) and their source code discovered in the selected object. These scripts will be executed by the client web browser. Such information might reveal information about the logic of the web application.
 - **Input Forms Sub-Tab** - A list of forms discovered in the selected object is shown in the top window. A list of parameters and their values is shown in the middle and bottom window.
 - **META Tags Sub-Tab** –A list of META tags discovered in the selected object. META tags contain information about the website, e.g. the description and keywords META tags used by search engines. META tags with an HTTP-EQUIV attribute are equivalent to HTTP headers. Typically, such META tags control the action of browsers and may be used to refine the information provided by the actual headers. Tags using this form should have an equivalent effect when specified as an HTTP header, and in some servers may be translated to actual HTTP headers automatically or by a pre-processing tool.
 - **AcuSensor Data** – Data discovered by AcuSensor Technology related to the selected object.
 - **Alerts** – A list of alerts (vulnerabilities) specific to the selected object.

Configuring the Crawler

Site Crawler Settings

Default Site Crawler configuration settings can be modified by navigating to 'Configuration > Settings > Tool Settings > Site Crawler'. The following Site Crawler options are available:

- **Start HTTP Sniffer for manual crawling at the end of the scan process** - This option will start the HTTP Sniffer at the end of the crawl to allow manual crawling by enabling the user to browse to parts of the site that were not discovered by the crawler. Typically the Acunetix WVS crawler is able to crawl every web application though there are some specific scenarios where it fails to do so automatically. The crawler will update the website structure with the newly discovered links and pages.
- **Get first URL only** - Scan only the index or first page of the target site and do not follow any links.
- **Do not fetch anything above start folder** - By enabling this option the crawler will not traverse any links which point to a location above the base link. E.g. if `http://testphp.vulnweb.com/wvs/` is the base URL, the crawler will not crawl to links which point to a location above the base URL like `http://testphp.vulnweb.com`.
- **Fetch files below base folder** - By enabling this option the crawler will follow links which point to locations outside the base folder. E.g. if `http://testphp.vulnweb.com/` is the base URL, it will still traverse the links which point to an object which resides in a sub directory below the base folder, like `http://testphp.acunetix.com/wvs/`. If this option is switched off, the crawler will not crawl any objects from the root's sub directories.
- **Fetch directory indexes even if not linked** - By enabling this option the crawler will try to request the directory index for every discovered directory even if the directory index is not directly linked from another source.
- **Retrieve and process robots.txt, sitemap.xml** - By enabling this option the crawler will scan for a robots.txt or sitemap.xml file in the target website and follow all the links specified in such files.
- **Ignore CASE differences in paths** - By enabling this option the crawler will ignore any case difference in the links found on the website. E.g. `"/Admin"` will be considered the same as `"/admin"`.
- **Submit forms** - Select this option so the crawler will automatically fill in and submit web forms to discover more objects during the crawl. If you would like the crawler to submit specific values instead of random values, you can configure these from 'Configuration > Settings (in Tools Explorer) > Scanner Settings > Input Fields' node.
- **Enable CSA (analyze and execute JavaScript/AJAX)** - Select this option to activate the Client Script Analyzer (CSA) during crawling. This will execute JavaScript/AJAX code on the website to gather a more complete site structure.
- **Fetch external scripts** - With this option enabled, the CSA engine will fetch all external resources linked through client scripts present on the target. The external resources will only be crawled and will not be scanned. If this option is not enabled and a client script uses external resources, the CSA engine will not be able to analyze the client script correctly.

- **Fetch default index files (index.php, Default.asp ...)** - If this option is enabled, the crawler will try to fetch common default index filenames (like index.php, Default.asp) for every folder, even if not directly linked.
- **Try to prevent infinite directory recursion** – In certain website structures, there is a small probability that the scanner will start looping when trying to fetch the same directory recursively (e.g. /images/images/images/images/...). Enabling this setting will instruct the scanner to try to prevent this situation by identifying repeated directory names in recursion.
- **Warn user if URL rewrite is detected** – If URL rewrite is detected when crawling a target website, a notification window will automatically pop up notifying the user that URL rewrite was detected. Switch off this option if you do not want to be automatically advised.
- **Maximum number of variations** – In this option you can specify the maximum number of variations for a file. E.g. index.asp has a GET parameter ID of which the crawler discovered 10 possible values of it from links requesting index.asp with the ID set to a different. Each of these links is a variation. Each variation will appear under the file in the Scan Tree during crawling.
- **Link Depth Limitation** – In this option you can configure the maximum number of links to crawl from the root URL.
- **Structure Depth Limitation** – In this option you can configure the maximum number of directories to crawl from the root URL.

Site Crawler Settings > File Extension Filters

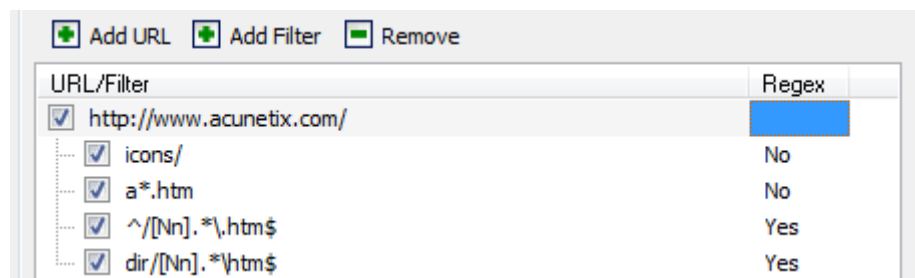
In this node a list of file extensions which will be included or excluded during a crawl can be configured. This is done by matching the respective extension of the files specified in any of the columns listed below.

- **Include List** - Process all files which fit the wildcard specified.
- **Exclude List** - Ignore all files which fit the wildcard specified.

Note: Binary files such as images, movies and archives are excluded by default to avoid unnecessary traffic.

Site Crawler Settings > Directory and File Filters

In this node you can specify a list of directories or filenames to be excluded during a crawl. When excluding a directory or filename, you can specify the exact directory name or filename or else use wildcards, to match a number of directories or files with one filter. You can also use regular expressions to match a number of directories or files. If a regular expression is specified as filter, toggle the value to 'Yes' under the 'Regex' column to by clicking on it.



Screenshot 31 – Directory and File Filter rules

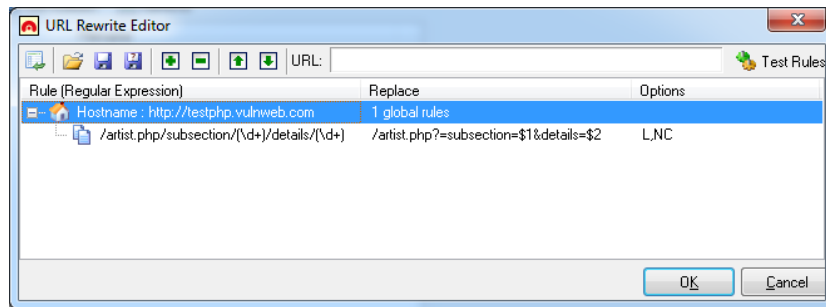
To add a directory or file rule:

1. Click on the 'Add URL' button and specify the address of the website where the directory or file is located.
2. Click on the 'Add Filter' button and specify the directory or filename, a wild card or a regular expression. When specifying a directory name, do not add a slash '/' in front of the directory name. A trailing slash is automatically added to the end of the website URL.

Note: Directory and file filters specified for the root or any other directory of a website, are not inherited by their sub directories. Therefore a filter for each sub directory should be specified separately, by adding the sub directory name in the filter, as can be seen in the screen shot above.


Site Crawler Settings > URL Rewrite

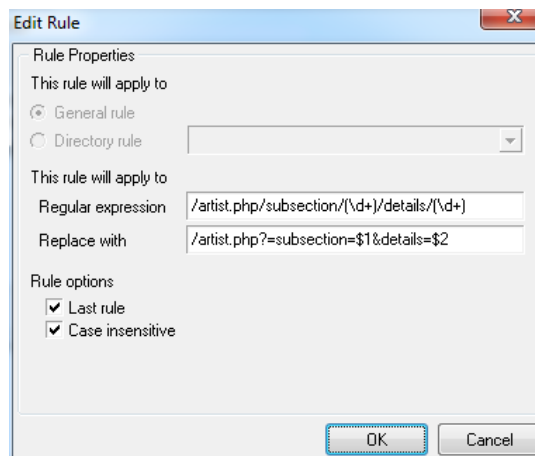
In this node, a list of URL rewrite rules for websites using this technology can be specified. The purpose of these rules is to configure the crawler to navigate and understand the website structure and actual files, instead of crawling inexistent objects.



Screenshot 32 – URL Rewrite Configuration

Adding a URL rewrite rule manually

1. Click on the 'Add Ruleset' button to open up the URL rewrite editor window and enter the host name of the target website for which the URL rewrite rule will be used. Click on the  button to open up the Add rule dialogue.




Screenshot 33 – URL Rewrite Rule

2. Specify if the rule set is generic for the whole website by ticking 'General rule'. If it is for a specific directory only, tick 'Directory rule' and specify the directory name.
3. In the 'Regular Expression' input field, specify a part of the URL including regular expressions (or a group of Regular expressions) which Acunetix WVS should use to recognize a rewritten URL. E.g. Details/.*/(d+). This means match everything after the Details/ directory, and after that matched string, match also a digit or more.


4. In the 'Replace with' input field, specify the URL Acunetix WVS should request instead of the rewritten URL. E.g. /Mod_Rewrite_Shop/details.php?id=\$1. The \$1 will be replaced with the value retrieved from the first regular expression group specified in the 'Regular Expression' input field, in this case (d+).
6. With the above configuration, when Acunetix finds the URL; /Mod_Rewrite_Shop/Details/network-storage-d-link-dns-313-enclosure-1-x-sata/1, it will request the following; /Mod_Rewrite_Shop/details.php?id=1.
7. Tick 'Last rule' option to specify that if this rule is executed no more rules should be executed afterwards.
8. Tick 'Case insensitive' if the URL's are not case sensitive. Click 'OK' to save the URL rewrite rule.
9. Test the URL rewrite rule by specifying a URL in the URL and click on 'Test Rule'.

Importing a URL Rewrite rule configuration from an Apache web server

1. Click on 'Add Ruleset' and then click on import rule button  to open the Import Rewrite rules wizard. Enter the path of the Apache httpd.conf or .htaccess file (the file which contains the URL rewrite rules) in the 'Filename' field.
2. Select the type of configuration to import (httpd.conf or .htaccess). If .htaccess is being used, the hostname of the website (e.g. www.acunetix.com) and directory (e.g. sales) on which the URL rewrite configuration is set on the web server needs to be specified.

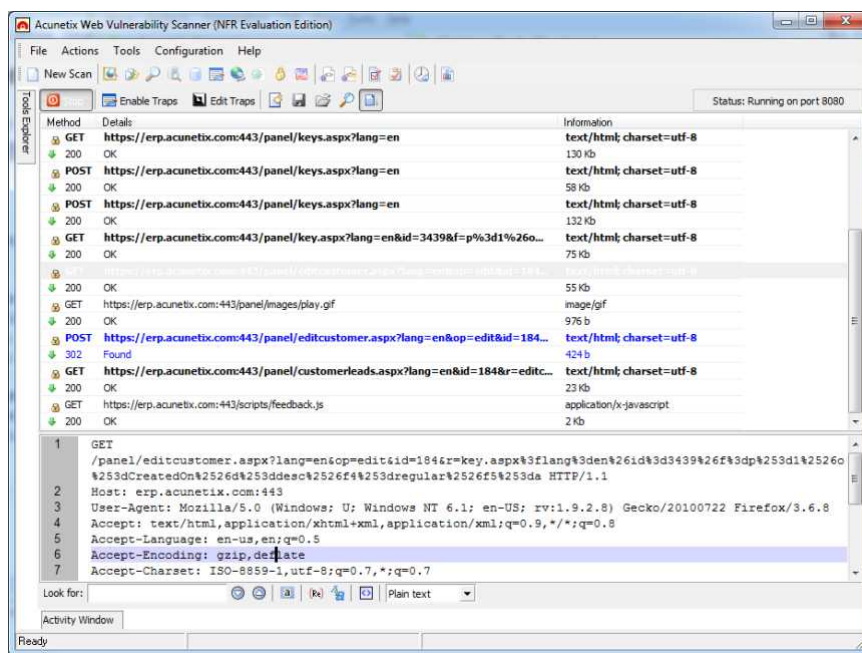
Site Crawler Settings > Custom Cookies

In this configuration node, you can define custom cookies for a particular URL. To add a custom cookie:

1. Click on  'Add Cookie' button to add a new blank cookie to the list.
2. Enter the URL of the site for which the cookie will be used in the 'URL' left hand column.
3. Enter the custom cookie string that will be sent with the cookie. E.g. if cookie name is 'Cookie_Name' and content is 'XYZ' enter 'Cookie_Name=XYZ'. Click 'Apply' button to save changes.

7. Manual crawling with the HTTP Sniffer Tool

Introduction



Screenshot 34 – The HTTP Sniffer

The HTTP sniffer tool can be used to manually crawl sections of your website that cannot be crawled automatically by Acunetix WVS. In these cases, you can use a web browser to manually browse these sections and capture the HTTP traffic using the HTTP Sniffer. Later you can launch an automated security scan against it. To do this you only have to configure the browser to send traffic through the HTTP Sniffer and then export the logs to the Site Crawler. You can read more about this process from the following URL; <http://www.acunetix.com/blog/docs/manual-crawling-http-sniffer/>

Other uses of the HTTP sniffer tool are to analyze the HTTP traffic between a web server and a web client and also to try and launch a number of attacks against a web application during the penetration testing, such as man in the middle attack.

In actual fact, the HTTP Sniffer tool is a proxy server which captures HTTP requests and responses exchanged between a web client (browser or other http application) and a web server, or vice versa. It then allows you to filter or edit them.

You can also use the HTTP Sniffer tool to create a rule to trap particular POST, GET HTTP requests and change them manually, like a man in the middle attack. You can create a rule that automatically changes particular HTTP requests or also create a rule to automatically log information in requests or responses.

Configuring and using the HTTP Sniffer

To start capturing traffic, you must first configure your browser to use the Acunetix HTTP Sniffer as proxy server. Follow any of the below procedures to configure your web browser of choice.

Mozilla Firefox

1. From the Tools drop down menu click on Options
2. Click on the Advanced Tab and on the Network Tab
3. In the Connection section click on Settings and tick 'Manual proxy configuration'
4. Set HTTP Proxy to 127.0.0.1 and port to 8080
5. If you also need to capture SSL traffic, configure the SSL Proxy to 127.0.0.1 and port to 8080
6. Click on OK to save all options and close all configuration windows.

Internet Explorer

1. From the Tools drop down menu click on Internet Options
2. Click on the Connections tab and then click LAN Settings button
3. Tick the option 'Use a proxy server for your LAN'
4. In the Address input field, enter 127.0.0.1 and enter 8080 in the Port input field.
5. If you also need to capture SSL traffic, click on the Advanced button and in the Secure input field, enter 127.0.0.0 as proxy address and 8080 as port number.
6. Click on OK to save all settings and close all configuration windows.

Google Chrome

Google Chrome uses Internet Explorer's proxy server settings. Therefore to use Google Chrome, follow the procedure above and configure Internet Explorer.

Capturing HTTP traffic

Toggle the Start / Stop button to enable and disable the HTTP Sniffer. All HTTP requests and responses will be listed in the main window. To view the complete request or response, click on the entry and all the request or response will be displayed in the lower details window pane. If the HTTP Sniffer is stopped, the configured web browser won't be able to access the target URL.

Configuration Options

By default, the HTTP Sniffer proxy server listens on localhost (127.0.0.1) and port 8080. This limits the capturing of traffic to web clients running on the same machine.

The HTTP Sniffer options can be accessed from 'Configuration > Settings > Tools Settings > HTTP Sniffer'.

You can set the HTTP Sniffer to listen on all interfaces, so web client applications running on other machines can proxy traffic through the HTTP Sniffer for analysis. The HTTP Sniffer port can also be configured.

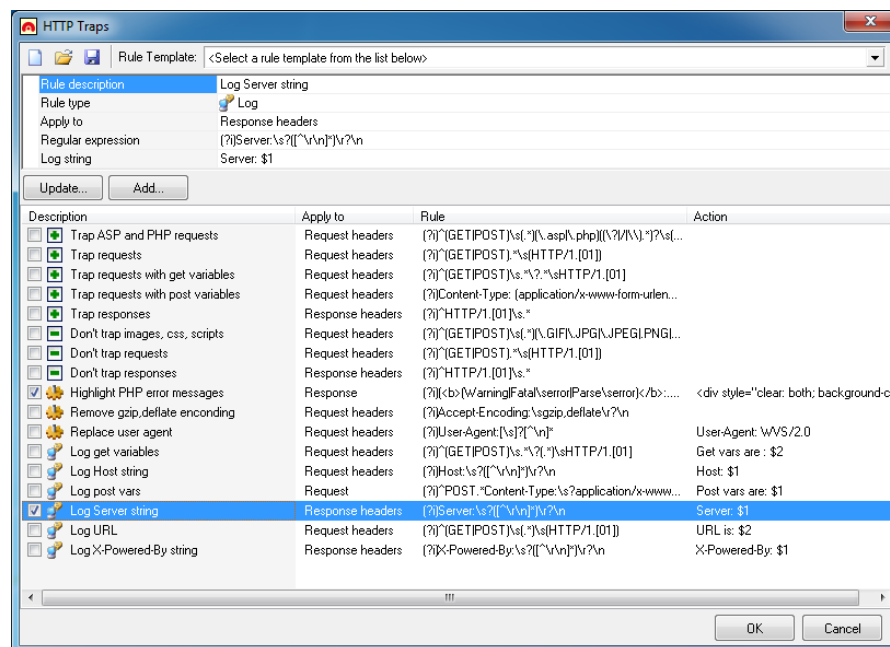
HTTP Sniffer Trap Filters

You can configure the HTTP Sniffer to intercept an HTTP request before it is sent so that you can edit the request and send the modified request to the server. You can do the same for HTTP responses.

To review and edit a HTTP request or response before it is sent to the client or server, you must create an HTTP Proxy trap filter.

Creating a HTTP Sniffer Trap Filter

1. In the HTTP Sniffer toolbar, click on the 'Edit traps' button to launch the HTTP traps window.







Screenshot 35 - HTTP Sniffer Edit Trap window

2. You can select a rule trap template, e.g. trap requests, and trap ASP or PHP requests. This will load up a preconfigured trap which you can edit.

3. Alternatively you can create a new trap by first entering a description for the rule.

4. Next step is to specify the rule type. Below are the four possible rule types;

-  **Include** - Configure which HTTP requests and responses should be trapped.
-  **Exclude** - Configure which HTTP requests and responses should be excluded.
-  **Replace or change rules** - Configure which HTTP requests should be automatically changed based on the given expression.
-  **Logging rules** - Configure which HTTP requests or responses should be logged in the 'Activity window'.

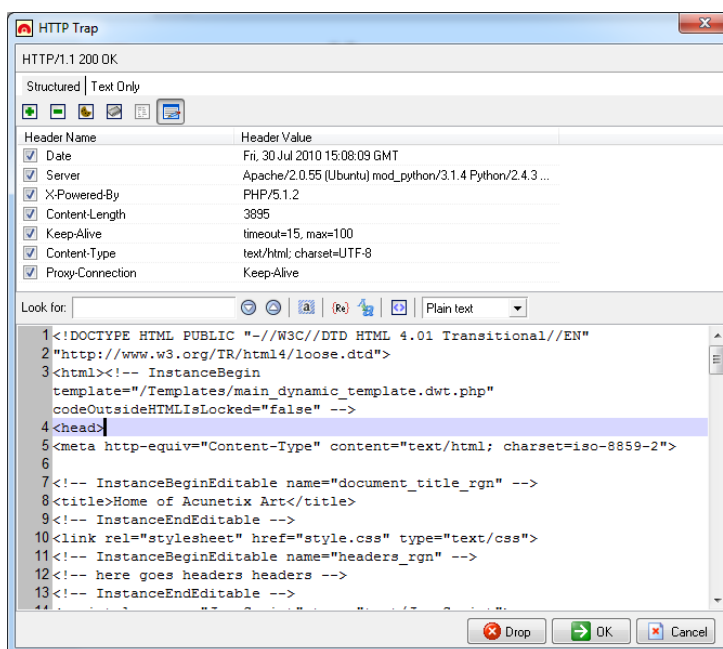
5. Now configure to which type of traffic the trap should apply. It can be configured to apply for all traffic, for HTTP requests only, request headers etc.

6. In the Regular expression option, enter a regular expression that matches the data you would like to trap.

7. Once the new trap is ready, click on the 'Add...' button to save the new trap. This will add the trap and automatically enable it. You can enable/disable traps by clicking on the tick box in front of the trap rule.

8. Click the 'OK' button to return to the HTTP Sniffer dialog and click on the 'Enable traps' button to activate the traps in the HTTP Sniffer.

The Trap Form



Screenshot 36 - HTTP Sniffer Trap form

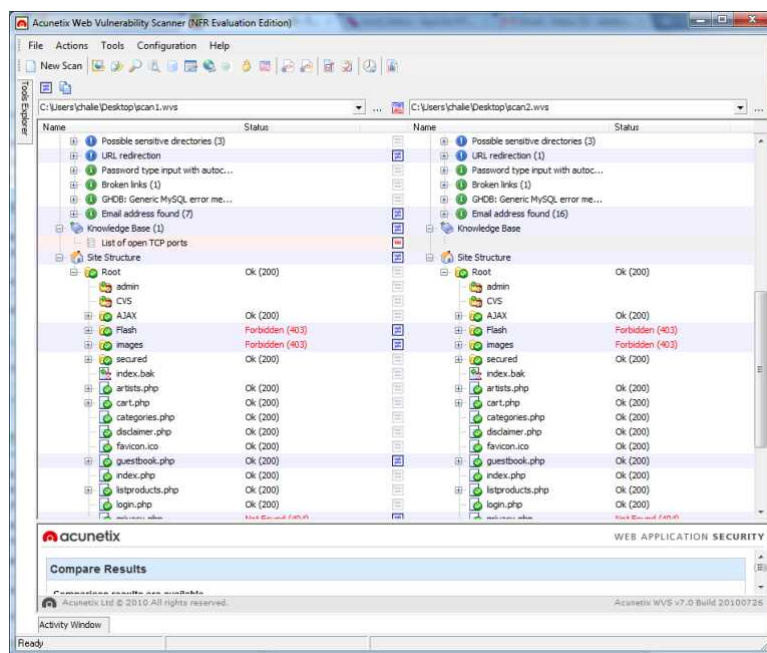
When an HTTP request or a response is trapped by the HTTP Sniffer, the 'HTTP trap' window will automatically pop up to allow you to edit the trapped HTTP request or response. Similar to the HTTP Editor, the Trap Form editor allows you to edit headers, cookies, queries and post variables. Click 'OK' to allow the HTTP request or response through.

Editing a HTTP Request without a Trap

If you want to edit a HTTP request without setting up an HTTP trap, right click on a request or a response and select 'Edit with the HTTP Editor'. Click Start in the HTTP Editor to send the HTTP request to the server.

8. Compare Results Tool

Introduction




Screenshot 37 – Compare Results Tool

The compare results tool allows you to analyze the differences between two saved scans performed at different dates. You can compare a full security scan or just the site crawler output.

Comparing Results





To compare two saved scan results;

1. Go to the 'Compare Results' node in the Tools Explorer.
2. In the Compare results toolbar, specify the path of the first scan file. In the second edit box, specify the path of the second scan.
3. Click on the Compare  button to launch the compare results wizard.
4. Specify which items you wish to compare such as Referrers, HTTP headers etc. The list of items that are enabled for compare can be saved as a new template by renaming the template and clicking the 'Save' button. Click 'Start' to start the compare process.

Note: For large websites, the file structure comparison process may take a long time to complete.

Analyzing the Results Comparison

Once the comparison is completed, the results are shown in a two-pane interface. The left pane contains the contents of the original scan while the right hand side pane contains the results of the second specified scan. The middle column shows icons indicating the comparison result of the items in that line. The legend of possible comparison results is shown below:

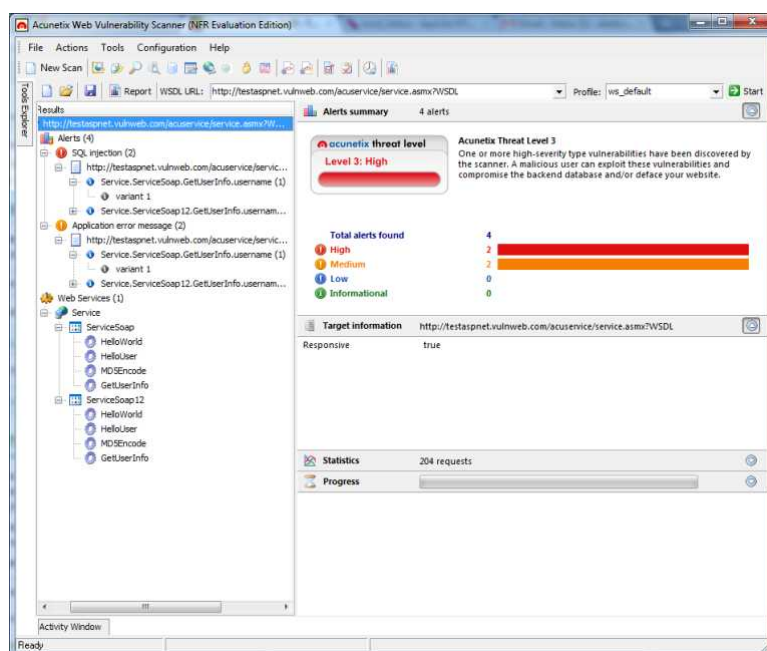
| | |
|-----------------------------------------------------------------------------------|---------------------------------------------|
|  | There are no changes. |
|  | This item was added in the new version. |
|  | This item was deleted from the new version. |
|  | This item was changed in the new version. |

Click on the result icon in the middle column to display the comparison result details in the window below the comparison. These details show the changes detected between the two scans, such as the number of items present in each scan and the items that have been added or deleted.

9. Scanning Web Services

Introduction

Web Services, like any other internet-dependent system, present new exploit possibilities and increase the need for security audits. The Web Services Scanner performs automated vulnerability scans for Web Services and generates a detailed security report of the results.

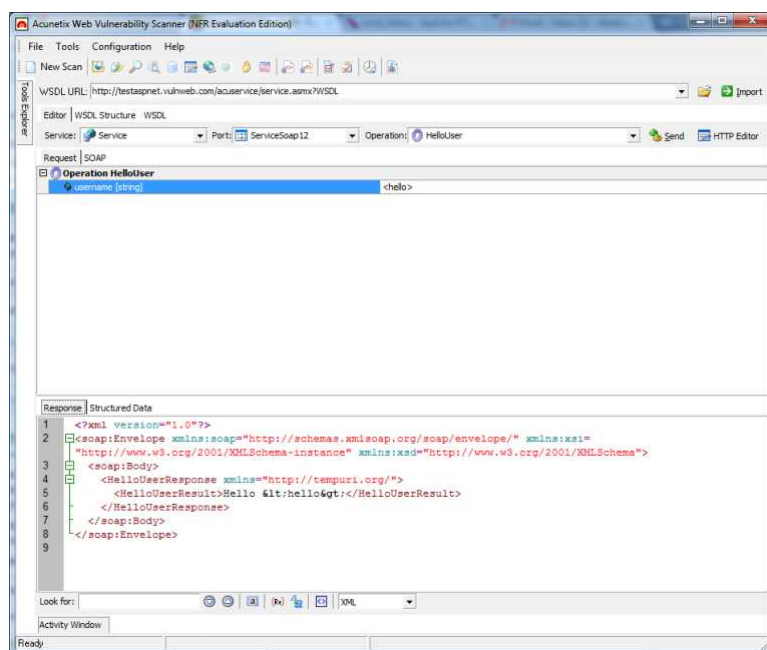


Screenshot 38 – Web Services Scanner

Starting a Web Service Scan

1. From the 'Tools Explorer' select 'Web Services Scanner' and click on 'New Scan' button in the toolbar to launch the Web Service Scan Wizard. Specify the URL of an online or local WSDL and choose a scanning profile. Click on 'Next' to proceed to the next step.
2. In the 'Selection' step, select the Web Services, Ports and Operations that will be scanned. The number of inputs accepted by each operation and the URL of the ports will be displayed in the Details section.
3. Enter specific input values (optional) for the scanner to use custom values for Web Service Operations during the scan in the 'Default Values' step. Proceed to the scan summary, review it and click 'Finish' to launch the scan.

Web Services Editor



Screenshot 39 – Web Services Editor

The Web Services Editor allows importation of online or local WSDL for custom editing, and execution of various web service operations for an in depth analysis of WSDL requests and responses. The editor also features syntax highlighting for all languages to easily edit SOAP headers and customize manual attacks. Editing and sending of Web Services SOAP messages is very similar to editing normal requests sent via the HTTP Editor.

Importing WSDL and Sending Request

1. Click on the 'Web Services Editor' node in the tools explorer and enter the URL of the WSDL, or locate the local directory where the local WSDL file is stored. Click 'Import' to import all WSDL information.
2. Once imported, select the Service, Port and the Operation from the drop down menus in the toolbar which will be tested.
3. Specify a value for the operation and click 'Send' to send the SOAP request to the web service. Once the web server responds, you can view the response in a structured or XML view type in the lower window pane.

Response Tab

This tab displays the response sent back from the web service in raw XML format.

Structured Data Tab

This tab presents the XML data received from the web service response in a different way, by showing the elements in a hierarchy of nodes showing the value for each element.

WSDL Structure Tab

This tab provides a detailed view of the web service data as provided by the WSDL Structure.

The WSDL information is structured in the form of nodes and sub-nodes and the main nodes of the tree structure are XML Schema and Services.

The XML Schema node lists all the ComplexTypes and the Elements of the web service. The Services node lists all the web service ports and their respective operations together with the resource details of the source of the SOAP data.

A more detailed WSDL structure can also be shown by ticking the 'Show detailed WSDL structure' at the bottom of the screen. This will provide extensive information for each sub-node of the Services node structure such as input messages and parameters.

WSDL Tab

This tab shows the actual WSDL data in the form of XML tags. Using the toolbar provided at the bottom of the screen you can search for certain keywords or elements in the source code and also change the syntax highlighting if needed.

HTTP Editor Export

In the Web Services Editor you can export a SOAP request to the HTTP Editor by clicking on the 'HTTP Editor' button in the Web Services Editor toolbar. The HTTP Editor tool will automatically import the data so the request can be customized and sent as an HTTP POST request.

10. Command Line Operation

Introduction

Acunetix WVS can be launched via the command line, allowing you to automate specific scans. Command line operation is done via the Acunetix WVS Console Scanner.

The Acunetix WVS Console Scanner is installed with Acunetix WVS and can be accessed from the default installation directory of the application. The default location of the WVS Console scanner is:

C:\Program Files\Acunetix\Web Vulnerability Scanner 7\wvs_console.exe

If the executable is run without parameters, usage information is presented together with all the details of every parameter and option available for your quick reference. For more WVS console Scanner help, use the '/?' switch.

Note: In 64 bit operating systems Acunetix WVS is installed in the 'Program Files (x86)' directory.

WVS Console Scanner Command Line Parameters

The Acunetix WVS Console Scanner supports most of the graphical user interface options. It allows the same degree of customization and flexibility via a set of command line switches. Acunetix WVS Console Scanner Parameters:

| Parameter | Description |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| /scan | Scans a single website. Syntax: /scan [url] Example: /scan http://testphp.vulnweb.com |
| /crawl | Crawls a single website. Syntax: /crawl [url] Example: /crawl http://testphp.vulnweb.com |
| /scanfromcrawl | Starts a scan from a saved crawl. Syntax: /scanfromcrawl [file name] Example: /scanfromcrawl c:\crawl\sitecrawl.cwl |
| /scanlist | Scans a group of websites defined in a text. Syntax: /scanlist [file name] |

| | |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>Example: /scanlist c:\lists\sites.txt</p> |
| /scanwsdl | <p>Starts a web services scan.</p> <p>Syntax: /scanwsdl [wsdlurl]</p> <p>Example: /scanwsdl http://test.vulnweb.com/service.asmx?WSDL</p> |
| /profile | <p>Uses specified scanning profile during the scan.</p> <p>Syntax: /profile [profile name]</p> <p>Example: /profile default</p> |
| /loginseq | <p>Uses specified login sequence during the scan.</p> <p>Syntax: /loginseq [filename]</p> <p>Example: /loginseq testphp_seq</p> |
| /save | <p>Saves scan to file.</p> <p>Syntax: /save [filename]</p> <p>Example: /save c:\results\scan1.wvs</p> |
| /exportxml | <p>Exports results to XML file.</p> <p>Syntax: /exportxml [filename]</p> <p>Example: /exportxml c:\results\scan1.xml</p> |
| /exportavdl | <p>Exports results as AVDL format.</p> <p>Syntax: /exportavdl [filename]</p> <p>Example: /exportavdl c:\results\scan1.xml</p> |
| /savetodatabase | <p>Saves scan results to reporting database. If this option is not specified, reports cannot be generated after the scan unless scan results are manually imported to reporting database.</p> <p>Syntax: /savetodatabase</p> |
| /savelogs | <p>Saves scan log files to the non default location.</p> <p>Syntax: /savelogs [filename]</p> <p>Example: /savelogs c:\logs\scan1logs.csv</p> |

| | |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /generatereport | <p>Generates and saves the scan report to a directory.</p> <p>Syntax:</p> <pre>/generatereport [dir]</pre> <p>Example:</p> <pre>/generatereport c:\reports\</pre> |
| /ReportFormat | <p>Generates the report in one of the specified formats; REP, PDF, RTF, HTML etc.</p> <p>Syntax:</p> <pre>/ReportFormat [format]</pre> <p>Example:</p> <pre>/ReportFormat PDF</pre> |
| /ReportExtraParams | <p>Here you can specify extra parameters for the Reporter, such as report template, compliance type etc. See the section Acunetix Reporter CLI reference on page 67 for more information on this parameter, or else type 'reporter_console.exe /?' for more information.</p> <p>Syntax:</p> <pre>/ReportExtraParams [parameter=value]</pre> <p>Example:</p> <pre>/ReportExtraParams "/r WVSComplianceReport.rep /k PC12.xml"</pre> |
| /sendmail | <p>Sends an email alert that the scan is finished to the user using the details configured in the scheduler settings.</p> <p>Syntax:</p> <pre>/sendmail</pre> |
| /verbose | <p>Enables verbose mode; the log file entries will also be displayed in the command line window.</p> <p>Syntax:</p> <pre>/verbose</pre> |
| /Password | <p>Application password if user interface password is enabled. Password can be enabled from the Application settings > General node.</p> <p>Syntax:</p> <pre>/Password [password string]</pre> <p>Example:</p> <pre>/Password TestPass123!</pre> |

WVS Console Scanner Command Line Options

| Option | Description |
|------------------------|------------------------------------------------------------------------------------------------------------|
| --GetFirstOnly | <p>Specifies to get the first URL only.</p> <p>Syntax:</p> <pre>--GetFirstOnly=[true false]</pre> |
| --RestrictToBaseFolder | <p>Specifies if crawler should fetch anything above start directory.</p> <p>Syntax:</p> |

| | |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | --RestrictToBaseFolder=[true false] |
| --FetchSubdirs | Specifies if the crawler should fetch files discovered in sub directories below base directory. Syntax: --FetchSubdirs=[true false] |
| --ForceFetchDirindex | Specifies if the crawler should fetch directory indexes even if not linked. Syntax: --ForceFetchDirindex=[true false] |
| --SubmitFoms | Submits forms during crawl to discover more links. Syntax: --SubmitFoms=[true false] |
| --RobotsTxt | Retrieves and processes robots.txt and sitemap.xml during crawl to discover more links. Syntax: --RobotsTxt=[true false] |
| --CaseInsensitivePaths | Specifies if the crawler should cater for case insensitive / sensitive paths. Syntax: --CaseInsensitivePaths=[true false] |
| --UseCSA | Enable Client Script Analyzer engine to analyze JavaScript and other client side scripts during crawling. For all kind of web 2.0 applications this option should always be enabled. Syntax: --UseCSA=[true false] |
| --scanningMode | Specify which scanning mode to use for this scan. Options available are Quick, Heuristic or extensive. Syntax: --scanningMode=[Quick Heuristic Extensive] |
| --TestWebAppsInAllDirs | Tests for well known web applications vulnerabilities in all directories. Enable only if popular web applications are installed on the target website, such as Wordpress, Joomla etc. Syntax: --TestWebAppsInAllDirs=[True False] |
| --ManipHTTPHeaders | Manipulate HTTP headers during scan. Syntax: --ManipHTTPHeaders=[True False] |
| --UseAcuSensor | Enable AcuSensor technology for this scan. AcuSensor Technology sensor files must be installed on the target website. Syntax: --UseAcuSensor=[True False] |
| --EnablePortScanning | Port scan target and run network alerts tests against target during web security scan. Syntax: |

| | |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | --EnablePortScanning=[True False] |
| -- UseSensorDataFromCrawl | You can specify to use the AcuSensor data from a saved crawl to proceed with scan or to re-crawl the target. Syntax: --UseSensorDataFromCrawl=[Yes No Revalidate] |

Note: The only mandatory parameter is the scan URL. If no parameter is specified, the default graphical user interface settings will be used. If the target website uses HTTP authentication, HTTP credentials have to be specified in the Configuration > Settings > Application Settings > HTTP Authentication node in the Acunetix WVS user interface. Since with every set of HTTP credentials, you also have to specify the URL, such credentials will be used automatically during command line scans.

The Acunetix WVS console Reporter

The Acunetix WVS console Reporter is installed with Acunetix WVS and can be accessed from the default installation directory of the application. The default location is:

C:\Program Files\Acunetix\Web Vulnerability Scanner 7\reporter_console.exe

For WVS console Reporter help, use the '/?' switch.

Note: In 64 bit operating systems Acunetix WVS is installed in the 'Program Files (x86)' directory.

The Acunetix WVS console Reporter command line options

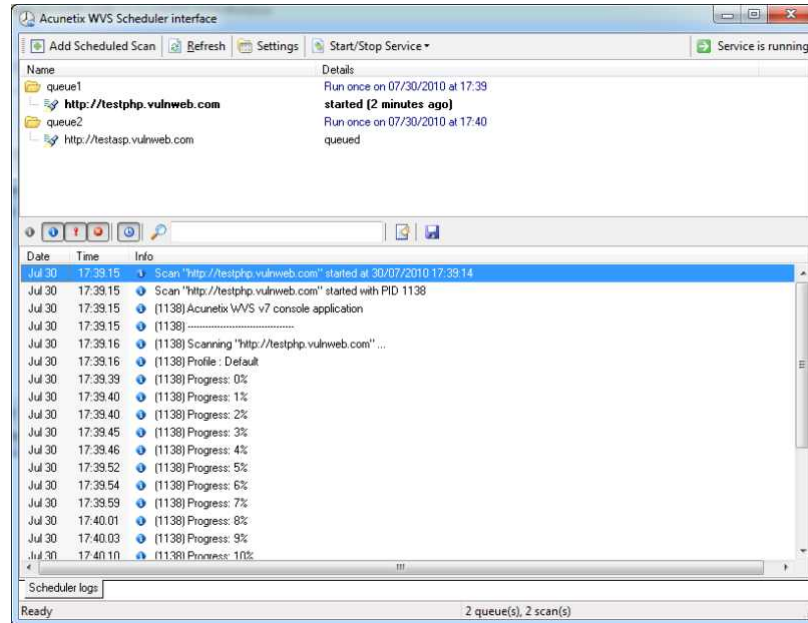
| Option | Description |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /v or /View | View a *.pre format report in the Acunetix reporter. Syntax: /v [report] Example: /v c:\report.pre |
| /o or /Output | The destination path where the generated report should be saved and the filename of the report. Syntax: /o [report name] Example: /o c:\reports\report |
| /r or /Report | Specify the report template to use for generating the report. Available report templates: WVSComplianceReport.rep: Compliance report. WVSDeveloperReport.rep: Developer report. WVSScanCompare.rep: Scan comparison report. WVSSingleScan.rep: Detailed Scan report. WVSSingleScanExecutive.rep: Executive Summary WVSVulnGroupTrends.rep: Monthly Vulnerabilities report. Syntax: |

| | |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>/r [report template]</p> <p>Example:</p> <p>/r WVSDeveloperReport.rep</p> <p>Note: For Compliance reports, one must use the /r option in conjunction with the /k option described below.</p> |
| /k or /Kind | <p>This parameter may be used only for compliance type reports. In fact, such parameter should only be used when the /r or /Report switches are set to WVSComplianceReport.rep. To see a list of compliance templates available, run the following command 'reporter_console.exe /?'</p> <p>Syntax:</p> <p>/r WVSComplianceReport.rep /k [compliance type template]</p> <p>Example:</p> <p>/r WVSComplianceReport.rep /k PCI12.xml</p> |
| /p or /Password | <p>Application password if user interface password is enabled. Password can be enabled from the Application settings > General node.</p> <p>Syntax:</p> <p>/p [password]</p> |
| /c or /Console | <p>Do not load Acunetix Reporter user interface. If this option is not specified, by default the user interface of the Acunetix Reporter will automatically pop up.</p> <p>Syntax:</p> <p>/c</p> |
| /a or /Action | <p>Specify the file type in which the generated report should be exported to. File types available:</p> <p>PDF, RTF, HTML, REP (Acunetix WVS proprietary format).</p> <p>Syntax:</p> <p>/a [format type]</p> <p>Example:</p> <p>/a PDF</p> |
| /p or /Parameters | <p>For each type or report template, there are different parameters. If no parameters are specified, the default parameter settings will be used. To specify the parameters to be passed to the reporter, use the "name=value" format delimited by ";". To find out what parameters are available for each type report template, use the following syntax:</p> <p>Reporter_console.exe /r ReportTemplate /?</p> <p>Syntax:</p> <p>/r [report template] /p [parameter=True/False]</p> <p>Usage Example:</p> <p>/r WVSSingleScan.rep /p "ShowHTTP=False "</p> |
| /t or /Target | <p>Scan identifiers from the database to use as a report source. From the Acunetix WVS reporter, in the Configuration > WVS Database node, you can find the ID for each scan stored in the reporting database. The identifier can be one integer for single target template, two integers for comparison templates delimited by ";". Can also be omitted for reports without specific scan target. For single scan templates, you can use "last" as target to indicate the last saved scan from the</p> |

| | |
|--|---------------------------------------------------------------------------|
| | database. Syntax: /t [report ID] Example: /t 24 |
|--|---------------------------------------------------------------------------|

11. The Scheduler

Introduction




Screenshot 40 – Acunetix WVS Scheduler

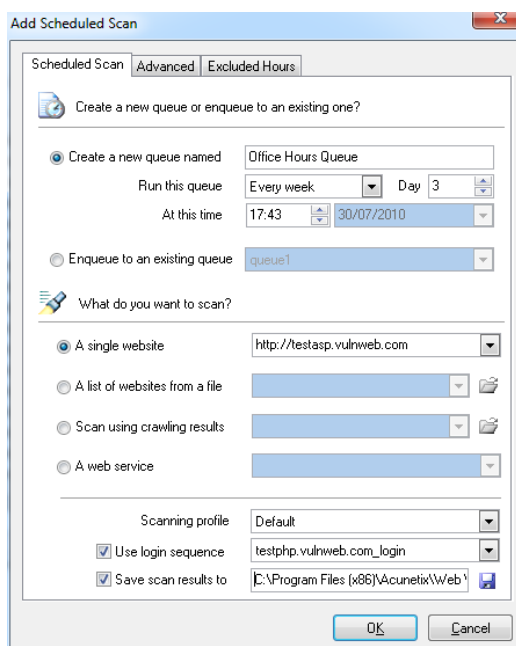
The Scheduler application allows you to schedule scans at a convenient time without requiring Acunetix WVS or the Acunetix WVS Scheduler Interface to be running.

Creating a Scheduled scan

NOTE: First a queue with a specific schedule must be created and then scans are assigned to the queue. Therefore schedule time and exclude hours must be set for each queue. Multiple scans will run sequentially in a queue and cannot run simultaneously. The schedule is set for a particular queue and not for a particular scan. Multiple queues with different schedules can be created with multiple scans assigned to each queue.

Creating a queue and a schedule

1. Start the Scheduler interface by clicking on the Scheduler icon  on the toolbar in the Acunetix WVS interface, or select Acunetix WVS scheduler from the Acunetix program group.



Screenshot 41 - Creating a schedule

2. Enter a queue name in the field 'Create a new queue named' to create a new queue or tick 'Enqueue to an existing Queue' to add the new scan to an existing queue. Select the scheduled recurrence of the queue from: Once, Every Day, Every Week, Every Month or Continuous. Set a specific day number if schedule is set to weekly or monthly, e.g. 2nd day of the week or 21st day of the month.

3. You can also specify the hours to pause an ongoing scan from the 'Excluded hours' tab. Tick 'Enable Excluded Hours' and highlight in red when the scan should be paused; e.g. you want to stop scanning your website during normal business hours.

Note: If a scan is still running during excluded hours, the scan will be automatically paused and resumed again when scanning is allowed.

4. In the 'What do you want to scan?' section, specify the target URL to scan a single website. You can also specify a text filename containing a list of URL's to be scanned, or a saved crawl result, or a web service URL.

5. Select which scanning profile should be used to scan the target and specify a Logon sequence if needed. Specify a location where the scan results should be saved to. Click 'OK' to save the scheduled job.

Advanced Options tab

In the Advanced Tab you can configure any of the following crawling, scanning and reporting options:

- Save options
- Logging options
- Scan options (e.g. scanning mode, AcuSensor technology etc)
- Crawling options
- Reporting options

Scheduler Settings

General settings tab

In this tab, you can configure to start Scheduler Interface on Windows startup, and also to automatically minimize to system tray.

Email notifications settings tab

In this tab you can specify the notification email settings, such as SMTP server IP or FQDN and port, SMTP server authentication (optional) and email addresses which will be used.

Scheduled Scans controls

By right clicking a running scan, you can select to pause or resume the scan. A paused scan will not be automatically resumed. You need to manually resume the scan. You can also stop the running scan and save partial scan results by right clicking the scan and select 'Stop Scan (save partial results)'.

12. Other Acunetix WVS tools

The Target Finder

The Target Finder is a port scanner which can be used to discover running web servers on a given IP or within a specified range of IP's. The list of ports on which the web servers are listening can also be configured. The default ports the scanner will scan are port 80 for HTTP and port 443 for SSL.

More information about the target finder can be found here:

<http://www.acunetix.com/blog/docs/target-finder/>

The Subdomain scanner

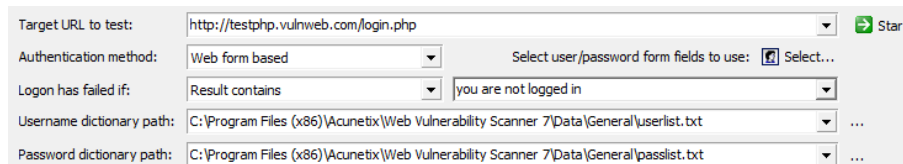
The Subdomain Scanner scans a top-level domain to discover any sub domains configured in its hierarchy, by using the target domain's DNS **Error! Bookmark not defined.** server, or any other DNS server specified by the user.

More information about the Subdomain scanner can be found here:

<http://www.acunetix.com/blog/docs/subdomain-scanner/>

The Authentication tester

The authentication tester is a tool used to test the strength of both usernames and passwords within HTTP or web forms authentication environments via a dictionary attack.



Screenshot 42 – Authentication Tester

More information about the Authentication tester tool can be found here:

<http://www.acunetix.com/blog/docs/authentication-tester/>


Login Sequence Recorder

The Login Sequence Recorder can be used to perform a number of tasks during a crawl and a scan;

- To configure Acunetix WVS to access a form based password protected section
- To create a pre-defined crawling sequence, such as a shopping cart
- To mark pages that require human / manual intervention each time they are accessed, such as pages with CAPTCHA, One-Time password, Two-Factor authentication etc.

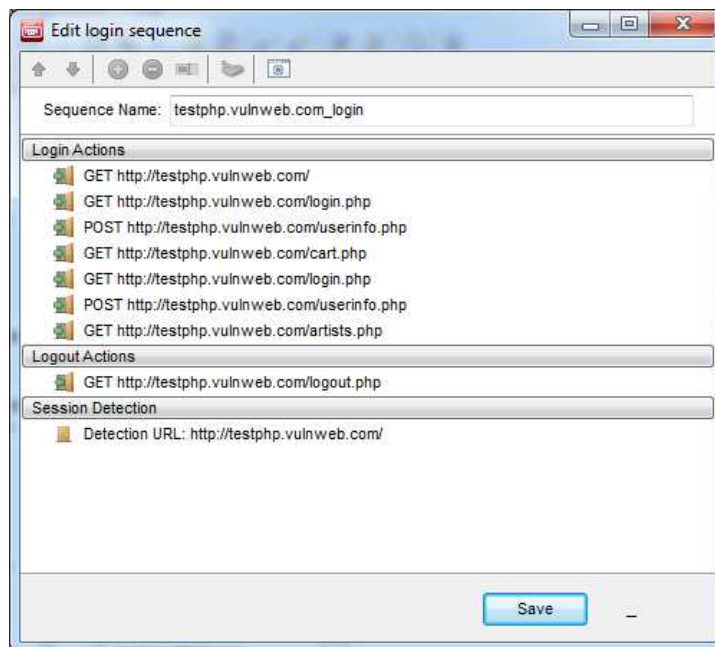
Creating or editing login sequences

1. Go to Settings > Scanner Settings > Login Sequences
-

2. In this configuration screen you can create or edit existing login sequences which are used by Acunetix WVS to access form based authentication protected areas in a website. Login sequences allow Acunetix WVS to replicate all events which are manually performed to access the area secured by a login page.
3. Click on the  button to open up the Login Sequence Recorder. Enter the URL of the website and click on 'Next'. One can also click 'Check URL' to confirm that the URL entered is reachable from Acunetix Login Sequence Recorder.
4. Record the login sequence. For more information refer to the section 'Scanning a form based password protected area' on page 28 in this user manual.

Editing a Login Sequence

The login sequence can be reviewed by clicking on the 'Edit sequence' button.

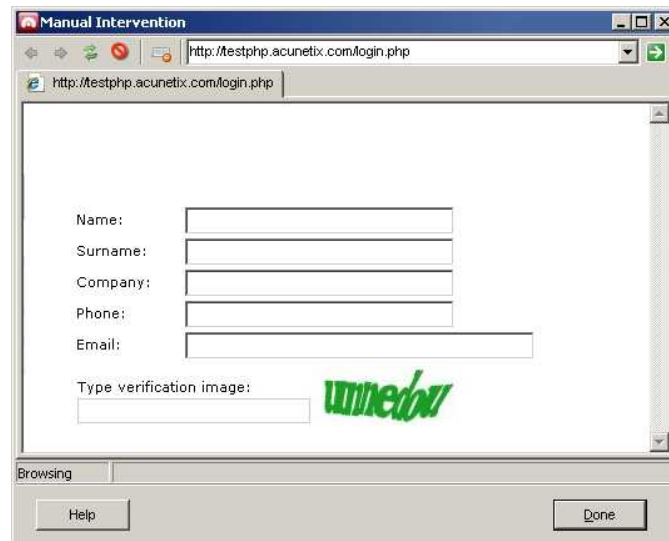


Screenshot 43 – Login Sequence Editing

You can change the request priority by highlighting the URL and clicking the up or down arrow in the top right hand side of the window.

Marking Pages for Manual Intervention (human input is required)

If some pages in your web application require manual intervention, such as pages with CAPTCHA, One-Time password or Two-Factor authentication, use the Login Sequence Recorder to configure the crawler to wait for user input when crawling such page. To mark a page for manual intervention:



Screenshot 44 – Manual browser window

1. Launch the Login Sequence Recorder and enter the web application URL in the first step.
2. In the second step of the wizard 'Record Login Sequence', click on the '⏸' (Pause) button to pause the recording, and enter the URL of the page which requires human input in the URL input field.
3. Once the page has loaded, click on '⌨' (Manual Intervention) button. Proceed by clicking the 'Next' button till the end of the wizard.

Once a scan is launched, a browser window will automatically pop up when the page is reached. You can now perform the action you need to do. Click 'Done' once the action is ready.

Note: Only one page has to be marked for manual intervention. If you have more than one page that requires manual intervention, specify these URLs the first time the browser window automatically pops up during the crawl and perform the action on those pages as well, so that the crawler will automatically crawl those pages without you having to wait for another pop-up.

More information and a video about the Login Sequence Recorder can be found here:

<http://www.acunetix.com/blog/docs/acunetix-wvs-login-sequence-recorder/>

Traversing Web Form pages

Many websites include web forms that capture visitor data, such as download forms. These forms can be automatically submitted with custom values. These values will be submitted by the crawler and scanner during an automated crawl.

Note: By default Acunetix WVS already has a generic submit form rule which will submit generic details to any kind of web form it might encounter during scanning.

To specify values that must be automatically entered on a web form:

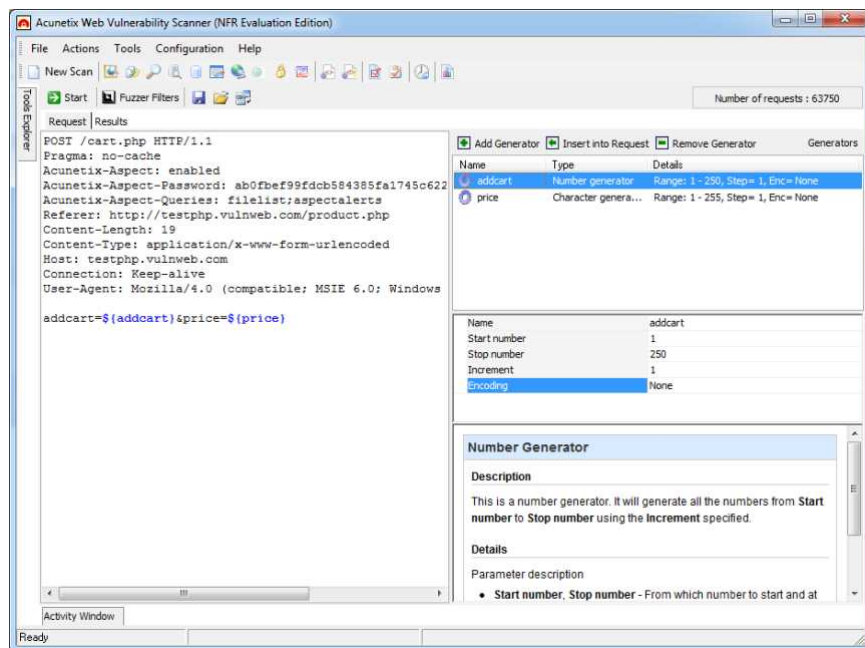
1. Go to Settings >Scanner settings > Input Fields
2. Enter the URL of the webpage or web service containing the specific form or list of operations to which custom parameters are to be passed, and click on "Parse from URL" button. The resulting list will then be automatically completed with the form fields found on the given URL.

3. Enter the values for the required fields from the list by clicking in the value column for that field. Click 'Apply' to save changes. Alternatively, you can configure Acunetix WVS to automatically randomize the values for each parameter by entering the below bolded variable name in the parameter's value field:

- **`\${alphanand}`** – Automatically submit random alphabetical characters (a – z)
- **`\${numbrand}`** – Automatically submit random numeric characters (0 - 9)
- **`\${alphanumrand}`** – Automatically submit random alphabetical and numeric characters (a – z, 0 – 9)

Note: If specific different details must be specified for each different web form, create a new web form rule for each form.

The HTTP Fuzzer tool



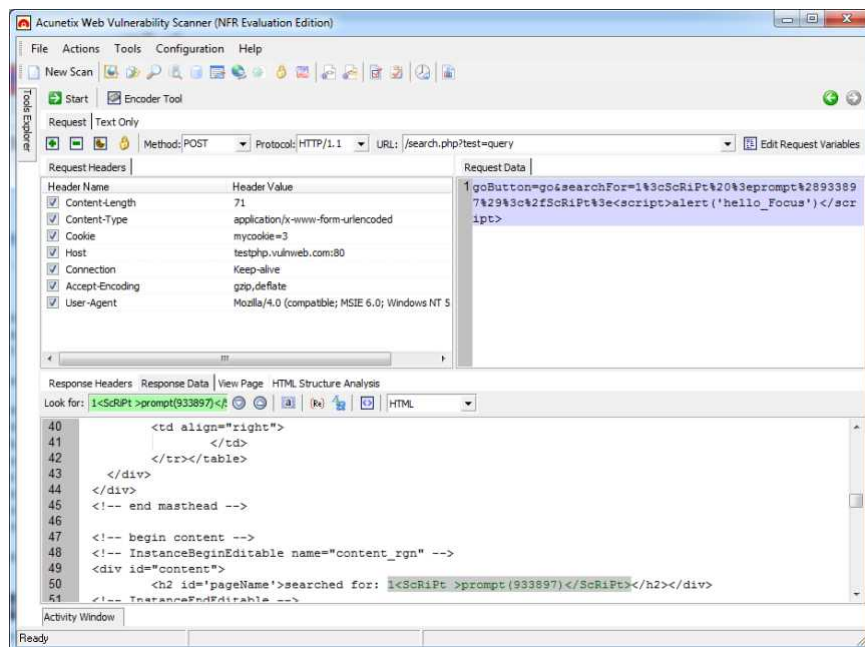
Screenshot 45 – The HTTP Fuzzer

The HTTP Fuzzer tool allows you to take a particular HTTP request and automatically create variations of it. For example, you can send a large number of HTTP requests containing invalid, unexpected and random data to the web application to test the website's input validation capabilities, and also handling of unexpected data.

More information about the HTTP Fuzzer can be found here:

<http://www.acunetix.com/blog/docs/http-fuzzer-tool/>

The HTTP editor tool



Screenshot 46 - The HTTP Editor

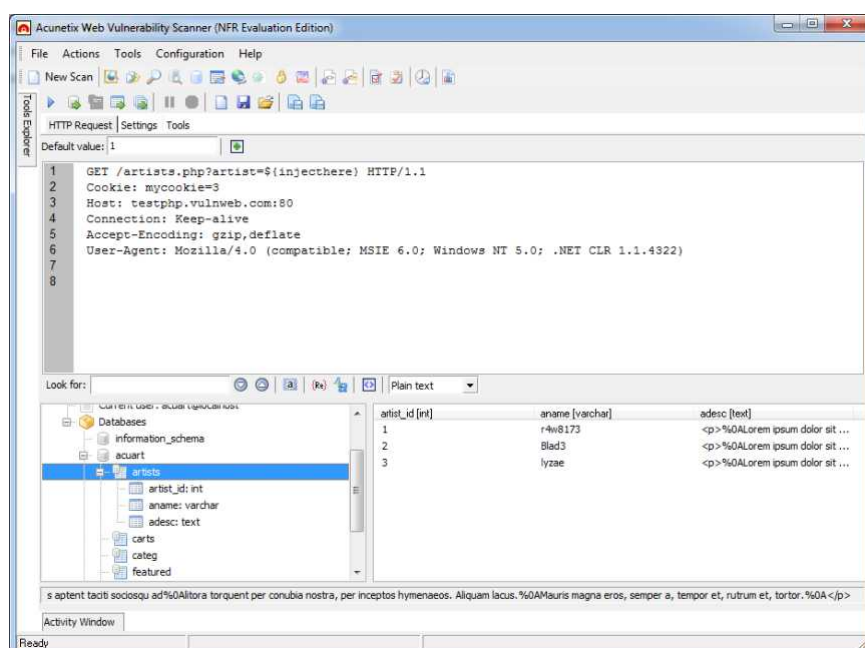
The HTTP Editor tool allows you to create, analyze and edit client HTTP requests and server responses. This allows you to further fine tune attacks and check if vulnerabilities were solved.

You can start the HTTP Editor from the 'Tools' node within the Tools Explorer window pane. The Top pane in the HTTP editor displays the HTTP request data and headers. The bottom pane displays the HTTP response headers data.

More information about the HTTP editor can be found here:

<http://www.acunetix.com/blog/docs/http-editor/>

The SQL injector tool



Screenshot 47 - SQL Injector

The Blind SQL injector is an automated database data extraction tool. By importing SQL injections discovered when scanning a website, you can see what a serious impact an SQL injection can have on the website.

With the Blind SQL Injector tool you can also make manual tests to test for different variants of SQL injections. You will also be able to enumerate databases, tables, dump data and also read specific files on the file system of the web server, depending on the seriousness of the vulnerability. Using this tool, you can also run custom SQL select queries against the database.

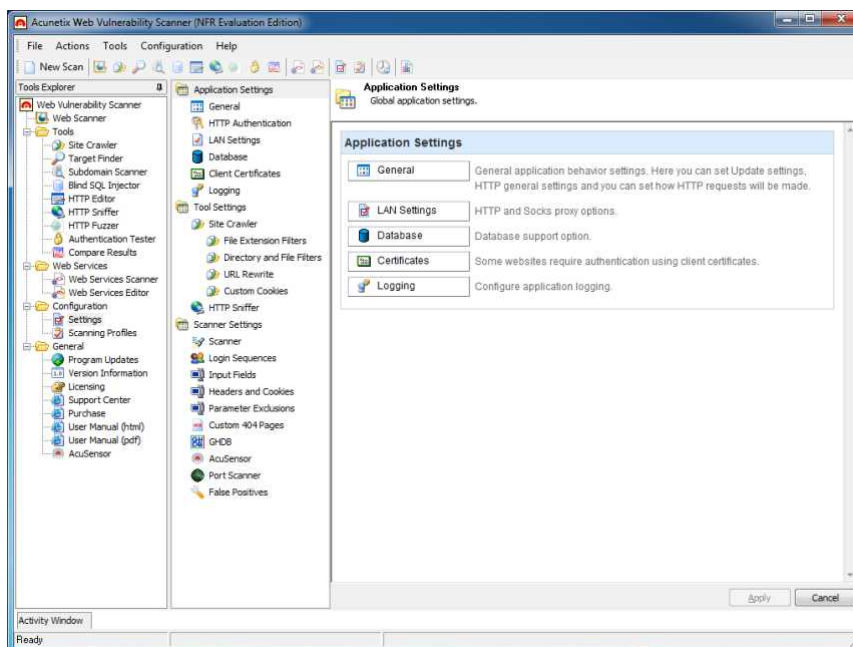
More information about the blind SQL injector can be found here:

<http://www.acunetix.com/blog/docs/blind-sql-injector-tool/>

13. Advanced Configuration Options

Introduction

The Acunetix WVS configuration settings can be accessed from the node 'Configuration > Settings' in the Tools Explorer window pane.



Screenshot 48 - Configuration Settings

General

From this node, the General Application Settings can be configured.

Updates

- **Updates URL** - The location from where vulnerability and application updates can be downloaded.
- **Check for updates** - Specify when the application should check for new vulnerability and application updates.

HTTP General

- **User agent string** - Configure what user agent header string Acunetix WVS should use when accessing a target website. You can also specify a custom user agent string by manually typing it in.
- **Maximum number of parallel connections** - Specify the maximum number of HTTP connections made to a target site at the same time. If overloaded with requests, some target servers might crash or reject new connections.
- **HTTP request timeout in seconds** – Specify the time interval of how long Acunetix WVS has to wait for a HTTP response before considering it as timed out.
- **Delay between consecutive requests in milliseconds** - Delay between each HTTP request Acunetix WVS sends to the target website.

- **HTTP response size limit in kilobytes** - Maximum HTTP response size accepted by the crawler. Larger HTTP responses than the specified size will not be crawled (with this option you are controlling the maximum size of the requested files).
- **Display custom HTTP status information** - Display the full HTTP response status line header and the corresponding status string.
- **Display HTTPS status icon** – Enable this option to show a padlock icon next to files or directories which are accessed via HTTPS and not HTTP.

Memory Optimization

Enabling this option instructs Acunetix WVS to store temporary data in the specified location instead of system memory. Acunetix WVS must have full access to this folder. This will greatly reduce overall memory usage.

Password Protection

In this section the user can set a password to restrict access to the Acunetix WVS main interface and all the other Acunetix WVS applications, such as the Reporter, Vulnerability Editor and Scheduler.

To create a new password, enter the password in the fields 'New Password' and 'Confirm New Password'.

To remove password protection, enter the current password in the field 'Current Password' and leave the other 2 fields blank.

Client Certifications

Some websites require client certificates to identify a client before access is granted. These certificates may be configured in Acunetix WVS by specifying the URL to be used during a crawl or a scan. To do this:

1. Go to Settings > Application Settings > Client Certificates
2. Specify a certificate location by browsing to the certificate by using the Browse icon next to the 'Certificate file' text box and enter the certificate password in the 'Password' text box.
3. Enter the URL which needs a client certificate to be accessed. Click on 'Import' and 'Apply' to save the certificate information.

Logging

You can enable or disable different logging levels in Acunetix WVS. You can configure logging from:

Settings > Application Settings > Logging

Scanner Settings

- **Disable Alerts generated by crawler** - Select this option to not report crawler related alerts, such as broken links, file inputs and files which their name indicates that they can be dangerous etc.
- **Test known web application (e.g. Joomla, Wordpress) vulnerabilities on every directory** - Select this option to launch the finger printing module and try to automatically detect Well Known Web Applications in every directory, and not just in their default directory installation (e.g. by default Wordpress is installed in blog directory). Once specific known web applications (such as Wordpress and Joomla) are discovered, Acunetix WVS launches number of vulnerabilities checks against them. This will drastically prolong the scan time because of the large number of

checks involved. If you do not have any well known web applications running on your website, such as Wordpress or Joomla there is no need to enable is option.

- **Scanning mode** - From this section you can select the **Scanning Mode** which will be used during both the crawling and scanning stage of the target website. The scan mode will determine how both the crawler and the scanner will treat website parameters (also known as inputs), which will affect the number of security checks launched against the website. The scanning mode options available are the following:
 - **Quick** - In this mode, the crawler will only fetch a very limited number of variations of each parameter, because they are not considered to be actions parameters. Action parameters are parameters which are designed to control the execution flow of the server scripts. Such scanning mode should only be used with small and static websites.
 - **Heuristic** - In this mode, the crawler will try to make heuristic decisions on which parameters should be considered as action parameters and which should not. It will try to fetch more possible values of each parameter. This will result in a larger number of different variations, and therefore the scanner will launch more security checks against the website. This scanning mode is the most efficient and accurate one. We suggest this should always be the scanning mode of choice unless there are specific reasons to use other scanning modes.
 - **Extensive** - In this mode, the crawler will fetch all possible values and combinations of all parameters. This will lead to a much larger number of variations, and therefore the scanner will launch an extensive amount of security checks against the website. This scanning mode should be rarely used. Scans using Extensive scanning mode can take a considerable amount of time to finish.
- **Limit crawl recursions to X iterations** - After a site is crawled and vulnerability scanning has started, the scanner can discover new objects; therefore a new crawl is restarted. This is called iteration. Configure the maximum number of crawl iterations that can happen while scanning a website.
- **Enable Port Scanning** – Enable this option to port scan the web server on which the target website is hosted during a web security scan by default. For more information about the Port Scanner and Network Alerts, refer to page 9 of this manual.
- **Collect uncommon HTTP Requests** - Select this option to configure Acunetix WVS to report back any server response which is not common and which might include sensitive data, such as internal server errors. These alerts are reported under the 'Knowledge Base' node in the Scan Results window.
- **Abort Scan if the server stops responding** - Configure the maximum number of network errors in a scan the scanner needs to encounter before completely aborting the scan.
- **List of hosts allowed** - By default, Acunetix WVS will not crawl links outside the target URL. However, some links on some websites link to external locations outside the target URL and may require being included in the scan. Configure Acunetix WVS to include and follow these links in the 'list of hosts allowed' field. Enter the host name or IP address of the domain to be included in a crawl and vulnerability scan and click the '+' button to add this entry to the list of hosts to be scanned. E.g. when scanning testphp.vulnweb.com there are links which link to www.acunetix.com.

Note: Hostnames can be specified using wildcards e.g. '*.domain.com', which includes all websites with a suffix of .domain.com such as sales.domain.com. A question mark can also be used as a wildcard, e.g. 'host?.domain.com', would include all websites with one character added after 'host' such as host1.domain.com.

Headers and Cookies

Settings > Scanner Settings > Headers and Cookies

In this node, you can configure all the options related to manipulation of HTTP Headers and Cookies. The options available are:

- **Test cookies for all files** – By default, Acunetix WVS will only try to manipulate cookie data and use it against files that contain GET and POST parameters. If this option is enabled, Acunetix WVS will also try to use manipulated cookie data against static files.
- **Manipulate the HTTP headers below** – A number of Acunetix WVS web security checks try to manipulate HTTP headers. This section lists which HTTP headers Acunetix WVS will try to manipulate during a scan. If you are testing a web application that uses other custom HTTP headers that you would like to test, you can add them to this list by clicking on the '+' button. Use the '-' button to remove the highlighted header from the list. By un-ticking the option 'Manipulate the HTTP headers listed below' you will be disabling all HTTP headers manipulation tests.

Parameter Exclusions

Settings > Scanner Settings > Parameter Exclusions

In this node you can specify the parameters to be excluded from a scan. Some parameters cannot be manipulated without affecting the user session and will therefore not be manipulated during a scan. You can also select not to test all possible values.

Note: Parameters specified in the Parameter Exclusions list will only be excluded from a scan and not from a crawl; therefore they will still be crawled by the crawler.

Adding a parameter to the exclusion list

1. Specify a URL in the 'URL' textbox to exclude the parameter when scanning the specified URL only. Use a '*' wildcard to exclude the parameter from every scan.
2. Type the parameter name to be excluded in the 'Name' textbox and select for which type of HTTP verb it should be excluded from the 'Type' drop down menu. Select 'Any' to exclude the parameter in any type of HTTP verb.
3. Select 'Exclude from Scan' to exclude any kind of parameter manipulation during scan or select 'Do not test all possible values' to try only a limited number of variations during a scan from the 'Action' drop down menu. Click 'Apply' button to save changes.

Settings > Scanner Settings > GHDB

By default, all GHDB (Google Hacking Database) tests (1450+) are launched against a website during a scan. From this node, you can exclude GHDB vulnerability checks which you would not like to launch against your website. You can also select previously deselected GHDB vulnerability checks to include them again in a default website security scan.

Filter the list by entering a keyword (e.g. sql) in the 'Filter GHDB' text box. Click on 'Uncheck Visible' to uncheck all vulnerabilities which match with the

keyword and exclude them from a default scan. Click 'Check Visible' to check all entries again and include them in a default scan.

Settings > Scanner Settings > Port Scanner

While scanning a website you can also choose to launch a port scan against the web server on which the website is hosted. The port scanner will scan the web server using a specific list of ports. If a port is found to be open, the port scanner will identify what network service is running on that port and will launch a number of security checks specifically targeting the discovered network service. Therefore if a DNS server is discovered, tests such as DNS open zone transfer and DNS open recursion tests are run against the network service. The Port Scanner configuration options are:

- **Number of sockets used for scanning** - Specify the amount of network sockets to be used by the Port Scanner module. The larger the number the faster the scan will be, but it will also increase the load on the web server.
- **Connection timeout (in seconds)** - Specify the timeout in seconds, i.e. if there is no response when trying to connect to a port within the specified amount of seconds, the port will be considered as closed.
- **List of scanned ports** - The list of specified ports for which the Port Scanner will check. Use the '+' button to add a port and a description and use the '-' button to remove selected ports from the list.

A list of open ports on the server will be displayed in the scan results under Knowledge Base > List of open TCP Ports in the Scan results window pane.

Note: The Network Alert Scripts (Network security checks) are fully scriptable and you can write new ones. The Acunetix Web Vulnerability Scanner Network Alert scripting reference is available from the following URL; <http://www.acunetix.com/vulnerability-scanner/scriptingreference/index.html>.

Settings > Scanner Settings > False Positives

When a specific vulnerability is marked as False Positive in the scan results, it will be listed in this node. Press on the '-' button to remove a vulnerability from the list of False Positives.

Note: False positives are specific per site (URL) and file. Therefore if you mark a XSS vulnerability on <http://www.testphp.vulnweb.com/artists.php> as false positive, if you scan another site this vulnerability will show up again if it is discovered.

Scanning Profiles

Via the scanning profiles you can specify which type of vulnerabilities (e.g. XSS, SQL Injection) you would like to check your website for. From the node 'Configuration > Scanning Profiles' in the Tools Explorer window pane, you can create new scanning profiles, or edit existing ones, including the default ones.


Default Scanning Profiles

Acunetix WVS is installed with a number of default scanning profiles: Below is a list of all the scanning profiles and a summary of the security checks they include. For a detailed list of which vulnerability checks are included in each scanning profile, navigate to the Configuration > Scanning Profiles node in the Tools Explorer, and select the profile name from the 'Profile' drop down menu. The ticked tests are those tests which will be launched when using such scanning profile.


| Profile | Description |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| default | All vulnerability types |
| AcuSensor | Security checks related to AcuSensor Technology, such as directory traversal, file tempering etc. |
| Blind_SQL_Injection | Blind SQL injection vulnerability checks only |
| CSRF | Cross-site request forgery vulnerability checks only |
| Directory_and_File_checks | A number of security checks related to files, such as text search and backup file checks, and directory checks, such as directory listing etc. |
| empty | This profile may be used as a clean base to create other profiles. |
| File_Upload | File upload form vulnerabilities only |
| GHDB | Google hacking database security checks only. |
| High_Risk_Alerts | Web and network vulnerability checks which are considered as High Risk, such as SQL Injection and XSS. |
| Network_Scripts | Network security checks only. If you would like to check if the network services are secured properly on the web server, use this scanning profile. Tests included are DNS cache poisoning, telnet brute force and much more. |
| parameter_manipulation | All parameter manipulation attacks, such as SQL injection, XSS 'Cross site scripting', Command execution etc. |
| SQL_Injection | SQL injection vulnerability checks only |
| Weak_Passwords | Web forms authentication audits related checks |
| Web_Applications | Well known web applications e.g. Joomla, Wordpress security checks |
| Ws_default | Web services vulnerability checks only |
| XSS | Cross-site scripting vulnerability checks only |
| | |

Creating/Modifying Scanning Profiles

Creating a new Scanning Profile

1. Select the Empty scanning profile from the 'Profile' drop down menu.
2. Check all the vulnerability checks / security checks you would like to include in the scanning profile.
3. Click on save  button to save the profile.

Modifying a Scanning Profile

1. Select the scanning profile you would like to edit from the 'Profile' drop down menu.
2. Check / un-check all the vulnerability checks / security checks you would like to include / exclude in the scanning profile.
3. Click on save  button to save the profile.

Creating custom vulnerability checks

Acunetix WVS allows you to create your own web and network vulnerability checks. For example if you are familiar with a particular web application and want to create specific checks for it you can use the Acunetix Vulnerability Check SDK to create your own vulnerability checks.

More information about creating vulnerability checks can be found here:

<http://www.acunetix.com/blog/uncategorized/creating-vulnerability-checks/>

14. Troubleshooting

Obtaining support

The main sources of information available to users are:

- The User Manual - most issues can be solved by reading the manual.
- Email Support - contact the Acunetix support department by email at support@acunetix.com
- The Acunetix Support Center – <http://www.acunetix.com/support/>
- Acunetix Web Application Security Blog – <http://www.acunetix.com/blog>

Request Support via E-Mail

If you have problems that you cannot resolve, please contact the Acunetix support department. The best way to do this is via e-mail (support@acunetix.com), since you can include vital information to enable us to solve the issues you have more quickly. Include the license key information in the support email.

You can also use the Acunetix WVS Troubleshooter wizard, which can be launched from the Acunetix WVS program group. The Troubleshooter will automatically generate a number of files needed for Acunetix to provide technical support. The files would include the configuration settings etc. To generate these files, start the troubleshooter and follow the instructions in the wizard.

In addition to collecting all the information, the troubleshooter will also ask you several questions. Answer these questions accurately as without proper information it will not be possible to diagnose your problem.

Then navigate to the support directory, located in the Acunetix installation directory, **ZIP the files** and send the generated files to support@acunetix.com.

We will answer your query within 24 hours or less, depending on your time zone. We will try our best to resolve the issue as quickly as possible.

Index

A
Acunetix SDK 11
AcuSensor Technology 9, 26
Authentication 26, 27
Authentication Tester 11
B
Blind SQL Injector 10
C
Command Line 63
Compare Results 57
Configuring Acunetix WVS 79
Custom 404 Error Pages 30
D
Database, Reporting 17
H
HTTP Editor 10
HTTP Fuzzer 10
HTTP Proxy 18
HTTP Sniffer 10
I
Installation 17
L
Licensing 14
Login Sequence 28
P
Port Scanner 9, 26, 83
R
Reporter 12, 37
S
Scanning Profiles 25, 83
Scheduler 70
Site Crawler 25, 45
Site Crawler Settings 48
SOCKS Proxy 18
Subdomain Scanner 10
Support 14, 87
System Requirements 17
T
Target Finder 10
test websites 17
Training 14
Troubleshooting 87
U
Upgrade 17
V
Vulnerability Editor 12
Vulnerability Scanner 6
W
Web Services Editor 11, 60
Web Services Scanner 11, 59
WVS Scripting Tool 11