Web Vulnerability Scanner v8

User Manual

http://www.acunetix.com

info@acunetix.com

Document version 8

Last updated: 22nd February 2013

Contents

1. Introduction to Acunetix Web Vulnerability Scanner

Why You Need To Secure Your Web Applications

Website security is 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 are web applications vulnerable?

- Websites and web applications are easily available via the internet 24 hours a day, 7 days a week to customers, employees, suppliers and therefore also hackers.
- 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.
- 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 which has to remain open to allow regular operation of the business. 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, since it generally involves processing a large volume of data. It also demands a high-level of expertise and the ability to keep track of considerable volumes of code used in a web application. In addition, hackers are constantly finding new ways to exploit your web application, which would mean that you have to constantly monitor the security communities, and find new vulnerabilities in your web application code before hackers discover them.

Automated vulnerability scanning allows you to focus on the already challenging task of building a web application. An automated web application scanner is always on the lookout for new attack paths that hackers can use to access your web application or the data behind it.

Within minutes, an automated web application scanner can scan your web application, identify all the files accessible from the internet and simulate hacker activity in order to identify vulnerable components.

In addition, an automated vulnerability scanner can also be used to assess the code which makes up a web application, allowing it to identify potential vulnerabilities which might not be obvious from the internet, but still exist in the web application, and can thus still be exploited.

Acunetix Web Vulnerability Scanner

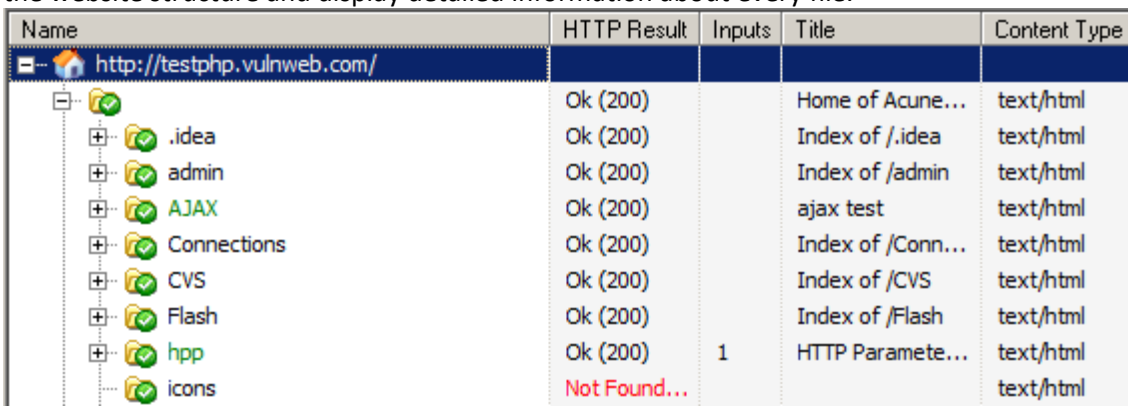
Acunetix Web Vulnerability Scanner is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injections, Cross site scripting and other exploitable vulnerabilities. In general, Acunetix Web Vulnerability Scanner scans any website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

Acunetix Web Vulnerability Scanner offers a strong and unique solution for analyzing off-the-shelf and custom web applications including those utilizing JavaScript, AJAX and Web 2.0 web applications. Acunetix has an advanced crawler that can find almost any file. This is important since what is not found cannot be checked.

How Acunetix Web Vulnerability Scanner Works

Acunetix Web Vulnerability Scanner works in the following manner:

1. The Crawler analyzes the entire website by following all the links on the site and in the robots.txt file and sitemap.xml (if available). Web Vulnerability Scanner will then map out the website structure and display detailed information about every file.



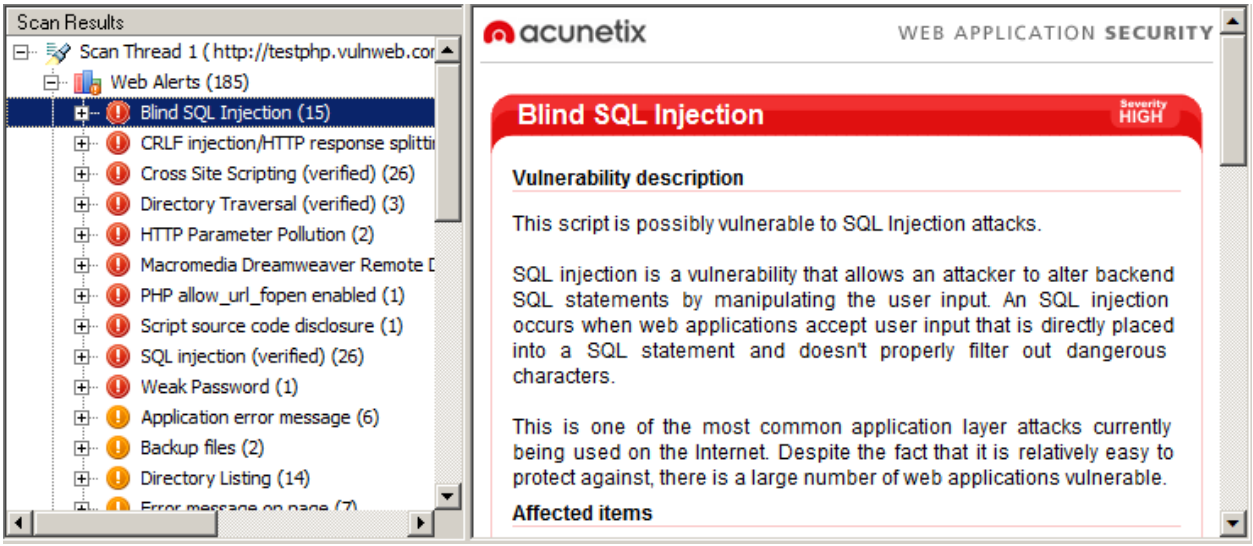
Screenshot 1 - Crawler Results

2. If Acunetix AcuSensor Technology is enabled, the sensor will retrieve a listing of all the files present in the web application directory and add 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. Acunetix AcuSensor also analyses files which are not accessible from the internet, such as *web.config*.

3. After the crawling process, Web Vulnerability Scanner automatically launches a series of vulnerability checks on each page found, in essence emulating a hacker. Also, Acunetix Web Vulnerability Scanner analyses 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 additional vulnerability checks are launched against the website. More information about AcuSensor is provided in the following section.

   As vulnerabilities are found, Acunetix Web Vulnerability Scanner reports these in the 'Alerts' node.



Screenshot 2- Scan Results

Each alert contains information about the vulnerability such as POST variable name, affected item, http response of the server and more.

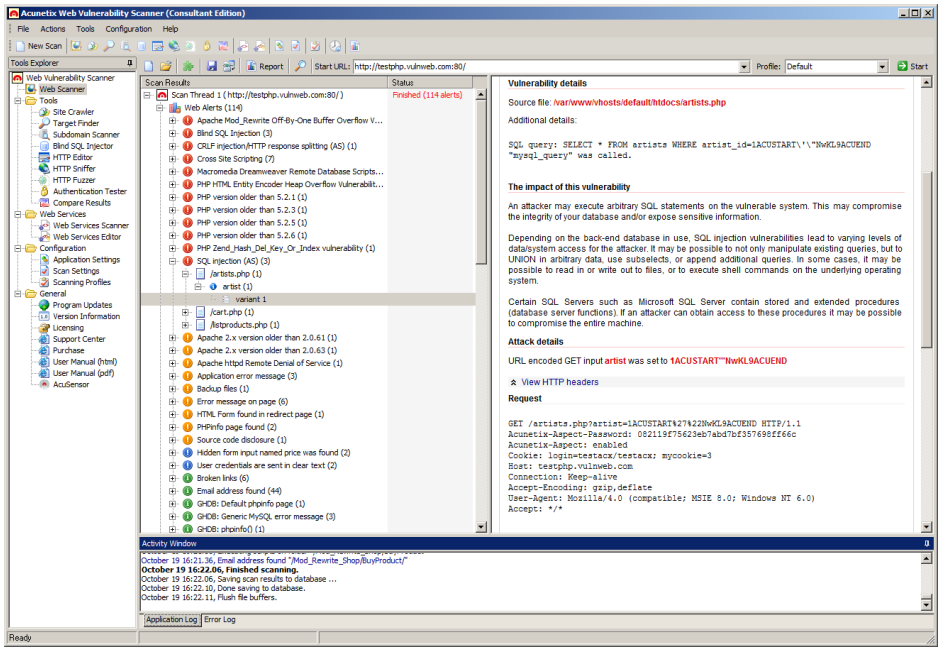
4. If AcuSensor Technology is used details such as source code line number, stack trace or affected SQL query which lead to the vulnerability are listed. Recommendations on how to fix the vulnerability are also shown.

5. In addition, a port scan is launched against the web server hosting the website. If open ports are found, Acunetix Web Vulnerability Scanner will perform a range of network security checks against the network service running on the open port. If open ports are found, they will be reported in the 'Port Scanner' 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, the scan results 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 allows you to identify more vulnerabilities than other Web Application Scanners, whilst generating less false positives. Acunetix AcuSensor indicates exactly where in your code the vulnerability is and reports additional debug information which is handy.



Screenshot 3 - AcuSensor pin-points vulnerabilities in code

The increased accuracy, available for PHP and .NET web applications, is achieved by combining black box scanning techniques with feedback from sensors placed inside the source code. 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. AcuSensor technology combines both techniques to achieve significantly better results than using source code analyzers and black box scanning independently.

The AcuSensor sensors can be inserted in the .NET and PHP code transparently. The .NET source code is not required; the sensors 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 readily available.

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

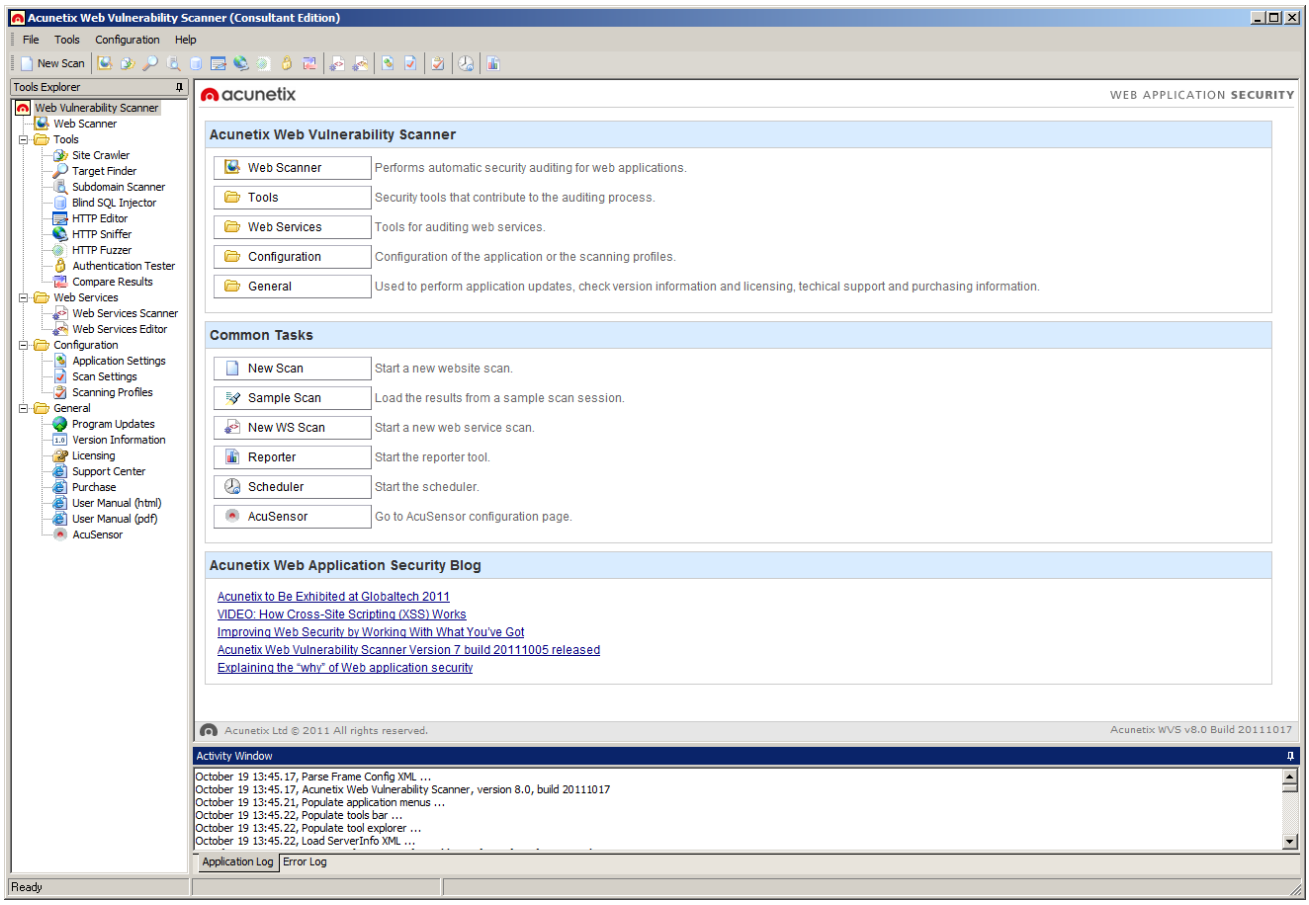
Advantages of using AcuSensor Technology

- 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 behavior of the web application better.
- Alerts you of web application configuration problems which can 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.
- Advises you how to better secure your web server settings, e.g. if write access is enabled on the web server.

- Detects more SQL injection vulnerabilities. Previously SQL injection vulnerabilities could only be found if database errors were reported, whereas now the source code can be analyzed for improve detection
- Ability to detect SQL Injection vulnerabilities in all SQL statements, including in SQL INSERT statements. Using a black box scanner such SQL injection vulnerabilities cannot be found. This significantly increases the ability for Acunetix Web Vulnerability Scanner to find vulnerabilities.
- Discovers all the files present and accessible through the web server. If an attacker gains access to the website and creates a backdoor file in the application directory, the file is 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 test 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 creation 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 or recipients or additional information to the message body to a vulnerable web form, to spam a large number of recipients anonymously.

2. Acunetix Web Vulnerability Scanner Program Overview

Acunetix Web Vulnerability Scanner is a suite of tools that allows you to secure your website in the most efficient manner. It consists of the following components:



Screenshot 4 - Acunetix Web Vulnerability Scanner

Web Scanner

The Web Scanner launches an automatic security audit of a website. A website security scan typically consists of two phases:

1. Crawling – the Crawler automatically analyzes and crawls the website and builds a site structure. The crawling process enumerates all files and is vital to ensure that all the files on your website are scanned.
2. Scanning – Acunetix Web Vulnerability Scanner launches a series of web vulnerability checks against each file in your web application – in effect, emulating a hacker.

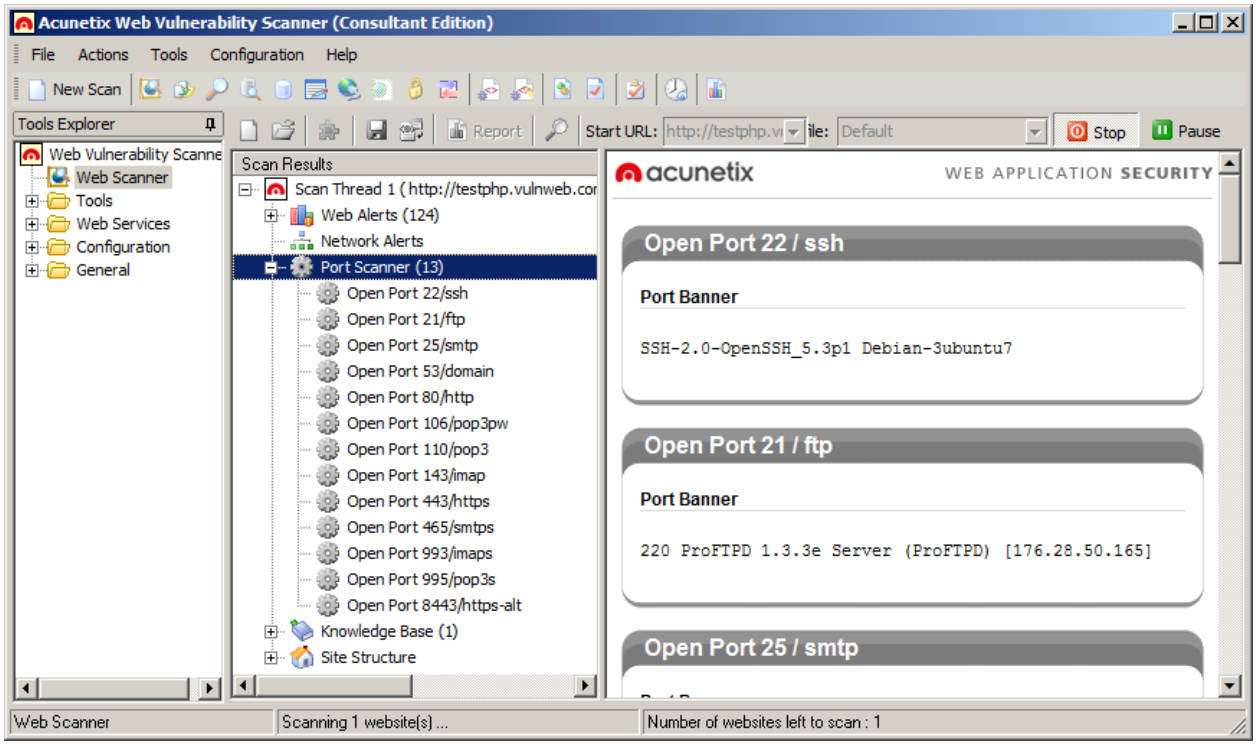
The results of a scan are displayed in the Alert Node tree and include comprehensive details on all the vulnerabilities found within the website.

AcuSensor Technology Agent

Acunetix AcuSensor Technology is a unique technology that allows you to identify more vulnerabilities than a traditional black box web security scanner, and is designed to further reduce false positives. Additionally, it also indicates the code where the vulnerability was found. This increased accuracy is achieved by combining black box scanning techniques with dynamic code analysis whilst the source code is being executed. For Acunetix AcuSensor to work, an agent must be

installed on your website to enable communication between Acunetix Web Vulnerability Scanner and AcuSensor. Acunetix AcuSensor can be used with PHP and .NET web applications.

Port Scanner

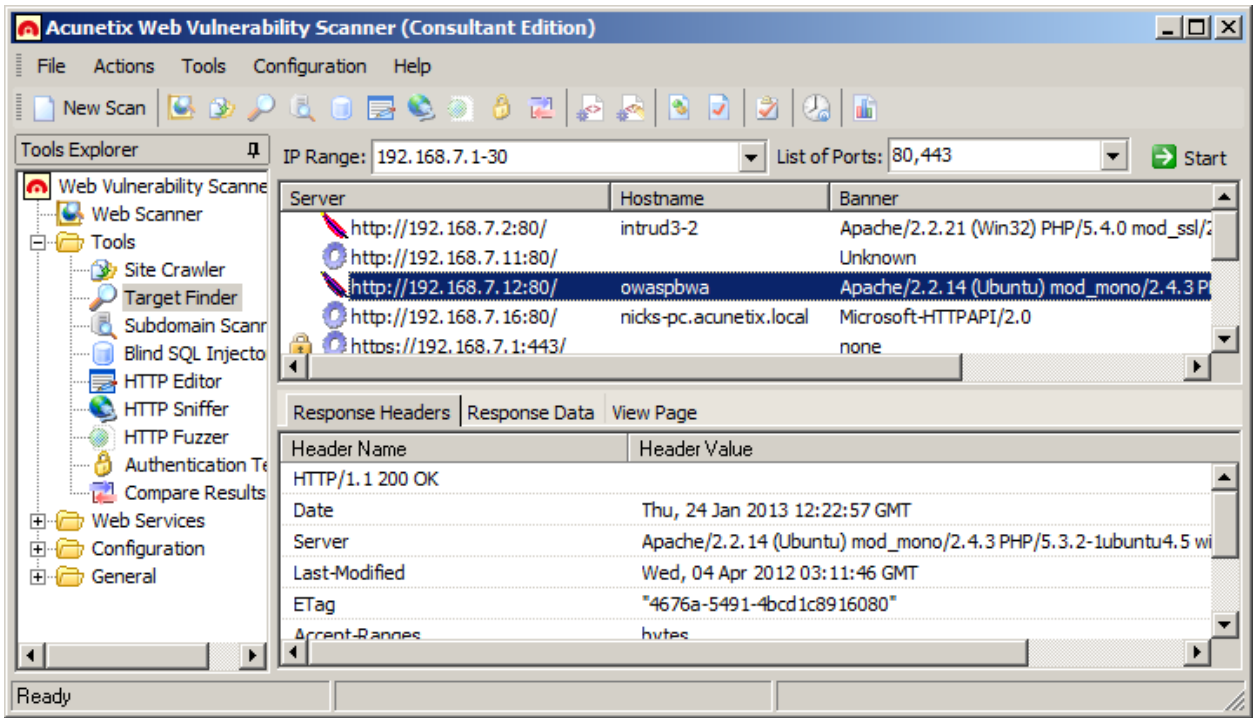


Screenshot 5- Port Scanning

The Port Scanner performs a port scan against the web server hosting the scanned website. When open ports are found, Acunetix Web Vulnerability Scanner will perform 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 using the script engine. A scripting reference is available from the following URL: http://www.acunetix.com/vulnerability-scanner/scriptingreference/index.html

Target Finder

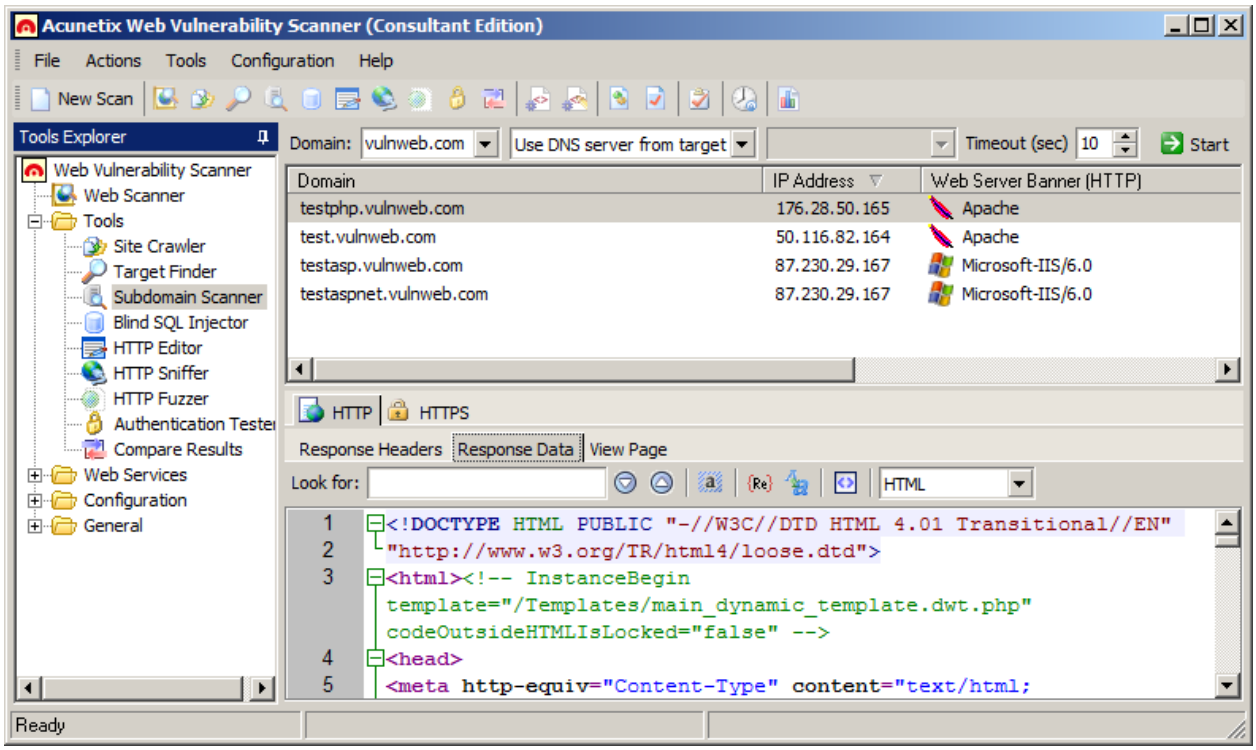


Screenshot 6- Target Finder

The Target Finder is a scanner that allows you to locate web servers (generally on ports 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.

More information about the target finder can be found here:
http://www.acunetix.com/blog/docs/target-finder/

Subdomain Scanner

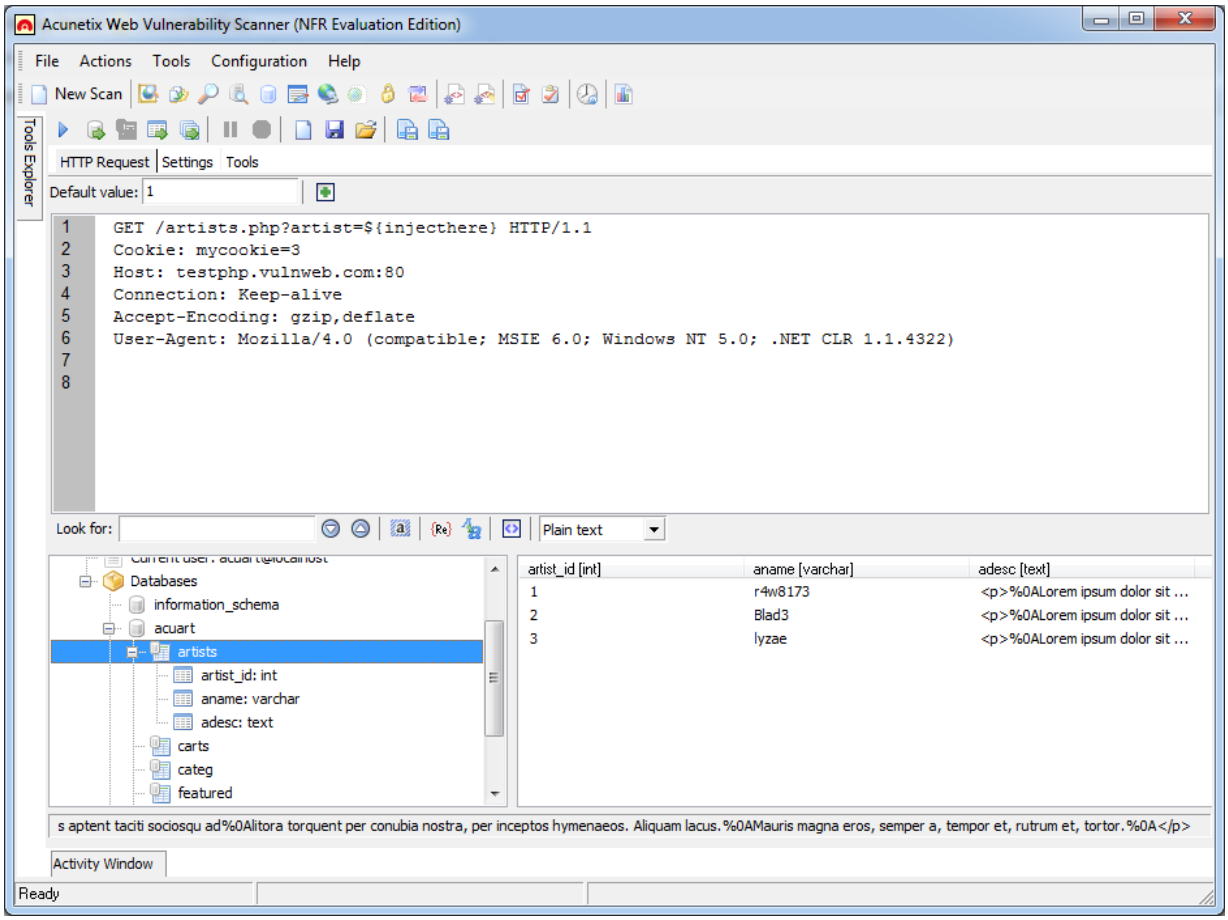


Screenshot 7 - Subdomain Scanner

Using various techniques, the Subdomain scanner allows fast and easy identification of active sub domains of a top-level domain. The Subdomain Scanner can be configured to use the target's DNS 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/

Blind SQL Injector



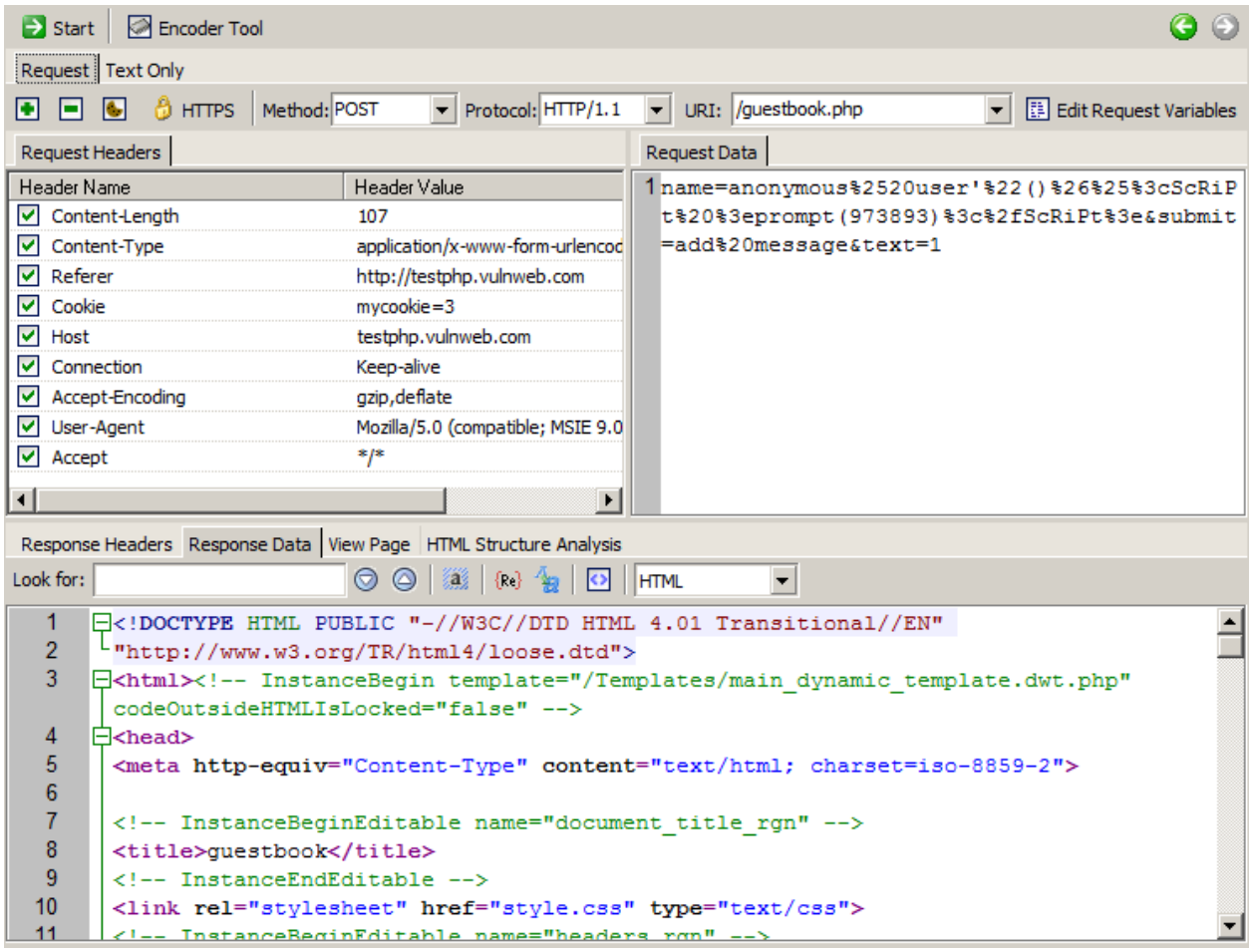
Screenshot 8 - Blind SQL Injector

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 SQL injections reported during a scan. The tool makes use of Blind SQL Injection techniques 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.

With the Blind SQL Injector tool you can also run manual tests to check for different variants of SQL injection. 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/

HTTP Editor



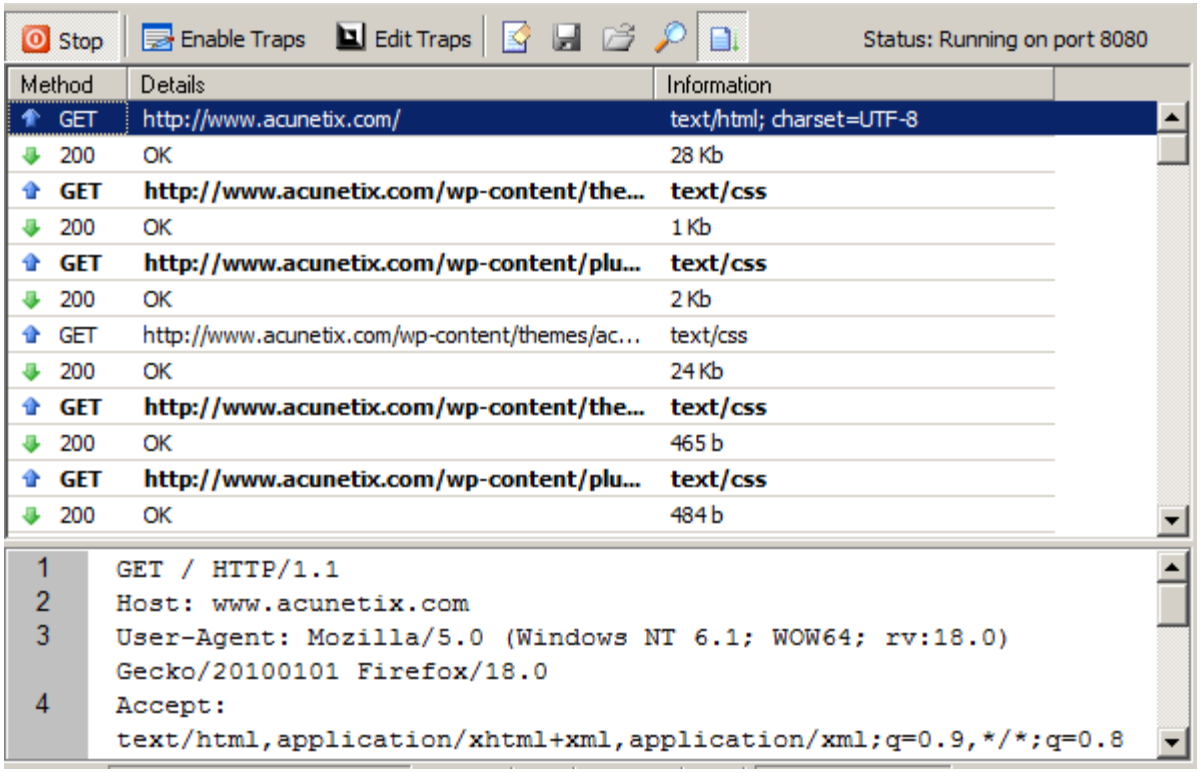
Screenshot 9 - HTTP Editor

The HTTP Editor allows you to create, analyze, and edit client HTTP requests and server 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.

You can start the HTTP Editor from the 'Tools' node within the Tools Explorer. 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/

HTTP Sniffer



Screenshot 10 - 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 capture traffic before it is sent to the web server or back to the web client. This tool is useful to:

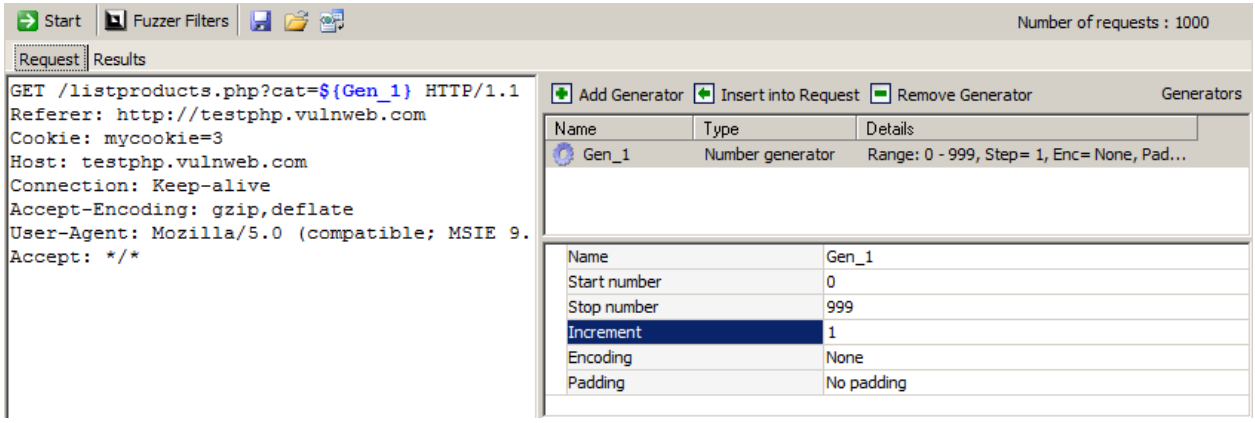
Analyze how Session IDs are stored and how inputs are sent to the server.

Alter any HTTP requests being sent back to the server before they get sent.

Manual crawling; navigate through parts of the website which cannot be crawled automatically, and import the results into the scanner to include them in the automated scan.

For http requests to pass through Acunetix Web Vulnerability Scanner, Acunetix Web Vulnerability Scanner must be configured as a proxy in your web browser. You can read more about the HTTP Sniffer and it's configuration in chapter 7 of this manual.

HTTP Fuzzer



Screenshot 11- HTTP Fuzzer

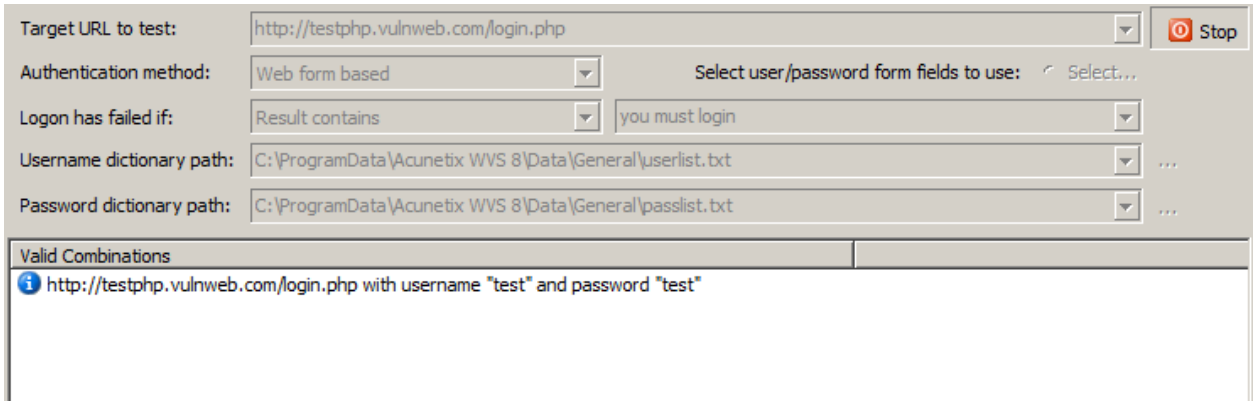
The HTTP Fuzzer enables you to launch a series of sophisticated fuzzing tests to audit the web application's handling of invalid and unexpected random data. The HTTP Fuzzer also allows you to easily create input rules for further testing in Acunetix Web Vulnerability Scanner.

An example would be the following URL: http://testphp.acunetix.com/listproducts.php?cat=1

Using the HTTP Fuzzer you can create a rule that 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.

More information about the HTTP Fuzzer can be found here:
http://www.acunetix.com/blog/docs/http-fuzzer-tool/

Authentication Tester

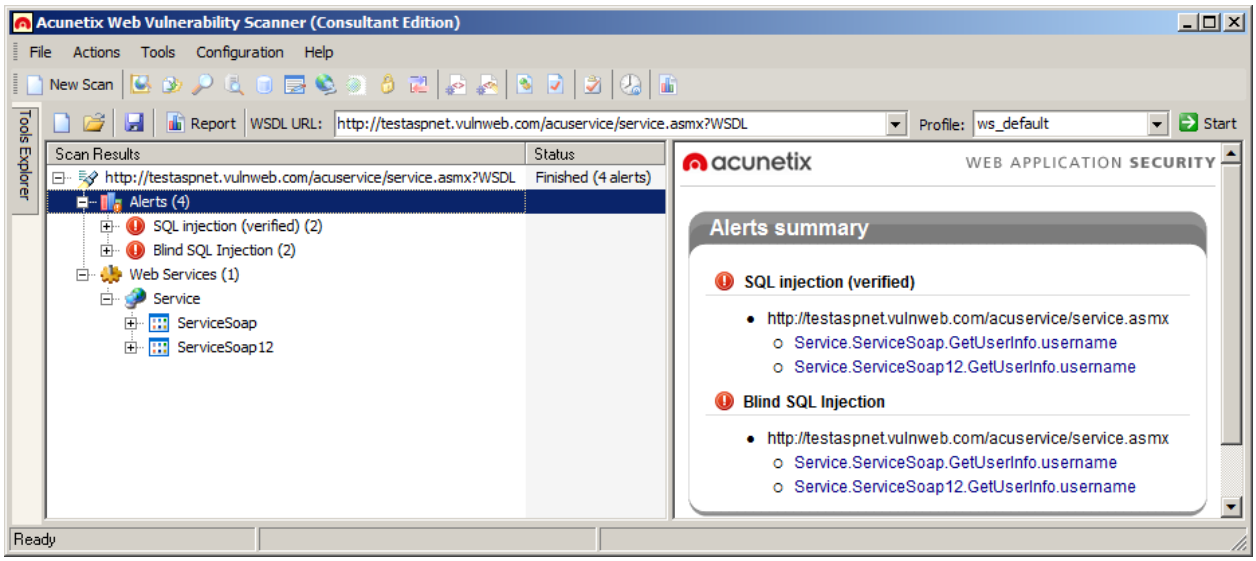


Screenshot 12 - Authentication Tester

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

More information about the Authentication tester can be found here:
http://www.acunetix.com/blog/docs/authentication-tester/

Web Services Scanner and Web Services Editor

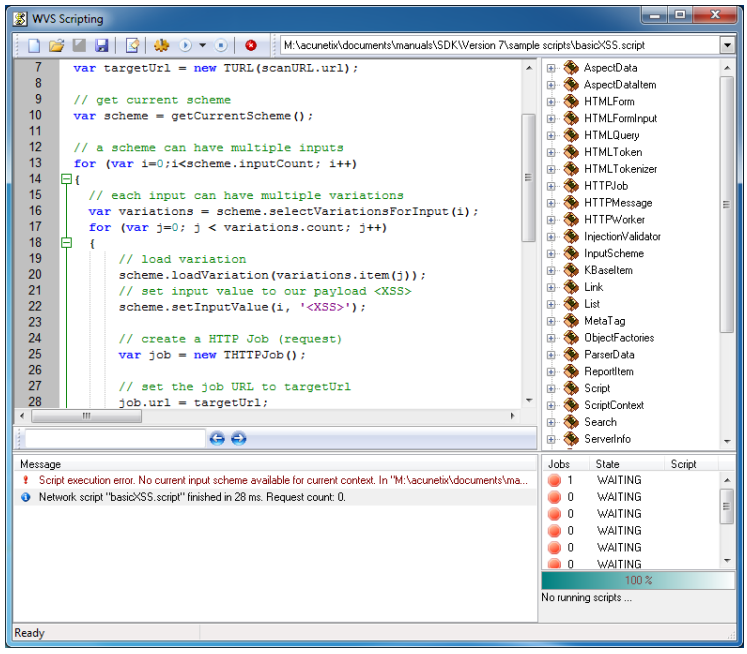


Screenshot 13 - Web Services Scanner

The Web Services Scanner allows you to launch automated vulnerability scans against WSDL based Web Services. Web Services are commonly used for to exchange data, and generally vulnerabilities in Web Services can easy be used to leak sensitive information.

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 analysis 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.

Acunetix Web Vulnerability Scanner SDK



Screenshot 14 – Web Vulnerability Scanner Scripting tool

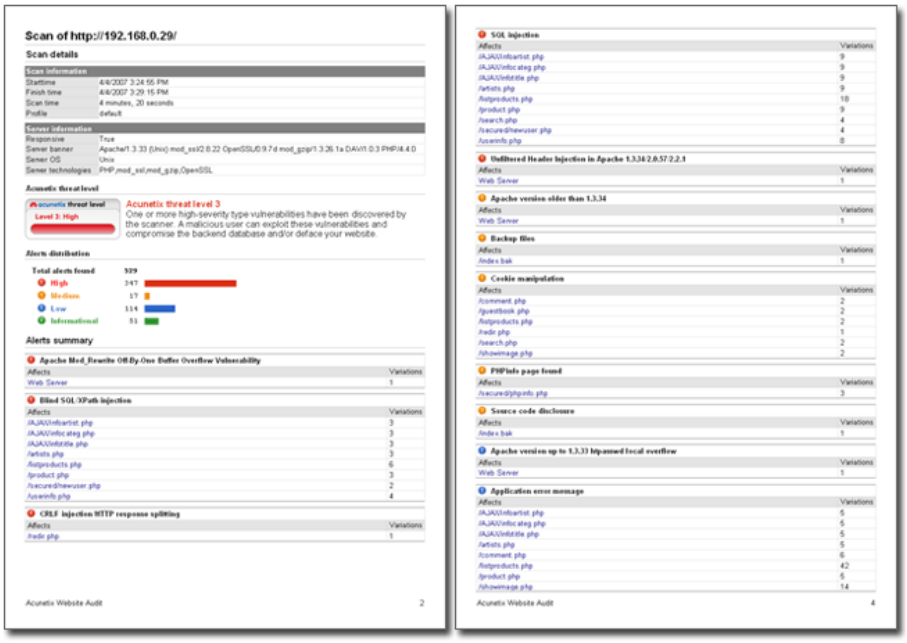
The Acunetix Web Vulnerability Scanner Scripting tool allows you to create new custom web vulnerability checks. These checks must be written in JavaScript and require installation of the SDK.

You can read more about writing custom web security checks from the following URL:
http://www.acunetix.com/blog/docs/creating-vulnerability-checks/

You can download the scripting SDK from:
http://www.acunetix.com/download/tools/Acunetix_SDK.zip

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 Acunetix Web Vulnerability Scanner allows customization of the generated report.



Screenshot 15 - Typical Report including Chart of alerts

New in Acunetix Web Vulnerability Scanner Version 8

- New test method: Manipulation of input parameters from URLs. More information at http://www.acunetix.com/blog/web-security-zone/web-vulnerabilities-path-fragments/
- Automatic IIS 7 rewrite rule interpretation
- Support for custom HTTP headers
- Imperva Web Application Firewall integration
- Detection of new vulnerability class: HTTP Parameter Pollution. More information at http://www.acunetix.com/blog/whitepaper-http-parameter-pollution/
- Support for multiple instances of Acunetix Web Vulnerability Scanner on the same workstation
- Web-based scheduler for easy access of scan results on any workstation, laptop, or smartphone
- Automatic custom 404 error page recognition and detection
- Scan Settings Templates

- Simplified Scan Wizard
- Smart memory management options
- Real-time Crawler status update
- Scan termination status included in report
- Web application coverage report, which shows the list of files detected during the scan at the end of the Developer Report.
- Log file retention settings

Acunetix Blog and Support Page

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 Web Vulnerability Scanner support page; http://www.acunetix.com/support.

Licensing Acunetix Web Vulnerability Scanner

Acunetix Web Vulnerability Scanner is available in 5 editions: Small Business, Enterprise, Enterprise x10 instances, Consultant and Consultant x10 instances. Ordering and pricing information can be found here:

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

Perpetual or Time Based Licenses

Acunetix Web Vulnerability Scanner Enterprise and Consultant editions are sold as a one-year or perpetual license. The 1-year license expires after 1 year from the date of activation. The perpetual license does not expire. 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.

Support and version upgrades are included in the price of the 1-year license.

Small Business Edition 1 Site/Server

The Small Business edition license allows you to install one copy of Acunetix Web Vulnerability Scanner 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 by the license agreement. Additional licenses are required for separate installs onto different workstations.

Enterprise Edition Unlimited Sites/Servers

The Enterprise edition license allows you to install one copy of Acunetix Web Vulnerability Scanner on one computer to 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 by the license agreement. Additional licenses are required for separate installs onto different workstations.

Enterprise Edition Unlimited Sites/Servers x10 instances

The ONLY difference between the Enterprise Edition and the Enterprise Edition x10 instances is that this edition of the Acunetix Web Vulnerability Scanner Enterprise allows you to run up to 10 instances of Acunetix Web Vulnerability Scanner on the same computer giving you the ability to scan up to 10 websites simultaneously.

Consultant Edition

The Consultant edition license allows you to install one copy of Acunetix on one computer to 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, hosting provider or 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. Additional licenses are required for separate installs onto different workstations.

Consultant Edition x10 instances

The ONLY difference between the Consultant Edition and the Consultant Edition x10 instances is that this edition of the Acunetix Web Vulnerability Scanner Consultant allows you to run up to 10 instances of Acunetix Web Vulnerability Scanner on the same computer giving you the ability to scan up to 10 websites simultaneously.

Limitations of Trial Version

The trial version of Acunetix Web Vulnerability Scanner – downloadable from the Acunetix website – is practically identical to the full version in functionality and features, but contains the following limitations:

- When scanning your website, all the Web Alerts will be reported. However you will not be able to drill down and find where the vulnerability is found in your website.
- Reports cannot be generated. Scan results will not be stored in the Reports database.
- Full scans (including detailed information on the vulnerabilities discovered) can be made against the following Acunetix test web sites:
    - http://testphp.vulnweb.com
    - http://testasp.vulnweb.com
    - http://testaspnet.vulnweb.com
- The Scan Scheduler is not available.
- The Vulnerability Editor Tool is not included in the trial version.

If you decide to purchase Acunetix Web Vulnerability Scanner, you will need to un-install the evaluation edition and install the purchased edition, which must be downloaded as a separate installer file. Download the installer file using the link provided by our sales team, and double-click to begin the setup. You will be prompted to remove the evaluation version and install the full edition. All settings from the previously installed version will be retained.

Once the installation is complete you will be prompted to enter the License key.

3. Installing Acunetix Web Vulnerability Scanner

Minimum System Requirements

- Operating system: Microsoft Windows XP and later
- CPU: 32 bit or 64 bit processor
- System memory: minimum of 2 GB RAM
- Storage: 200 MB of available hard-disk space
- Microsoft Internet Explorer 7 (or later) – some components of Internet Explorer are used by Acunetix
- Optional: Microsoft SQL Server – for the reporting database. By default a Microsoft Access database is used - Microsoft Access is not required

Installing Acunetix Web Vulnerability Scanner

1. Download the latest version of Acunetix Web Vulnerability Scanner from the download location provided to you when you purchased the license.
2. Double click the webvulnscan8.exe file to launch the Acunetix Web Vulnerability Scanner installation wizard and click **Next** when prompted.
3. Review and approve the License Agreement
4. Select the folder location where Acunetix Web Vulnerability Scanner will be installed.
5. Further install options – such as the Acunetix Firefox toolbar and desktop shortcut – can be enabled. The Acunetix Firefox toolbar can be used to instantly launch a security scan of the web page you are browsing.
6. Click Install to start the installation. Setup will now copy all files and install the Acunetix Web Vulnerability Scanner Scheduler service.
7. Click Finish when ready.

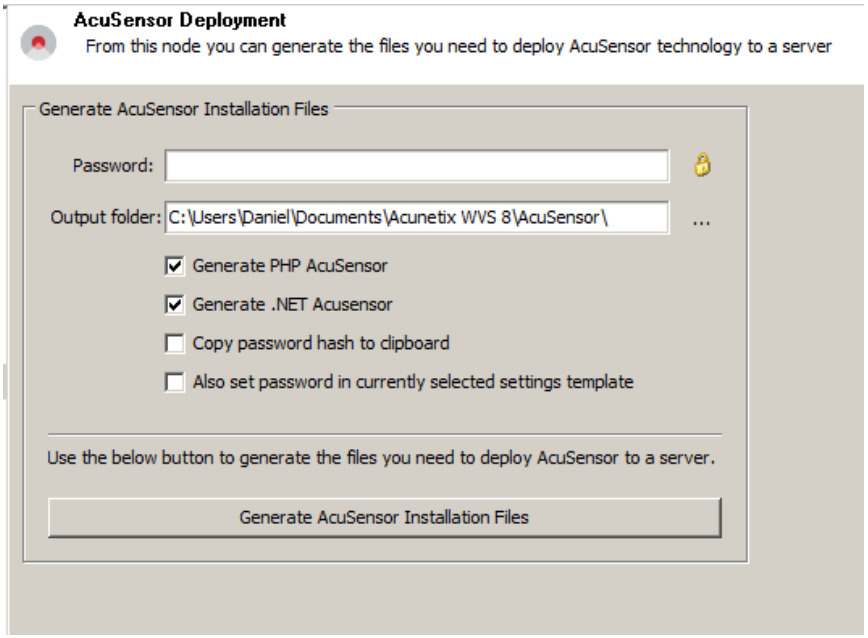
Installing the AcuSensor Agent

NOTE: Installing the AcuSensor Agent is optional. Acunetix Web Vulnerability Scanner still is best in class as a “black box” scanner but the AcuSensor Agent improves accuracy and vulnerability results.

The unique Acunetix AcuSensor Technology identifies more vulnerabilities than a black box Web Application Scanner while generating less false positives. In addition, it indicates exactly where vulnerabilities are detected in your code and also reports debug information

Acunetix AcuSensor requires an agent to be installed on your website. This agent is generated uniquely for your website for security reasons.

Generating the AcuSensor files

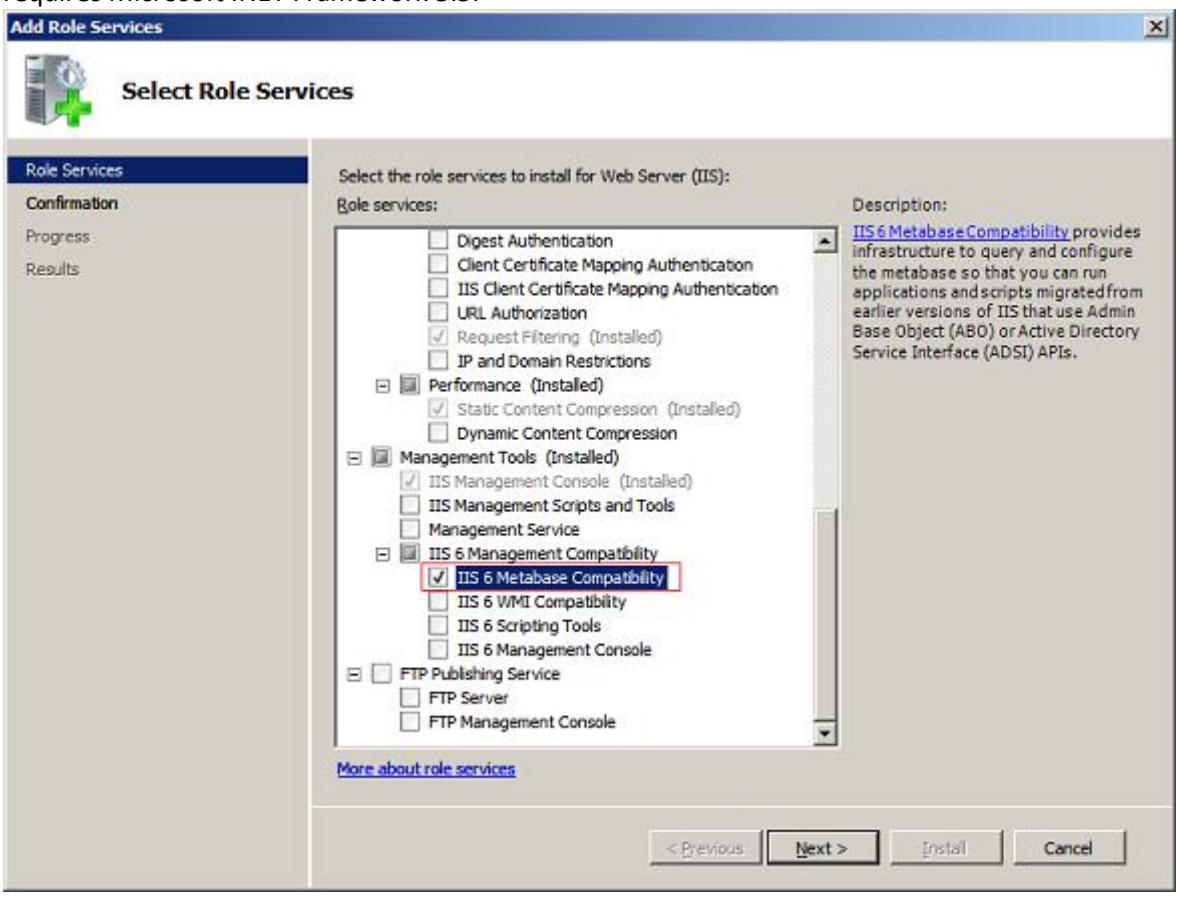


Screenshot 16 – AcuSensor Deployment settings node

1. Navigate to the 'Configuration > Application Settings' node in the Tools Explorer. Click on the 'AcuSensor Deployment' node.
2. Enter a password or click on the padlock icon to randomly generate a password unique to the AcuSensor file.
3. Specify the path where you want the AcuSensor files to be generated.
4. Select whether to generate files for a PHP website or a .NET website.
5. Select 'Also set password in currently selected settings template' to store the password specified in the scan settings template.
6. Click on **Generate AcuSensor Installation Files** to generate the files.
7. Depending on if you are using a ASP .NET or a PHP website, use one of the following procedures to install the AcuSensor files.

Installing the AcuSensor agent for ASP .NET Websites

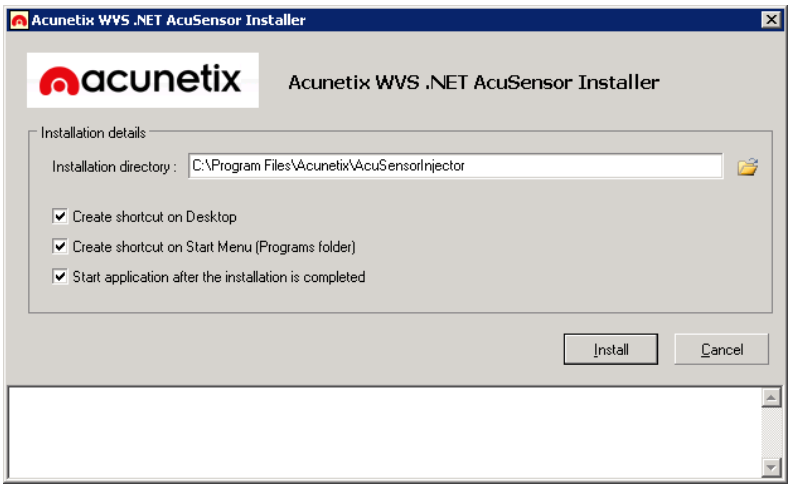
1. **Install Prerequisites on the server hosting the website:** The AcuSensor installer application requires Microsoft .NET Framework 3.5.



Screenshot 17 - Enable IIS 6 Metabase Compatibility on Windows 2008

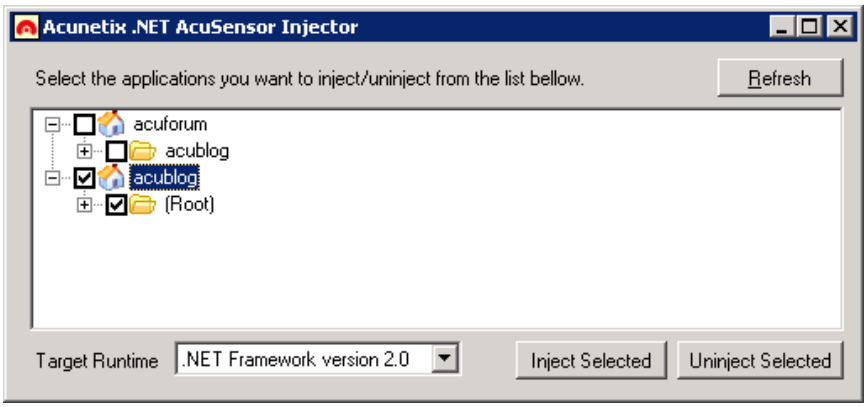
On Windows 2008, you must also install IIS 6 Metabase Compatibility from 'Control Panel > Turn Windows features On or Off > Roles > Web Server (IIS) > Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility' to enable listing of all .NET applications running on server.

2. Copy the AcuSensor installation files to the server hosting the .NET website.



Screenshot 18 – Acunetix .NET AcuSensor Agent installation

3. Double click **Setup.exe** to install the Acunetix .NET AcuSensor agent and specify the installation path. The application will start automatically once the installation is ready. If the application is not set to start automatically, click on **Acunetix .NET AcuSensor Technology Injector** from the program group menu.



Screenshot 19 – Acunetix .NET AcuSensor Technology Agent

4. On start-up, the Acunetix .NET AcuSensor Technology Installer 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. 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.

Note: The AcuSensor installer will try to automatically detect the .NET framework version used to develop the web application so you do not have to manually specify which framework version was used from the Target Runtime drop down menu.

Installing the AcuSensor agent for PHP websites

If your web application is written in PHP:

1. Locate the PHP AcuSensor file of the website you want to install AcuSensor on. Copy the **acu_phpaspect.php** file to the remote webserver hosting the web application. The AcuSensor agent file should be in a location where it can be accessed by the web server software. Acunetix AcuSensor Technology works on websites using PHP version 5 and up.
2. There are 2 methods to install the AcuSensor agent, one method can be used for Apache servers, and the other method can be used for both IIS and Apache servers.

Method 1: Apache .htaccess file

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: IIS and Apache php.ini

1. Locate the file 'php.ini' on the server by using *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.

Testing your AcuSensor Agent

To test if the AcuSensor agent is working properly on the target website, do the following:

1. In the **Tools Explorer**, Navigate to 'Configuration > Scan Settings' node and select the AcuSensor node.
2. Enter the password of the AcuSensor agent file which was copied to the target website.
3. Click **Test AcuSensor installation on a Specific URL**. A dialog will prompt you to submit the URL of the target website where the AcuSensor Agent file is installed. Enter the desired URL and click **OK**.

Changing the AcuSensor Password

If you need to change the password used by the AcuSensor agent on your website, you will need to re-generate the AcuSensor Files and re-install them on your website.

Perform the following if you are using a .NET website:

1. Use the procedure in the next section to Disable and Uninstall the AcuSensor agent.
2. Proceed with installing the AcuSensor with the new password.

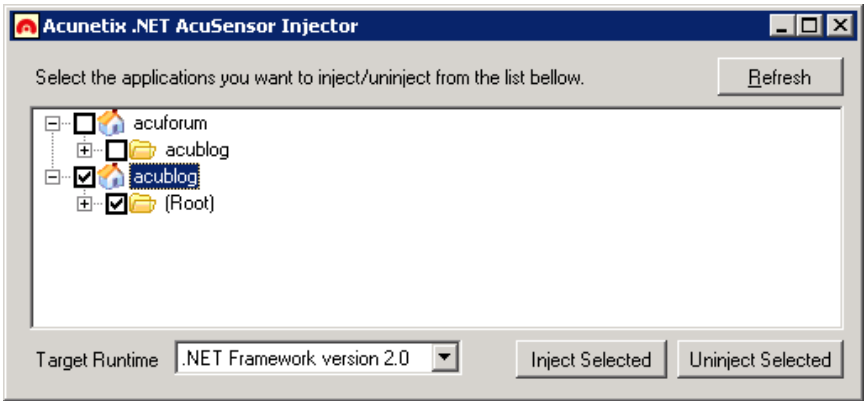
If you are using a PHP file, you will just need to overwrite the old **acu_phpaspect.php** with the one with the new **acu_phpaspect.php** file.

Disabling and uninstalling AcuSensor

To uninstall and disable the sensor:

AcuSensor for ASP .NET websites

1. Browse to the installation directory where the AcuSensor Agent had been installed
2. Open AcuSensorInjector.exe.



Screenshot 20 - Select website and click Uninject Selected

3. Select the website where the AcuSensor agent is installed and click on Uninject to remove the AcuSensor Agent form the site.
4. Close AcuSensorInjector.exe
5. From the same directory, double click uninstall.exe to uninstall the AcuSensor Agent files.

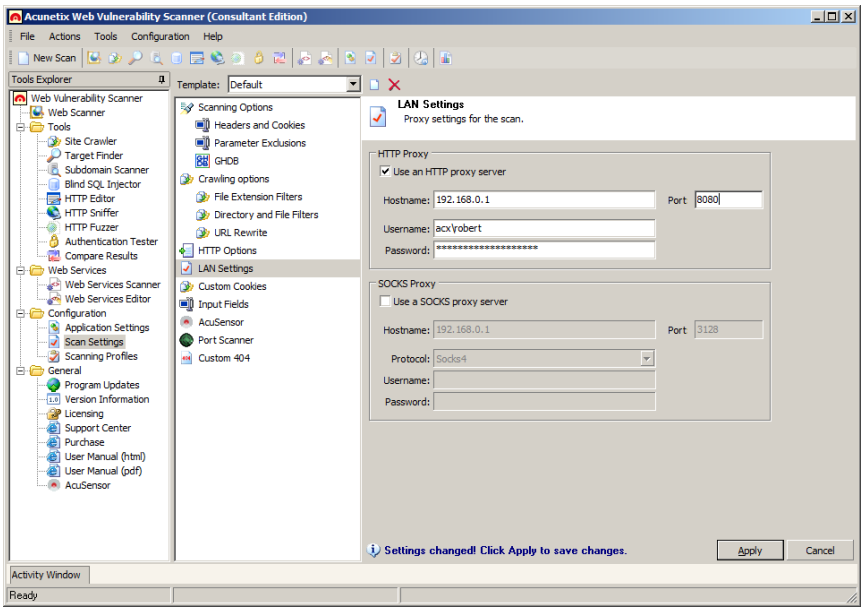
Note: If you uninstall the Acunetix .NET AcuSensor Technology Injector without un-injecting the .NET application, then the AcuSensor Technology code will not be removed from your .NET application.

AcuSensor for PHP

1. If using method 1 (.htaccess file), delete the directive: **php_value auto_prepend_file="[path to acu_phpaspect.php file]"** from the .htaccess file configuration
2. If using method 2, delete the directive: **auto_prepend_file="[path to acu_phpaspect.php file]"** from the php.ini file.
3. Delete the Acunetix AcuSensor PHP file: acu_phpaspect.php.

Note: Although the Acunetix AcuSensor agent requires authentication, uninstall / remove the AcuSensor client files if they are no longer in use.

Configuring an HTTP Proxy or SOCKS proxy Server



Screenshot 21 - LAN HTTP Proxy Settings

If your machine is located behind a proxy server, the Acunetix Proxy server settings must be configured for the scanner to connect to the target application.

Navigate to the Configuration > Scan 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 Web Vulnerability Scanner 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 Web Vulnerability Scanner to use a SOCKS proxy server.

Hostname and Port - Hostname (or IP address) and port number for the SOCKS proxy server.

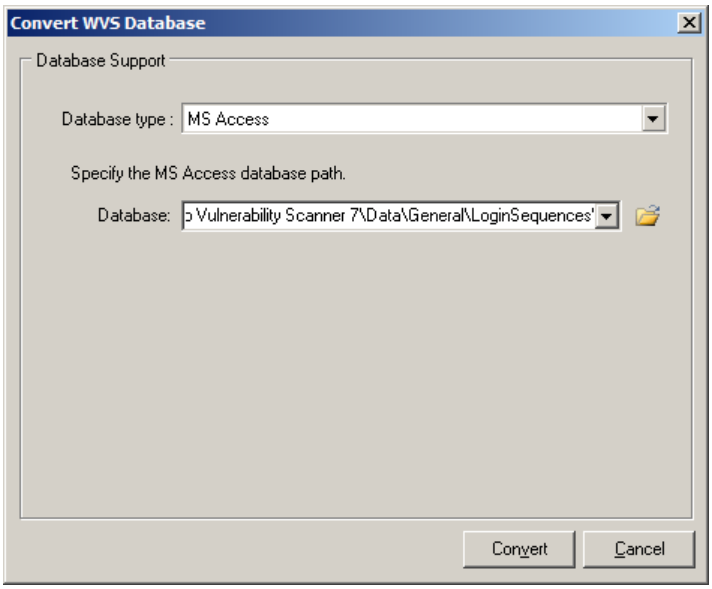
Protocol - Select which SOCKS protocol to use. Both Socks v4 or v5 protocols are supported by Acunetix Web Vulnerability Scanner.

Username and Password - The credentials used to access this proxy. If no authentication is required, leave these options empty.

Upgrading from Acunetix Web Vulnerability Scanner 7

Perform the following to upgrade from Acunetix Web Vulnerability Scanner version 7 to version 8:

1. Close Acunetix Web Vulnerability Scanner version 7 (and related utilities such as the Reporter)
2. Optionally backup the Login Sequences if you would like to use these in version 8. These can be copied from <C:\Program Files (x86)\Acunetix\Web Vulnerability Scanner 7\Data\General\LoginSequences'>
3. Optionally backup Reporting Database if you would like to use it in version 8. If you are using an Access Database, the default location of the database is < C:\Program Files (x86)\Acunetix\Web Vulnerability Scanner 7\Data\Database\vulnscanresults.mdb>
4. From the Acunetix Web Vulnerability Scanner 7 Program Group, select to uninstall the product.
5. Install the Acunetix Web Vulnerability Scanner version 8.
6. To restore the Login Sequences, copy the files backed up in (2) to <C:\Users\Public\Documents\Acunetix WVS 8\LoginSequences>
7. The Reporting database from version 7 needs to be updated before it can be used in version 8. This can be done using the Reporting Database Upgrade tool which can be downloaded from http://www.acunetix.com/download/tools/ConvertWVSDatabase.zip. Proceed as follows:
    a. If you are using an **SQL database**, select MS SQL Server, and specify the Server, credentials and Database which needs to be upgraded and click on the Convert button. Then configure Acunetix Web Vulnerability Scanner 8 to use the upgraded database.



Screenshot 22 - Upgrade Reporting Database

b. If you are using an **Access database**, select MS Access, and select the database backed up in (3), and click on the Convert button. Once ready, copy the upgraded database to <C:\ProgramData\Acunetix WVS 8\Data\Database\vulnscanresults.mdb>

4. Scanning a Website

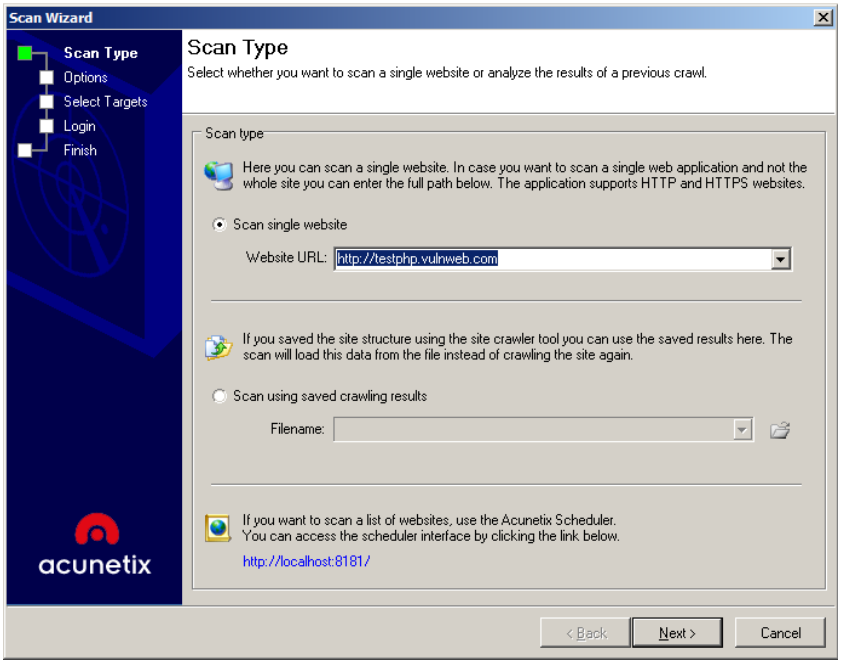
NOTE: DO NOT SCAN A WEBSITE WITHOUT PROPER AUTHORIZATION!

The web server logs will show your IP address and all the attacks made by Acunetix Web Vulnerability Scanner. 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.

To scan a website, you first need to perform the following steps:

Step 1: Select Target(s) to Scan

1. Click on File > New > New Website Scan to start the Scan Wizard, or click the **New Scan** button on the top left hand of the Acunetix Web Vulnerability Scanner menu bar.



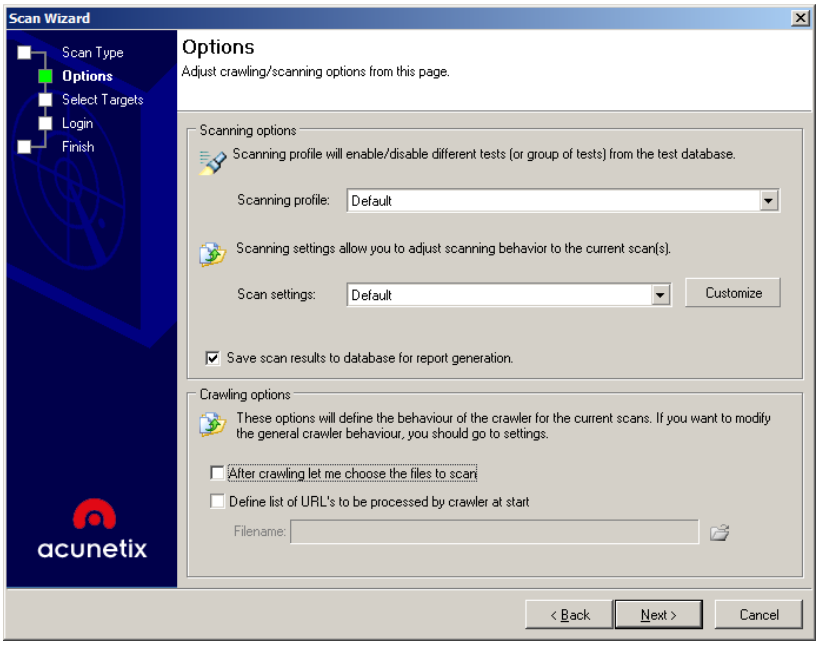
Screenshot 23 – Scan Wizard Select Scan Type

2. Specify the scan options:
   - Scan single website - Enter the URL of the target website, e.g. http://testphp.vulnweb.com.
   - Scan using saved crawling results - If you previously performed a crawl on a website, you can use the saved results to launch a scan instead of having to crawl the website again.

   Note: The **Acunetix Web Vulnerability Scanner Scheduler** can be used to scan multiple websites at the same time since it launches an instance of Acunetix Web Vulnerability Scanner per each simultaneous scan. You can read more about the Acunetix Web Vulnerability Scanner scheduler in page 69 of this manual.

3. Click **Next** to continue.

Step 2: Specify Scanning Profile, Scan Settings Template and Crawling Options



Screenshot 24 – Scanning Profile and Scan Settings template

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. The Default scanning profile will test your website for all known web vulnerabilities. Refer to the 'Scanning Profiles' section on page 78 for more information on how to customize or create scanning profiles.

Scan Settings template

The Scan Settings template will determine what Crawler and Scanner settings are to be used during a scan. Refer to the 'Scan Settings templates' section on page 78 for more information on how to customize or create new Scan Settings templates.

Save scan Results

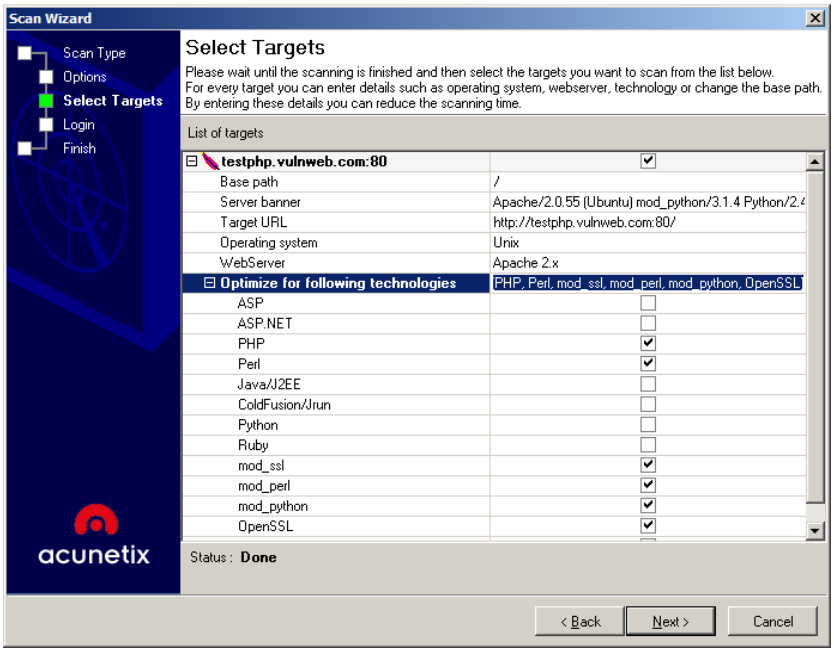
If you want to automatically save the scan results to the reporting database, enable the **Save scan results to the database for report generation** option. You can read more about the Acunetix Reporter in page 42 of this user manual.

Crawling Options

Tick the option **After crawling let me choose which files to scan** if you would like to select / deselect files from the automated website security scan, instead of scanning the whole website.

Tick the option **Define list of URLs to be processed by crawler at start** if you would like a specific URL to be crawled before any other (not available if using saved crawling results).

Step 3: Confirm Targets and Technologies Detected



Screenshot 25 – Scan Wizard Selecting Targets and Technologies

Acunetix Web Vulnerability Scanner will automatically fingerprint the target website for the server's operating system, the web server, its web server technologies, and custom 404 error page in use. If a custom 404 error-page is being used, Acunetix Web Vulnerability Scanner will automatically detect it and determine a pattern for it, removing the need for manual configuration. For more details on Custom 404 Error Pages refer to page 82 of this manual.

The web vulnerability scanner will reduce the scan time by scanning only for the selected web technologies. E.g. Acunetix Web Vulnerability Scanner will not launch IIS security checks against a Linux system running an Apache web server.

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.

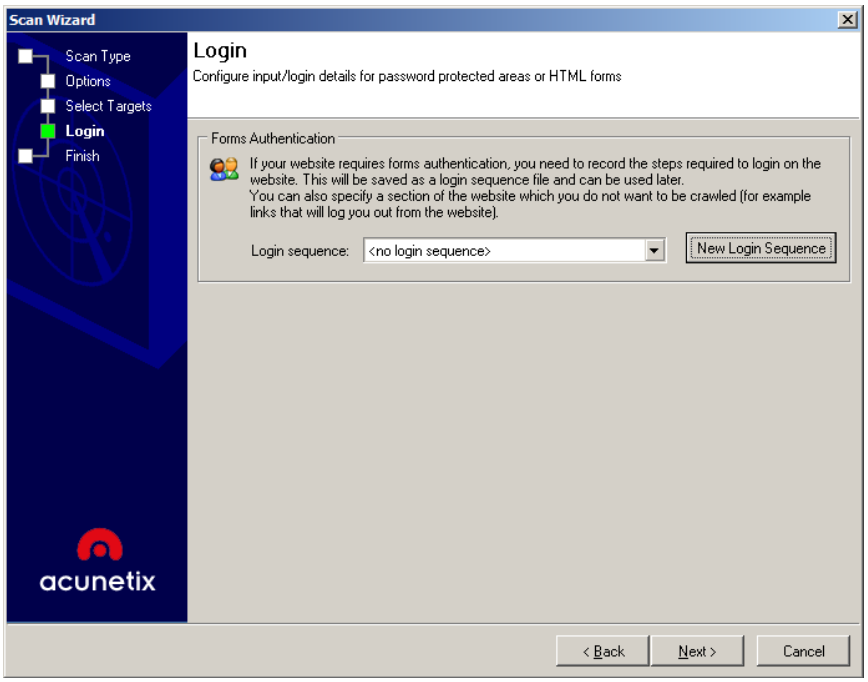
Note: if a specific web technology is not listed under **Optimize for the following technologies**, it does not mean that it is unsupported by Web Vulnerability Scanner, but that there are no vulnerability tests exclusive to that technology.

Step 4: Configure Login for Password Protected Areas

Two types of Login mechanisms are commonly used on the web:

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 and not via HTTP. The credentials are sent to the server for validation by a custom script.

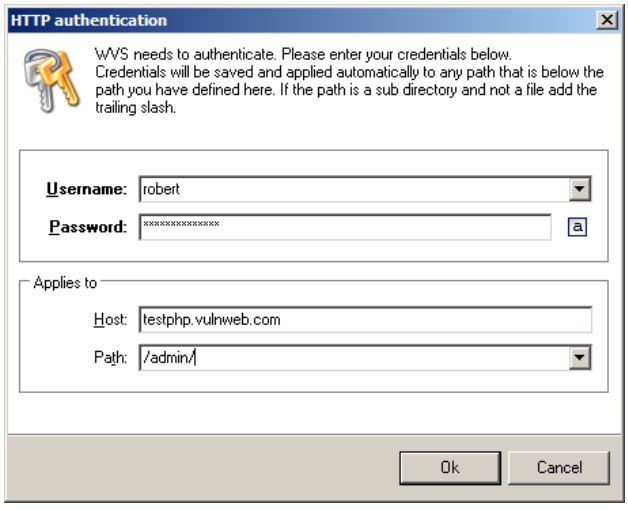


Screenshot 26 - Login Details Options

Scanning a HTTP password protected area:

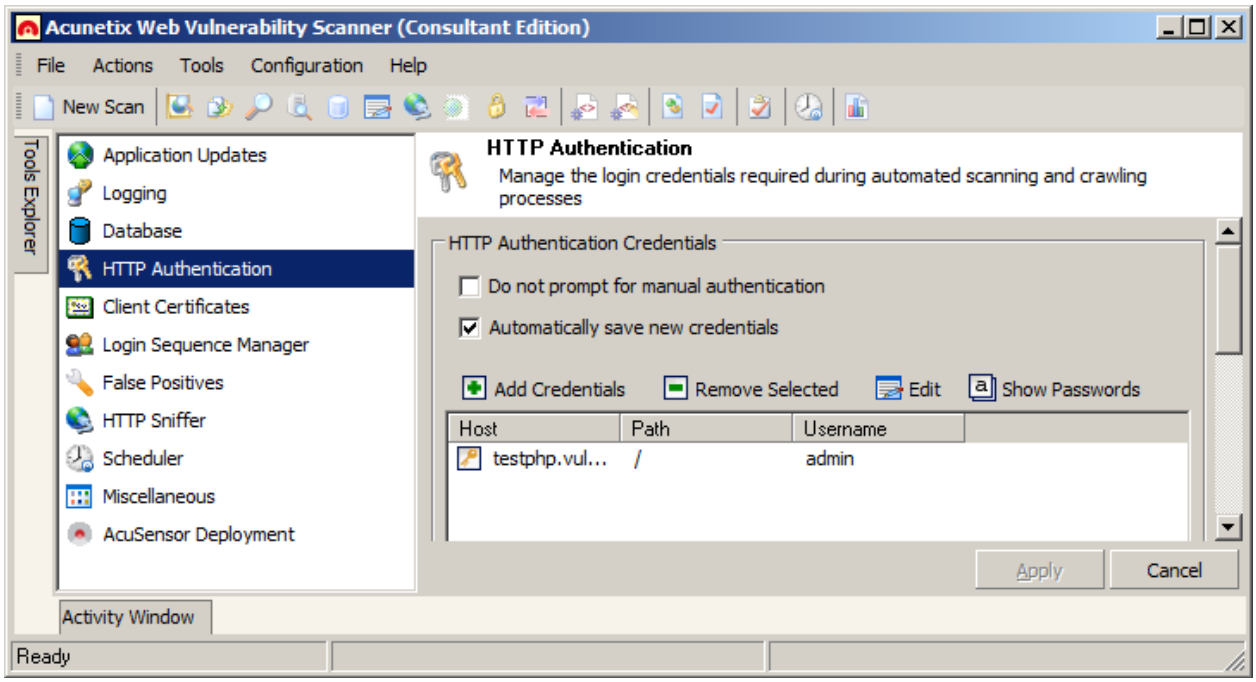
If you scan an HTTP password protected website, you will be automatically prompted to specify the username and password, unless they are predefined. Acunetix Web Vulnerability Scanner supports multiple sets of HTTP credential for the same target website. HTTP authentication credentials can be configured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

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



Screenshot 27 – 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 used site wide.



Screenshot 28 - HTTP Authentication Options

Do not prompt for manual authentication– By default, when a target website requires HTTP authentication during a crawl and scan, Acunetix Web Vulnerability Scanner will ask you for the credentials. If this option is switched off, Acunetix Web Vulnerability Scanner will continue scanning the website without authenticating, therefore protected website parts will not be crawled and scanned.

Automatically save new credentials – When this option is enabled, new credentials (and the URL) specified during a scan are automatically saved in the Acunetix Web Vulnerability Scanner HTTP Authentication settings, and will be automatically used when the same site is scanned.

Step 5: Scanning a Form Based Password Protected Area

In order to scan a form based password protected area, you will need to make use of a Login Sequence during the scan. You can pre-define login sequences from the Configuration > Application Settings > Login Sequence Manager, or directly from the New Scan Wizard.

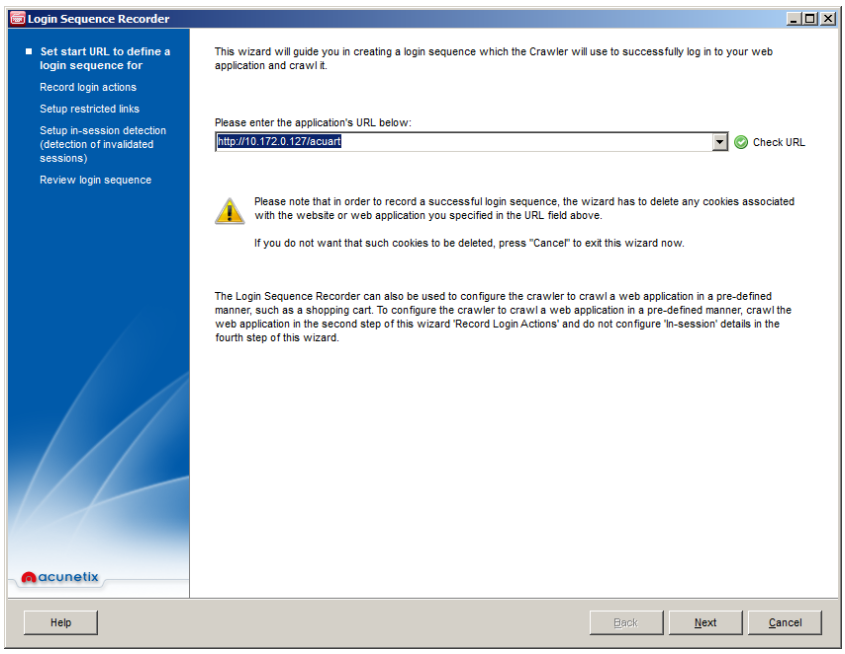
The Login Sequence Recorder can be used to perform a number of tasks during a crawl and a scan:

- To configure Acunetix Web Vulnerability Scanner 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.

The Login Sequence Recorder can also be used to configure Acunetix Web Vulnerability Scanner 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, refer to http://www.acunetix.com/blog/docs/acunetix-wvs-login-sequence-recorder/.

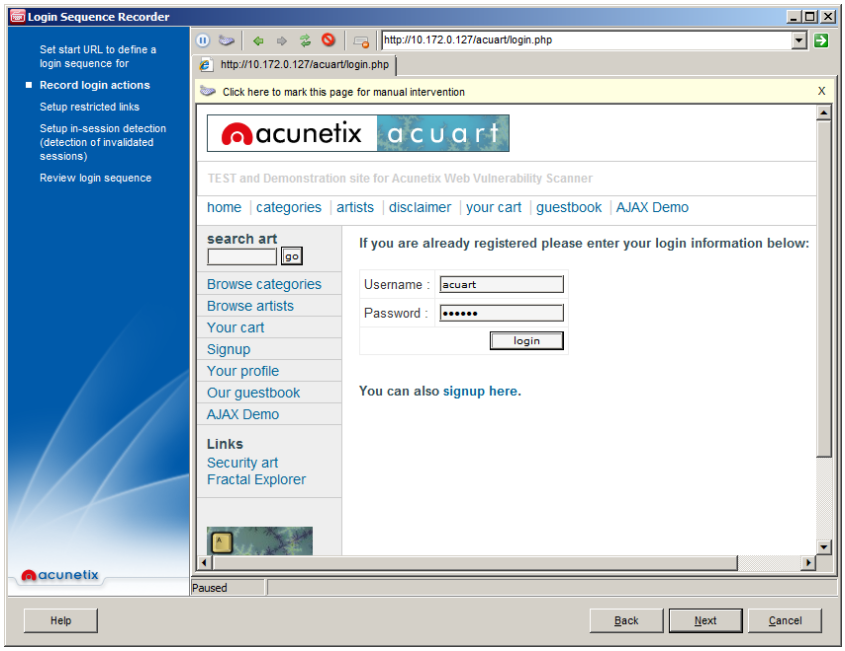
Proceed as follows to create a new login sequence

1. Click **New Login Sequence** to launch the Login Sequence Recorder



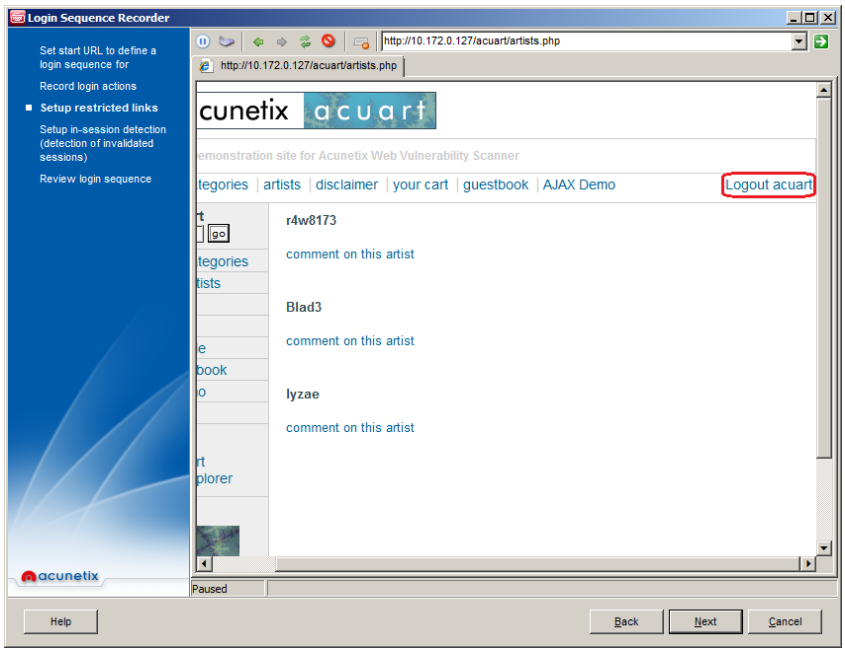
Screenshot 29 – Login Sequence Wizard

2. 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



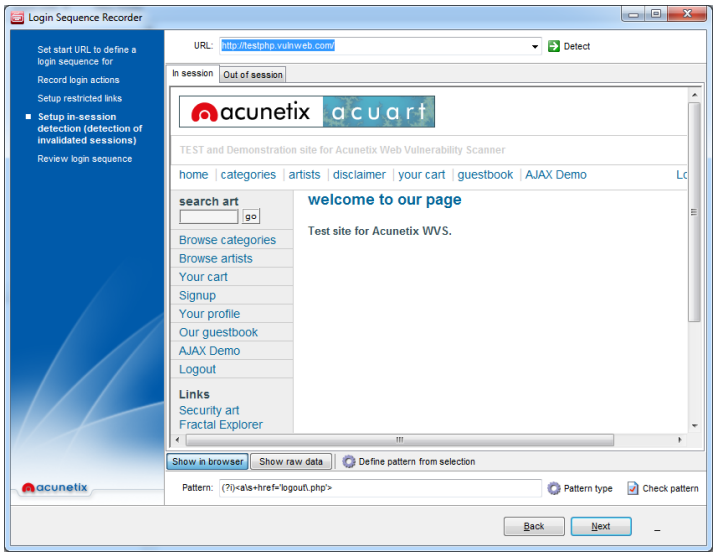
Screenshot 30 – Login Sequence Recorder

3. On the second page of the wizard, browse to the website's login page and submit the authentication credentials in the login form to log in. Wait for the page to fully load, indicating that you are logged in. Click **Next** to proceed.



Screenshot 31 – Specify an excluded link

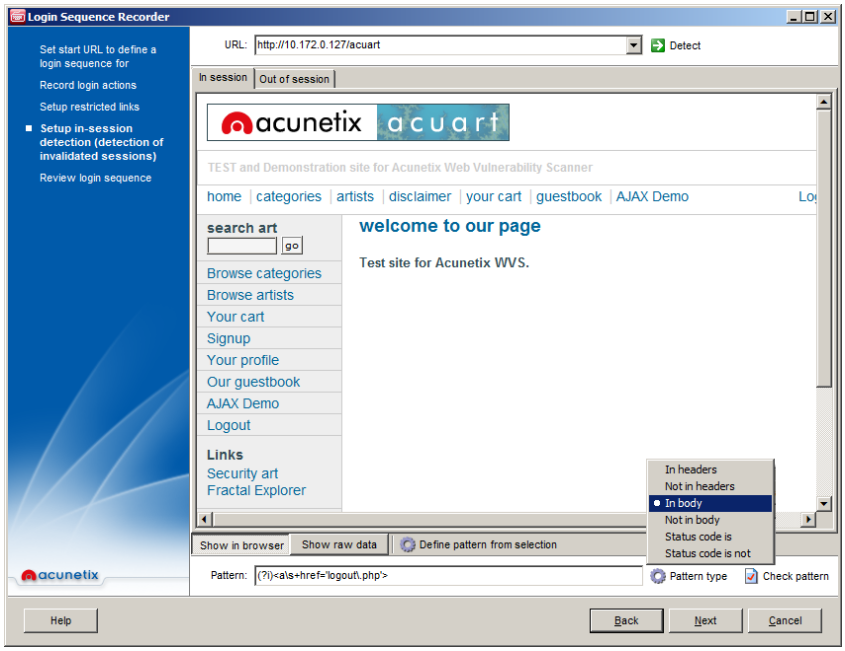
4. Once logged in, you also need to identify the logout link so the crawler will ignore it to prevent ending the session. In the 'Setup restricted links' step of the wizard, click the logout link for it to be ignored. If the logout link is not on the same page, click the **Pause** button in the top menu, navigate to a page where the logout link is found, resume the session and then click on the logout link. Click **Next** to proceed.



Screenshot 32 – Specify an 'In session' or 'Out of session' pattern

5. In this step, you have to specify **In Session** or **Out of Session** detection patterns. For the **In Session detection,** specify a pattern which allows the crawler to detect the session is still valid. If for some reason the session expires during a crawl, the Crawler will automatically log in again. Click on **Detect** to make Acunetix Web Vulnerability Scanner attempt to automatically detect the pattern.

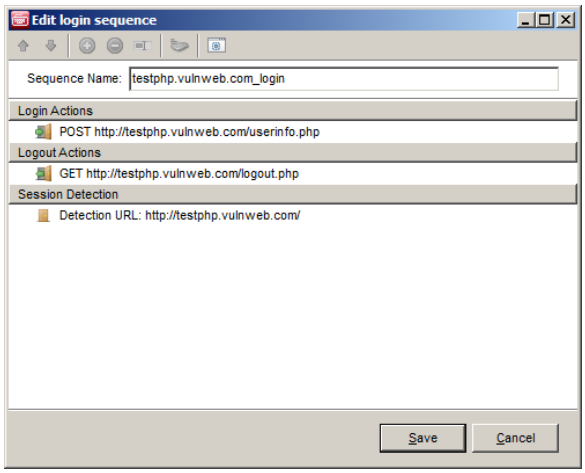
6. There are situations where the session state cannot be detected automatically, in which case, you will need to specify this manually. The pattern can be plain text or a regular expression, e.g. (?!)<a\s+href='logout\.php'>. You can also highlight specific content and click on **Define pattern from selection** and a regular expression will be automatically generated.



Screenshot 33 – Specify an 'In session' or 'Out of session' pattern - Drop down menu

You also have to specify where the pattern can be found in the response. From the **Pattern Type** drop down menu select if the pattern is **In headers**, **Not in headers**, **In body**, **Not in body**, **Status code is** and **Status code is not**.

7. 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.



Screenshot 34 – Recorded login sequence review

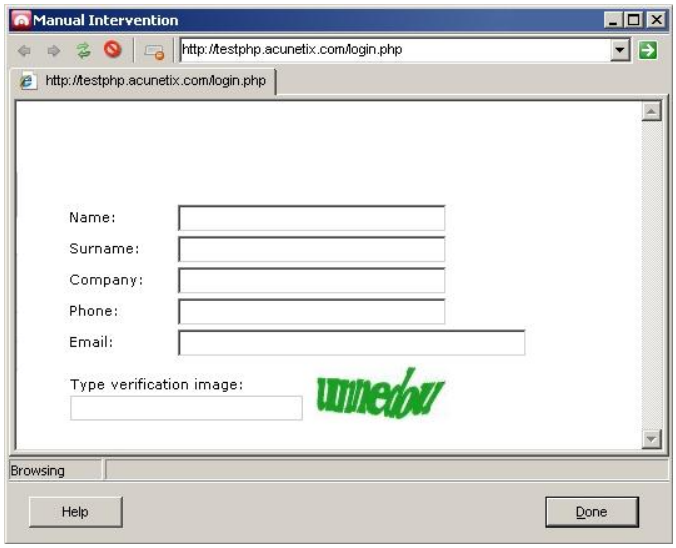
8. Review the recorded sequence. You can change priority of URL's using the up and down arrows, edit requests and add or remove requests. Click 'Finish' to finalize the session recording.

Note: Login sequences are saved in the Documents folder of the Public profile. The default path is <C:\Users\Public\Documents\Acunetix WVS 8\LoginSequences>.

Marking Pages for Manual Intervention (used for Captchas)

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:

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.



Screenshot 35 – Manual browser window

3. Once the page is loaded, click on  **Manual Intervention** button. Proceed by clicking the **Next** button till the end of the wizard.

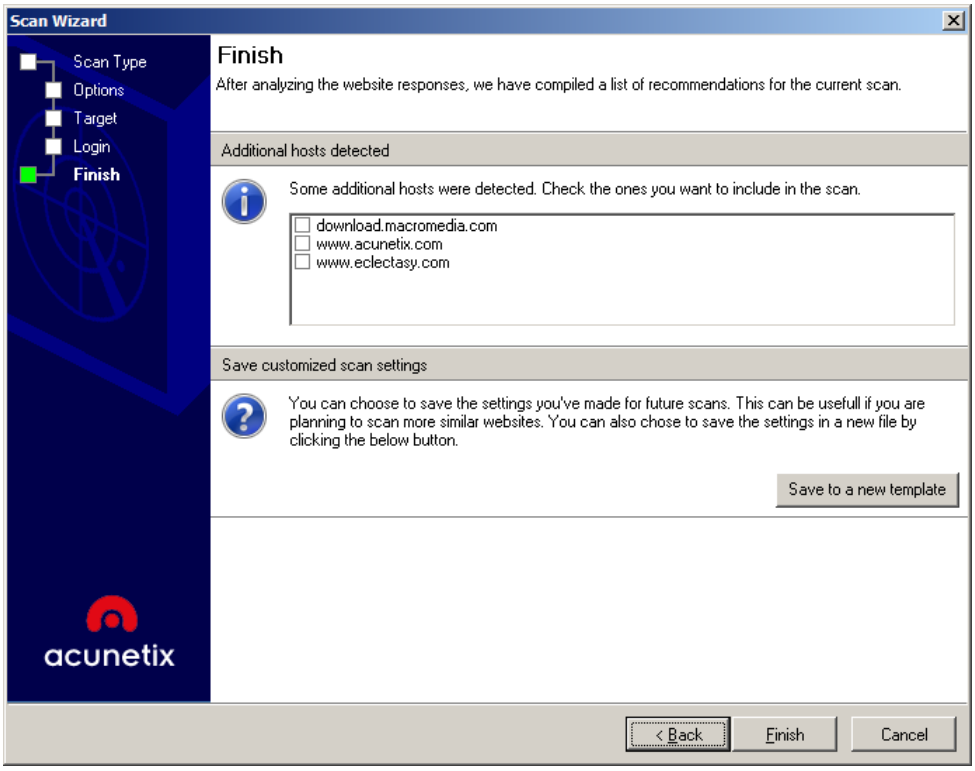
Once a scan is launched, a browser window will automatically pop up when the application page is reached. You can now perform the required action. Click **Done** once the action is complete.

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 appears during the crawl and perform the action on those pages as well. This allows the crawler to automatically process those pages without you having to wait for another dialog to appear.

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/

Step 6: Finalize Scan Options



Screenshot 36 - Finalize Scan Options

Before the Scan is started, the Scan Wizard will show if any further actions are required. The following is a list of actions which you might be presented:

- If an error is encountered while connecting to the target server, the error will be shown.
- If Acunetix Web Vulnerability Scanner is unable to automatically detect a custom 404 error page pattern, you will have to configure a custom 404 error page rule by clicking the **Customize** button. You can read more about Custom 404 error pages at page 82 of the manual.

- If the target server is using CASE insensitive URLs, you must force case insensitive crawling. This can be done from Configuration > Scan Settings > Crawling Options > Ignore CASE differences in paths.
- If AcuSensor Technology is enabled and the target server is PHP or .NET, you must install the agent. Click the **Customize** button to install AcuSensor on the target server. You can read more about AcuSensor on page 18 of this manual.
- If additional hosts have been found to be linked to from the web site being scanned, you can optionally select to scan these too.
- If you have made changes to the Scan Settings template, you can also save the modifications to the existing or new template. Refer to page 78 of this user manual to read more about the Scan Settings templates.

Step 7: Completing the scan

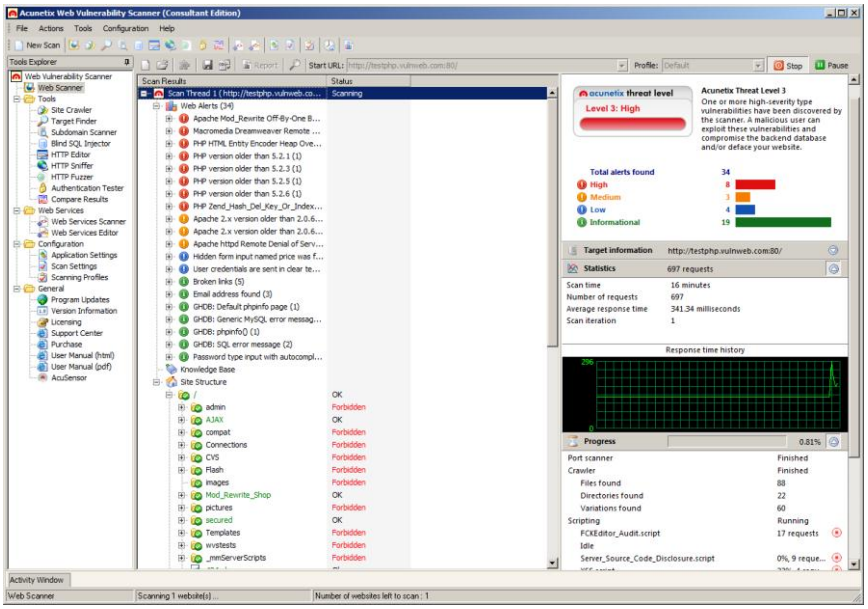
Click on **Finish** to start the automated scan. If the option **After crawling let me choose the files to scan** was selected in the crawling options, you will be asked to select the files to scan after Acunetix Web Vulnerability Scanner has finished crawling the site.

Depending on the size of the website, scanning profile selected, and the server response time, a scan may take up to several hours.

5. Analyzing the Scan Results

Introduction

The vulnerabilities discovered during the scan of a website are displayed in real-time in the Alerts node in the **Scan Results** window. A 'Site Structure' node is also shown listing the files and folders discovered.



Screenshot 37 - Scan Result and Information window

Web Alerts

The Web Alerts node displays all vulnerabilities found on the target website. Web Alerts are categorized according to 4 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 misconfiguration and site-coding flaws, which facilitate server disruption and intrusion.
Severity LOW	**Low Risk Alert Level 1** – Vulnerabilities derived from lack of encryption of data traffic, or directory path disclosures.
Severity INFO	**Informational Alert** – Sites which are susceptible to revealing information through Google hacking search strings, or email address disclosure.

If a vulnerability is detected by the 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 vulnerable to the discovered vulnerability.

The impact of this vulnerability – Level of impact on the website or web server if this 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 exploited input variable and the string it was set to will be displayed. You can also find the HTTP request sent to the web server and the response sent back by the web server (including the HTML response). The attack can be inspected and re-launched manually by clicking **Launch the attack with HTTP Editor**. For more information, please refer to the HTTP Editor chapter on page **Error! Bookmark not defined.**.

How to fix this vulnerability - How to fix the vulnerability.

Detailed information - Information about the reported vulnerability.

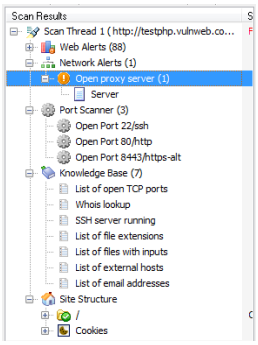
Web references - A list of web links providing more information on the vulnerability to help you understand and fix it.

Marking an Alert as a False Positive

If you are certain that the vulnerability discovered is a false positive, you can flag the alert as a False Positive to avoid it being reported in subsequent scans of the same website. To do this, click on the **Mark alert as false positive** link or right click on the alert and select the menu option.

You can remove an alert from the false positives list by navigating to the 'Configuration > Application Settings' node in the Tools Explorer and select the 'False Positives' node.

Network Alerts



Screenshot 38 - Network, Port Scanner and Knowledge base nodes

The Network Alerts node displays network level vulnerabilities discovered in scanned network services, such as DNS, FTP, SMTP and SSH servers. Network alerts are categorized by 4 severity levels (similar to web alerts). The number of vulnerabilities detected is displayed in brackets () next to the alert categories. Click an alert category node to view more information (similar to web alerts).

Note: You can disable network security checks by un-ticking the **Enable Port Scanning** option in the Scan Wizard. Network Security Checks are only performed on open ports detected during the scan, thus disabling port scanning will effectively disable all the network security checks.

Port Scanner

The Port Scanner node displays all the discovered open ports on the server. Network service banners can be viewed by clicking on an open port.

Note: Port Scanning of the target server can be disabled by un-ticking the **Enable Port Scanning** option in the Scan Wizard.

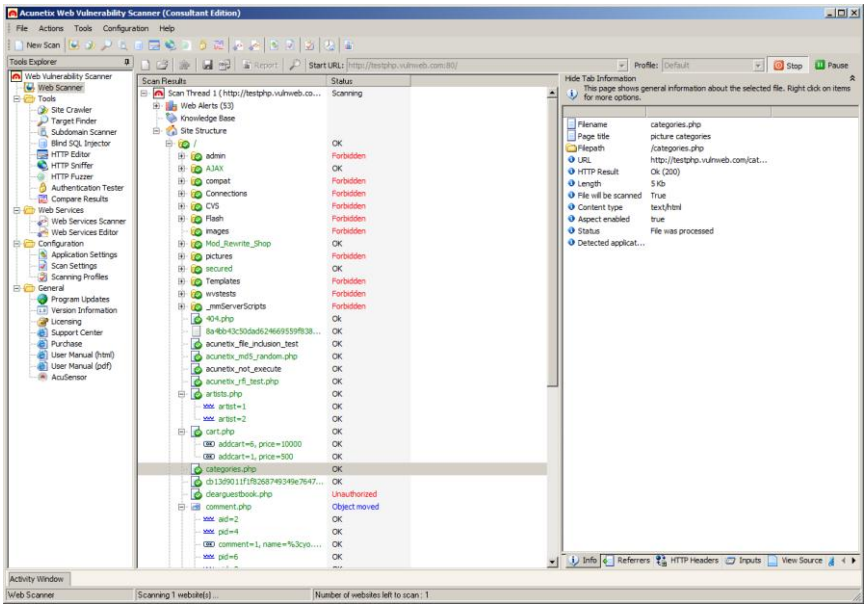
Knowledge Base

The knowledge base node is a high level report that displays:

- 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. Number of inputs per file are also shown.
- List of links to external hosts found on the website. E.g. testphp.vulnweb.com contains a link to www.acunetix.com.
- List of Client and Server HTTP error responses together with the HTTP requests that generated them. An example would be the response code Server Internal Error – HTTP 500. Check the response for information exposure.

Site Structure

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



Screenshot 39 - Scan Result and Information window

In the Crawler results (Site Structure node), color-codes are used to show different file statuses. The filename color coding is as follows;

Green – These files will be tested with AcuSensor Technology, resulting in more advanced security checks and less false positive alerts. From the AcuSensor data tab, the user can see what data related to these files is being returned by the AcuSensor. Such information is useful to know what SQL queries were executed or if the selected file is using functions which are monitored by AcuSensor.

Blue – File was detected during a vulnerability test, and not by the crawler. Most probably such files are not linked from anywhere on the target website.

Black – Files discovered by the crawler.

For every discovered item, more detailed information is available in the information pane on the right-hand side:

Info - Generic information such as file name, page title, path, length, URL etc.

Referrers – The files or pages that linked to the tested file.

HTTP Headers - The HTTP headers of the request sent to the web server to retrieve the selected file, and the HTTP response headers received.

Inputs – Possible input parameters and values for the file.

View Source - The source HTML of the page.

View Page - The page is displayed as it is shown in a web browser. Most client side scripts are disabled in this tab for security purposes to avoid launching vulnerabilities against the computer on which Acunetix Web Vulnerability Scanner is running.

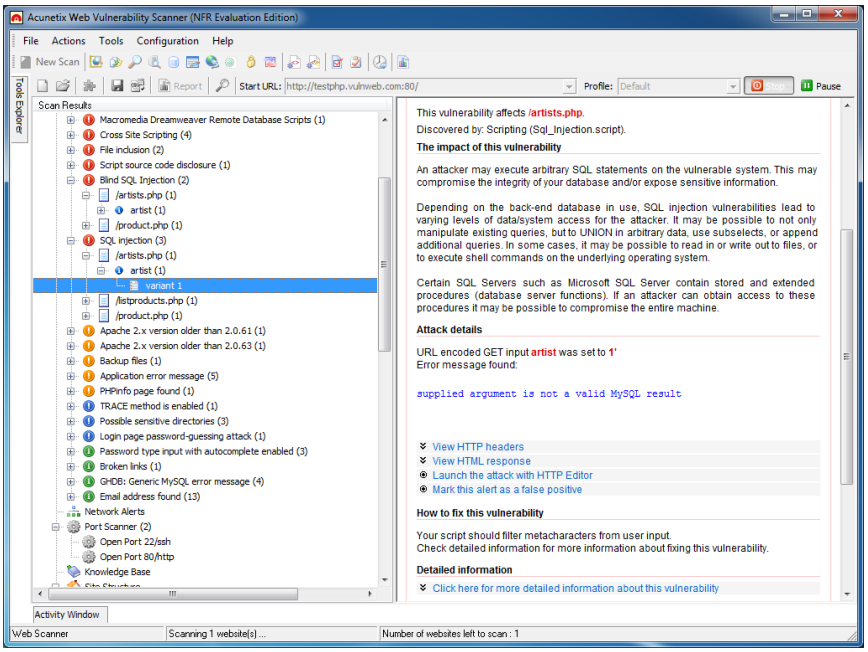
HTML Structure Analysis - HTML structure information such as

- A list of links discovered in the file.
- Comments discovered in the selected page. The information contained in the comments cannot be automatically analyzed but may reveal interesting information about the construction and coding of the website.
- Any client side scripts (JavaScript, VBScript etc.) and their source code discovered in the selected page. The client web browser will execute these scripts. Such information might reveal information about the logic of the web application.
- Any forms discovered in the selected object are shown in the top window. A list of parameters and their possible values are shown in the middle and bottom window.
- 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 – Any AcuSensor Technology data returned.

Alerts –A list of alerts for the selected file.

Grouping of Vulnerabilities



Screenshot 40 – Grouping of vulnerabilities

If the same vulnerability is detected on multiple pages, the scanner will group them under one alert node. Expanding the alert node will reveal all the vulnerable pages. Expand further to view the vulnerable parameters for the selected page.

Saving a Scan Result

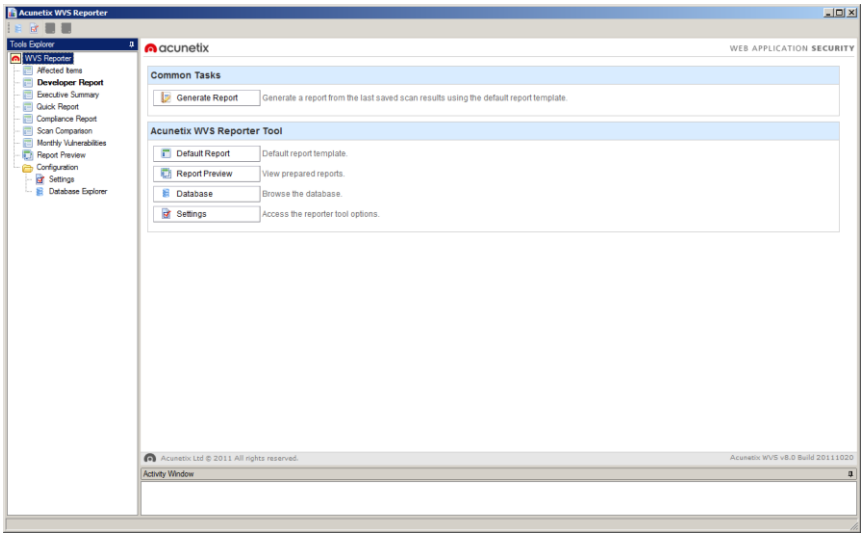
When a scan is completed you can save the scan results to an external file for analysis and comparison at a later stage. The saved file will contain all the scans from the current session including alert information and site structure.

To save the scan results click the **File** menu and select **Save Scan Results**.

To load the scan results click the **File** menu and select **Load Scan Results**.

6. Generating a Report from the results

Introduction to the Reporter

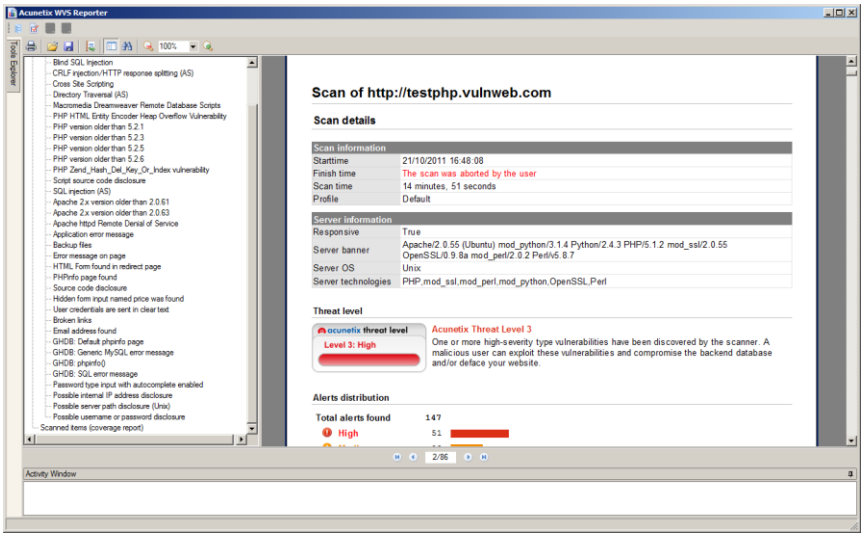


Screenshot 41 – The Reporter Application

The Acunetix Web Vulnerability Scanner Reporter is a standalone application that allows you to generate reports for the security scans performed using Acunetix Web Vulnerability Scanner. The Reporter can be launched after completing a scan, or from Acunetix Web Vulnerability Scanner program group, and can be used to generate various types of reports including developer reports, executive reports, compliance standard reports or a report that compare the results of two scans.

Generating a Report from the Scan Results

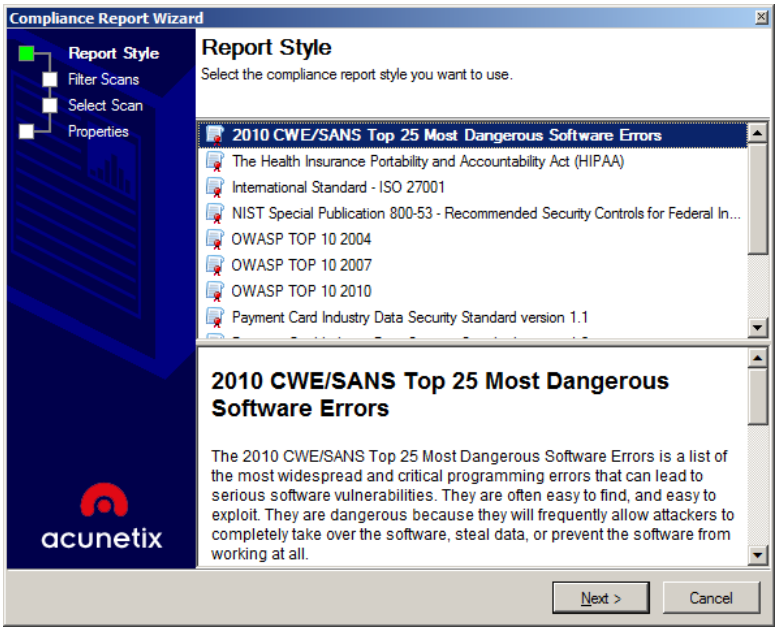
There are two ways to generate a report. After scanning a site, click on the **Report** button on the Acunetix toolbar. This will start the Acunetix Web Vulnerability Scanner Reporter and will load the Default Report for the scan. The Default Report used can be selected from the Reporter Settings.



Screenshot 42 – Sample Report

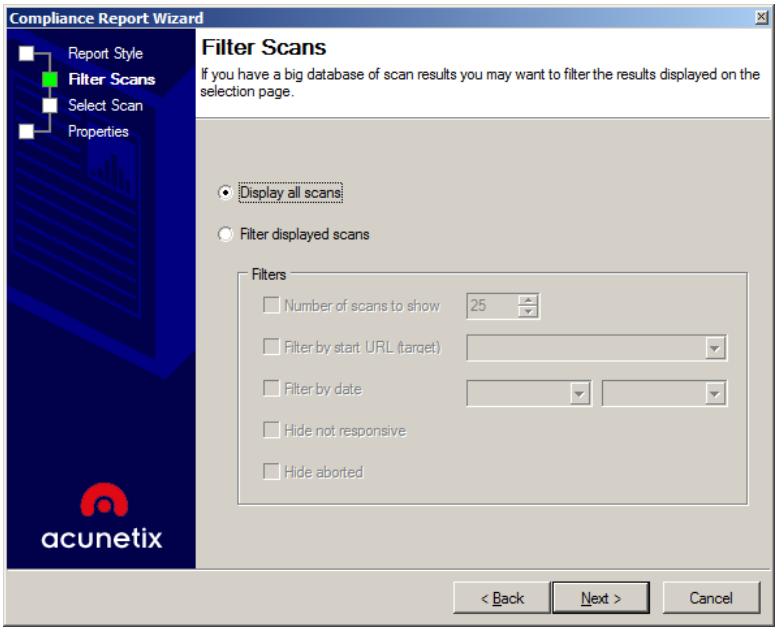
The second method is to load the Acunetix Web Vulnerability Scanner Reporter from the Acunetix Web Vulnerability Scanner Program Group. This will allow you to report on the scans that have been saved to the Reports database.

1. From the Reports list, select the type of report and click on 'Report Wizard'.
2. In the case of Compliance Report, select the Regulatory body or Standard to be used in the report. Click 'Next'.



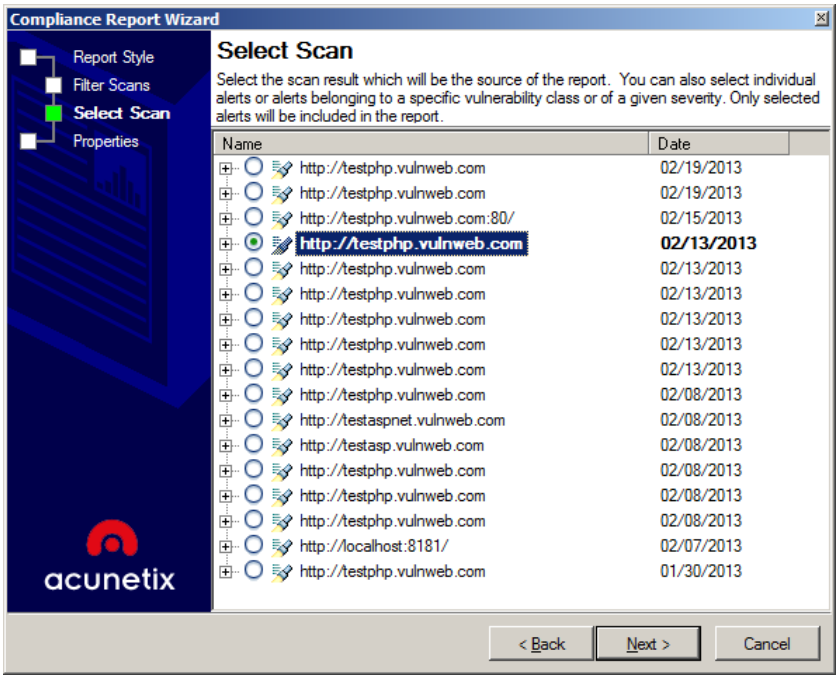
Screenshot 43 - Select Compliance Report

3. You can then select to show the results of all the scans stored in the reports database or to filter the scans that are displayed based on specific scan criteria. Click 'Next'.



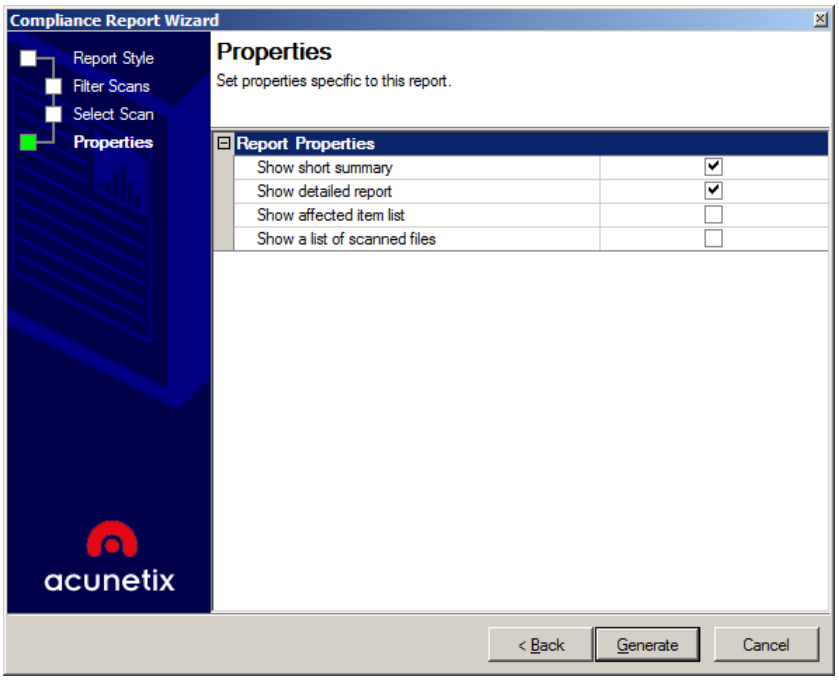
Screenshot 44 - Filter Scans

4. Select the scan that you would like to report on.



Screenshot 45 - Select Scan

5. Select what properties and details the report should include. The Report Properties will vary depending on the type of report that you are generating.



Screenshot 46 - Select Report Properties

6. Click the 'Generate' button to generate the report.
7. Once the report is generated, it can be printed or exported to various formats including PDF, Word and HTML.

Types of Reports

The following is a list of the reports that can be generated using the Acunetix Web Vulnerability Scanner Reporter:

Affected Items Report

The Affected Items report shows the files and locations where vulnerabilities have been detected during a scan. The report shows the severity of the vulnerability detected, together with other details about how the vulnerability has been detected.

Developer Report

The Developer Report is targeted to developers who need to work on the website in order to address the vulnerabilities discovered by Acunetix Web Vulnerability Scanner. The report provides information on the files which have a long response time, a list of external links, email addresses, client scripts and external hosts, together with remediation examples and best practice recommendations for fixing the vulnerabilities.

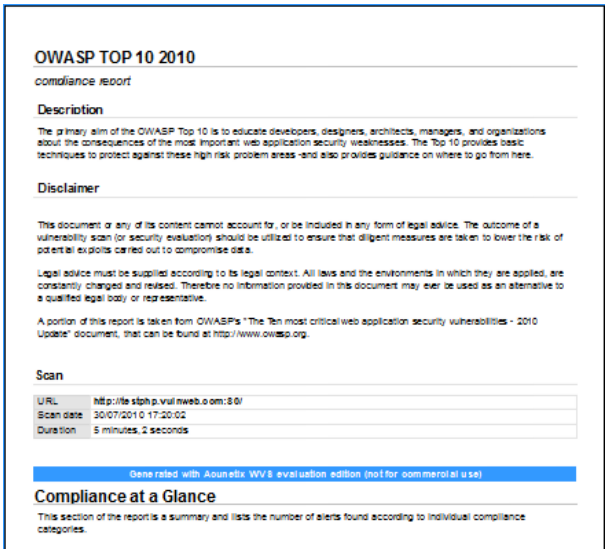
Executive Report

The Executive Report summarizes the vulnerabilities detected in a website and gives a clear overview of the severity level of the website.

Quick Report

The Quick Report provides a detailed listing of all the vulnerabilities discovered during the scan.

Compliance Reports


OWASP TOP 10 2010

compliance report

Description

The primary aim of the OWASP Top 10 is to educate developers, designers, 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 diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

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

A portion of this report is taken from OWASP's "The Ten most critical web application security vulnerabilities - 2010 Update" document, that can be found at http://www.owasp.org.

Scan

URL	http://testphp.vulnweb.com:80/
Scan date	30/07/2010 17:20:02
Duration	5 minutes, 2 seconds

Generated with Acunetix WVS evaluation edition (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.

Screenshot 47 – Compliance Report

Compliance Reports are available for the following compliance bodies and standards:

CWE / SANS – Top 25 Most Dangerous Software Errors

This report shows a list of vulnerabilities that have been detected in your website which are listed in the CWE / SANS top 25 most dangerous software errors. These errors are often easy to find and exploit and are dangerous because they will often allow attackers to take over the website or steal data. More information can be found at http://cwe.mitre.org/top25/.

The Health Insurance Portability and Accountability Act (HIPAA)

Part of the HIPAA Act defines the policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information. This report identifies the vulnerabilities that

might be infringing these policies. The vulnerabilities are grouped by the sections as defined in the HIPAA Act.

International Standard – ISO 27001

ISO 27001, part of the ISO / IEC 27000 family of standards, formally specifies a management system that is intended to bring information security under explicit management control. This report identifies vulnerabilities which might be in violation of the standard and groups the vulnerabilities by the sections defined in the standard.

NIST Special Publication 800-53

NIST Special Publication 800-53 covers the recommended security controls for the Federal Information Systems and Organizations. Once again, the vulnerabilities identified during a scan are grouped by the categories as defined in the publication.

OWASP Top10

The Open Web Application Security Project (OWASP) is web security project led by an international community of corporations, educational institutions and security researchers. OWASP is renown for its work in web security, specifically through its list of top 10 web security risks to avoid. This report shows which of the detected vulnerabilities are found on the OWASP top 10 vulnerabilities.

Payment Card Industry (PCI) standards

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard, which applies to organizations that handle credit card holder information. This report identifies vulnerabilities which might breach parts of the standard and groups the vulnerabilities by the requirement that has been violated.

Sarbanes Oxley Act of 2002

The Sarbanes Oxley Act was enacted in 2002 to prevent fraudulent financial activities by corporations and top management. Vulnerabilities which are detected during a scan which might lead to a breach in sections of the Act are listed in this report

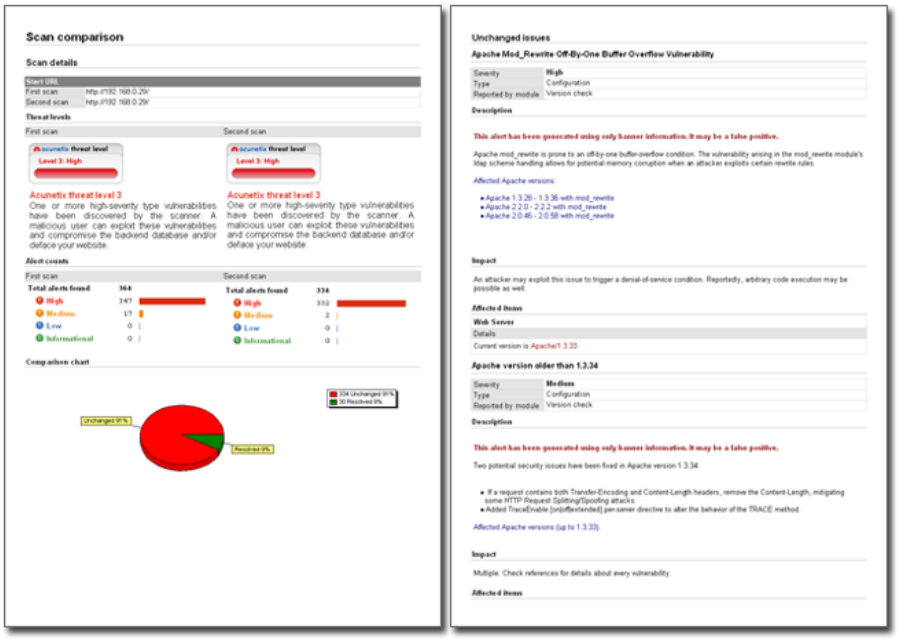
DISA STIG Web Security

The Security Technical Implementation Guide (STIG) is a configuration guide for computer software and hardware defined by the Defense Information System Agency (DISA), which part of the United States Department of Defense. This report identifies vulnerabilities which violate sections of STIG and groups the vulnerabilities by the sections of the STIG guide which are being violated.

Web Application Security Consortium (WASC) Threat Classification

The Web Application Security Consortium (WASC) is a non-profit organization made up of an international group of security experts, which has created a threat classification system for web vulnerabilities. This report groups the vulnerabilities identified on your site using the WASC threat classification system.

Scan Comparison Report



Screenshot 48 – Comparison Report

The Scan Comparison Report allows the user to track the changes between two scan results for the same application. This report will highlight resolved, unchanged and new vulnerabilities, making it easy to track development changes affecting the security of your web application.

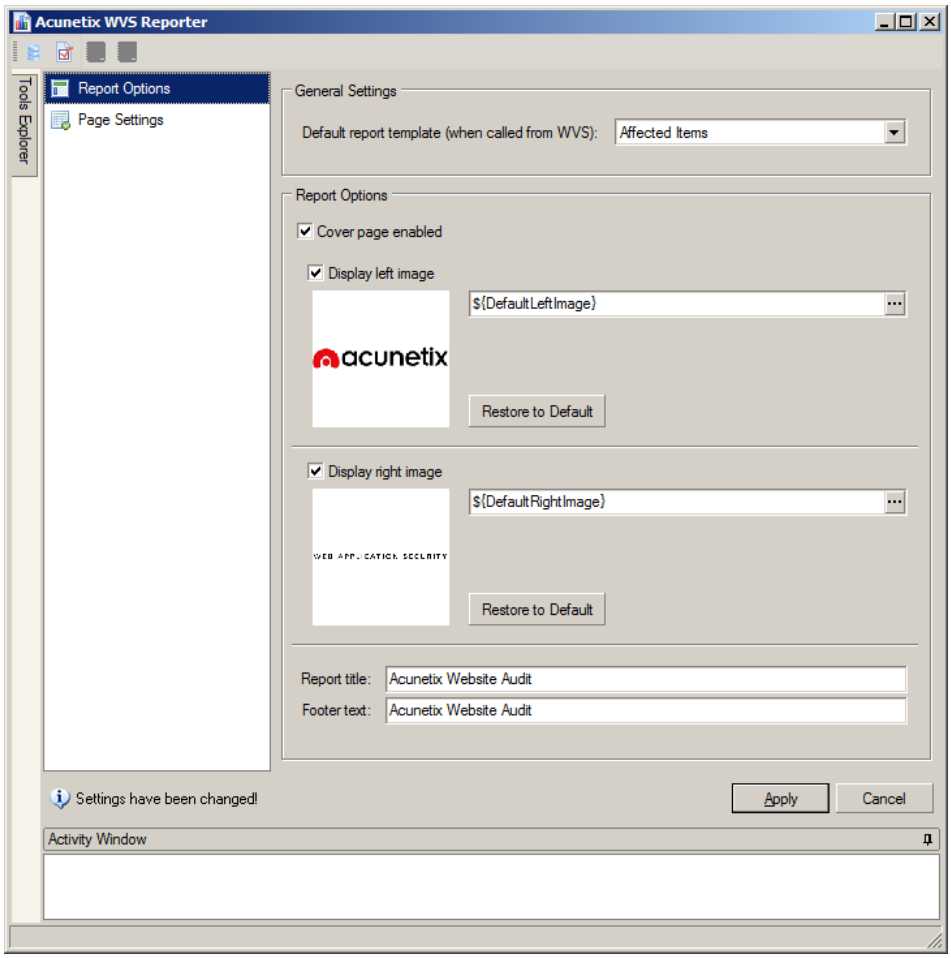
Monthly Vulnerabilities Report

This statistical report correlates the data from the scans performed in a specific month, and reports on the vulnerabilities identified during that month.

Reporter Settings

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.

From the Report Options node, you can customize the layout, titles, and images in the headers of the report.



Screenshot 49 - Reporter Options

General Settings - Configure the default report template for generating a report.

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

From the Page Settings node you can configure the default page size, orientation and margins of your reports.

These settings will apply to all reports.

Saving Reports

Once you have generated your report, you can use the toolbar at the top to save the report in PRE (prepared reports) format, which will allow you to review the report later. You can also export the report to PDF, HTML, Text, Word Document and BMP or print the report.

Changing the Reporter Database

Acunetix Web Vulnerability Scanner stores the scan results in a backend database. By default, Microsoft Access is used. You might want to switch to using Microsoft SQL server. This is recommended when scanning a lot of sites or larger sites. This can be done as follows:

1. Navigate to the 'Configuration > Application Settings > Database' node in the Acunetix Web Vulnerability Scanner interface. Select MS SQL Server from the 'Database Type' drop down menu.
2. Enter 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, you will be prompted with a confirmation to overwrite the current database structure and data.

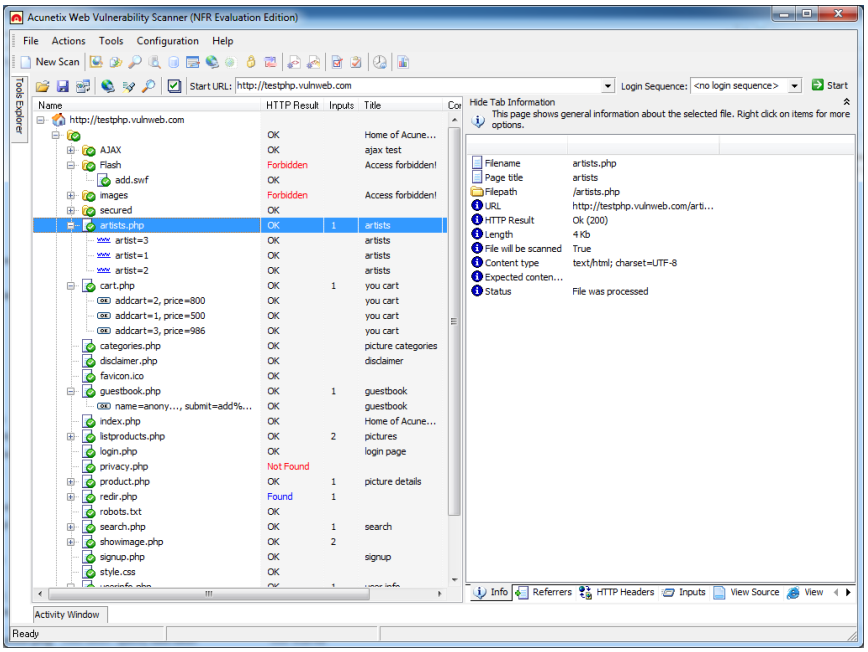
Note: The creation of the database requires a user SQL Administrator privileges. Once the database is created, you can change the SQL credentials to a user account with read and write permissions on the database.

It is also possible to 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.

7. Site Crawler

Introduction

The Site Crawler analyses a target website and builds the site structure using the information collected, including the site's directories and files / objects.



Screenshot 50 – The crawler tool interface

The interface of the Site Crawler consists of:

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.).
A series of tabs at the bottom of the Details window display further information about the selected object.

Starting a Website Crawl

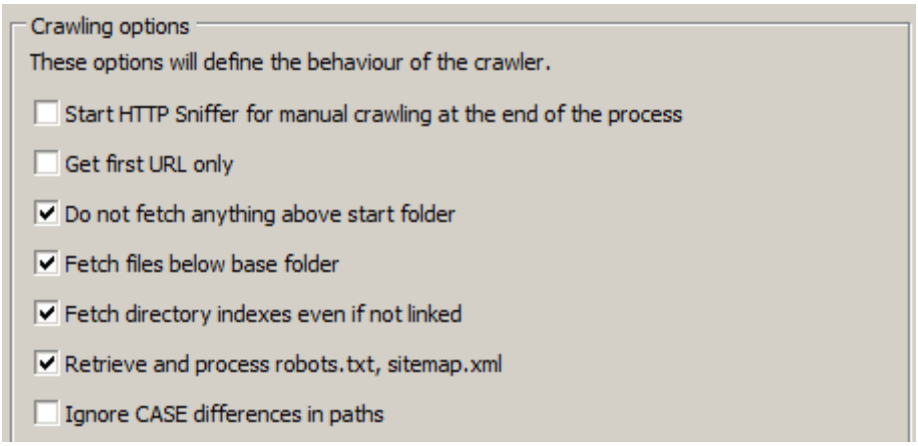
1. Select 'Tools > Site Crawler'
2. Enter the URL of the target website (e.g. http://testphp.vulnweb.com/).
3. If you want to use a recorded login sequence during the crawl, select it from the 'Login Sequence' drop down menu.
4. Click on the start button to start the crawling process.
5. If the website or any parts of it require HTTP authentication to be accessed, a pop-up window will automatically appear for you to enter the correct credentials, unless they were already 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.

It is also possible to load the results of a previously saved crawl or save the results of a completed crawl.

Crawling

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



Screenshot 51 - Crawling Options

Start HTTP Sniffer for manual crawling at the end of the scan process - This starts the HTTP Sniffer at the end of the crawl to allow the user to browse parts of the site that were not discovered by the crawler. Typically the Acunetix Web Vulnerability Scanner crawler is able to crawl the entire website though there are some scenarios were it fails to do so automatically. The crawler will update the website structure with the newly discovered links and pages.

Get first URL only - Scans the index or first page of the target site only and does not crawl any links.

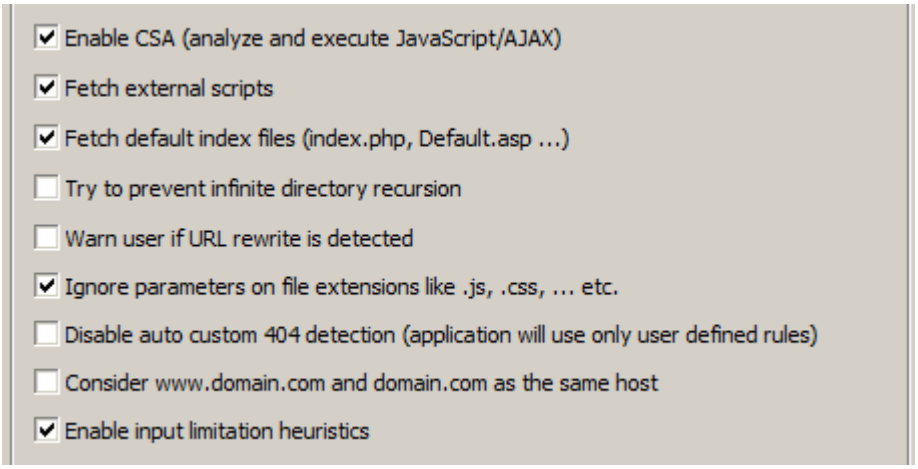
Do not fetch anything above start folder - By enabling this option the crawler will not traverse any links that point to a location above the base link. E.g. if http://testphp.vulnweb.com/wvs/ is the base URL, the crawler will not crawl to links which point to a location above the base URL like http://testphp.vulnweb.com.

Fetch files below base folder - By enabling this option the crawler will follow links that 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/. With this option disabled, the crawler will not crawl any objects from the root's sub directories.

Fetch directory indexes even if not linked – When enabled 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 search for a robots.txt or sitemap.xml file in the target website, and follow all the links specified if robots or sitemap are detected..

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".



Screenshot 52 - Crawling Options

Enable CSA (analyze and execute JavaScript/AJAX) – The Client Script Analyzer (CSA) is enabled by default 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 running 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, which might result in an incomplete crawl.

Fetch default index files (index.php, Default.asp …) - If this option is enabled, the crawler will try to fetch common default index filenames (such as index.php, Default.asp) for every folder, even if not directly linked.

Try to prevent infinite directory recursion – Certain websites are designed in a way which may cause the scanner to enter a loop when trying to fetch the same directory recursively (e.g. /images/images/images/images/…). This setting tries to prevent this situation by identifying repeated directory names in recursion.

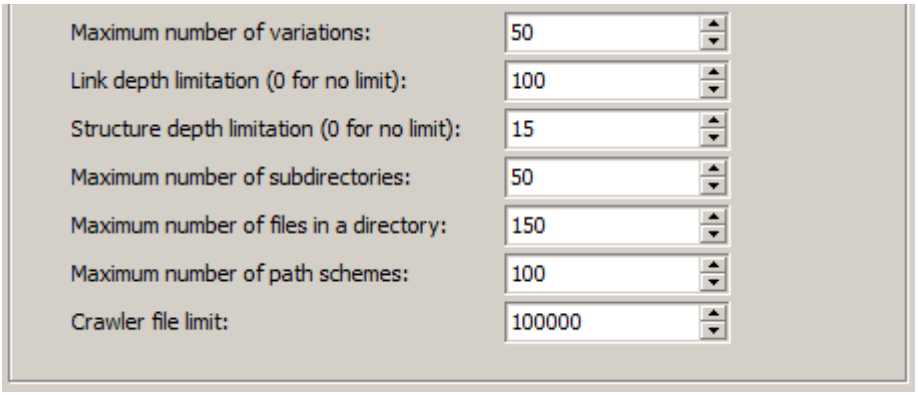
Warn user if URL rewrite is detected – Enable this option to be notified if URL rewrite is detected during the crawling stage of a scan.

Ignore parameters on file extensions like .js, .css etc– When enabled, Acunetix Web Vulnerability Scanner will not scan parameters on files which are not typically accessed directly by a user, such as js, css etc.

Disable auto custom 404 detection –With this option enabled, Acunetix Web Vulnerability Scanner will not automatically detect 404 error pages, thereby requiring 404 recognition patterns to be configured manually. You can read more about Custom 404 Error Page rules from page 82 of this manual.

Consider www.domain.com and domain.com as the same host – If this option is enabled, Acunetix Web Vulnerability Scanner will scan both sites www.domain.com and domain.com and treat them as one instead of separate hosts.

Enable Input limitation heuristics – If this option is enabled and more than 20 identical input schemes are detected on files in the same directory, the crawler will only crawl the first 20 identical input schemes.



Screenshot 53 – Crawling Options

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 from links requesting the page. Each of these links is considered a variation and each variation will appear under the file in the Scan Tree during crawling.

Link Depth Limitation – This option allows you to configure the maximum number of links to crawl from the root URL.

Structure Depth Limitation – This option allows you to configure the maximum number of directories to crawl from the root URL.

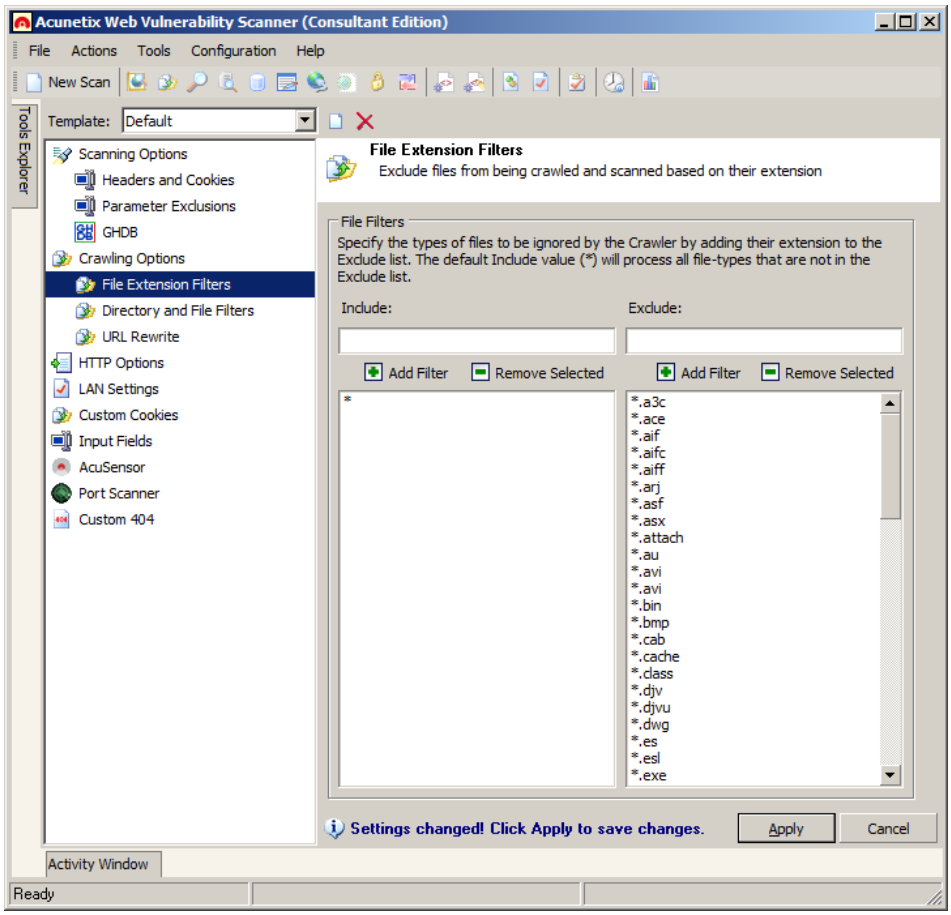
Maximum number of sub-directories – This option allows you to configure the maximum number of sub directories Acunetix Web Vulnerability Scanner should crawl in a website.

Maximum number of files in a directory – In this option you can configure the maximum number of files in a directory.

Maximum number of path schemes – In this option you can specify the maximum number of path schemes that should be detected by the crawler. You should only tweak this setting if you are crawling a very large website and notice that some path schemes are not being crawled.

Crawler file limit – This option allows you to configure the maximum number of files the crawler should crawl during a website crawl.

File Extension Filters



Screenshot 54 - Crawling Options - File Extension Filters

It is possible to configure a list of file extensions to be included or excluded during a crawl. This is done by configure the extensions in one of the following:

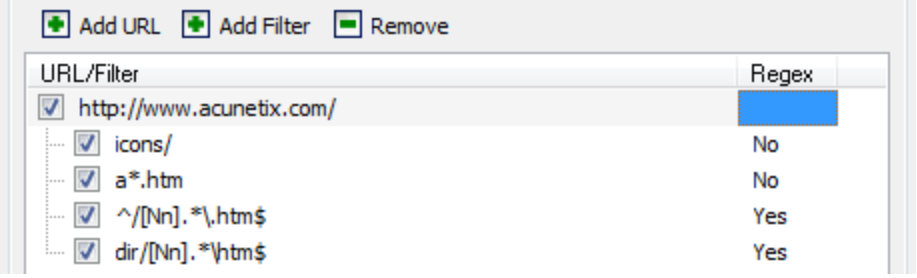
Include List - Process all files fitting the wildcard specified.

Exclude List - Ignore all files fitting the wildcard specified.

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

Directory and File Filters

This node enables you to specify a list of directories or filenames to be excluded from a crawl. Filters can be configured according to directory or file names, as well as through the use of wildcards to match multiple directories or files with the same filter. Regular expressions can also be used to match a number of directories or files. If a regular expression is specified as a filter, toggle the value to **Yes** under the 'Regex' column by clicking on it.



Screenshot 55 – Directory and File Filter rules

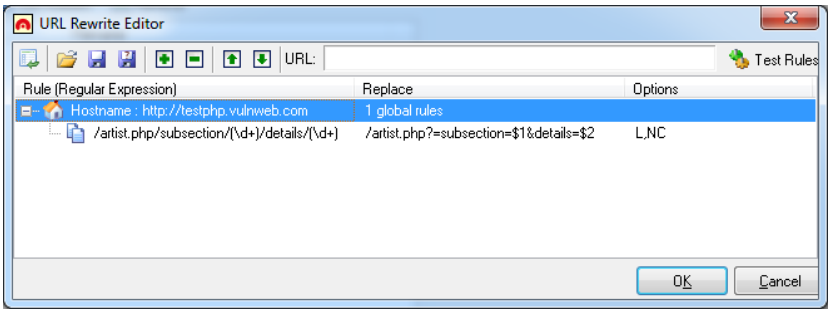
To add a directory or file rule:

1. Click the **Add URL** button and specify the address of the website where the directory or file is located.
2. Click the **Add Filter** button and specify the directory or filename, a wild card, or a regular expression. When specifying a directory 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 filters must be specified separately for sub-directories, as shown in the screen shot above.

URL Rewrite rules

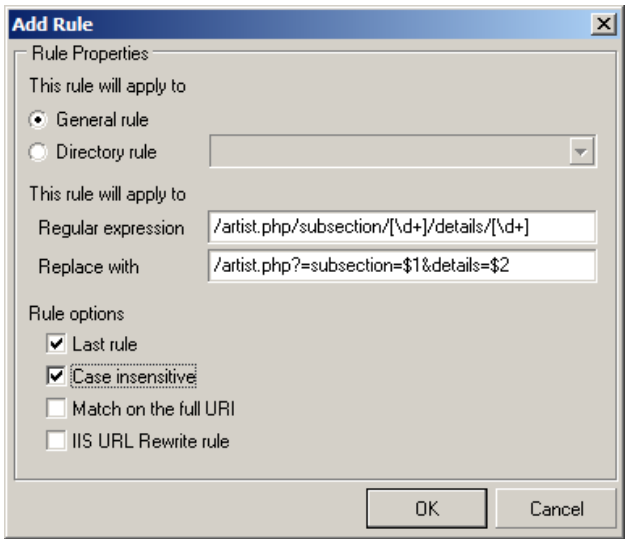
Many web applications – such as shopping carts and off the shelf applications such as WordPress and Joomla – use URL rewrite rules. Acunetix needs to understand these rewrite rules in order to navigate and understand the website structure and actual files better, and to avoid crawling of inexistent objects.



Screenshot 56 – URL Rewrite Configuration

Adding a URL rewrite rule manually

1. Navigate to the 'Configuration > Scan Settings > Crawling Options > URL rewrite' node.
2. Click the **Add Ruleset** button to open up the URL rewrite editor window and enter the host name of the target website for which the rule will be used. Click on the button to open up the Add rule dialogue.



Screenshot 57 – URL Rewrite Rule

1. Specify if the rule-set is generic for the whole website by ticking **General rule**. If for a specific directory only, tick **Directory rule** and specify the directory name.
2. In the **Regular Expression** input field, specify a part of the URL including regular expressions (or a group of Regular expressions) which Acunetix Web Vulnerability Scanner should use to recognize a rewritten URL. E.g. “Details/.*/(\d+)” indicates that everything must be matched after the Details/ directory, as well as subsequent strings beginning with digits.
3. In the **Replace with** input field, specify the URL Acunetix Web Vulnerability Scanner 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+). For example, if Acunetix finds this 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.
4. Tick the **Last rule** option to indicate that no more rules should be executed after this one.
5. Tick **Case insensitive** if the URLs are not case sensitive.
6. Tick **Match on the full URI** option so that the regular expression is executed on the whole URI with the query, instead of the path only.
7. Tick **IIS URL rewrite rule** if the target website is using Microsoft Windows IIS URL rewrite rules (http://www.iis.net/download/urlrewrite).
8. To test the URL rewrite rule, enter a URL and click **Test Rule**.

Importing a URL Rewrite rule configuration from an Apache web server

To import the rewrite rule logic for Apache web servers:

1. To open the Import Rewrite rules wizard, click **Add Ruleset** and then click **Import rule** . In the filename field, enter the path of the Apache httpd.conf or .htaccess file (the file which contains the URL rewrite rules).
2. Select the type of configuration to import (httpd.conf or .htaccess). If .htaccess is used, it is important to specify the hostname of the website (e.g. www.acunetix.com) and webserver directory (e.g. sales) on which the URL rewrite configuration is set.

Importing a URL Rewrite rule configuration from an IIS web server

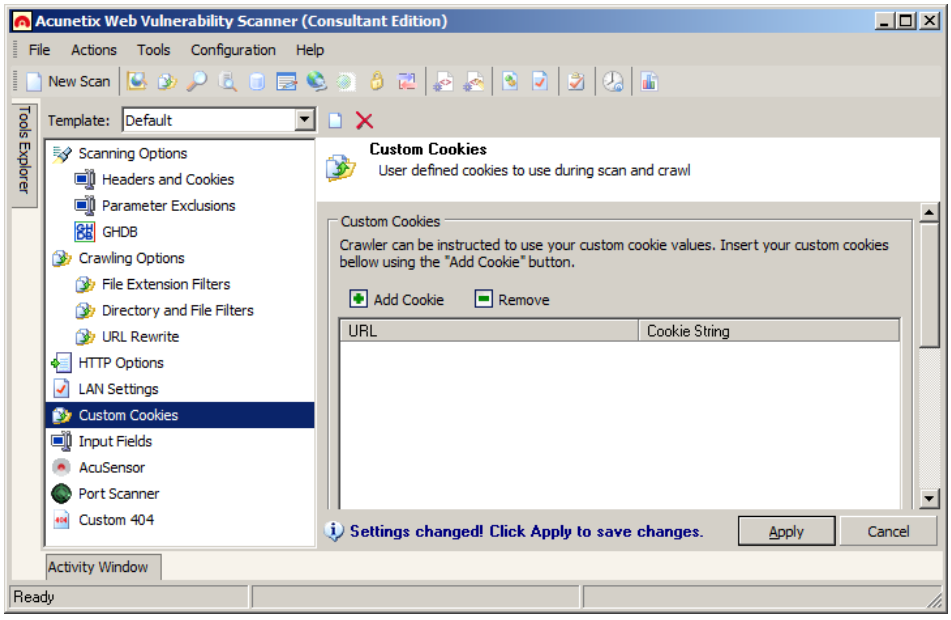
If using Microsoft IIS as your web server, you can automatically import the rewrite rule logic:

1. To open the Import Rewrite rules wizard, click **Add Ruleset** and then click **Import rule** . In the **Filename** field, enter the path of the web application web.config file that contains the URL rewrite rules.
2. Select the 'IIS URL Rrewrite' (web.config) node and specify the hostname of the website (e.g. www.acunetix.com) and webserver directory (e.g. sales) on which the URL rewrite configuration is set.

Note: Every Scan Settings template can have different crawler settings. Refer to page 78 of this user manual to read more on how to modify or create new Scan Settings templates.

Custom Cookies

You can create a custom cookie, which can be used during a website crawl to emulate a user or to automatically login to a section of the website (without requiring the Login Sequence Recorder).



Screenshot 58 - Custom Cookies

To add a custom cookie:

1. Navigate to Configuration > Scan Settings > Custom cookies node

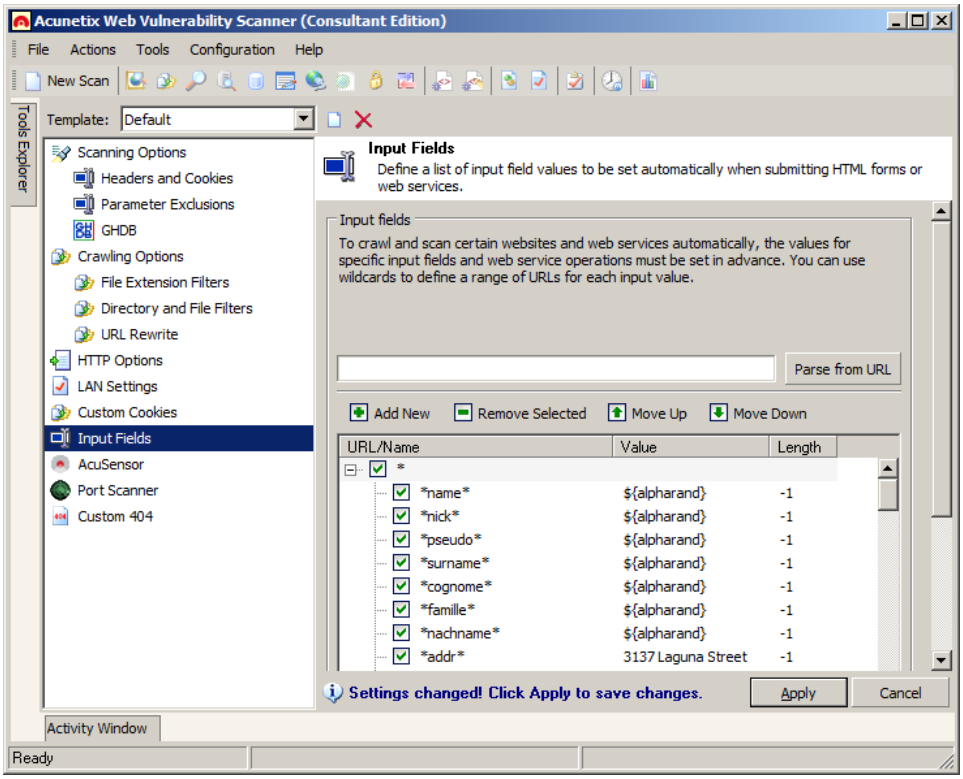
2. Click on the **Add Cookie** button to add a new blank cookie to the list.
3. Enter the URL of the site for which the cookie will be used in the left hand **URL**column.
4. Enter the custom string that will be sent with the cookie. E.g. if cookie name is 'Cookie_Name' and content is 'XYZ' enter 'Cookie_Name=XYZ'.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

Tick the option "Lock custom cookies during scanning and crawling" so to never overwrite the custom cookies with new ones sent from the website during a crawl or scan.

Configuring Input Fields to Traverse Web Form Pages

Many websites include web forms that capture visitor data, like download forms. Acunetix Web Vulnerability Scanner can be configured to automatically submit random data or specific values to web forms during the crawl and scan stages of a security audit.

Note: By default Acunetix Web Vulnerability Scanner uses a generic submit rule that will submit generic and random values to any kind of web form encountered during a crawl or scan.



Screenshot 59 - Input Fields

To specify a list of pre-defined values that must be automatically entered on a web form or web service:

1. Navigate to the Configuration > Scan Settings > Input Fields node.
2. Enter the URL of the webpage or web service containing the specific form or list of operations to which pre-defined values must be passed, and click **Parse from URL** button.
3. The resulting list will then be automatically completed with the form fields found in the given URL.
4. Enter the values for the required fields by double clicking the respective value column. Click **Apply** to save changes.

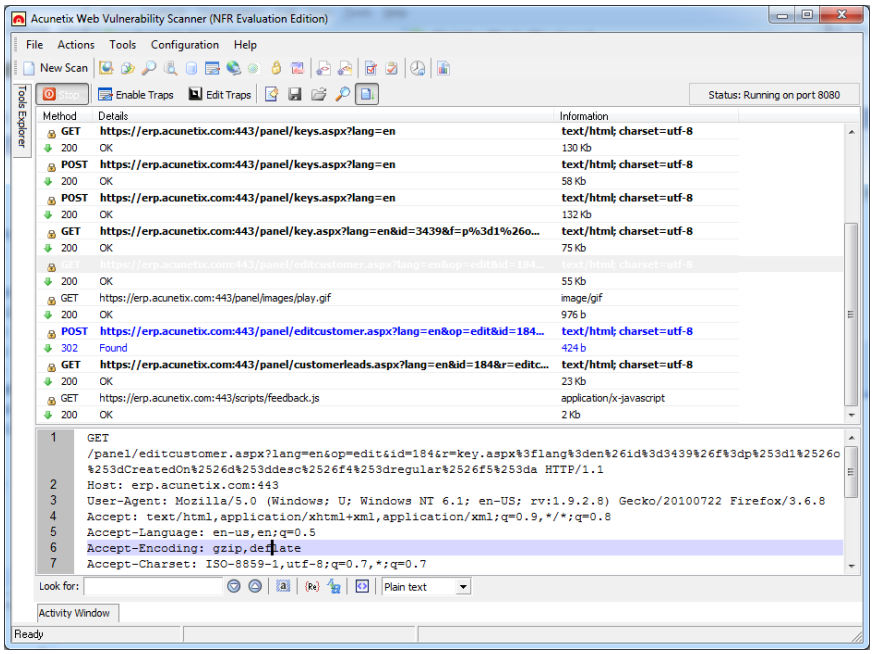
5. Input fields also support wildcards to match a broad range of data. Below you can find a number of examples:
    - **cus** is used to match any number of characters before and after the pattern 'cus'
    - **cus* is used to match any number of characters before the pattern 'cus'
    - *cus** is used to match any number of characters after the pattern 'cus'
    - *?cus* is used to match a single character before the pattern 'cus'
    - *c?us* is used to match a single character as a second character in the pattern specified
6. Alternatively, you can configure Acunetix Web Vulnerability Scanner to automatically randomize the values for each input field by entering the bolded variable names below in the parameter's value field:
    - **${alpharand}** – Automatically submit random alphabetical characters (a –z)
    - **$[numrand}** – Automatically submit random numeric characters (0 - 9)
    - **${alphanumrand}** – Automatically submit random alphabetical and numeric characters (a – z, 0 – 9)

You can also change the priority of a specific input field by highlighting it, and then using the **Up** and **Down** arrows to give it higher or lower priority respectively.

Note: If a unique set of data must be submitted to different forms, then a new rule-set must be created for each form respectively.

8. Manual Crawling using the HTTP Sniffer

Introduction



Screenshot 60 – The HTTP Sniffer

The HTTP Sniffer is a proxy server that enables you to capture and edit HTTP requests and responses exchanged between a web client (browser or other http application) and a web server.

The HTTP Sniffer can be used to manually crawl sections of a website that cannot be crawled automatically by Acunetix Web Vulnerability Scanner. The captured data can then be loaded into the Crawler and used to launch a scan.

To capture live traffic, your web browser must be configured to proxy 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/

The HTTP Sniffer can also be used to analyze HTTP traffic and to trap particular POST or GET requests that can be changed on-the-fly (manually or automatically) to emulate a 'man in the middle' attack.

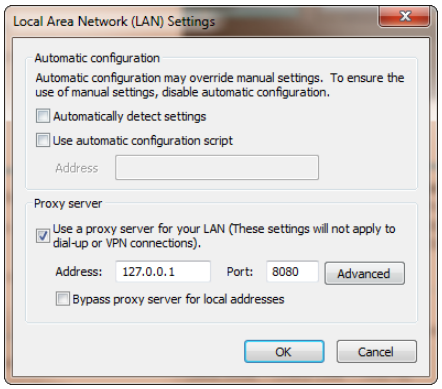
Configuring Your Browser

To start capturing traffic, you must first configure your browser to use the Acunetix HTTP Sniffer as proxy server:

Mozilla Firefox

1. From the Tools drop down menu select **Internet Options**
2. Select **Lan Settings** from the **Connections** 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 **OK** to save all options and close all configuration windows.

Internet Explorer



Screenshot 61- Browser Proxy Server Settings

1. From the **Tools** drop down menu click **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.

Note: 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 in Acunetix Web Vulnerability Scanner can be accessed from the Configuration > Application Settings > HTTP Sniffer node.

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.

Capturing HTTP traffic

To capture HTTP traffic:

1. Go to the Tools > HTTP sniffer node
2. Click on the **Start** button to enable the HTTP Sniffer.
3. From your browser, browse the website that you are interested in. All HTTP requests and responses will be listed in the main window.
4. Click on a request or response to view the complete details. All the requests/responses will be displayed in the lower window pane.
5. Click **Stop** when browsing is complete. Keep in mind that when the HTTP Sniffer is stopped, the web browser will lose its connection to the target URL.
6. You can then save the browsing logs, and load them into the crawler. Click **Save** to store the logs.

Go to Tools > Site Crawler and click on the **Build structure from HTTP sniffer log** button. Browse to the sniffer log you just saved.

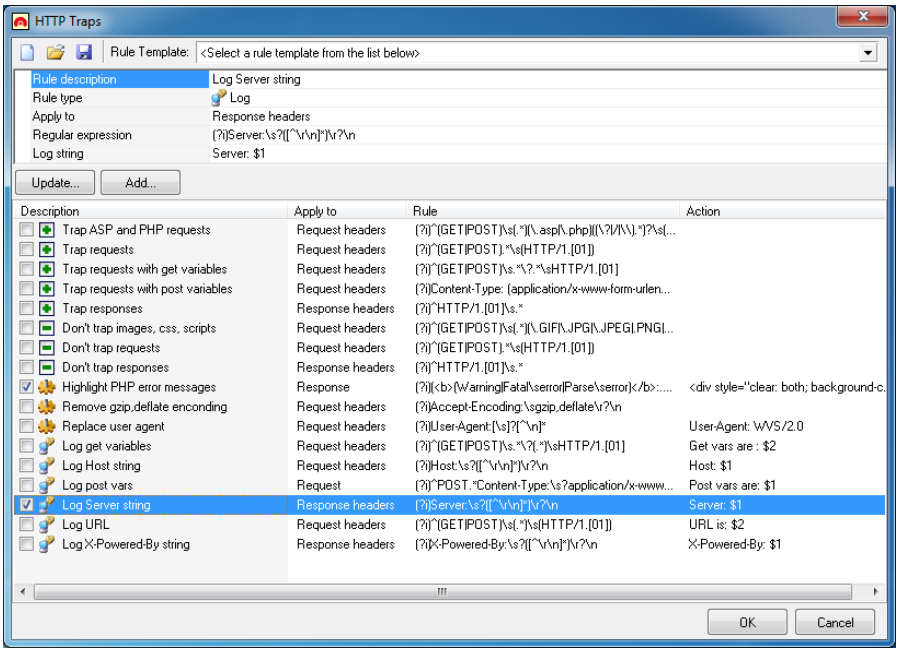
The crawler will build the structure. You can then right click on the site and scan it from within the Crawler, or save the crawl results and load them into the web scanner.

For more information about using the HTTP sniffer:

http://www.acunetix.com/blog/docs/manual-crawling-http-sniffer/

HTTP Sniffer Trap Filters

Through an HTTP Proxy trap filter, you can configure the HTTP Sniffer to intercept an HTTP request for it to be manipulated in real-time before it arrives to the server. You can do the same for HTTP responses.



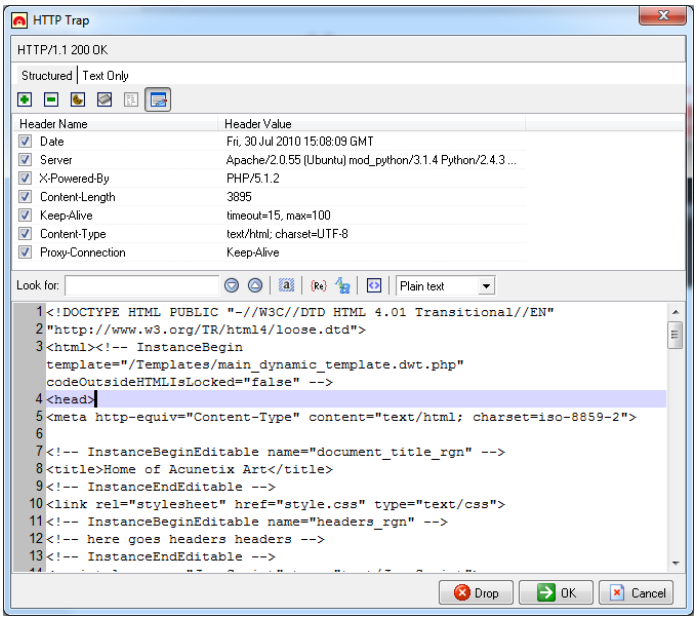
Screenshot 62 - HTTP Sniffer Edit Trap window

Creating a HTTP Sniffer Trap Filter

1. In the HTTP Sniffer toolbar, click on the **Edit traps** button to launch the HTTP Traps window.
2. Select a trap rule 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. Specify the rule type from the following 4 options:
    - **Include -** Configure which HTTP requests and responses should be trapped.
    - **Exclude -** Configure which HTTP requests and responses should 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. The type of traffic that will be captured by the trap must also be configured. Traps can be set to capture all traffic, HTTP requests only, request headers only, 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 63 - HTTP Sniffer Trap form

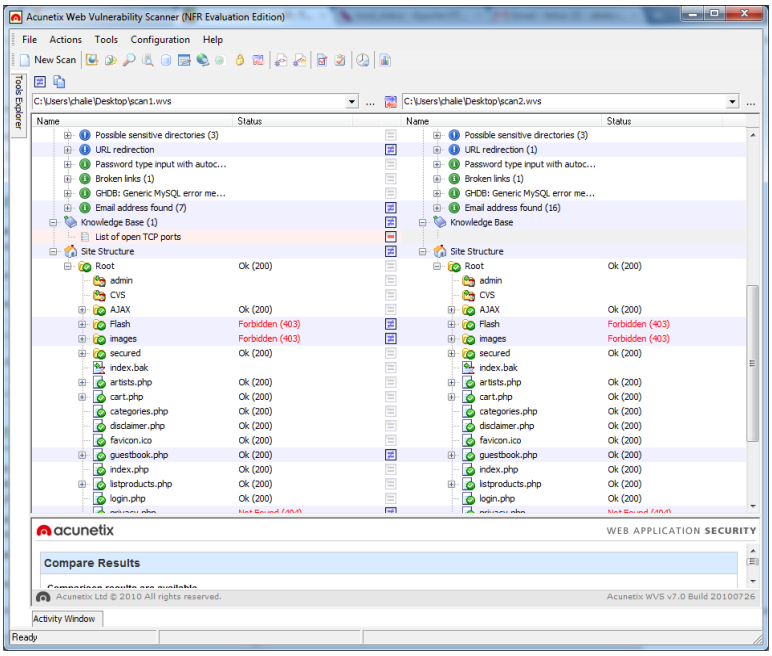
When an HTTP request or a response is trapped by the HTTP Sniffer, the **HTTP Trap** window will automatically appear to allow you to edit the captured data. Similarly to the HTTP Editor, the Trap Form editor allows you to edit headers, cookies, queries, and post variables. Click **OK** to allow the 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

9. Compare Results Tool

Introduction



Screenshot 64 – Compare Results Tool

The Compare Results tool allows you to analyze the differences between the results of two separate scans of the same application. You can compare a full security scan or just the site crawler data.

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 tool.
4. Specify which items you wish to compare such as Referrers, HTTP headers etc. The list of items that are enabled for comparison can be saved as a new template by renaming the template and clicking the **Save** button. Click **Start** to begin the comparison.

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

Analyzing the Results Comparison

Once the comparison is complete, the results are shown in a two-pane interface. The left pane contains the contents of the original scan while the right hand pane contains the results of the second scan. The middle column shows icons indicating the comparison result for the items in that line based on the following indicators:

	There are no changes.
	This item was added in the new version.

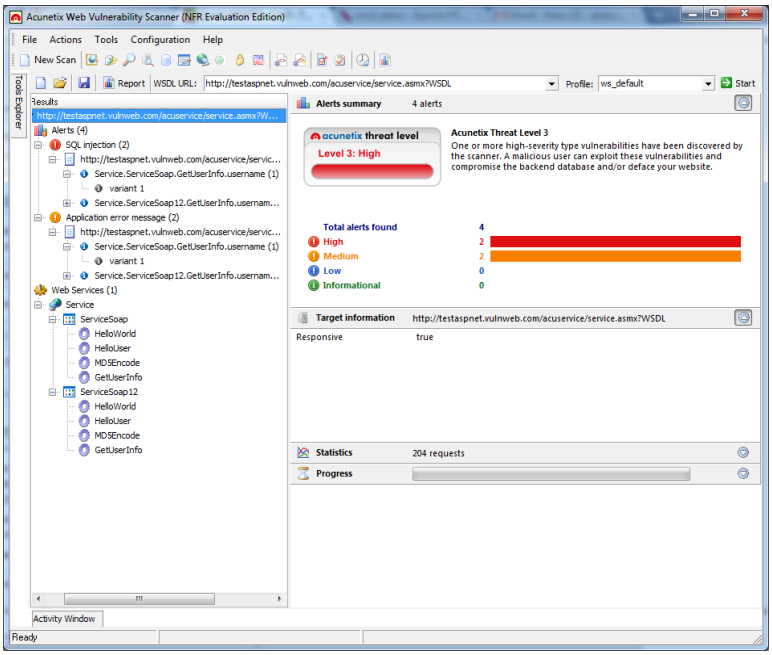
	This item was deleted from the new version.
	This item was changed in the new version.

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

10. Scanning Web Services

Introduction

Web Services, like any other internet-dependent systems, 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.

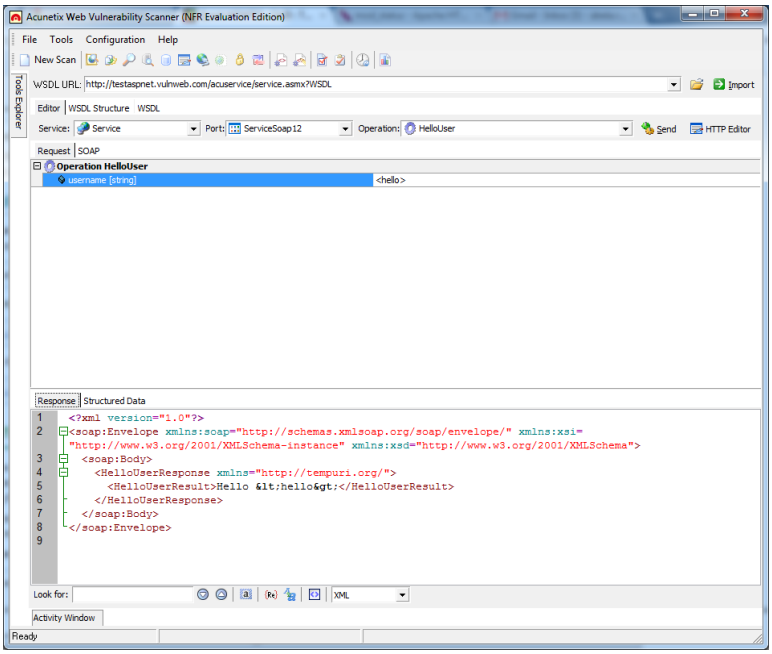


Screenshot 65 – Web Services Scanner

Starting a Web Service Scan

1. From the 'Tools Explorer' select **Web Services Scanner** and click the **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 **Next** to proceed.
2. In the 'Selection' step, select the Web Services, Ports and Operations that must 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 as Web Service Operations in the 'Default Values' step.
4. Proceed to the scan summary, review it and click **Finish** to launch the scan.

Web Services Editor



Screenshot 66 – Web Services Editor

The Web Services Editor allows importing 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, making it easy to 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 WDSL 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. From the drop down menus in the toolbar, select the Service, Port and Operation that must be tested.
3. Specify a value for the operation and click **Send** to pass the SOAP request to the web service. The web server response can then be viewed in a structured or XML view type in the lower window pane.

Response Tab

Displays the response sent back from the web service in raw XML format.

Structured Data Tab

Presents the XML data received from the web service response using a hierarchy of nodes that show the value for each element.

WSDL Structure Tab

Presents 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 WDSL 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.

11. The Scheduler

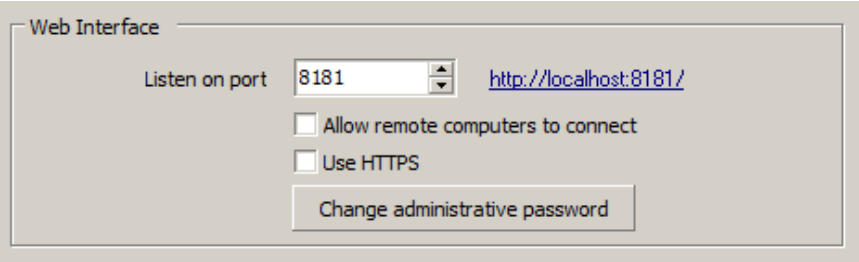
Introduction

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

Configuring the Scheduler service

The Acunetix Scheduler has a web-based interface that can be configured through the Acunetix Web Vulnerability Scanner application settings. To access the Scheduler service settings navigate to Configuration > Application Settings > Scheduler node.

Configuring the Scheduler web interface

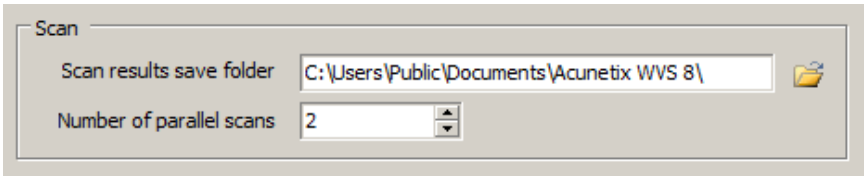


Screenshot 67 – Scheduler web interface configuration

By default, the Scheduler web interface is only accessible via localhost and on port 8181 (http://localhost:8181). If you would like the Scheduler web interface to be accessible from other remote computers, tick the **Allow remote computers to connect** option. When enabled, you will be prompted to specify a username and password for HTTPS to be automatically enabled. For security reasons, login credentials must always be defined when the scheduler web interface is configured to be accessed remotely.

Note: When you change any of the Web Interface settings, upon clicking the 'Apply' button restart the 'Acunetix WVS Scheduler v8' Windows service from the Windows Services console.

Scan Options



Screenshot 68 – Scheduler scan options

In this section you can specify the path where the Acunetix Web Vulnerability Scanner scan results should be saved. By default, the scan results are saved in the My Documents folder of the Windows Public user profile in the Acunetix WVS 8 sub directory.

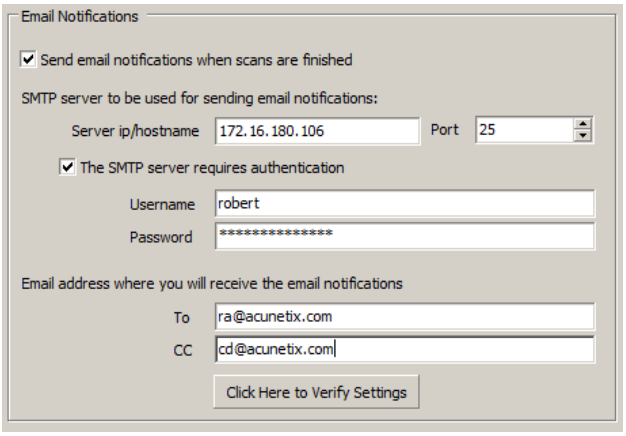
Scanning multiple websites

From this section you can also configure the number of parallel scans launched in Acunetix Web Vulnerability Scanner. E.g. if you want to scan 4 websites and their scan schedule overlaps, instead of the scans being queued, another instance of Acunetix Web Vulnerability Scanner is automatically started and the scans will be launched in parallel. If you are scanning a large number of websites it is

suggested to increase the number of parallel scans so their schedule does not overlap. Maximum number of parallel scans is 10 if you have the x10 instances license.

Note: The maximum number of scheduled scans that can be configured in the Acunetix Web Vulnerability Scanner scheduler is 2000.

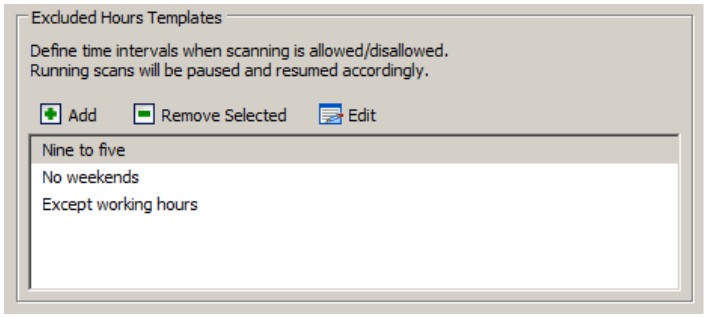
Configuring Email notifications



Screenshot 69 – Scheduler email notifications

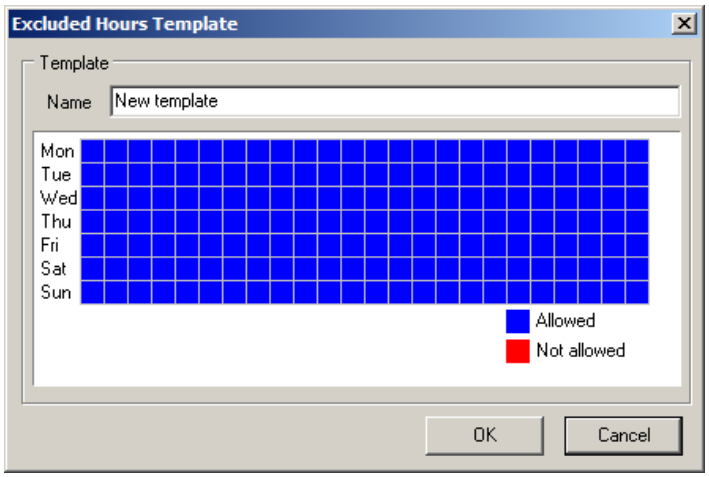
In this section you can specify the settings for email notifications, such as SMTP server IP or FQDN, port, SMTP server authentication (optional), and the email address where notifications will be sent.

Excluded hours templates



Screenshot 70 – Excluded Hours Templates

In the 'Excluded Hours Templates' section you can specify a range of hours to pause on-going scans. E.g. if you do not want to scan your website during times of high-traffic.



Screenshot 71 – Excluded Hours Configuration

To add a new 'Excluded Hours Template' click on the Add button and then:

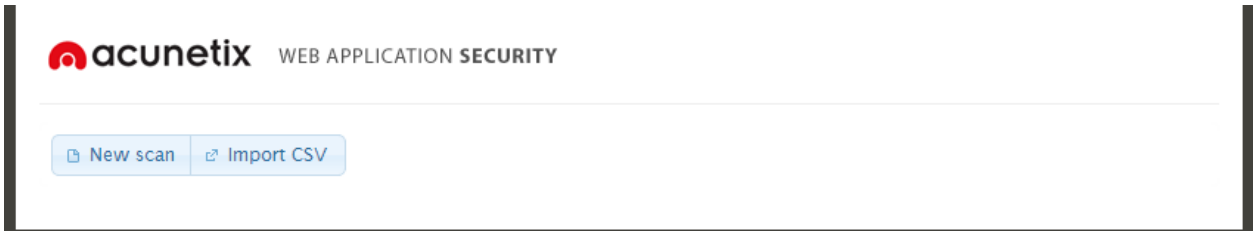
1. Specify a name of the template in the Name input field.
2. Highlight the hours of the day when scans should not run.
3. Click **OK** to save the new template.

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

Creating a Scheduled scan

1. Access the Scheduler interface by clicking the Scheduler Icon on the toolbar in the Acunetix Web Vulnerability Scanner interface, or browse http://127.0.0.1:8181 using a web browser.

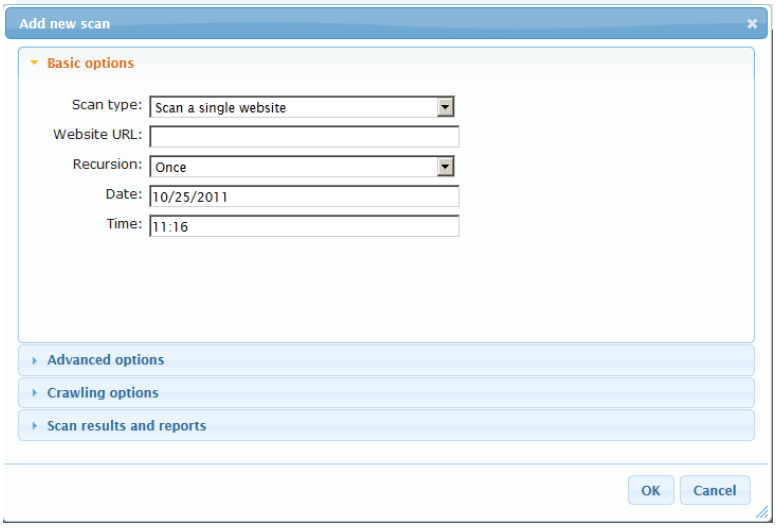
Note: JavaScript should be enabled to access the Acunetix Scheduler web interface.



Screenshot 72 – Acunetix Scheduler web interface

2. Click on the **New scan** button to add a new scan. You can add as many scans as you wish. If the scan schedule overlaps, they will be scanned in parallel. You can increase or decrease the number of parallel scans from the Scheduler configuration in the Acunetix Web Vulnerability Scanner application settings.
3. If you would like to import a number of scans (up to 2,000) using a CSV file, click on the **Import CSV** button. You can read more about this feature from page 73.

Scheduled Scan Basic Options

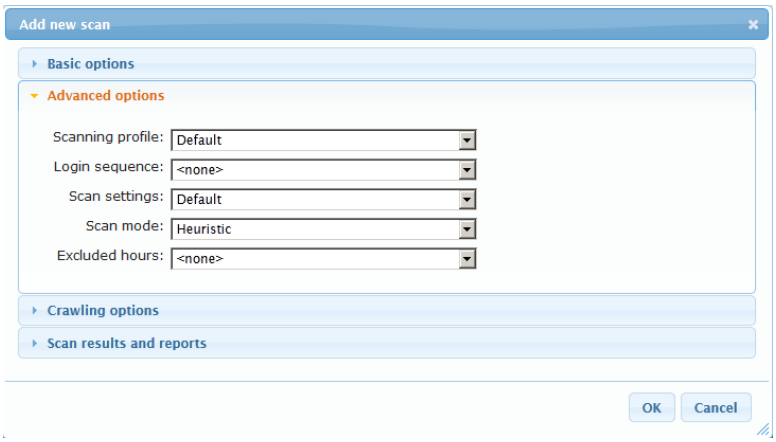


Screenshot 73 – Acunetix Scheduler Basic options

The Basic Options allow you to specify what target/s to scan as well as the scan recursion. The recursion option gives you the option to configure the Scheduler to run a scan 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.

Scheduled Scan Advanced Options

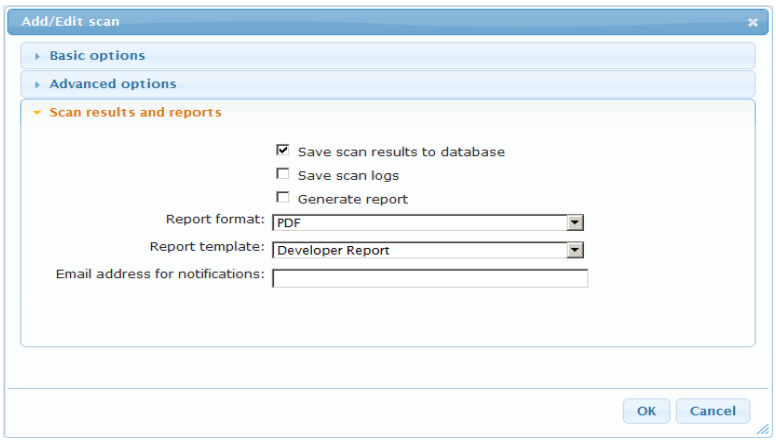


Screenshot 74 – Acunetix Scheduler Advanced options

The Advanced Options allow you to configure:

- Scanning Profile
- Login Sequence
- Scan Settings template
- Scan Mode
- Excluded Hours Template

Scheduled scan results and reports



Screenshot 75 – Acunetix Scheduler Scan results and Reports

In this section you can specify to save the scan results to the reporting database, save the scan logs, and generate a report. You can also specify in which format you want the report to be generated and an email address where the scan result is to be sent. If no email address is specified in this section, the email address specified in the scheduler settings is used.

In addition, the Report template field allows you to specify what report template to use. You can choose among four templates which are Affected Items, Developer Report, Executive Summary and Quick Report.

Importing Scheduling Scans

If you would like to schedule up to 2,000 scans you can use a CSV file to import the scheduled scans properties.

CSV File Properties

Each line in the CSV file should only contain 1 scan. For each scan you should specify the below properties:

- **URL**- Specify the URL with or without protocol (http and https). If no protocol is specified, http is used. This entry is mandatory.
- **Date**- Specify the date when the scan should be launched. The date format is DDMMYYYY and should be single string. E.g. If a scan is to be scheduled for the 5th of November 2012, the date should be 05112012. This entry is mandatory.
- **Time**- Specify the time when the scan should be launched. The time format is 24 hours and should be a single string of 4 digits. E.g. 10am should be 1000 and 10pm should be 2200. This entry is mandatory.
- **Scanning Profile**- Specify the name of an existing scanning profile to be used during the scan. If not specified, the default scanning profile will be used during the scan.
- **Login Sequence**- Specify the name of an existing login sequence if you want to use a login sequence during the scan. If nothing is specified, no login sequence will be used during the scan.
- **Scan Settings**- Specify the name of an existing scan settings template. If no scan settings template is specified, the default scan settings template will be used.
- **Scan Mode**- Specify the scan mode to be used during the scan. The options are quick, heuristic and extensive. If no scan mode is specified, the default scan mode will be used.
- **Generate Report** – Specify if a report should be generated after the scan. The options are yes or no. If nothing is specified, no report will be generated.
- **Report Format**- If you specified the generate report option, then you have to specify the report format as well. The options available are PDF, RTF, REP or HTML. If you do not specify any format, a PDF report will be generated.
- **Notification Email Address**- Specify the email address where the email should be sent upon completion of the scan. If an email is not specified, the default email address configured in the Acunetix Web Vulnerability Scanner GUI will be used.

If you would like to omit an entry so the default value is used, simply leave a space between the commas. Some examples follow:

Example 1: To scan testphp.vulnweb.com on the 5th of November 2012 at 10pm using the default values, use the below line in the CSV file:

http://testphp.vulnweb.com,05112012,2200, , , , , ,

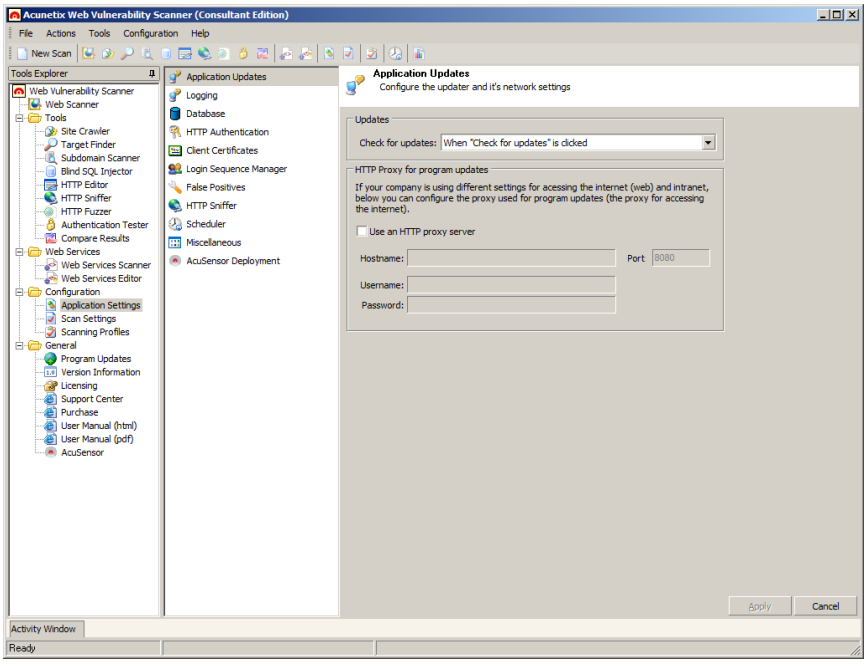
Example 2: To scan testasp.vulnweb.com on the 5th of November 2012 at 3:15pm using the XSS (Cross-site scripting) scanning profile, without login sequence, default scan settings, using the extensive scanning mode, generate a PDF report and send the results to results@myemail.com , use the below example:

http://testasp.vulnweb.com,05112012,1515,XSS, , ,extensive,yes,PDF,results@myemail.com

Note: Scans imported from a CSV file will only be executed once. It is not possible to configure recurring scans using the CSV file import feature.

12. Application Settings

Acunetix Web Vulnerability Scanner configuration settings can be accessed from the 'Configuration > Application Settings' node in the Tools Explorer window pane.



Screenshot 76 – Application Settings

Application Updates

From this node you can configure when the application checks for both vulnerability and application updates. You can also configure the Proxy Server settings if your Internet connection must be accessed via a proxy server.

Logging

From the Logging node, you can configure which actions logging severities are logged. You can also specify how many log files to retain. Note that some log files may contain a lot of information (such as the one which logs the HTTP requests and responses)

Database

You can configure the database that you would like to use for the scan results. This database will be used to generate reports using the Web Vulnerability Scanner Reporter.

HTTP Authentication

Refer to page 28 of this manual for information about the HTTP Authentication options.

Client Certificates

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

Navigate to 'Configuration > Application Settings > Client Certificates'

Specify a certificate location by browsing to the certificate with the Browse icon next to the **Certificate file** text box and enter the certificate password in the **Password** text box.

Enter the URL which needs a client certificate to be accessed. Click on **Import** and **Apply** to save the certificate information.

Login Sequence Manager

The Login Sequence Manager allows you to manage your recorded login sequences, including the ones that have been defined prior to a scan. You can add, edit or remove Login Sequences from this node.

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 site-specific, by 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.

HTTP Sniffer

From the HTTP Sniffer node, you can specify the interface and the port that the HTTP Sniffer will listen on.

Scheduler

From the Scheduler node, you can configure the settings for the Acunetix Web Vulnerability Scanner Scheduler service. More information can be found in The Scheduler chapter on Page 69

Miscellaneous

From this node, you can configure the options specified below:

Memory Optimization

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

In this section you can also configure the amount of memory the crawler should use. If during a crawl the crawler consumes the configured amount of memory, the crawl will stop and the scanning will proceed.

Display Options

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 that are accessed via HTTPS and not HTTP.

Password Protection

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

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

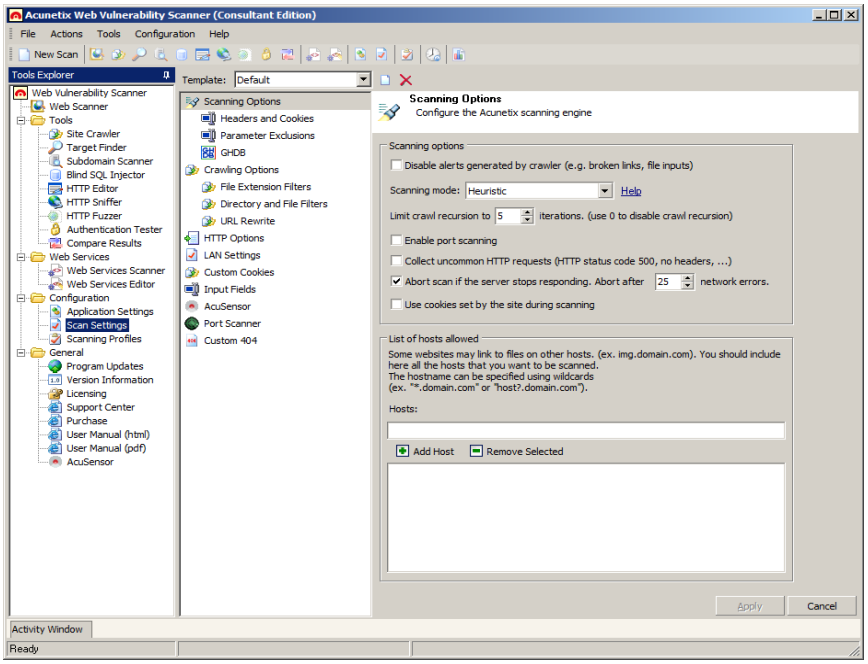
To remove password protection, enter the current password in the field **Current Password** and leave the other 2 fields blank.

AcuSensor Deployment

From the AcuSensor Deployment node, you can configure the settings for the AcuSensor and generate the AcuSensor Installation Files. More information on this can be found in the Installing the AcuSensor Agent Chapter on page 18.

13. Scan Settings Templates

Scan Settings can be configured exclusively for a specific URL and saved as Scan Settings Templates. If you frequently need to scan multiple websites that require different settings, Scan Settings Templates can be recalled quickly and easily without the need of any reconfiguration.



Screenshot 77 – Scan Settings templates

Creating, modifying, or deleting Scan Settings templates

To create a new Scan Settings template click the ╳ button and specify a name for the New Scan Settings template. To delete an existing Scan Settings template, select it from the 'Template' drop down menu and click the ╳ button. To modify an existing Scan Settings template, select it from the 'Templates' drop down menu, make the necessary changes and then click **Apply**. Below is a detailed list of all the options available for each Scan Settings template.

Scanning Options

Disable Alerts generated by crawler - Select this option to disable crawler related alerts – such as broken links, file inputs and files which their name indicates that they can be dangerous etc. – from being reported.

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 following scanning mode options are available:

- **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 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. It will

try to fetch the most 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, and is recommended as 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 only be used for specialized security audits since it 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 still discover new objects – for which a new crawl will be started. This is called iteration. Configure the maximum number of crawl iterations that can happen during a website scan.

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 7 of this manual.

Collect uncommon HTTP Requests - Acunetix Web Vulnerability Scanner can report any uncommon server response that 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 the scanner must encounter before completely aborting the scan.

Use cookies set by the site during scanning – By default, Acunetix Web Vulnerability Scanner ignores the cookies sent by the website during the scan but uses the ones discovered during the crawling process. Enable this option to always use the latest cookies provided by the website; ignore the cookies discovered in the crawl and use the ones the website is sending during the scan.

List of hosts allowed - By default, Acunetix Web Vulnerability Scanner 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 Web Vulnerability Scanner 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 / scan and click the **+** button to add the entry. 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

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

Test cookies for all files – By default, Acunetix Web Vulnerability Scanner will only try to manipulate cookie data and use it against files that contain GET and POST parameters. If this option is enabled, Acunetix Web Vulnerability Scanner will also try to use manipulated cookie data against static files.

Manipulate the HTTP headers below – A number of Acunetix Web Vulnerability Scanner security checks try to manipulate HTTP headers. This section lists the HTTP headers Acunetix Web Vulnerability Scanner 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 **Manipulate the HTTP headers listed below** option you will disable all HTTP headers manipulation tests.

Parameter Exclusions

Enables you to specify parameters that must 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 but will still be crawled.

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. Click **Apply** to save your changes.

GHDB (Google Hacking Database) Options

By default, all GHDB (Google Hacking Database) tests (1450+) are launched against a website during a scan. From the 'Settings > GHDB' node, you can configure which GHDB vulnerability checks you want to test for.

Filter the list by entering a keyword (e.g. sql) in the 'Filter GHDB' text box. Click on **Uncheck Visible** to uncheck all vulnerabilities that match with keyword and exclude them from a default scan. Click **Check Visible** to check all entries again and include them in a default scan.

Crawling Options

Refer to page 51 of this manual for more information on the crawling options.

HTTP Options

HTTP General

User agent string – Configure what user agent header string Acunetix Web Vulnerability Scanner should use when accessing a target website. You can click on ⨯ to use a predefined user agent string or you can specify your own 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 website. If overloaded with requests, some target servers might crash or reject new connections.

HTTP request timeout in seconds – Specify how long Acunetix Web Vulnerability Scanner must wait for a HTTP response before considering it as timed out.

Delay between consecutive requests in milliseconds – Configure the delay between each HTTP request Acunetix Web Vulnerability Scanner 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).

Custom HTTP Headers

In this section you can specify custom HTTP Headers that Acunetix Web Vulnerability Scanner should include with the other standard HTTP headers while automatically crawling and scanning a website.

LAN Settings

For more details on configuring LAN and proxy settings refer to page 23 of this manual.

Custom Cookies

For more details on configuring custom cookies refer to page 57 of this manual.

Input Fields

For more details on configuring input fields refer to page 58 of this manual.

AcuSensor

For more details on configuring AcuSensor refer to page 18 of this manual.

Port Scanner

While scanning a website you can also choose to launch a port scan against the web server hosting the site. 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.

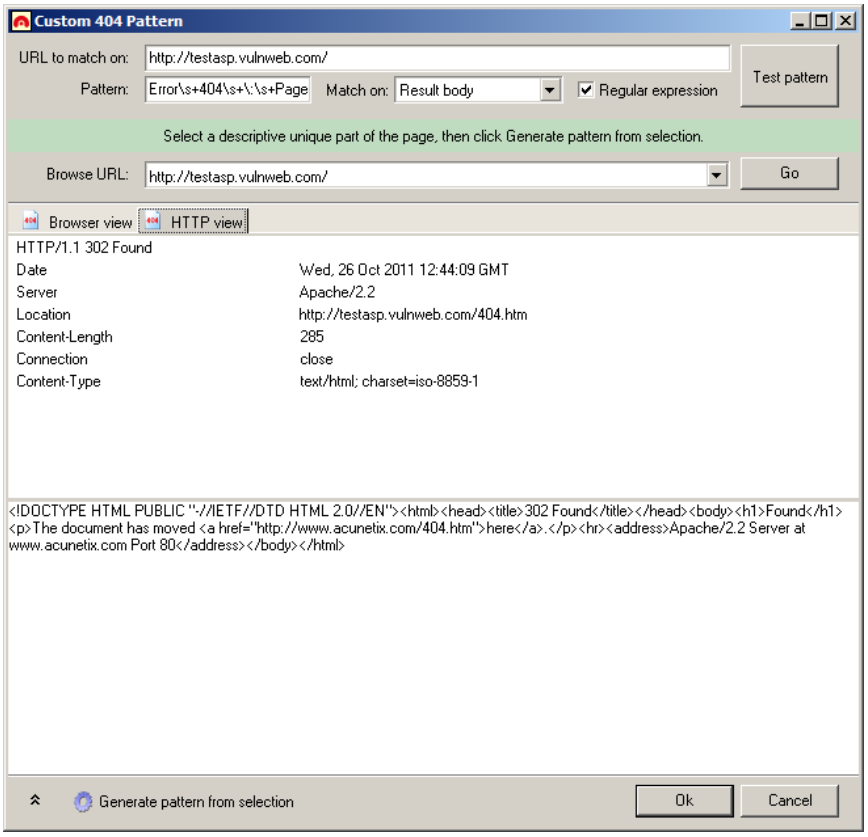
Note: The Network Alert Scripts (Network security checks) are fully scriptable thereby allowing you to write new ones. The Acunetix Web Vulnerability Scanner Network Alert scripting reference is available from the following URL;

http://www.acunetix.com/vulnerability-scanner/scriptingreference/index.html.

Custom 404 Error Pages

A 404 error page is the page that 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 Web Vulnerability Scanner must be able to automatically identify these pages, to detect the difference between a non-existent URL and a valid web page.

By default Acunetix Web Vulnerability Scanner will automatically detect custom 404 pages and patterns to match them, therefore you do not need to configure Custom 404 Error Pages rules manually. In case you want to override the Acunetix Web Vulnerability Scanner automatic detection, you can configure a custom error page rule by completing the following steps:



Screenshot 78 – Custom 404 Error page configuration

1. Specify the URL of the website for which you would like to create a custom 404 error page rule in the ‘URL to match on’ input field.
2. In the **Pattern** input field, you should specify a text pattern or regular expression which matches some unique text on the custom 404 error page.
3. Specify where the pattern can be found in the custom 404 error page response from the ‘Match on’ drop down menu:
    - **Location header** – The defined pattern can be found in the header of the custom error page.
    - **Result Body** – The defined pattern can be found in the body of the custom error page.

- **Result** – The defined pattern can be found in both the header and body of the custom error page.

You can also generate such pattern automatically:

1. Enter the website's URL in the 'Browse URL' input field and click **GO**. The browser will request non existing URL's to trigger the Custom 404 error page.
2. Highlight the unique text from the custom error page.
3. Click Generate pattern from selection.

14. Scanning Profiles

The scanning profiles enable you to specify which type of vulnerability checks (e.g. XSS, SQL Injection) you would like to run on your website. From the 'Configuration > Scanning Profiles' node in the Tools Explorer window pane, you can create or edit scanning profiles, including the default set.

Default Scanning Profiles

A number of default scanning profiles are included with Acunetix Web Vulnerability Scanner. Below is a list of all the scanning profiles and a summary of the security checks they perform. For a detailed list of the vulnerability checks that 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 tests selected with a checkbox will be launched when the scanning profile is used.

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. From the 'Profile' drop down menu, select the scanning profile that you would like to use as the base for the new scanning profile. If you want to start with all the scripts disabled, you should select the Empty scanning profile.
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 / 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 Web Vulnerability Scanner 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/

15. Troubleshooting

Obtaining support

User Manual

The most common issues can be solved by consulting this manual.

Support

The Acunetix support team can be contacted by email at support@acunetix.com.

The Acunetix Support Center

Browse to http://www.acunetix.com/support/ to view all the support options available.

Acunetix Forums

Browse to http://www.acunetix.com/forums to interact with our expert community.

Request Support via E-Mail

If you encounter persistent problems that you cannot resolve we encourage you to contact the Acunetix Support team via e-mail (support@acunetix.com), since you can include vital information to help us diagnose and resolve your issues as quickly as possible. Please ensure you include the license key information in the support email.

We will do our best to answer your query within 24 hours or less, depending on your time zone.

Acunetix Blog

We highly recommend that you follow our security blog by browsing to:
http://www.acunetix.com/blog/

Acunetix Facebook page

Join us on Facebook for the latest product and industry updates:
http://www.facebook.com/Acunetix

Knowledge base / Help / Support page

You can also explore the Acunetix knowledge base by browsing to:
http://www.acunetix.com/support/