



Web Vulnerability Scanner v10
Product Manual

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

Acunetix Web Vulnerability Scanner is copyright of Acunetix Ltd. 2004–2015.

Acunetix Ltd. All rights reserved.

<http://www.acunetix.com>

info@acunetix.com

Document version 10

Last updated: 26th June 2015

Table of Contents

- Introduction
- Overview
- Installing Acunetix
- Installing AcuSensor
- Scanning a Website
- Analysing Scan Results
- Scanning Web Services
- Generating Reports
- Acunetix Reports
- Scheduling Scans
- Troubleshooting and Support

Introduction to Acunetix Web Vulnerability Scanner

Why You Need To Secure Your Web Applications

Website security is today's most overlooked aspect of securing an 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.

The hacking community is also very close-knit; newly discovered web application intrusions, known as Zero Day exploits, are posted on a number of forums and websites known only to members of that exclusive underground group. 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 means that you would 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 Injection, 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. Acunetix DeepScan analyses the entire website by following all the links on the site, including links which are dynamically constructed using JavaScript, and links found in robots.txt and sitemap.xml (if available). The result is a map of the site, which Acunetix Web Vulnerability Scanner will use to launch targeted checks against each part of the site.

Name	HTTP Result	Inputs	Title	Content Type
http://testphp.vulnweb.com/				
+	Ok (200)		Home of Acune...	text/html
+.idea	Ok (200)		Index of /.idea	text/html
+.admin	Ok (200)		Index of /admin	text/html
+.AJAX	Ok (200)		ajax test	text/html
+.Connections	Ok (200)		Index of /Conn...	text/html
+.CVS	Ok (200)		Index of /CVS	text/html
+.Flash	Ok (200)		Index of /Flash	text/html
+.hpp	Ok (200)	1	HTTP Paramete...	text/html
+.icons	Not Found...			text/html

Screenshot - 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, the Web Vulnerability Scanner automatically launches a series of vulnerability checks on each page found, in essence emulating a hacker. Acunetix Web Vulnerability Scanner also 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.

Scan Results

Scan Thread 1 (http://testphp.vulnweb.com)

Web Alerts (185)

- Blind SQL Injection (15)
- CRLF injection/HTTP response splitting (1)
- Cross Site Scripting (verified) (26)
- Directory Traversal (verified) (3)
- HTTP Parameter Pollution (2)
- Macromedia Dreamweaver Remote File Include (1)
- PHP allow_url_fopen enabled (1)
- Script source code disclosure (1)
- SQL injection (verified) (26)
- Weak Password (1)
- Application error message (6)
- Backup files (2)
- Directory Listing (14)
- Error message on page (7)

acunetix WEB APPLICATION SECURITY

Blind SQL Injection Severity HIGH

Vulnerability description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter backend SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Affected items

Screenshot - Scan Results

4. The vulnerabilities identified are shown in the Scan Results. Each vulnerability alert contains information about the vulnerability such as POST data used, affected item, http response of the server and more.
5. 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.

6. Various reports can be generated on completed scans, including Executive Summary report, Developer report and various compliance reports such as PCI or ISO 270001.

Acunetix AcuSensor Technology

Acunetix's 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.

SQL injection (verified)Severity HIGH

Vulnerability description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This vulnerability affects [/listproducts.php](#).

Discovered by: Scripting (Sql_Injection.script).



Vulnerability details

Source file: [/hj/var/www/listproducts.php](#) line: **43**

Additional details:

```
SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"C33MmACUEND' AND pass=''
"mysql_query" was called.
```

Attack details

Cookie input **login** was set to **1ACUSTART"C33MmACUEND**

[View HTTP headers](#)

[View HTML response](#)

Screenshot - AcuSensor pinpoints 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 to 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 improved 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 of recipients or additional information to the message body to a vulnerable web form, to spam a large number of recipients anonymously.

Network Vulnerability Scanning

As part of a website audit, Acunetix will execute a network security audit of the server hosting the website. This network security scan will identify any services running on the scanned server by running a port scan on the system. Acunetix will report the operating system and

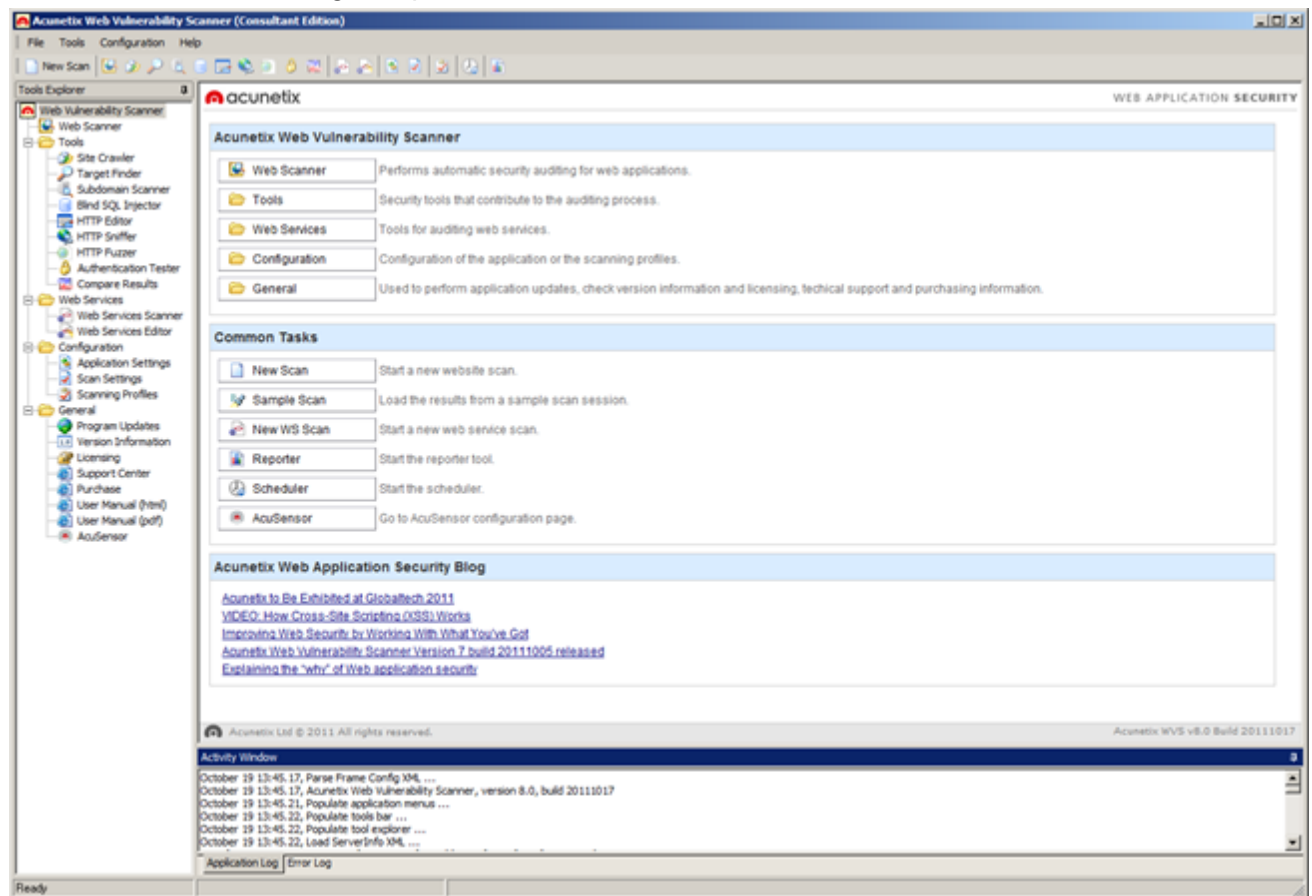
the software hosting the services detected. This process will also identify Trojans which might be lurking on the server.

The network vulnerability scan assesses the security of popular protocols such as FTP, DNS, SMTP, IMAP, POP3, SSH, SNMP and Telnet. Apart from testing for weak or default passwords, Acunetix will also check for misconfiguration in the services detected which could lead to a security breach. Acunetix will also check that any other servers running on the machine are not using any deprecated protocols. All these lead to an insecure system, which would allow an intruder to damage your web site and your reputation.

Acunetix Online Vulnerability Scanner (OVS) also integrates the popular OpenVAS network scanner to check for over 35,000 network vulnerabilities. During a network scan, Acunetix OVS makes use of various port probing and OS fingerprinting techniques to identify a vast number of devices, Operating Systems and server products. Numerous security checks are then launched against the products identified running on the scanned server, allowing you to detect all the vulnerabilities that exist on your perimeter servers.

Acunetix Web Vulnerability Scanner Overview

Acunetix Web Vulnerability Scanner allows you to secure your website quickly and efficiently. It consists of the following components:



Screenshot - 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** – Making use of Acunetix DeepScan, Acunetix Web Vulnerability Scanner automatically analyzes and crawls the website in order to build the site's structure. The crawling process enumerates all files and is vital to ensure that all the files of 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 of all the vulnerabilities found within the website.

AcuSensor Technology Agent

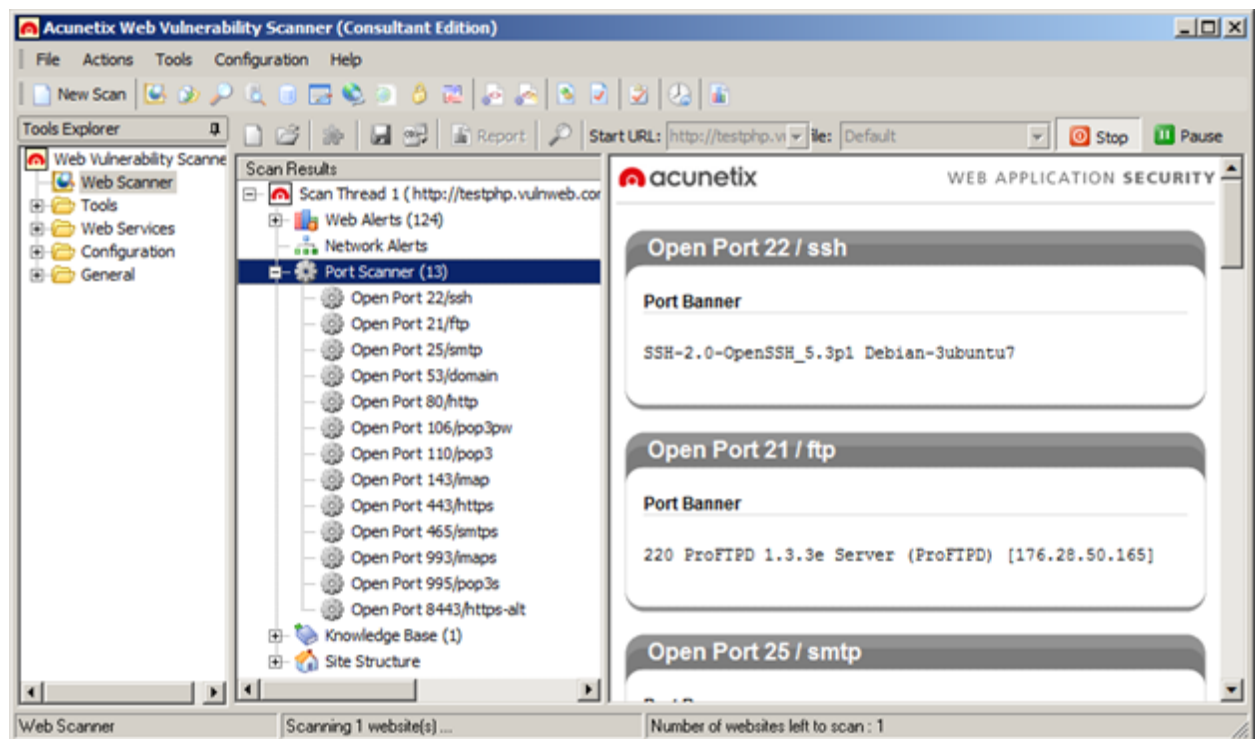
Acunetix AcuSensor Technology is a unique technology that allows you to identify more vulnerabilities than a traditional black box web security scanner, and is designed to further

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 both PHP and .NET web applications.

AcuMonitor Service

Some vulnerabilities can only be detected using an intermediate service. The Acunetix AcuMonitor service allows Acunetix Web Vulnerability Scanner to detect such vulnerabilities. Depending on the vulnerability, AcuMonitor can either report the vulnerability immediately during a scan, or send a notification email directly to the user if the vulnerability is identified after the scan has finished. More information on the AcuMonitor Service can be found at <http://www.acunetix.com/websitesecurity/acumonitor/>

Port Scanner



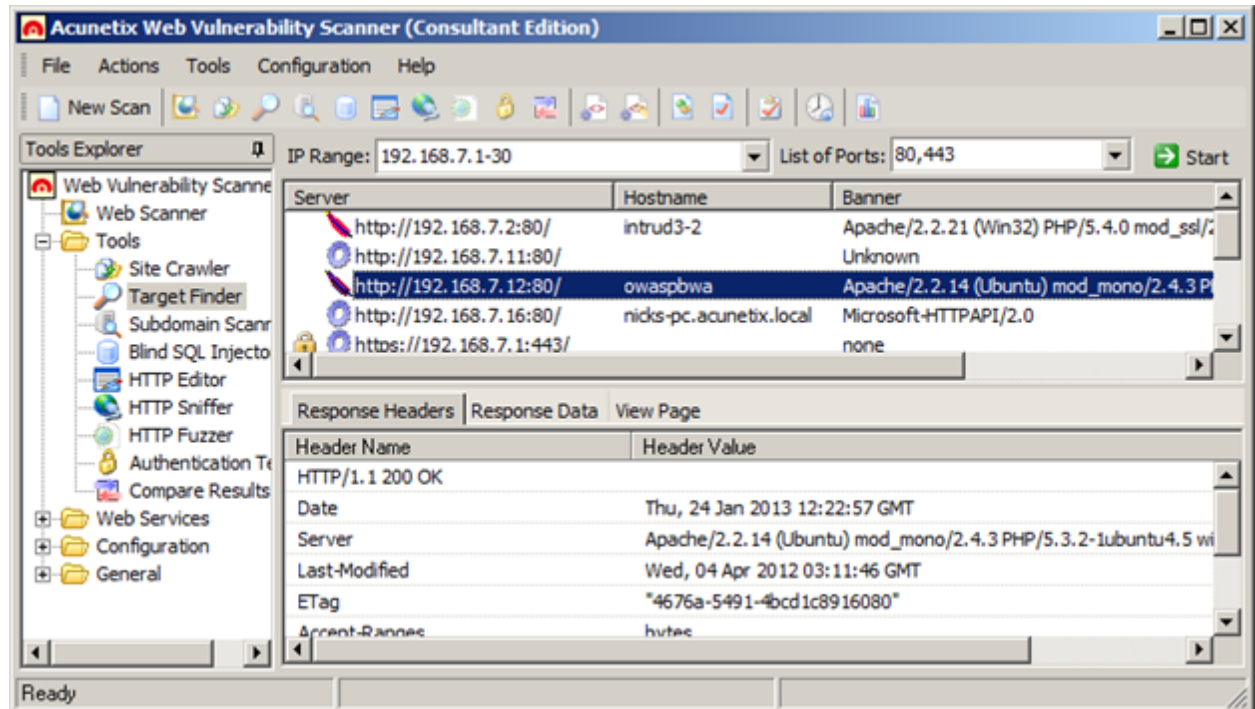
Screenshot - Port Scanning

The Port Scanner performs a port scan against the web server hosting the scanned website. Where open ports are found, Acunetix Web Vulnerability Scanner will perform network level security checks against the network service running on that port. These include 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:

<http://www.acunetix.com/blog/docs/creating-custom-checks-acunetix-web-vulnerability-scanner/>

Target Finder



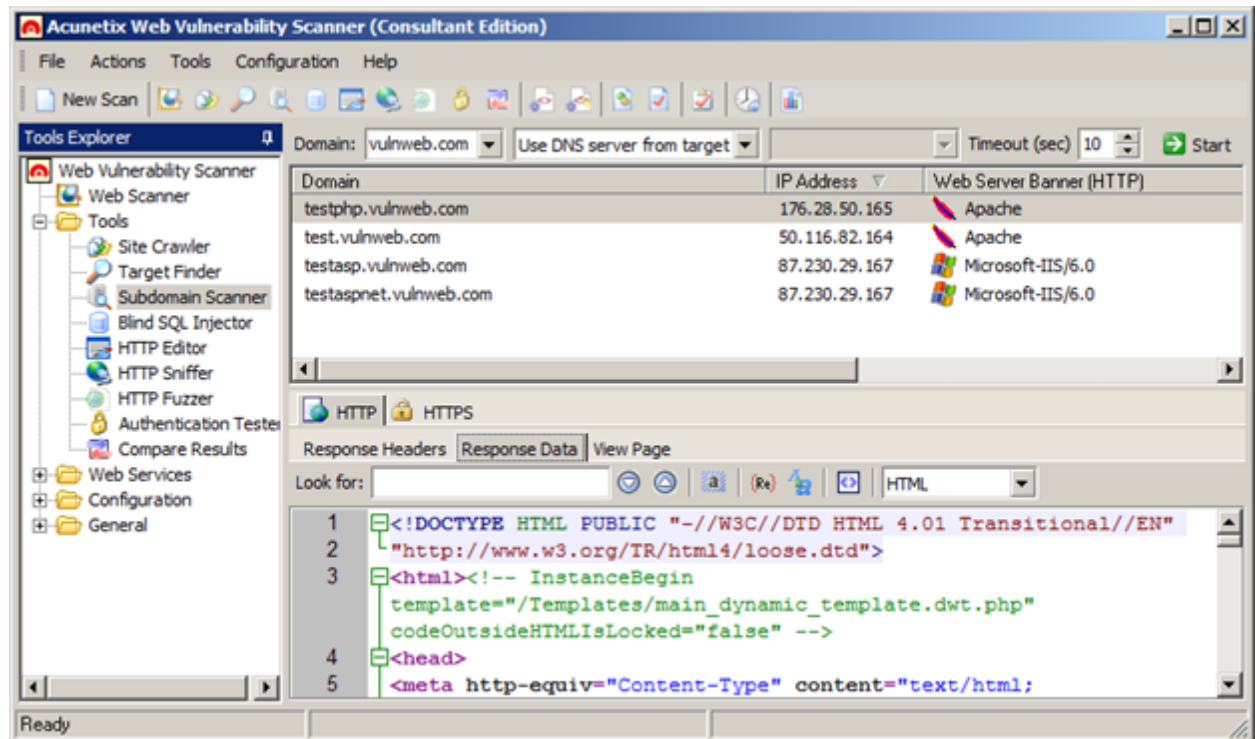
Screenshot - Target Finder

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



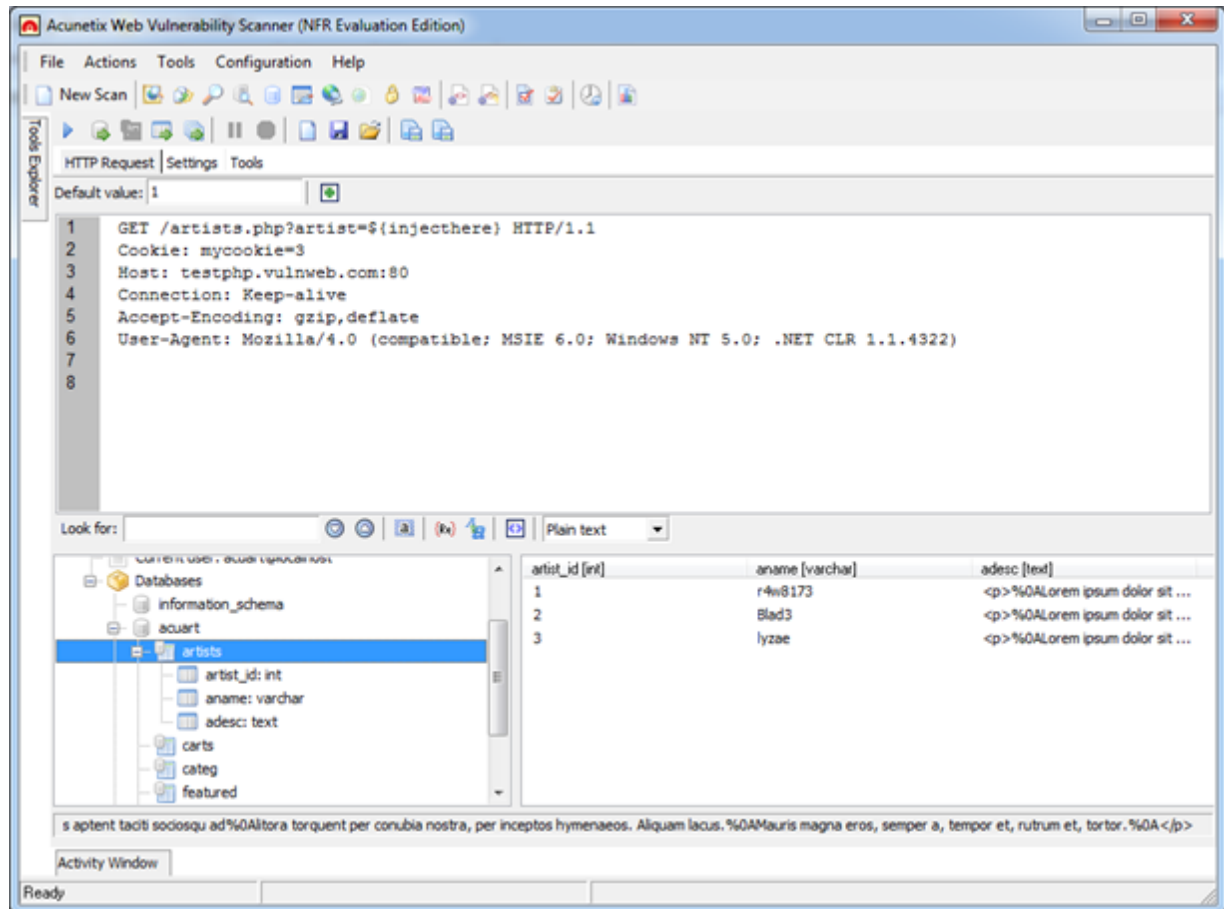
Screenshot - Subdomain Scanner

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 - Blind SQL Injector

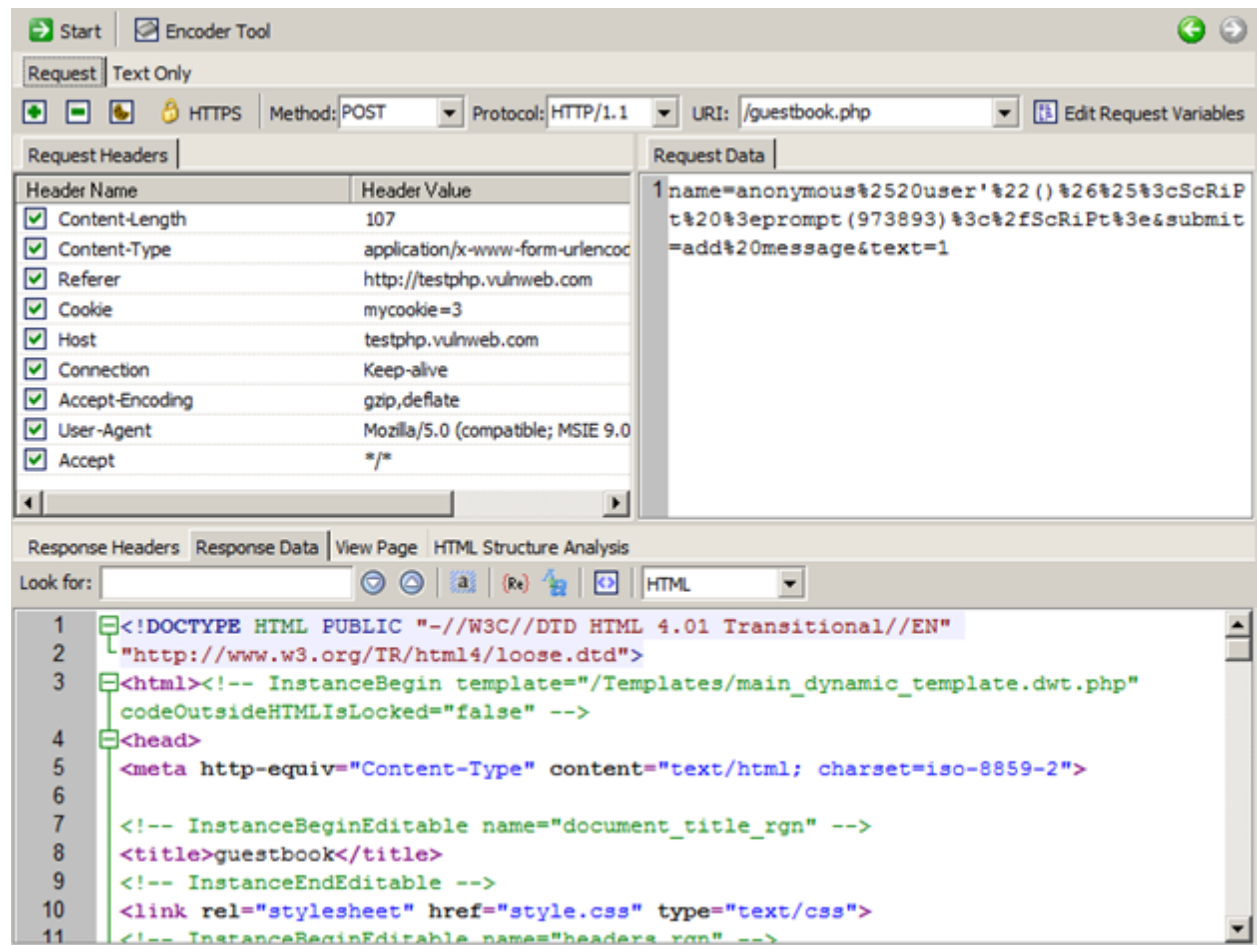
Ideal for penetration testers, the Blind SQL injector is an automated database data extraction tool with which you can make manual tests to further analyze SQL injections reported during a scan. The tool makes use of Blind SQL Injection techniques to enumerate databases and tables, dump data and also 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 - HTTP Editor

The HTTP Editor allows you to create, analyze, and edit client HTTP requests and server responses. It also contains 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

Method	Details	Information
GET	http://www.acunetix.com/	text/html; charset=UTF-8
200	OK	28 Kb
GET	http://www.acunetix.com/wp-content/the...	text/css
200	OK	1 Kb
GET	http://www.acunetix.com/wp-content/plu...	text/css
200	OK	2 Kb
GET	http://www.acunetix.com/wp-content/themes/ac...	text/css
200	OK	24 Kb
GET	http://www.acunetix.com/wp-content/the...	text/css
200	OK	465 b
GET	http://www.acunetix.com/wp-content/plu...	text/css
200	OK	484 b

1	GET / HTTP/1.1
2	Host: www.acunetix.com
3	User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:18.0) Gecko/20100101 Firefox/18.0
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

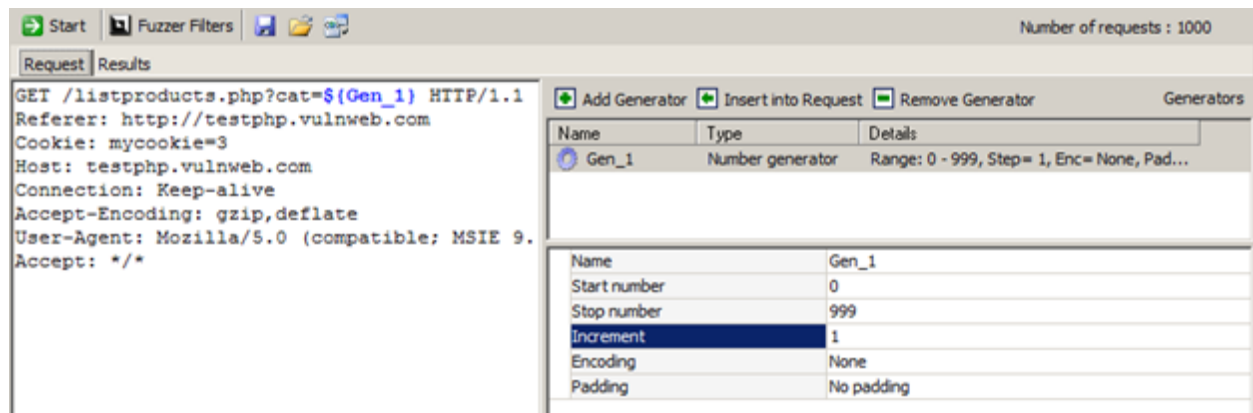
Screenshot - HTTP Sniffer

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.

HTTP Fuzzer



Screenshot - 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.

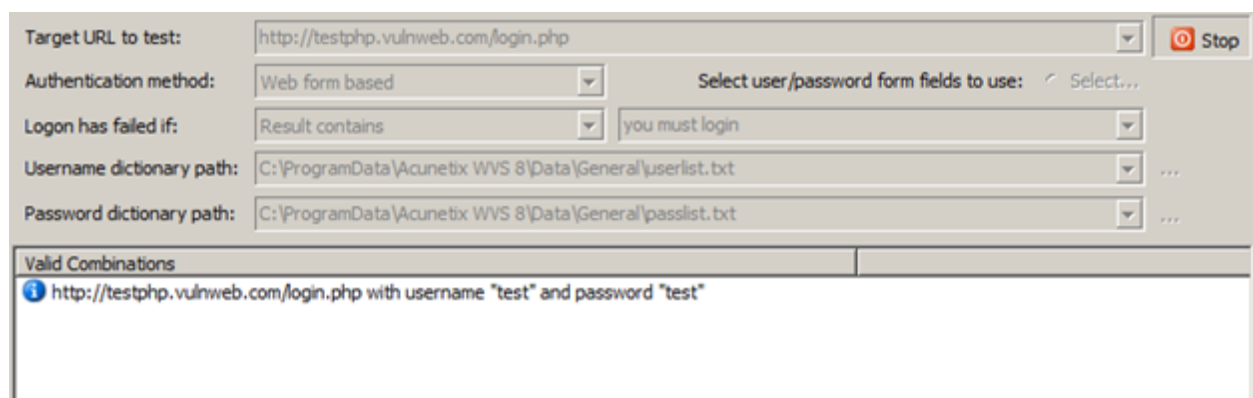
An example would be the following URL: <http://testphp.acunetix.com/listproducts.php?cat=1>

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 - Authentication Tester

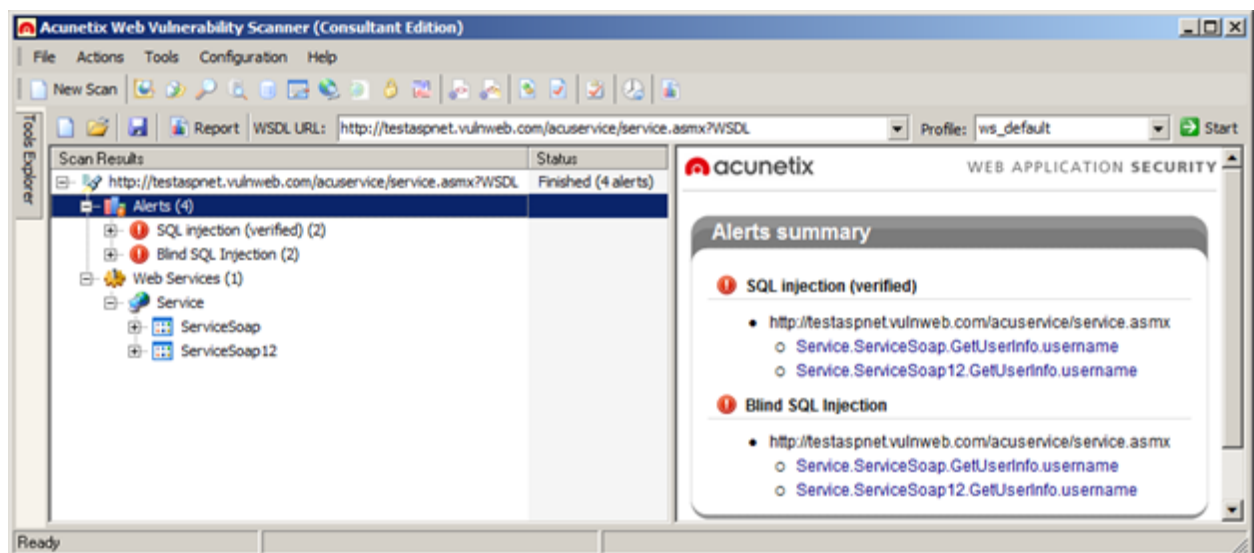
With the Authentication Tester you can perform a dictionary attack against login pages that use both HTTP (NTLM v1, NTLM v2, digest) or form based authentication. This tool uses two

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

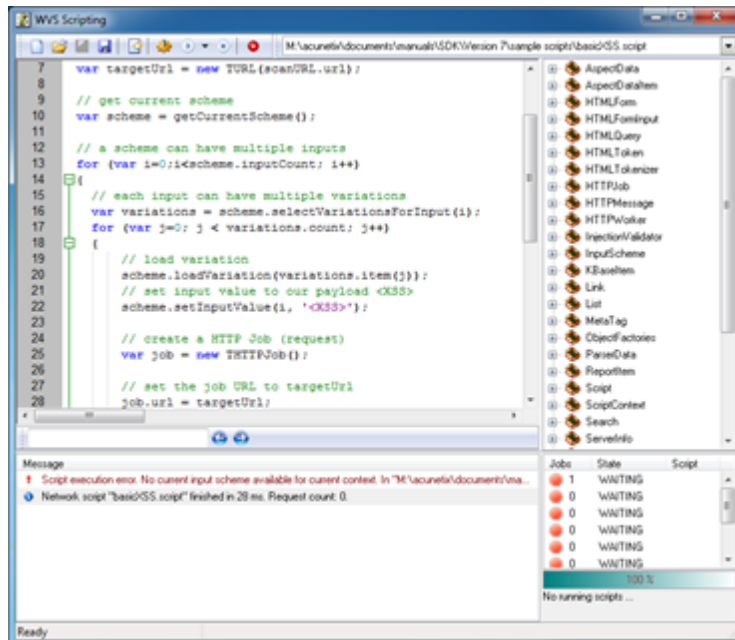


Screenshot - Web Services Scanner

The Web Services Scanner allows you to launch automated vulnerability scans against WSDL based Web Services. Web Services are commonly used to exchange data and generally vulnerabilities in Web Services can easily be exploited in order 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 – 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 Software Development Kit (SDK). You can read more about writing custom web security checks at the following URL:

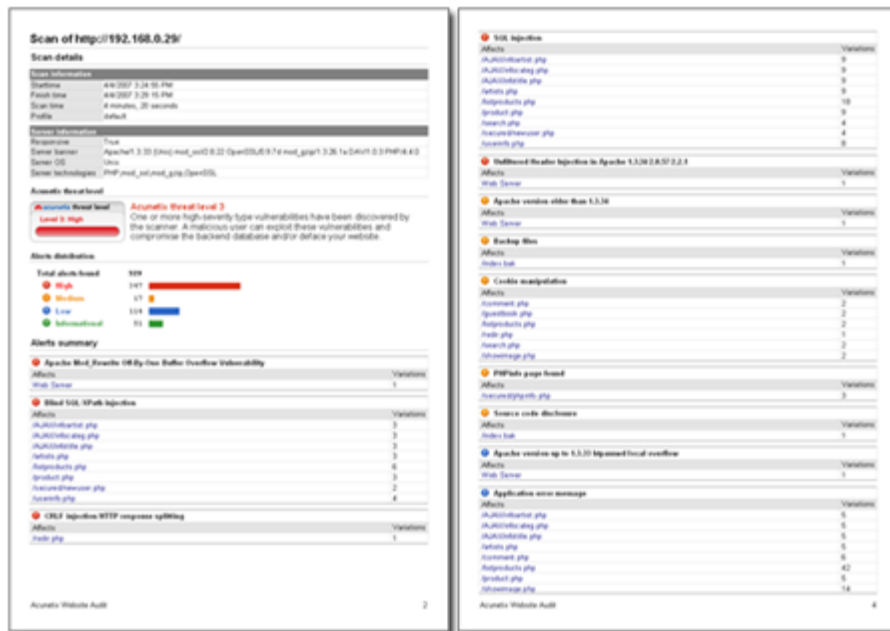
<http://www.acunetix.com/blog/docs/creating-custom-vulnerability-checks/>

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 - Typical Report including Chart of alerts

New in Acunetix Web Vulnerability Scanner Version 9

- Introduction of Acunetix DeepScan, which makes use of the same rendering engine used in Google Chrome and Apple Safari to better identify the web site's structure during a scan. Acunetix DeepScan provides a huge improvement in scanning of AJAX sites, JavaScript-based sites and Single Page Applications (SPA).
- Introduction of the Acunetix AcuMonitor service, which is used to identify specific vulnerabilities which require an intermediate server.
- Improved support in detecting and scanning smartphone / tablet friendly websites. When a mobile friendly site is scanned, the user is given the option to crawl and scan the site as a normal browser or as a smartphone browser.
- Full support for HTML5 websites.
- Detection of DOM-based XSS vulnerabilities.
- Detection of Blind XSS vulnerabilities (using AcuMonitor).
- Detection of Server Side Request Forgery (SSRF), XML External Entity (XXE), Mail Header Injection and Host Header-based vulnerabilities (using AcuMonitor).

New in Acunetix Web Vulnerability Scanner Version 9.5

- Detection of SQL Injection, XSS and other vulnerabilities in web applications implemented in Google Web Toolkit.
- Detection of vulnerabilities in JSON and XML data and HTTP HOST Headers.
- Alerts are now tagged with their CVE, CWE and CVSS.
- AcuSensor now supports .NET 4.5.
- Introduced support for CRUD (create, read, update and delete).
- New report for NIST 800-53 rev4.

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 1 year subscription or perpetual license. The 1 year subscription license expires after 1 year from the date of download or 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 one-year license.

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. This edition can also be upgraded to allow up to 10 simultaneous scans.

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 or are a 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. This edition can also be upgraded to allow up to 10 simultaneous scans.

Limitations of the Trial

The trial 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:

- The Trial edition will expire after 15 days. 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>
 - <http://testhtml5.vulnweb.com>
- The Scan Scheduler is not available.

If you decide to purchase Acunetix Web Vulnerability Scanner, you will need to uninstall the trial 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 trial 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.

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 when you purchased the license.
2. Double click the webvulnscan.exe file to launch the Acunetix Web Vulnerability Scanner installation wizard and click **Next** when prompted.
3. Review and accept the License Agreement.
4. Select the folder location where Acunetix Web Vulnerability Scanner will be installed.
5. The installation will prompt you to install a unique root certificate used for HTTPs traffic and to create a desktop shortcut.
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.

Registering with AcuMonitor Service



Screenshot - AcuMonitor Registration

When you start Acunetix Web Vulnerability Scanner the first time, you will be asked to register with the AcuMonitor Service. The AcuMonitor Service is used to automatically detect certain vulnerabilities which can only be detected using an intermediate server, such as Blind XSS, Server Side Request Forgery (SSRF) and Email Header Injection.

You can register to the AcuMonitor service using your email address and your license key. Registration can also be done at a later stage from Acunetix Web Vulnerability Scanner > Configuration > Application Settings > AcuMonitor. More information on the AcuMonitor Service can be found at

<http://www.acunetix.com/vulnerability-scanner/acumonitor-blind-xss-detection/>.

Installing AcuSensor in your web application

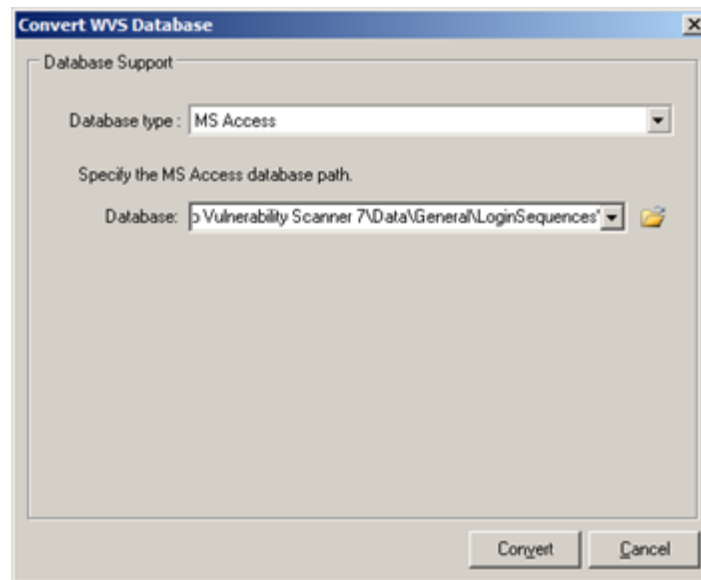
If you need to scan a .NET or PHP web application, you should [install Acunetix AcuSensor on your web application](#) in order to improve the detection of vulnerabilities, get the line in the source code where vulnerabilities are located and to decrease false positives.

Upgrading Acunetix Web Vulnerability Scanner

It is recommended that you backup your settings before proceeding with the upgrade as per <http://www.acunetix.com/blog/docs/backup-acunetix-settings-customizations/>.

To upgrade a previous version of Acunetix Web Vulnerability Scanner to the latest version:

1. Close all instances of Acunetix Web Vulnerability Scanner (and related utilities such as the Reporter)
2. Optionally backup the Login Sequences if you would like to use these in the newer version. Depending on the version, these can be copied from <C:\Program Files (x86)\Acunetix\Web Vulnerability Scanner X\Data\General\LoginSequences'> for version 7 or older or <C:\Users\Public\Documents\Acunetix WVS X\LoginSequences> for newer versions.
3. Optionally backup the Reporting Database if you would like to use it in the newer version. If you are using an Access Database, the default location of the database is <C:\Program Files (x86)\Acunetix\Web Vulnerability Scanner X\Data\Database\vuInscanresults.mdb>
4. From the Acunetix Web Vulnerability Scanner Program Group, select to uninstall the product.
5. Install the newer version of Acunetix Web Vulnerability Scanner.
6. To restore the Login Sequences, copy the files backed up in (2) to <C:\Users\Public\Documents\Acunetix WVS X\LoginSequences>
7. If upgrading from version 7, the Reporting database needs to be updated before it can be used in a newer version. 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:
 - 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 the new version of Acunetix Web Vulnerability Scanner to use the upgraded database.



Screenshot - Upgrade Reporting Database

- 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 X\Data\Database\vulnscanresults.mdb>

Installing AcuSensor

Acunetix AcuSensor increases the efficiency of an Acunetix scan by improving the crawling, detection and reporting of vulnerabilities, while decreasing false positives. Acunetix AcuSensor can be used on .NET and PHP web applications.

Installing the AcuSensor Agent

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

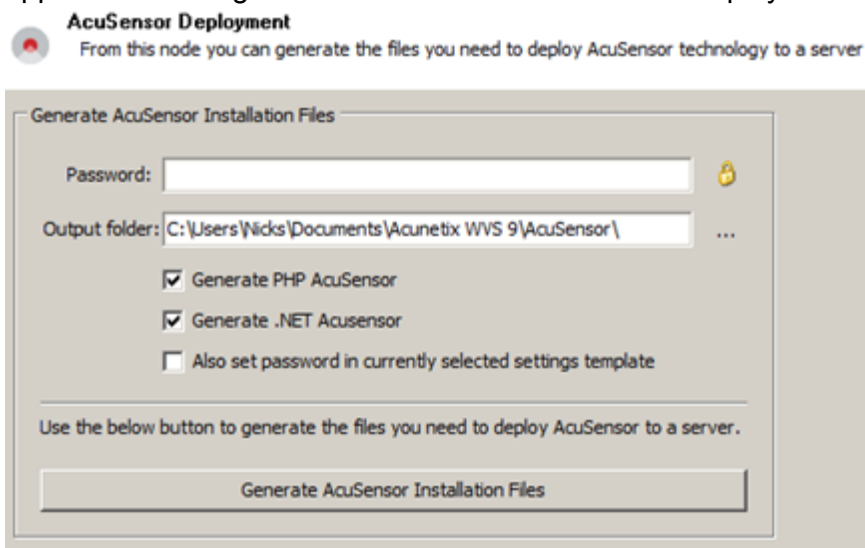
The unique Acunetix AcuSensor Technology identifies more vulnerabilities than a black box Web Application Scanner while generating less false positives. In addition, it indicates exactly where vulnerabilities are detected in your code and also reports debug information

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

First you will need to generate your unique AcuSensor files. Proceed as follows:

1. If using Acunetix WVS, open Acunetix WVS and navigate to the 'Configuration > Application Settings' node. Click on the 'AcuSensor Deployment' node.



Screenshot – AcuSensor Deployment settings node

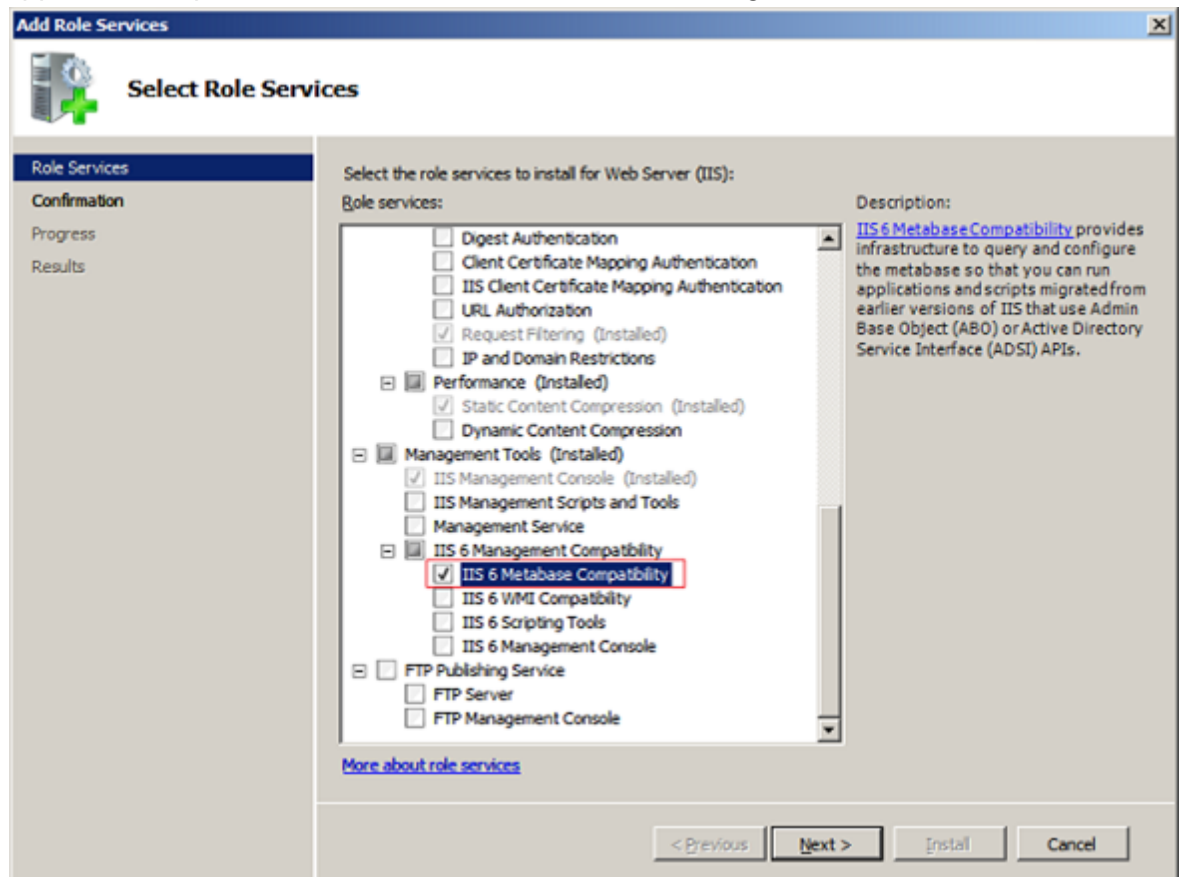
2. If using Acunetix Online Vulnerability Scanner, you can generate the AcuSensor files from the Scan Target's configuration. From Acunetix OVS, change to Scan Targets > List Scan Targets > Click on the Scan Target's name. Skip to step 6.
3. Enter a password or click on the padlock icon to randomly generate a password unique to the AcuSensor file.
4. Select 'Also set password in currently selected settings template' to store the password specified in the scan settings template.
5. Specify the path where you want the AcuSensor files to be generated.
6. Select whether to generate files for a PHP website or a .NET website.
7. Click on **Generate AcuSensor Installation Files** to generate the files.

8. Depending on if you are using an 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

The AcuSensor agent will need to be installed in your web application. This section describes how to install AcuSensor in an ASP.NET web application.

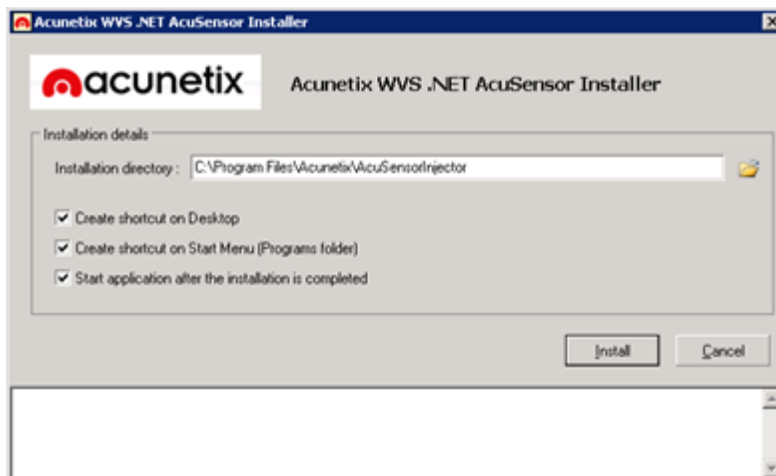
1. **Install Prerequisites on the server hosting the website:** The AcuSensor installer application requires Microsoft .NET Framework 3.5 or higher.



Screenshot - Enable IIS 6 Metabase Compatibility on Windows 2008

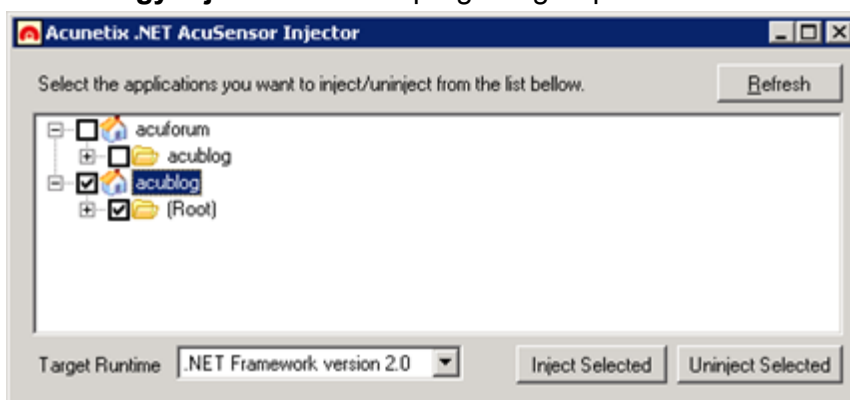
On Windows 2008, you must also install IIS 6 Metabase Compatibility from 'Control Panel > Turn Windows features On or Off > Roles > Web Server (IIS) > Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility' to enable listing of all .NET applications running on server.

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



Screenshot – 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 – 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

This section describes how to install AcuSensor in an ASP.NET web application.

1. Locate the PHP AcuSensor file of the website you want to install AcuSensor on. Copy the **acu_phpaspect.php** file to the remote web server 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 reinstall them on your website.

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

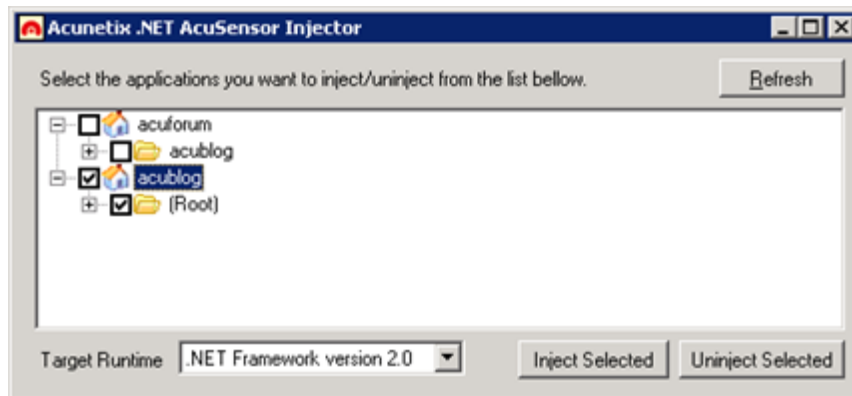
1. Use the procedure in the next section to Disable and Uninstall the AcuSensor agent.
2. Configure a new password.
This step can be omitted if you are using Acunetix Online Vulnerability Scanner, since a new unique and secure password is automatically generated each time the AcuSensor files are generated. The unique password is stored with the Scan Target's settings.
3. Click on Generate AcuSensor installation files.
4. Proceed with installing the new AcuSensor files. If you are using a PHP web application, you will just need to overwrite the old **acu_phpaspect.php** with the new **acu_phpaspect.php** file.

Disabling and uninstalling AcuSensor

To uninstall and disable the sensor from your web site:

AcuSensor for ASP .NET websites

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



Screenshot - 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 from 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 code will not be removed from your .NET application.

AcuSensor for PHP

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

Note: Although the Acunetix AcuSensor agent requires authentication, it is recommended that the AcuSensor client files are uninstalled and removed from the web application if they are no longer in use.

Scanning a Website

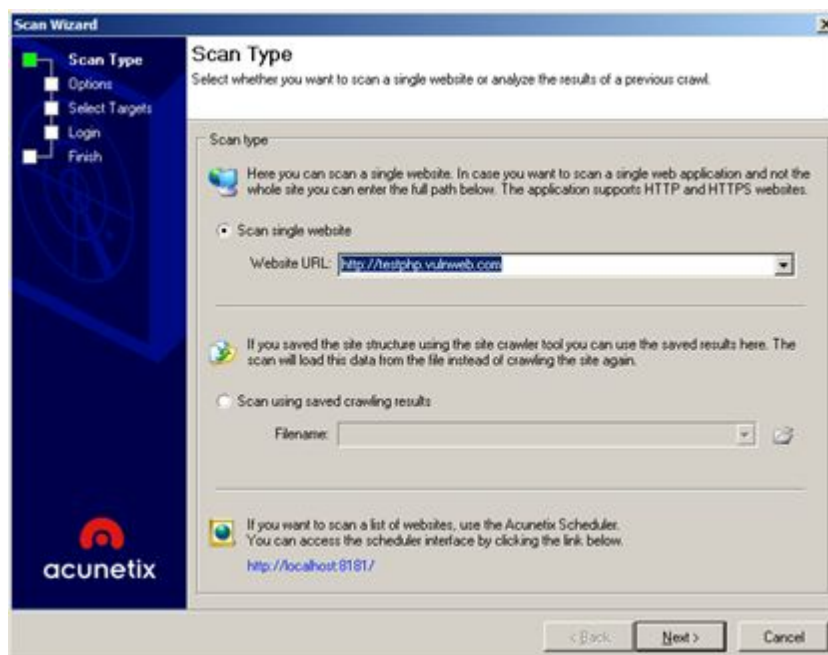
NOTE: DO NOT SCAN A WEBSITE WITHOUT PROPER AUTHORIZATION!

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.

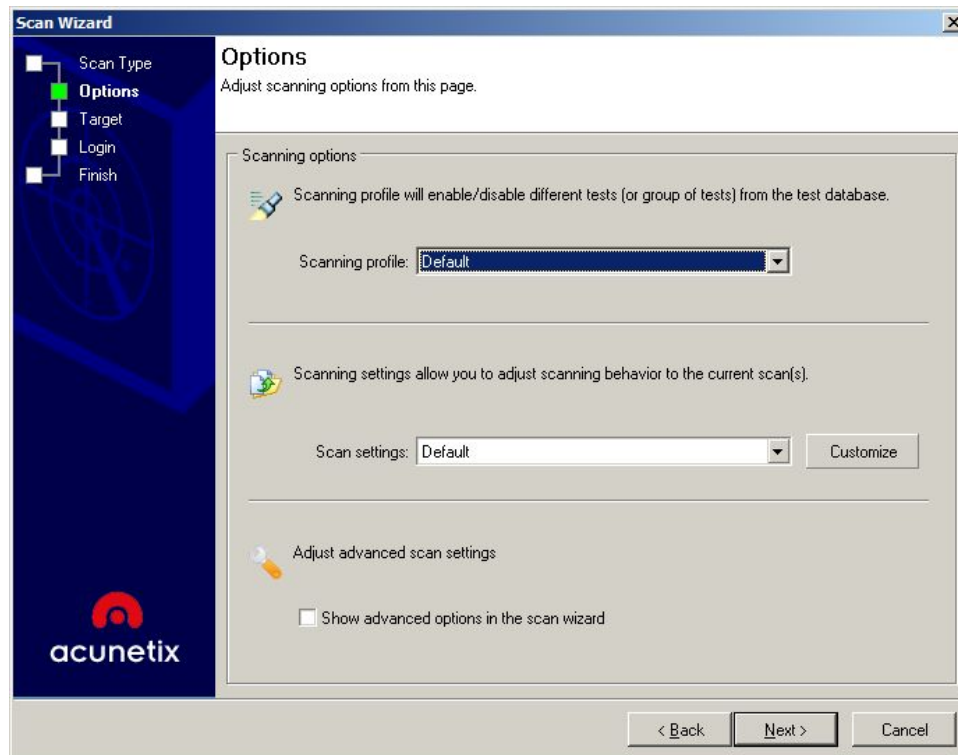


Screenshot - Scan Wizard: Select Scan Type

2. Specify the scan options:
 - a. Scan single website - Enter the URL of the target website, e.g. <http://testphp.vulnweb.com>.
 - b. 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.
3. Click **Next** to continue.

Note: The [Acunetix Web Vulnerability Scanner Scheduler](#) can be used to scan websites at a specific time and to configure recurring scans.

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



Screenshot – 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 for more information on how to customize or create scanning profiles.

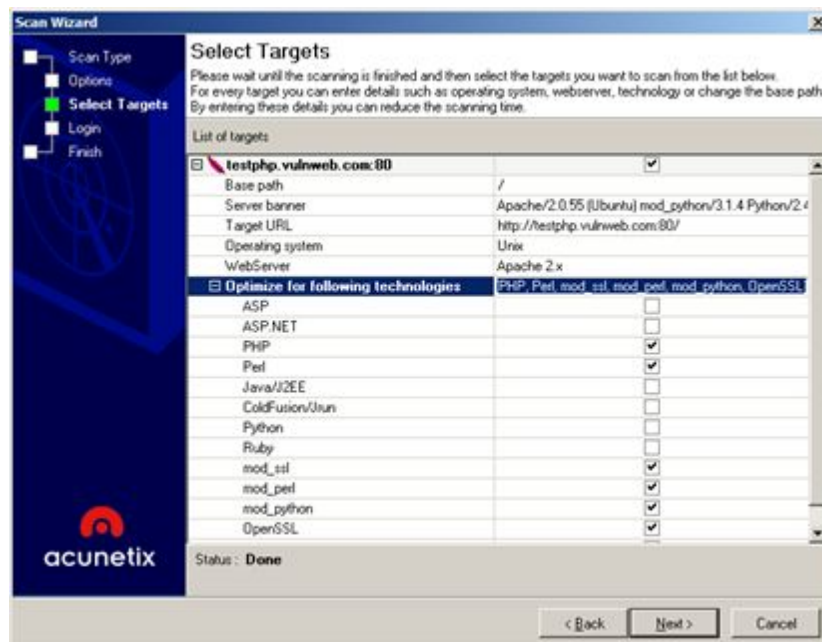
Scan Settings template

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 for more information on how to customize or create new Scan Settings templates.

Advanced Crawling Options

Tick the option **Show advanced options in the scan wizard** to proceed to the Advanced Crawl options, allowing you to [pre-seed a crawl using Selenium scripts](#), [Fiddler Session Archives](#), [Burp Saved files](#) and [Acunetix HTTP Sniffer log files](#). You can also configure the Acunetix to show you the list of files identified by the Crawler, giving you the option to choose which files to scan.

Step 3: Confirm Targets and Technologies Detected



Screenshot – 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 and its web server technologies. 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, only that there are no vulnerability tests exclusive to that technology.

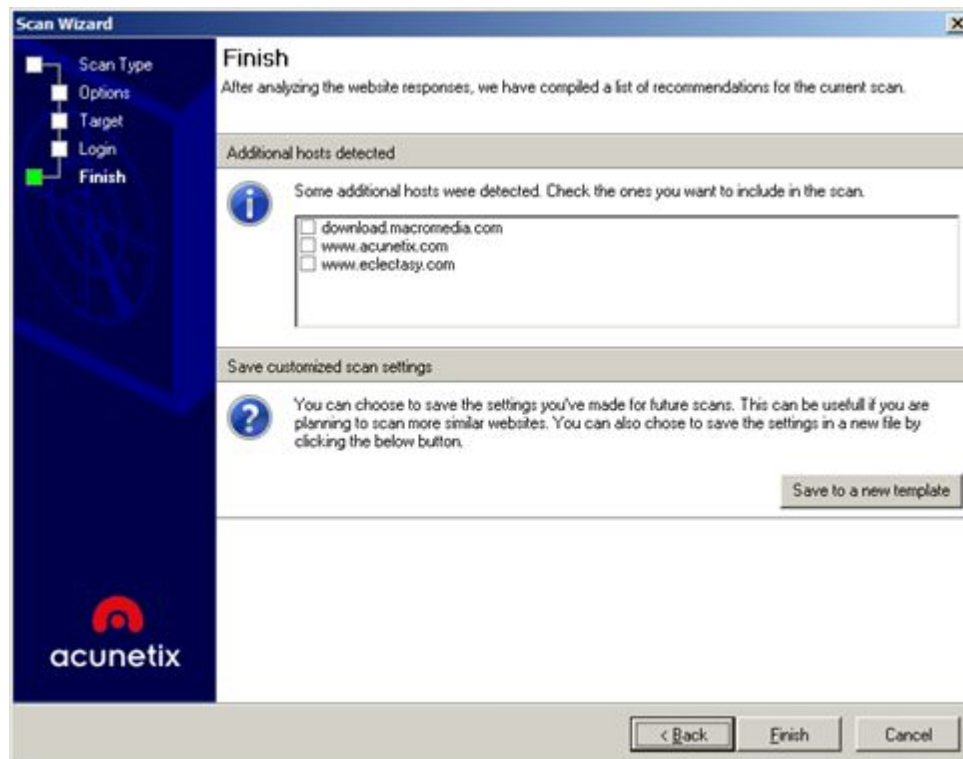
Step 4: Configure Login for Password Protected Areas

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. Scanning an HTTP password protected area requires that you either enter the credentials during the crawling of your web application, or you have the credentials pre-configured in Acunetix. This is covered in more detail [here](#).

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. Scanning websites using forms-based authentication is done using the Login Sequence Recorder and is covered in more detail [here](#).

Step 5: Finalize Scan Options



Screenshot - Finalize Scan Options

Before the Scan is started, the Scan Wizard will report issues which might hinder the scan. The following is a list of actions which you might be presented with:

- 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. [Read more](#) about configuring Acunetix to handle Custom 404 error pages.
- 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 running PHP or .NET, you will get an error if the AcuSensor agent is not detected. Click the **Customize** button to [install AcuSensor on the target web application](#).
- If additional hosts have been found to be linked to from the web site being scanned, you can optionally select to scan these too. You will require permissions to scan the selected hosts too.
- If a smartphone friendly version of the website is detected, you will be given the option to crawl and scan the site as a normal browser or a mobile browser.
- If you have made changes to the Scan Settings template, you will be asked if you want to save the modifications to the existing or new template.

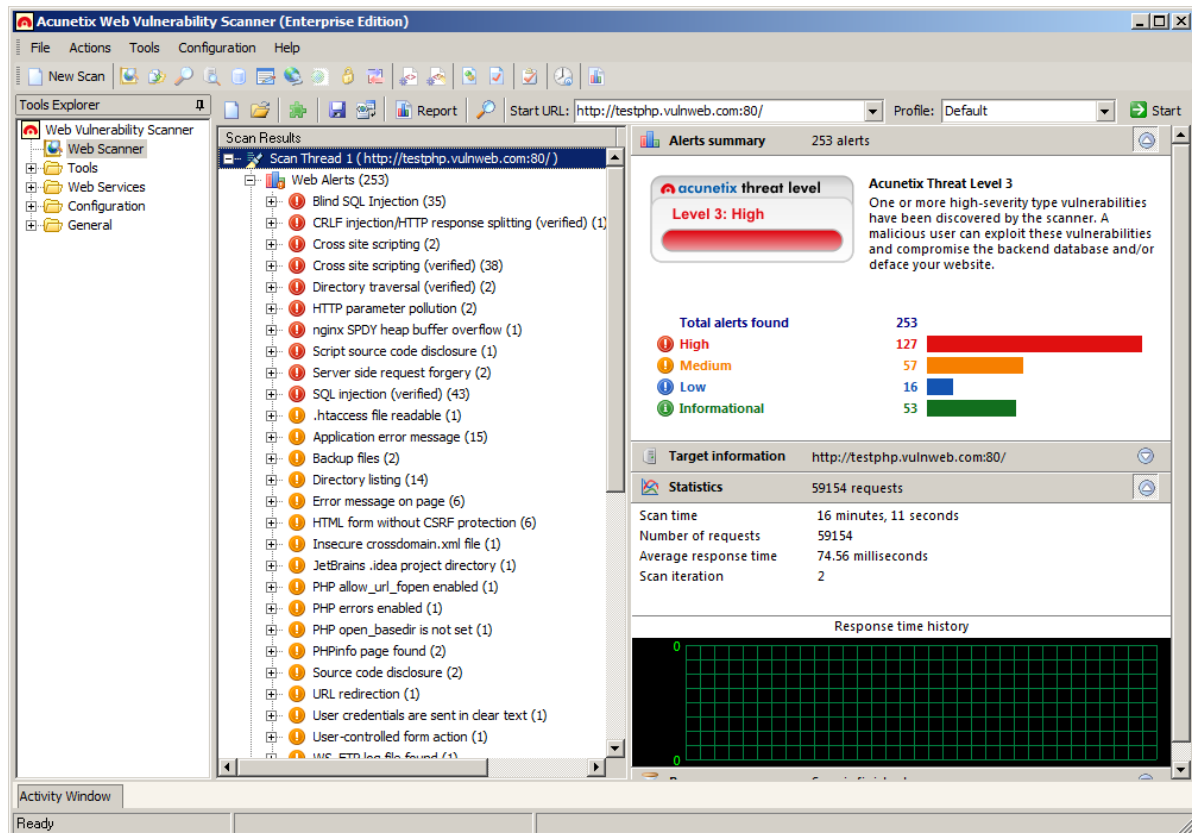
Step 6: Start the scan

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's response time, a scan may take several hours.

Analyzing the Scan Results

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 - Scan Results showing Alerts Summary

Web Alerts

The Web Alerts node displays all vulnerabilities found on the target website. Web Alerts are categorized according to 4 severity levels:



High Risk Alert Level 3 – Vulnerabilities categorized as the most dangerous, which put a site at maximum risk for hacking and data theft.



Medium Risk Alert Level 2 – Vulnerabilities caused by server misconfiguration and site-coding flaws, which facilitate server disruption and intrusion.



Low Risk Alert Level 1 – Vulnerabilities derived from lack of encryption of data traffic, or directory path disclosures.



Informational Alert – These are items which have been discovered during a scan and which are deemed to be of interest, e.g. the possible disclosure of an internal IP address or email address, or matching a search string found in the Google Hacking Database

More information about the vulnerability is shown when you click on an alert category node:

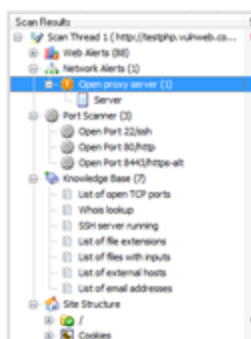
- **Vulnerability description** - A description of the discovered vulnerability. The AcuSensor logo is displayed in the Vulnerability Description for the vulnerabilities that are detected using the AcuSensor Technology.
- **Affected items** - The list of files vulnerable to the discovered vulnerability.
- **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 <http://www.acunetix.com/blog/docs/http-editor/>.
- **How to fix this vulnerability** - Guidance on how to fix the vulnerability.
- **Detailed information** - More 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 - 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 into 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 enabled or disabled from Acunetix WVS > Configuration > Scan Settings > Scanning Options > Enable Port Scanning.

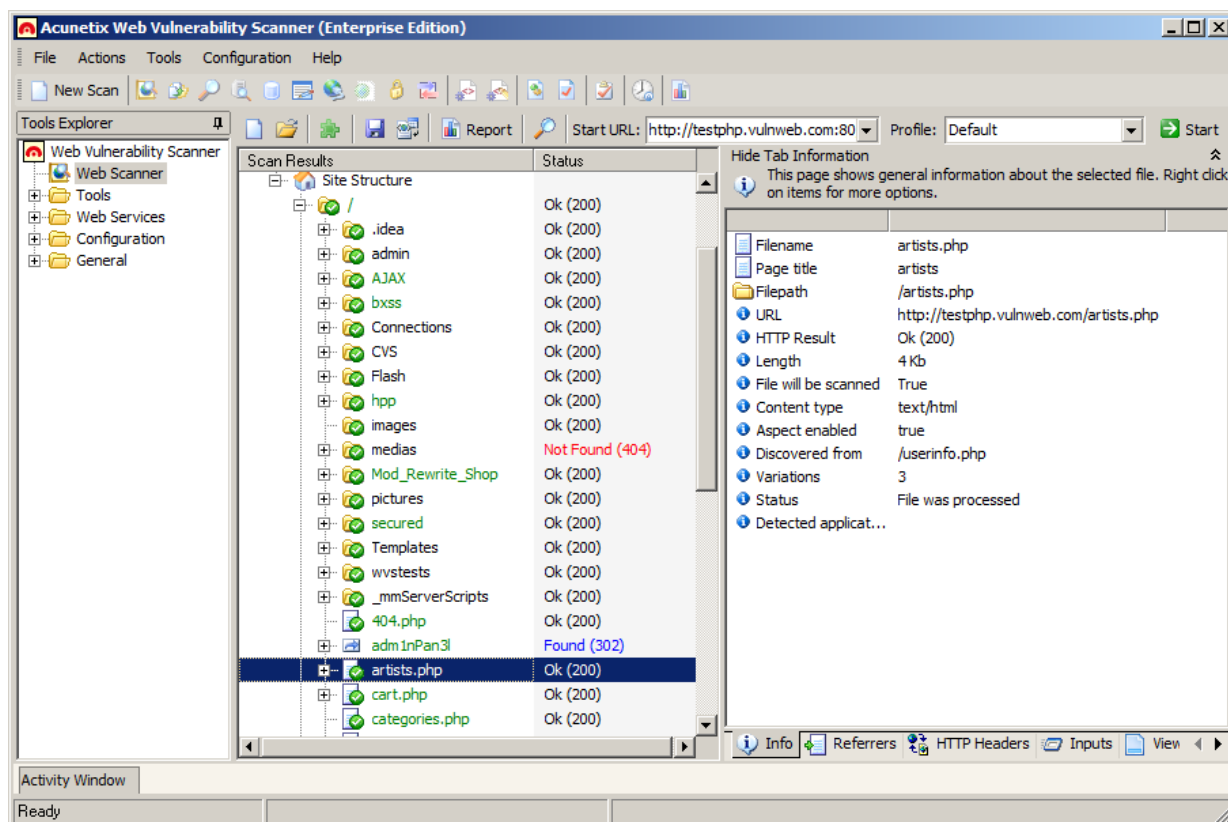
Knowledge Base

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. The 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 - Site Structure

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:

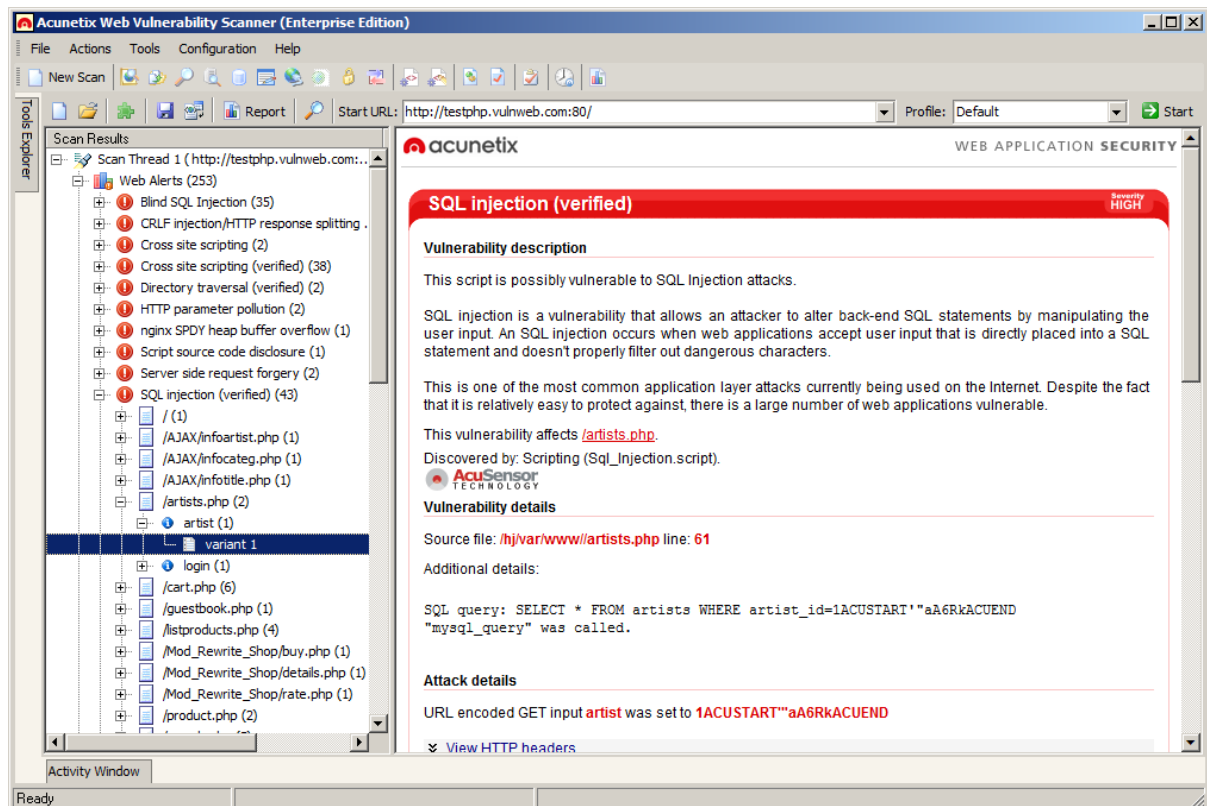
- **Info** - Generic information such as file name, page title, path, length, URL etc.
- **Referrers** – The files or pages that linked to the tested file.
- **HTTP Headers** - The HTTP headers of the request sent to the web server to retrieve the selected file, and the HTTP response headers received.
- **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.

- **AcuSensor Data** – Any AcuSensor Technology data returned.
- **Alerts** – A list of alerts for the selected file.

In addition, each item contains the **HTML Structure Analysis**, which includes:

- 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. This 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.

Grouping of Vulnerabilities



Screenshot – Grouping of vulnerabilities

If the same type of 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.

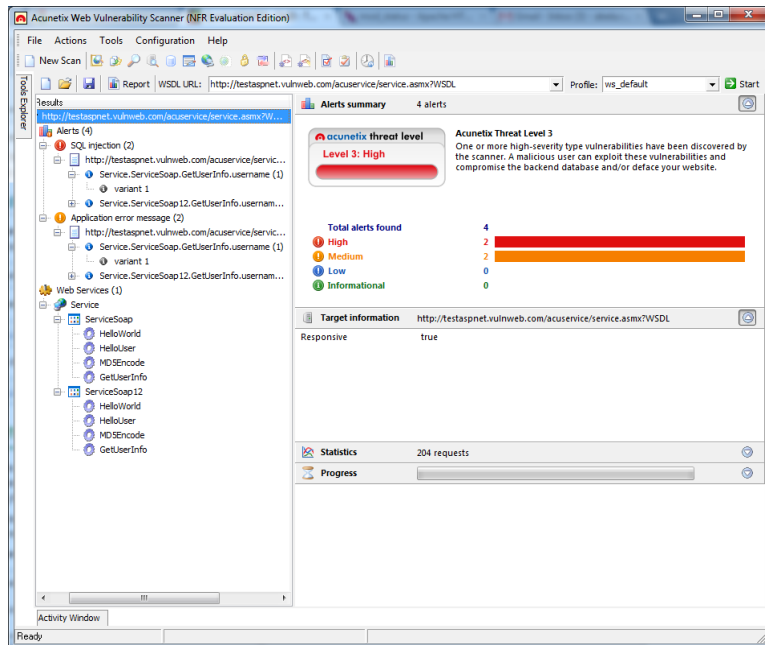
Saving / Loading Scan Results

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**.

Scanning Web Services

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.

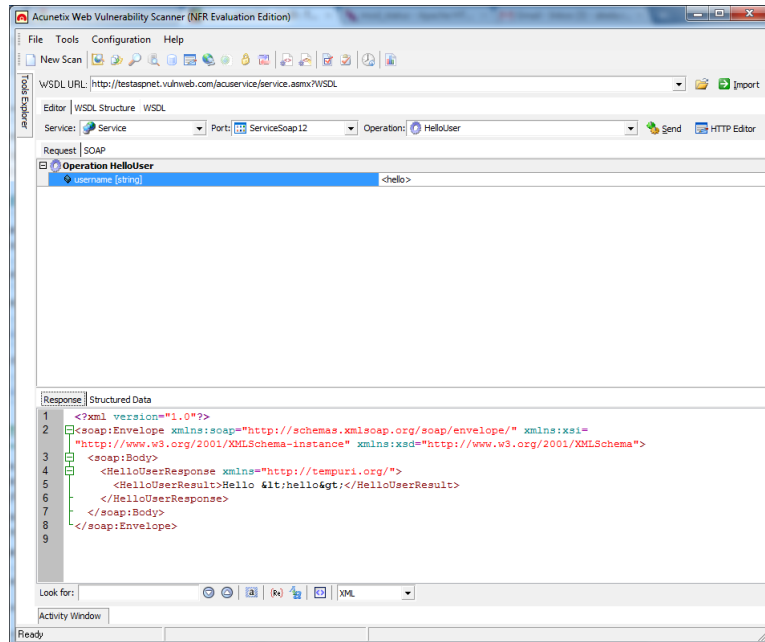


Screenshot 66 – Web Services Scanner

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 67 – 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 WSDL and Sending Request

1. Click on the 'Web Services Editor' node in the tools explorer and enter the URL of the WSDL, or locate the local directory where the local WSDL file is stored. Click **Import** to import all WSDL information.
2. 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.

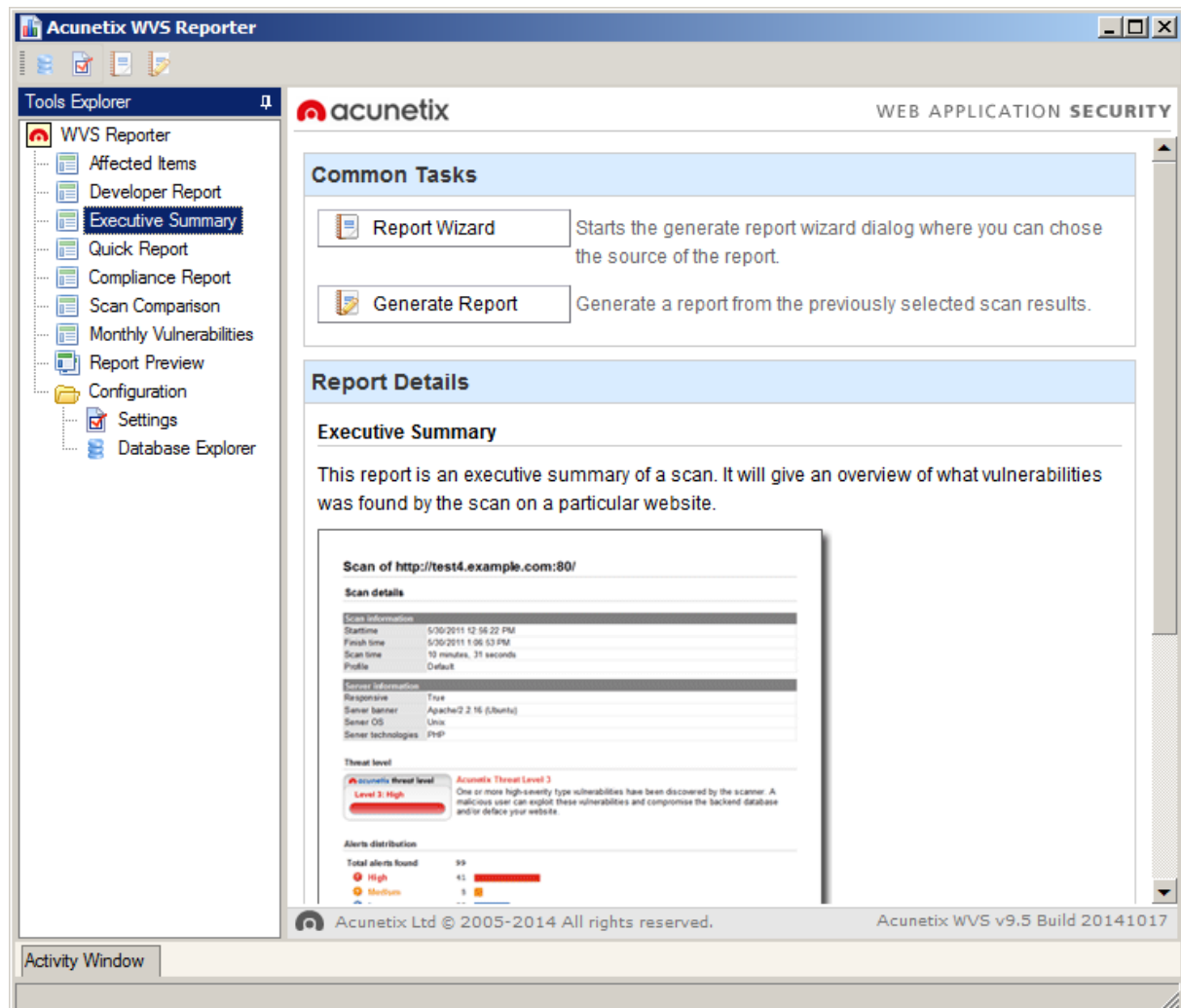
WSDL Tab

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

HTTP Editor Export

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


Generating Reports

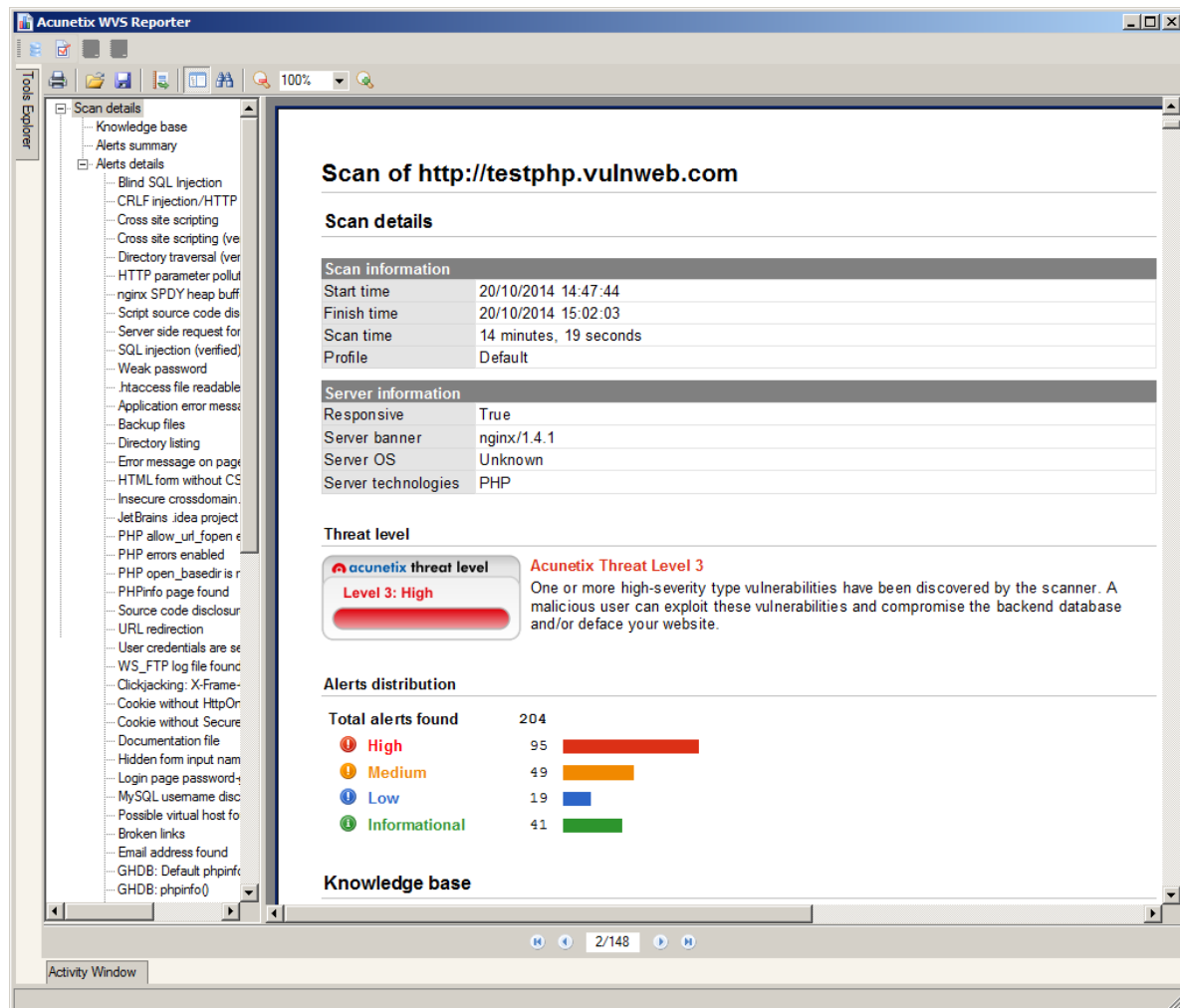


Screenshot – The Reporter Application

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 the 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 compares 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 – 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 - 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'.

Compliance Report Wizard

Report Style
Filter Scans
Select Scan
Properties

Filter Scans

If you have a big database of scan results you may want to filter the results displayed on the selection page.

☒ Display all scans

☐ Filter displayed scans

Filters

☐ Number of scans to show 25

☐ Filter by start URL (target)

☐ Filter by date

☐ Hide not responsive

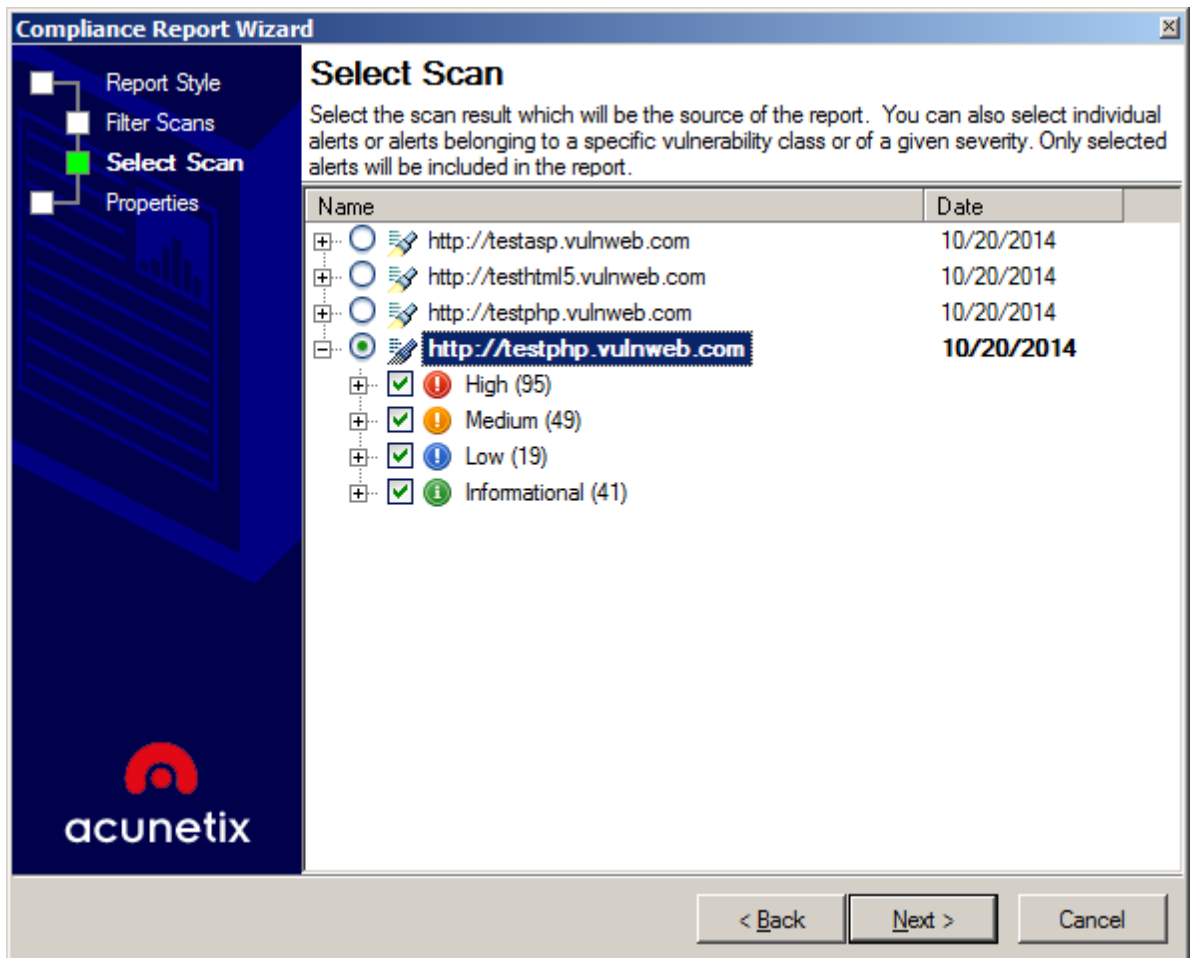
☐ Hide aborted

< Back Next > Cancel

acunetix

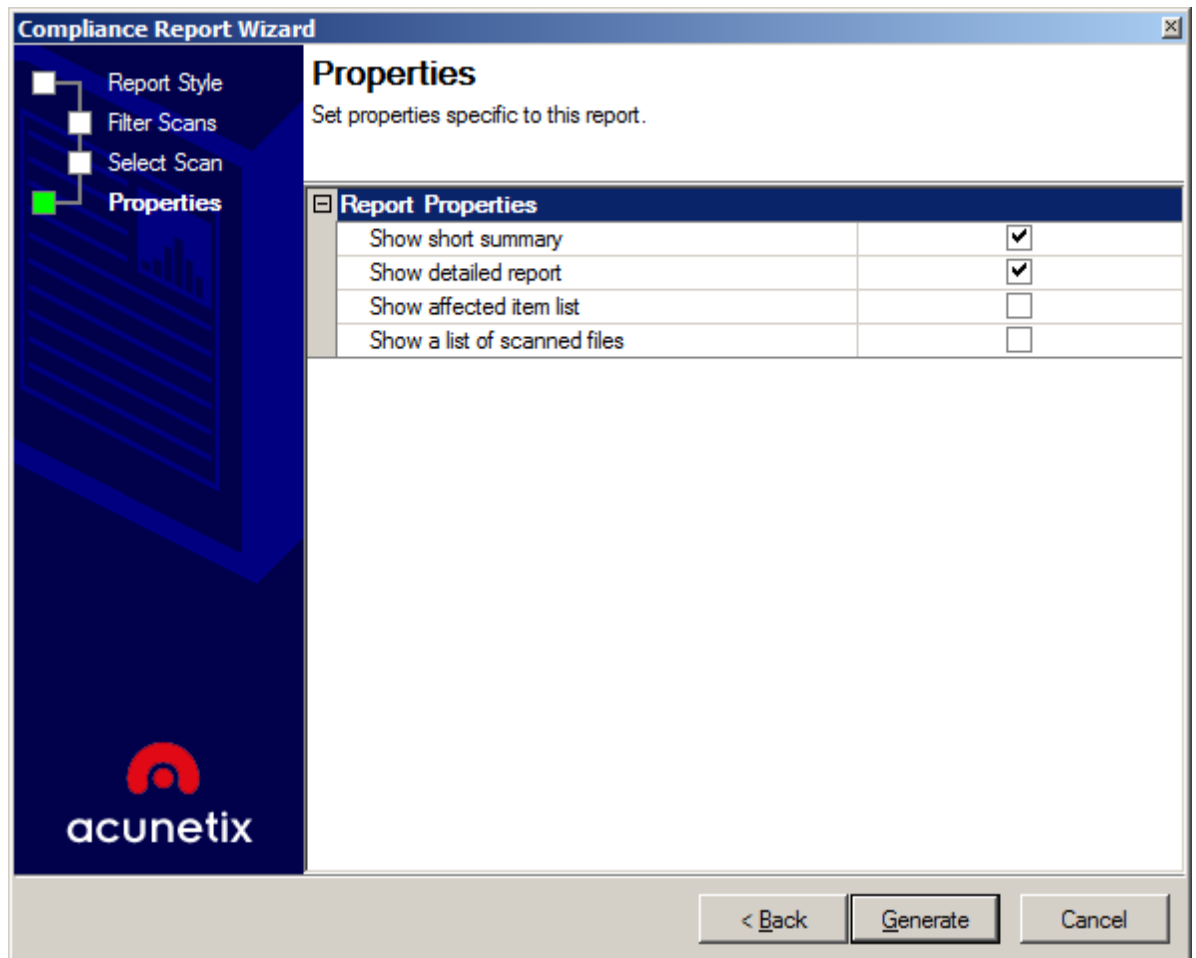
Screenshot - Filter Scans

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



Screenshot - 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.



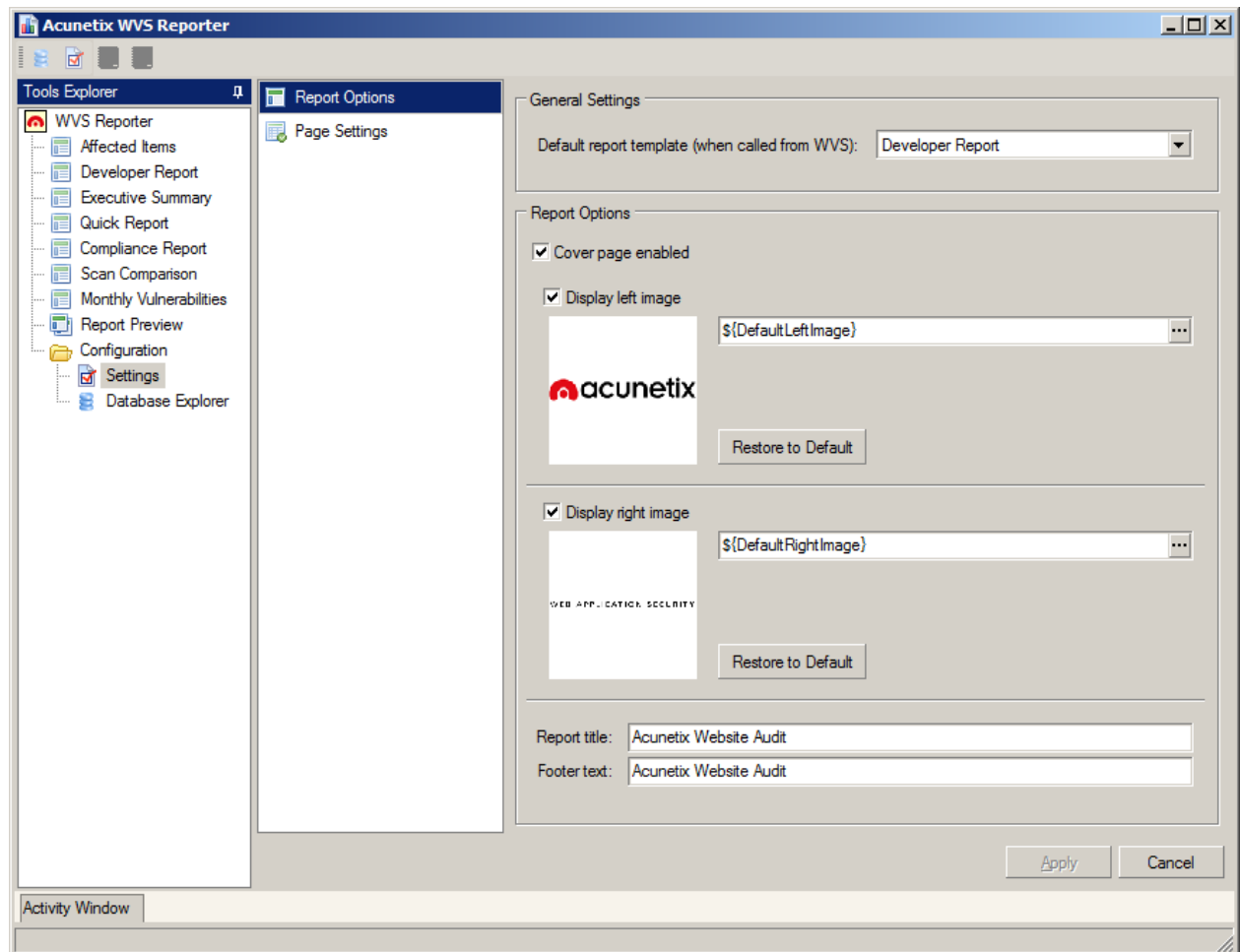
Screenshot - Select Report Properties

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

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 - 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. Only SQL Authentication is supported.
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 with 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.

Acunetix Reports

The following is a list of the reports that can be generated from Acunetix Web Vulnerability Scanner (WVS) and Acunetix Online Vulnerability Scanner (OVS):

Affected Items Report

Availability: OVS and WVS

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

Availability: OVS and WVS

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

Availability: OVS and WVS

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

Quick Report

Availability: OVS and WVS

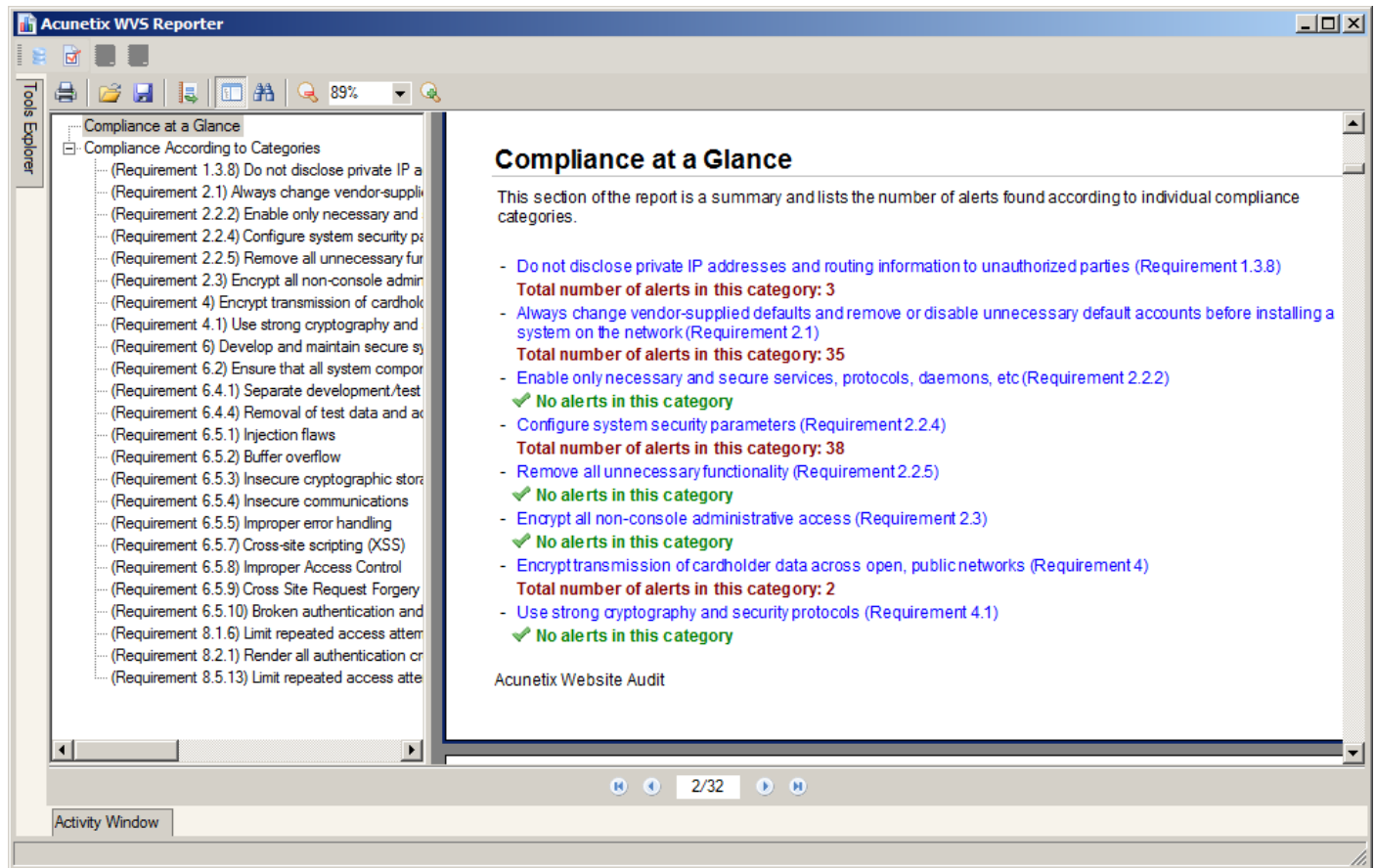
The Quick Report provides a detailed listing of all the vulnerabilities discovered during the scan.

Network Security Report

Availability: OVS only

The Network Security Report provides detailed security information about the perimeter network server scanned by Acunetix Online Vulnerability Scanner. This information is very useful for a network security auditor or pen tester who is tasked with analysing the security of the perimeter network.

Compliance Reports



Screenshot – PCI Compliance Report

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

CWE / SANS - Top 25 Most Dangerous Software Errors

Availability: OVS and WVS

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)

Availability: OVS and WVS

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

Availability: OVS and WVS

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

Availability: OVS and WVS

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 2013

Availability: OVS and WVS

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

Availability: OVS and WVS

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

Availability: OVS and WVS

The Sarbanes Oxley Act was enacted 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

Availability: OVS and WVS

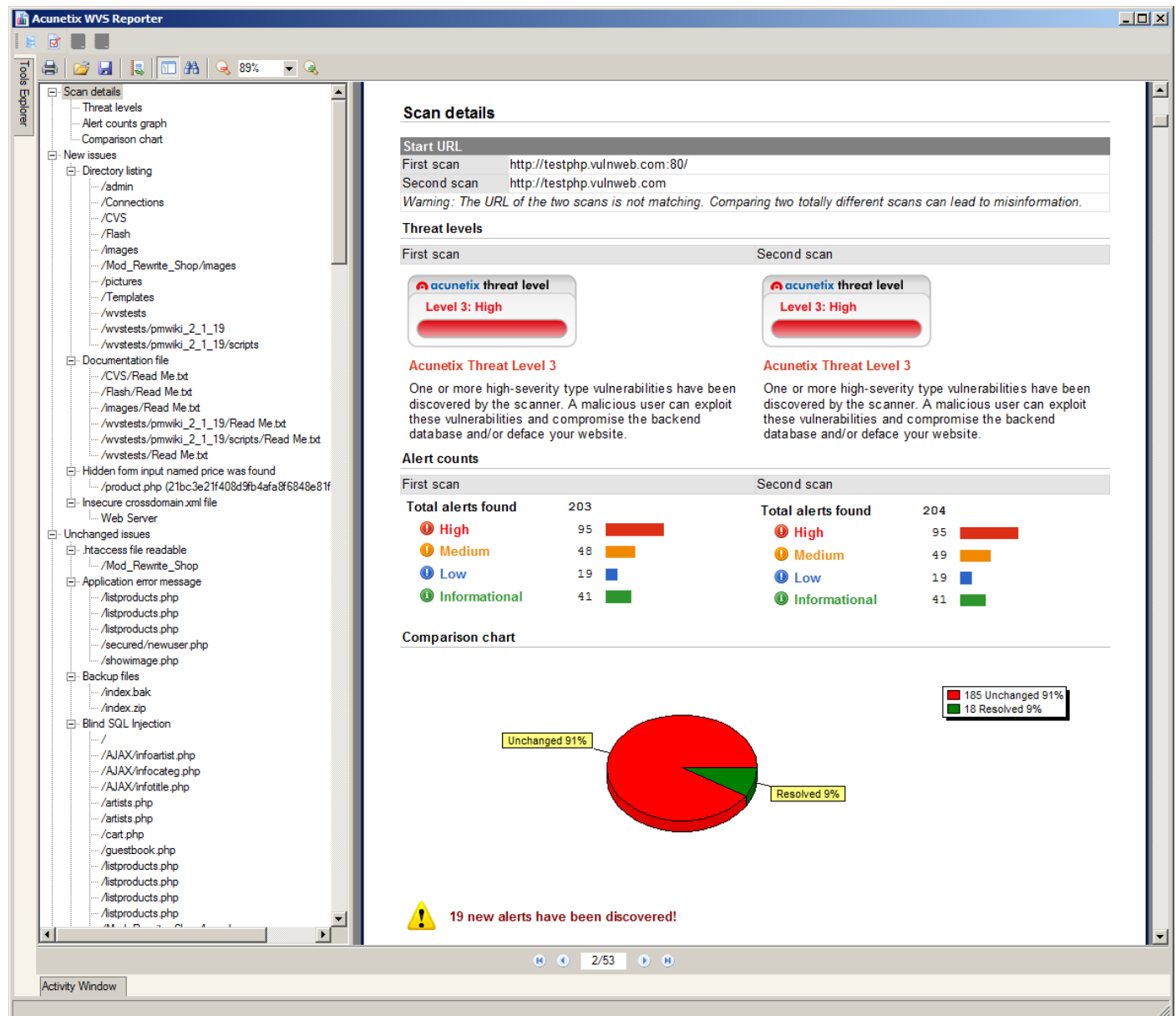
The Security Technical Implementation Guide (STIG) is a configuration guide for computer software and hardware defined by the Defense Information System Agency (DISA), which part of the United States Department of Defense. This report identifies vulnerabilities which violate sections of STIG and groups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

Web Application Security Consortium (WASC) Threat Classification

Availability: OVS and WVS

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 – Scan Comparison Report

Availability: WVS only

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

Availability: WVS only

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

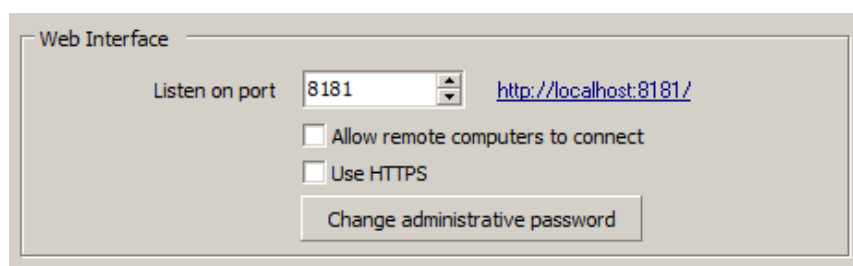
Scheduling Scans

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

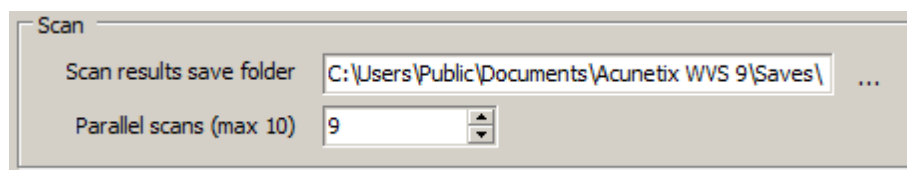
A screenshot of the 'Web Interface' configuration window. It features a 'Listen on port' label with a text box containing '8181' and a dropdown arrow. To the right is a URL field with 'http://localhost:8181/'. Below these are two checkboxes: 'Allow remote computers to connect' and 'Use HTTPS', both of which are currently unchecked. At the bottom is a button labeled 'Change administrative password'.

Screenshot – 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' service from the Windows Services console.

Scan Options

A screenshot of the 'Scan' configuration window. It contains a 'Scan results save folder' label followed by a text box showing the path 'C:\Users\Public\Documents\Acunetix WVS 9\Saves\' and a browse button ('...'). Below this is a 'Parallel scans (max 10)' label with a text box containing the number '9' and a dropdown arrow.

Screenshot – Scheduler scan options

In the Scheduler Scan Options, 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 sub directory.

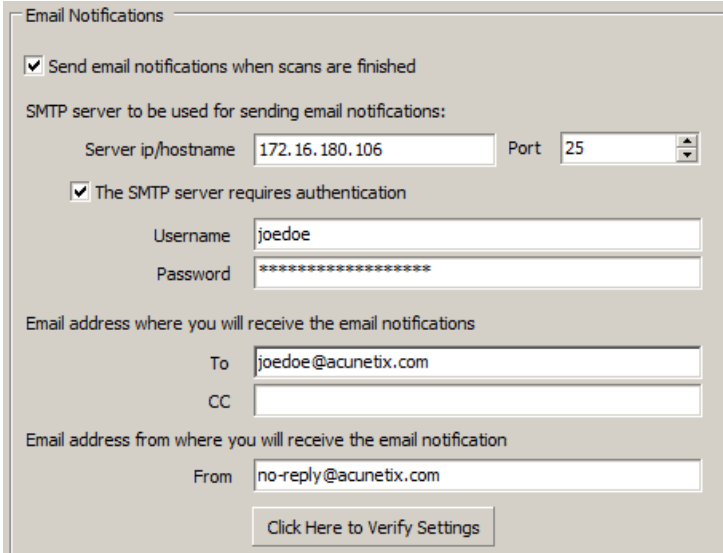
Scanning multiple websites

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

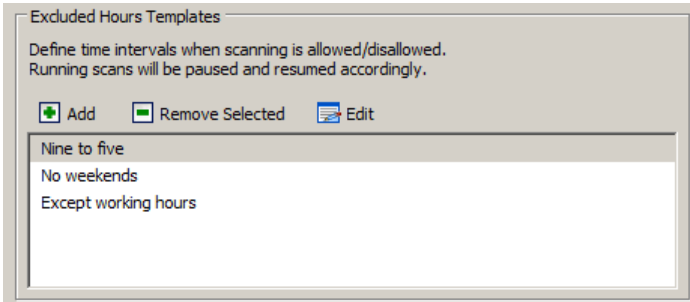


The screenshot shows the 'Email Notifications' configuration window. It has a title bar 'Email Notifications'. Inside, there is a checkbox 'Send email notifications when scans are finished' which is checked. Below this is the section 'SMTP server to be used for sending email notifications:'. It contains two input fields: 'Server ip/hostname' with the value '172.16.180.106' and 'Port' with the value '25'. Below these is another checkbox 'The SMTP server requires authentication' which is also checked. This is followed by 'Username' (value 'joedoe') and 'Password' (masked with asterisks). Then, there is a section 'Email address where you will receive the email notifications' with 'To' (value 'joedoe@acunetix.com') and 'CC' (empty) fields. Finally, there is a section 'Email address from where you will receive the email notification' with a 'From' field (value 'no-reply@acunetix.com'). At the bottom right is a button 'Click Here to Verify Settings'.

Screenshot – 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.

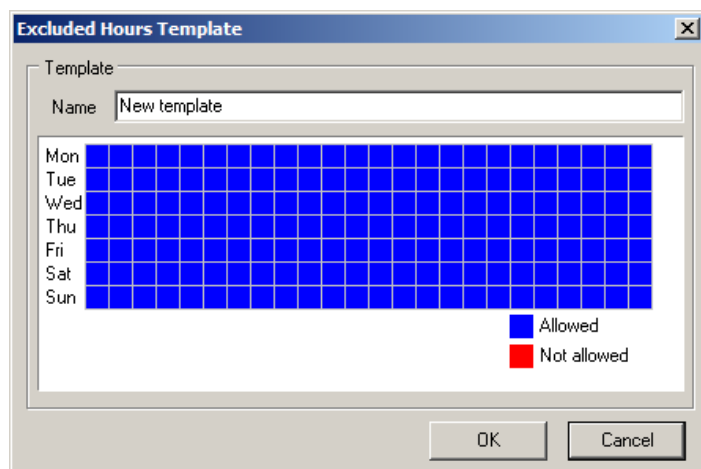
Excluded hours templates



The screenshot shows the 'Excluded Hours Templates' configuration window. It has a title bar 'Excluded Hours Templates'. Inside, there is a text description: 'Define time intervals when scanning is allowed/disallowed. Running scans will be paused and resumed accordingly.' Below this are three buttons: 'Add' (with a green plus icon), 'Remove Selected' (with a green minus icon), and 'Edit' (with a blue pencil icon). Below the buttons is a list box containing three items: 'Nine to five', 'No weekends', and 'Except working hours'.

Screenshot – 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 – Excluded Hours Configuration

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

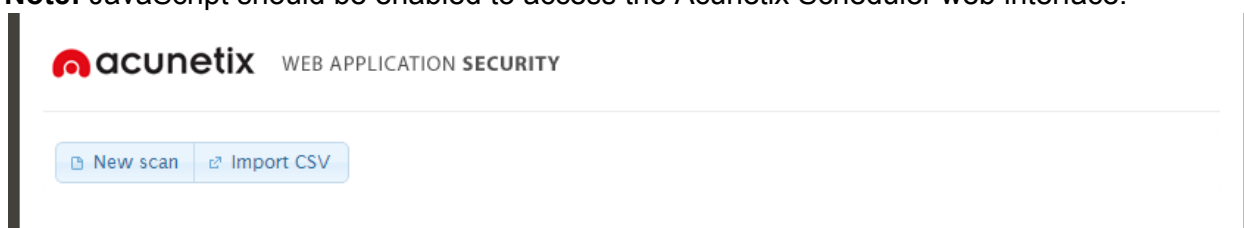
1. Specify a name of the template in the Name input field.
2. Highlight the hours of the day when scans should not run.
3. Click **OK** to save the new template.

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.

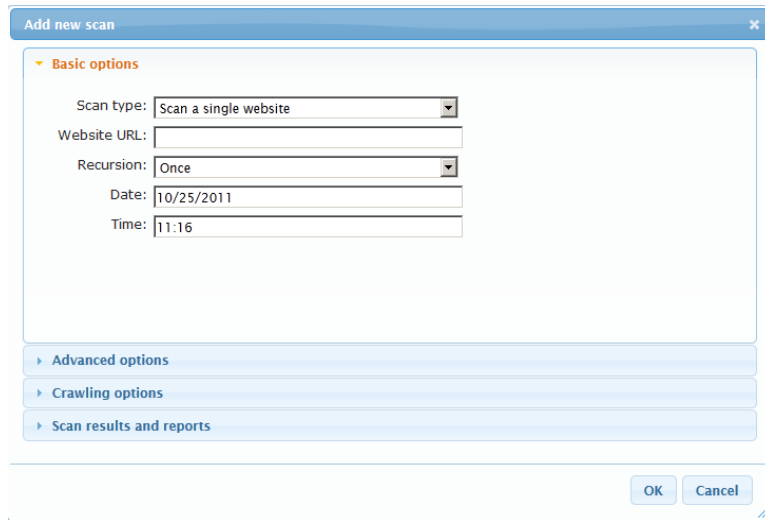
Note: JavaScript should be enabled to access the Acunetix Scheduler web interface.



Screenshot – 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 later in this chapter.

Scheduled Scan Basic Options



Add new scan

Basic options

Scan type: Scan a single website

Website URL:

Recursion: Once

Date: 10/25/2011

Time: 11:16

Advanced options

Crawling options

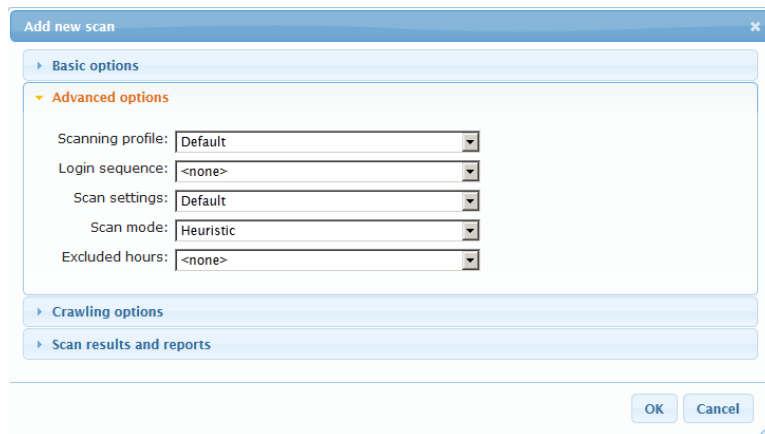
Scan results and reports

OK Cancel

Screenshot – Acunetix Scheduler Basic options

The Basic Options allow you to specify which 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



Add new scan

Basic options

Advanced options

Scanning profile: Default

Login sequence: <none>

Scan settings: Default

Scan mode: Heuristic

Excluded hours: <none>

Crawling options

Scan results and reports

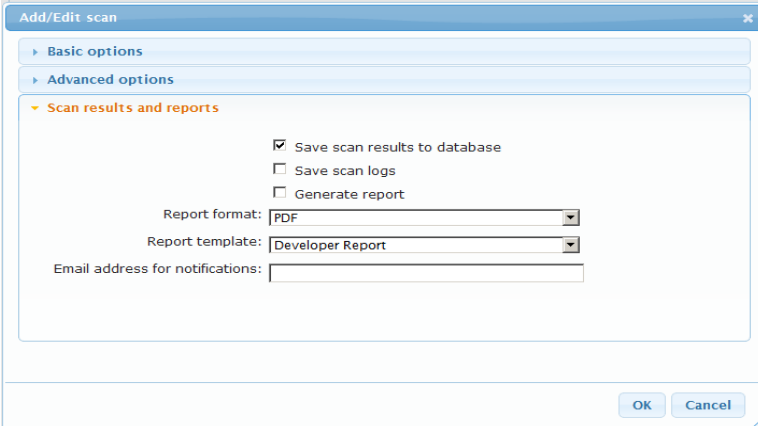
OK Cancel

Screenshot – 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 – Acunetix Scheduler Scan results and Reports

In the Scan results and reports section, you can select 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 results are sent. If no email address is specified, the email address configured 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

You can also import scheduled scans from a CSV file. The format of the CSV files are described next.

CSV File Properties

Each line in the CSV file should only contain one scan. For each scan you should specify the following 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 2014, the date should be 05112014. 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 2014 at 10pm using the default values, use the below line in the CSV file:

http://testphp.vulnweb.com,05112014,2200, , , , , ,

Example 2: To scan testasp.vulnweb.com on the 5th of November 2014 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,05112014,1515,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.

Troubleshooting and Support

User Manual

The most common queries can be answered by consulting this user manual.

Frequently Asked Questions

Our support team maintains a list of frequently asked questions at <http://www.acunetix.com/support/faq/>.

Acunetix Blog

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

Request Support

If you encounter persistent problems that you cannot resolve, we encourage you to contact the Acunetix Support team via email at support@acunetix.com. Please include any information you think is useful to help us diagnose your issue, such as information on the web technologies being used, screenshots showing the problem etc. Please include also 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.

Knowledge base / Support page

You can also explore the Acunetix knowledge base and other support options by browsing to: <http://www.acunetix.com/support/>.

Acunetix Facebook page

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