Acunetix Web Vulnerability Scanner

Web Vulnerability Scanner v8

User Manual v.1 2012

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

Acunetix WVS is copyright of Acunetix Ltd. 2004–2012.

Acunetix Ltd. All rights reserved.

http://www.acunetix.com

info@acunetix.com

Document version 8

Last updated 3rd October 2012

Contents

PAGE LEFT BLANK INTENTIONALLY

1. Introduction to Acunetix Web Vulnerability Scanner

Why You Need To Secure Your Web Applications

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

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

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

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

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

Why does this happen?

- Websites and 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 (default for websites) which has to remain open to allow regular operation of the business.

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

The need for automated web application security scanning

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

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

Acunetix Web Vulnerability Scanner

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

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

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

How Acunetix WVS Works

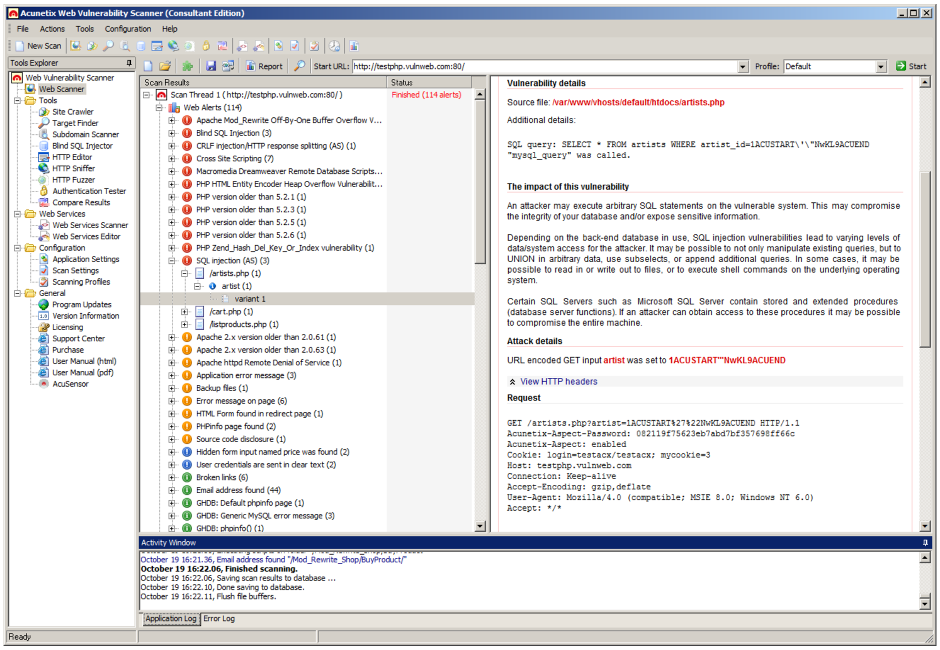
Acunetix WVS works in the following manner:

1. The Crawler analyzes the entire website by following all the links on the site and in the robots.txt file and sitemap.xml (if available). WVS will then map out the website structure and display detailed information about every file. If Acunetix AcuSensor Technology is enabled, the sensor will retrieve a listing of all the files present in the web application directory and 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. It also analyses hidden application files, such as *web.config*.
2. After the crawling process, WVS automatically launches a series of vulnerability attacks on each page found, in essence emulating a hacker. Also, WVS 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.

3. During the scan process, a port scan is also launched against the web server hosting the website. If open ports are found, Acunetix WVS will perform a range of network security checks against the network service running on that port.
4. As vulnerabilities are found, Acunetix WVS reports these in the 'Alerts' node. Each alert contains information about the vulnerability such as POST variable name, affected item, http response of the server and more. If AcuSensor Technology is used details such as source code line, stack trace, SQL query which lead to the vulnerability are listed. Recommendations on how to fix the vulnerability are also shown.
5. If open ports are found, they will be reported in the 'Knowledge Base' node. The list of open ports contains information such as the banner returned from the port and if a security test failed.
6. After a scan has been completed, it can be saved to file for later analysis and for comparison to previous scans. Using the Acunetix reporter a professional report can be created summarizing the scan.

Acunetix AcuSensor Technology

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



```
Scan Thread 1 ( http://testphp.vulnweb.com:80/ )          Finished (114 alerts)
  Web Alerts (114)
    Apache Mod_Rewrite Off-By-One Buffer Overflow V...
    Blind SQL Injection (3)
    CRLF injection/HTTP response splitting (AS) (1)
    Cross Site Scripting (7)
    Macromedia Dreamweaver Remote Database Scripts...
    PHP HTML Entity Encoder Heap Overflow Vulnerabilit...
    PHP version older than 5.2.1 (1)
    PHP version older than 5.2.3 (1)
    PHP version older than 5.2.5 (1)
    PHP version older than 5.2.6 (1)
    PHP Zend_Hash_Del_Key_Or_Index vulnerability (1)
    SQL injection (AS) (3)
      /artists.php (1)
        artist (1)
          variant 1
      /cart.php (1)
      /listproducts.php (1)
    Apache 2.x version older than 2.0.61 (1)
    Apache 2.x version older than 2.0.63 (1)
    Apache httpd Remote Denial of Service (1)
    Application error message (3)
    Backup files (1)
    Error message on page (6)
    HTML Form found in redirect page (1)
    PHPinfo page found (2)
    Source code disclosure (1)
    Hidden form input named price was found (2)
    User credentials are sent in clear text (2)
    Broken links (6)
    Email address found (44)
    GHDB: Default phpinfo page (1)
    GHDB: Generic MySQL error message (3)
    GHDB: phpinfo() (1)
```

Vulnerability details

Source file: /var/www/vhosts/default/htdocs/artists.php

Additional details:

```
SQL query: SELECT * FROM artists WHERE artist_id=1ACUSTART\'\"NwKL9ACUEND
"mysql_query" was called.
```

The impact of this vulnerability

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use subselects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Attack details

URL encoded GET input artist was set to 1ACUSTART'"NwKL9ACUEND

View HTTP headers

Request

```
GET /artists.php?artist=1ACUSTART%27%22NwKL9ACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Cookie: login=testacx/testacx; mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
Accept: */*
```

```
October 19 16:21.36, Email address found "/Mod_Rewrite_Shop/BuyProduct/"
October 19 16:22.06, Finished scanning.
October 19 16:22.06, Saving scan results to database ...
October 19 16:22.10, Done saving to database.
October 19 16:22.11, Flush file buffers.
```

Screenshot 1 - Acusensor pin-points vulnerabilities in code

The increased accuracy is achieved by combining black box scanning techniques with feedback from sensors placed inside the source code while the source code is executed. Black box scanning does not know how the application reacts and source code analysers do not understand how the application will behave while it is being attacked. AcuSensor technology combines these techniques together to achieve significantly better results than using source code analysers and black box scanning independently.

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

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

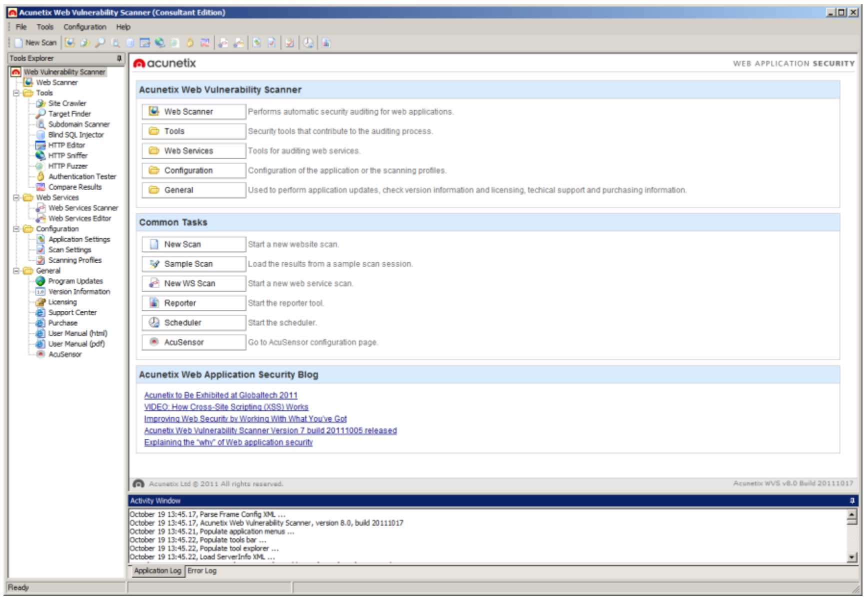
Advantages of using AcuSensor Technology

- Ability to provide more information about the vulnerability, such as source code line number, stack trace, affected SQL query.
- Allows you to locate and fix the vulnerability faster because of the ability to provide more information about the vulnerability, such as source code line number, stack trace, affected SQL query, etc.
- Significantly reduces false positives when scanning a website because it understands the behavior of the web application better.
- Can alert you of web application configuration problems which could result in a vulnerable application or expose sensitive information. E.g. If 'custom errors' are enabled in .NET, this could expose sensitive application details to a malicious user.
- It can advise you how to better secure your web application and web server settings, e.g. if write access is enabled on the web server.
- Detects many more SQL injection vulnerabilities. Previously SQL injection vulnerabilities could only be found if database errors were reported or via other common techniques.
- Ability to detect SQL Injection vulnerabilities in all SQL statements, including in SQL INSERT statements. With a black box scanner such SQL injection vulnerabilities cannot be found.
- Ability to know about all the files present and accessible through the web server. If an attacker will gain access to the website and create a backdoor file in the application directory, the file will be found and scanned when using the AcuSensor Technology and you will be alerted.
- AcuSensor Technology is able to intercept all web application inputs and build a comprehensive list with all possible inputs in the website and test them.
- No need to write URL rewrite rules when scanning web applications which use search engine friendly URL's! Using the AcuSensor Technology the scanner is able to rewrite SEO URL's on the fly.
- Ability to test for arbitrary file creation and deletion vulnerabilities. E.g. Through a vulnerable script a malicious user can create a file in the web application directory and execute it to have privileged access, or delete sensitive web application files.
- Ability to test for email injection. E.g. A malicious user may append additional information such as a list or recipients or additional information to the message body to a vulnerable web form, to spam a large number of recipients anonymously.
- Ability to test for file upload forms vulnerabilities. E.g. A malicious user can bypass file upload form validation checks and upload a malicious file and execute it.

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

Acunetix WVS Program Overview

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



Acunetix Web Vulnerability Scanner

Web Scanner	Performs automatic security auditing for web applications.
Tools	Security tools that contribute to the auditing process.
Web Services	Tools for auditing web services.
Configuration	Configuration of the application or the scanning profiles.
General	Used to perform application updates, check version information and licensing, techical support and purchasing information.

Common Tasks

New Scan	Start a new website scan.
Sample Scan	Load the results from a sample scan session.
New WS Scan	Start a new web service scan.
Reporter	Start the reporter tool.
Scheduler	Start the scheduler.
AcuSensor	Go to AcuSensor configuration page.

Acunetix Web Application Security Blog

Acunetix to Be Exhibited at Globaltech 2011
VIDEO: How Cross-Site Scripting (XSS) Works
Improving Web Security by Working With What You've Got
Acunetix Web Vulnerability Scanner Version 7 build 20111005 released
Explaining the "why" of Web application security

Acunetix Ltd © 2011 All rights reserved. Acunetix WVS v8.0 Build 20111017

```
October 19 13:45.17, Parse Frame Config XML ...
October 19 13:45.17, Acunetix Web Vulnerability Scanner, version 8.0, build 20111017
October 19 13:45.21, Populate application menus ...
October 19 13:45.22, Populate tools bar ...
October 19 13:45.22, Populate tool explorer ...
October 19 13:45.22, Load ServerInfo XML ...
```

Screenshot 2 - Acunetix Web Vulnerability Scanner

Web Scanner

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

1. Crawling – the Crawler automatically crawls and analyzes the website and then builds a site structure.
2. Scanning – Acunetix WVS launches a series of web vulnerability checks against the website or web application – in effect, emulating a hacker.

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

AcuSensor Technology Agent

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

Port Scanner and Network Alerts

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

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

Target Finder

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

Subdomain Scanner

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

Blind SQL Injector

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

HTTP Editor

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

HTTP Sniffer

The HTTP Sniffer acts as a proxy and allows you to capture, examine and modify HTTP traffic between an HTTP client and a web server. You can also enable, add or edit traps to 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 WVS, Acunetix WVS must be configured as a proxy in your web browser. You can read more about the HTTP Sniffer and it's configuration in chapter 7 of this manual.

HTTP Fuzzer

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 Fuzzer also allows you to easily create input rules for further testing in Acunetix WVS.

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.

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.

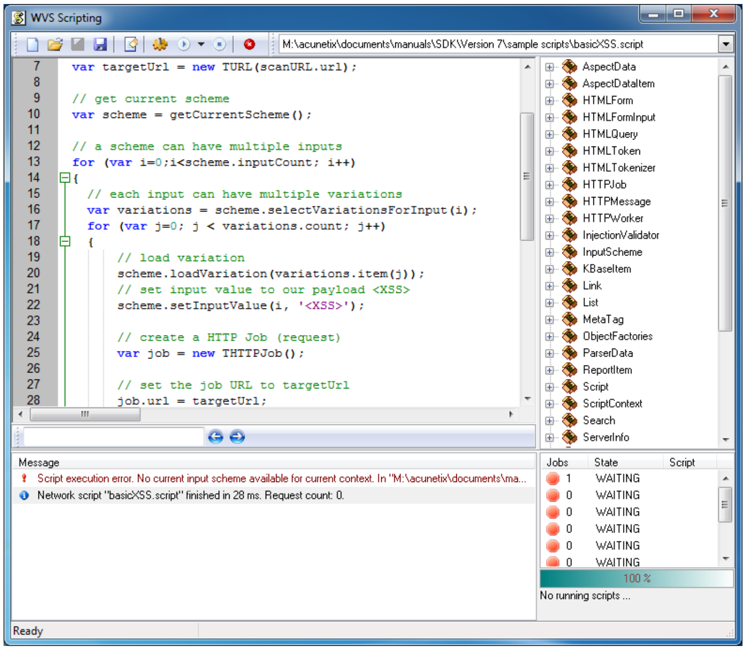
Web Services Scanner

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

Web Services Editor

The Web Services Editor allows you to import an online or local WSDL for custom editing and execution of various web service operations over different port types for an in depth 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.

WVS Scripting tool and Acunetix SDK



M:\acunetix\documents\manuals\SDK\Version 7\sample scripts\basicXSS.script

```
var targetUrl = new TURL(scanURL.url);

// get current scheme
var scheme = getCurrentScheme();

// a scheme can have multiple inputs
for (var i=0;i<scheme.inputCount; i++)
{
  // each input can have multiple variations
  var variations = scheme.selectVariationsForInput(i);
  for (var j=0; j < variations.count; j++)
  {
      // load variation
      scheme.loadVariation(variations.item(j));
      // set input value to our payload <XSS>
      scheme.setInputValue(i, '<XSS>');

      // create a HTTP Job (request)
      var job = new THTTPJob();

      // set the job URL to targetUrl
      job.url = targetUrl;
```

```
Message
Script execution error. No current input scheme available for current context. In "M:\acunetix\documents\ma...
Network script "basicXSS.script" finished in 28 ms. Request count: 0.
```

```
Jobs  State     Script
1     WAITING
0     WAITING
0     WAITING
0     WAITING
0     WAITING
0     WAITING
100 %
No running scripts ...
```

Ready

Screenshot 3 – WVS Scripting tool

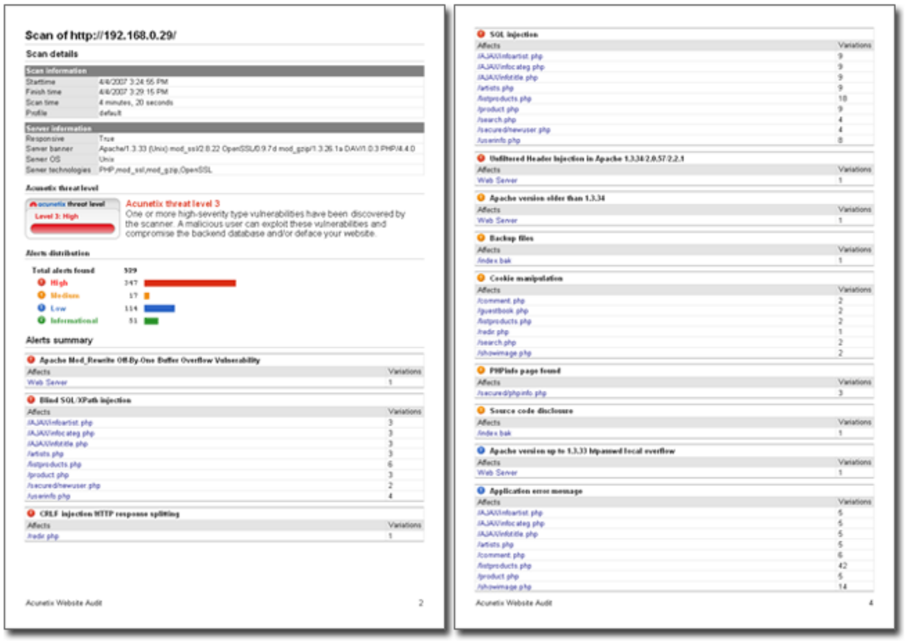
The WVS Scripting tool allows you to create new custom web vulnerability checks. These checks must be written in JavaScript and require installation of the SDK. You can read more about writing custom web security checks from the following URL: http://www.acunetix.com/blog/docs/creating-vulnerability-checks/.

You can download the scripting SDK from:

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

Reporter

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



Scan of http://192.168.0.29/

Scan details

Scan information	
Starttime	4/4/2007 3:24:55 PM
Finish time	4/4/2007 3:29:15 PM
Scan time	4 minutes, 20 seconds
Profile	default

Server information	
Responsive	True
Server banner	Apache/1.3.33 (Unix) mod_ssl/2.8.22 OpenSSL/0.9.7d mod_gzip/1.3.26.1a DAV/1.0.3 PHP/4.4.0
Server OS	Unix
Server technologies	PHP,mod_ssl,mod_gzip,OpenSSL

Acunetix threat level

Acunetix threat level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	329
High	147
Medium	17
Low	114
Informational	51

Alerts summary

Apache Mod_Rewrite Off-By-One Buffer Overflow Vulnerability

Affects	Variations
Web Server	1

Blind SQL/XPath injection

Affects	Variations
/AJAX/infoartist.php	3
/AJAX/infocateg.php	3
/AJAX/infotitle.php	3
/artists.php	3
/listproducts.php	6
/product.php	3
/secured/newuser.php	2
/userinfo.php	4

CRLF injection/HTTP response splitting

Affects	Variations
/redir.php	1

Acunetix Website Audit 2

SQL injection

Affects	Variations
/AJAX/infoartist.php	9
/AJAX/infocateg.php	9
/AJAX/infotitle.php	9
/artists.php	9
/listproducts.php	18
/product.php	9
/search.php	4
/secured/newuser.php	4
/userinfo.php	8

Unfiltered Header Injection in Apache 1.3.34/2.0.57/2.2.1

Affects	Variations
Web Server	1

Apache version older than 1.3.34

Affects	Variations
Web Server	1

Backup files

Affects	Variations
/index.bak	1

Cookie manipulation

Affects	Variations
/comment.php	2
/guestbook.php	2
/listproducts.php	2
/redir.php	1
/search.php	2
/showimage.php	2

PHPInfo page found

Affects	Variations
/secured/phpinfo.php	3

Source code disclosure

Affects	Variations
/index.bak	1

Apache version up to 1.3.33 htpasswd local overflow

Affects	Variations
Web Server	1

Application error message

Affects	Variations
/AJAX/infoartist.php	5
/AJAX/infocateg.php	5
/AJAX/infotitle.php	5
/artists.php	5
/comment.php	6
/listproducts.php	42
/product.php	5
/showimage.php	14

Acunetix Website Audit 4

Screenshot 4 - Typical WVS Report including Chart of alerts

New to Version 8 of Acunetix WVS

- New test method: manipulation of input parameters from URLs
- Automatic IIS 7 rewrite rule interpretation
- Support for custom HTTP headers
- Imperva Web Application Firewall integration
- Detection of new vulnerability class: HTTP Parameter Pollution
- Support for multiple instances of Acunetix WVS on the same workstation
- Web-based scheduler for easy access of scan results on any workstation, laptop, or smartphone
- Automatic custom 404 error page recognition and detection
- Scan Settings Templates
- Simplified Scan Wizard
- Smart memory management options

- Real-time Crawler status update
- Scan termination status included in report
- Web application coverage report
- Log file retention settings

Acunetix training and Support

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

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

Licensing Acunetix

Acunetix Web Vulnerability Scanner (WVS) 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 WVS Enterprise and Consultant editions are sold as a one-year or perpetual license. The 1-year license expires after 1 year from the date of activation. The perpetual license does not expire. The Small Business version is available as a perpetual license only.

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

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

Small Business Edition 1 Site/Server

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

Additional licenses are required for separate installs onto different workstations.

Enterprise Edition Unlimited Sites/Servers

The Enterprise edition license allows you to install one copy of Acunetix WVS on one computer to scan an unlimited number of sites or servers. The sites or servers must be owned by yourself (or your company) and not by third parties. Acunetix Enterprise edition will leave a trail in the log files of the scanned server and scanning of third party sites is prohibited by the license agreement. Additional licenses are required for separate installs onto different workstations.

Enterprise Edition Unlimited Sites/Servers x10 instances

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

Consultant Edition

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

Consultant Edition x10 instances

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

Limitations of Evaluation Edition

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

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

If you decide to purchase Acunetix WVS, you will need to un-install the evaluation edition and install the purchased edition, which must be downloaded as a separate installer file.

Download the installer file and double-click to begin the setup, which will prompt you to remove the evaluation version and install the full edition. All settings detected in the previously installed version will be retained.

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

2. Installing Acunetix WVS

System Minimum Requirements

- Operating system: Microsoft Windows XP and later.
- CPU: 32 bit or 64 bit processor.
- System memory: minimum of 1 GB RAM.
- Storage: 200 MB of available hard-disk space.
- Microsoft Internet Explorer 7 (or later) – some components of IE are used by Acunetix.
- Microsoft SQL Server / Microsoft Access – for optional use of the reporting database

Installing Acunetix Web Vulnerability Scanner

1. Download the latest version of Acunetix Web Vulnerability Scanner from the download location provided to you when you purchased the license.
2. Double click the webvulnscan8.exe file to launch the Acunetix WVS installation wizard and click **Next** when prompted.
3. Review and approve the License Agreement
4. Select the folder location where Acunetix Web Vulnerability Scanner will be installed. Further install options – such as the Acunetix Firefox toolbar and desktop shortcut – can be enabled..
5. Click Install to start the installation. Setup will now copy all files and install the necessary Windows Service. Click Finish when ready.

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

- http://testphp.vulnweb.com (built on PHP)
- http://testasp.vulnweb.com (Built on ASP)
- http://testaspnet.vulnweb.com (Built on ASP.NET)

Furthermore, you will not be able to save the scan results when using the evaluation version.

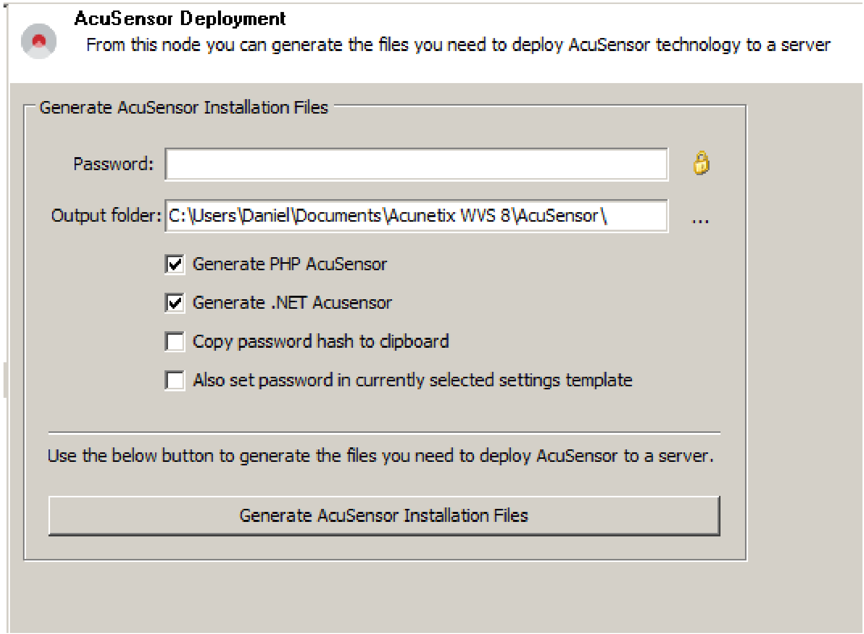
Installing the AcuSensor Agent

NOTE: Installing the AcuSensor Agent is optional. Acunetix WVS still is best in class as a "black box" scanner. However, the AcuSensor Agent improves selection accuracy and vulnerability results, especially when used for scanning PHP websites.

The unique Acunetix AcuSensor Technology identifies more vulnerabilities than a traditional 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

To install the AcuSensor Agent the file must first be generated and then deployed to the target server.

Generating the AcuSensor files



AcuSensor Deployment

From this node you can generate the files you need to deploy AcuSensor technology to a server

Generate AcuSensor Installation Files

Password:

Output folder: C:\Users\Daniel\Documents\Acunetix WVS 8\AcuSensor\

☑ Generate PHP AcuSensor

☑ Generate .NET Acusensor

□ Copy password hash to clipboard

□ Also set password in currently selected settings template

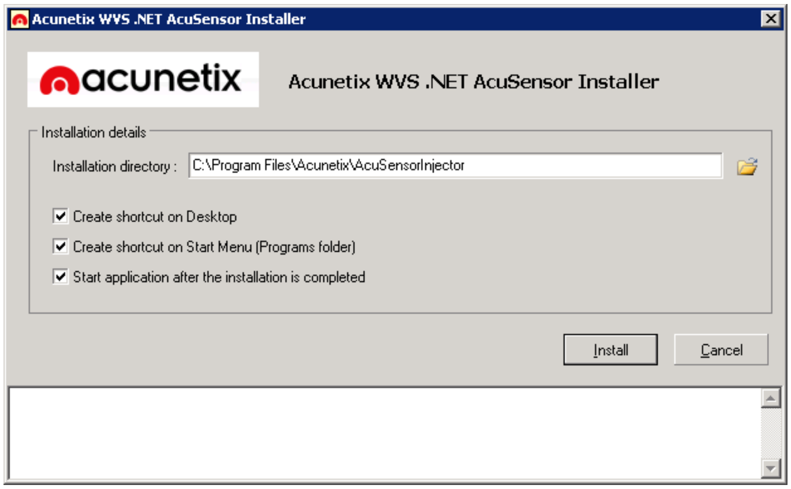
Use the below button to generate the files you need to deploy AcuSensor to a server.

Screenshot 5 – AcuSensor Deployment settings node

1. Navigate to the ‘Configuration > Application Settings’ node in the Tools Explorer. Click on the ‘AcuSensor Deployment’ node.
2. Enter a password or click on the padlock icon to randomly generate a password unique to the AcuSensor file. .
3. Specify the path where you want the AcuSensor files to be generated.
4. Furthermore you can choose to generate files for a PHP website, .NET website, or both by ticking the options available. By default, an AcuSensor file will be generated for both PHP and .NET.
5. Click on **Generate AcuSensor Installation Files** and an explorer window will automatically open showing the generated AcuSensor files.

Installing AcuSensor agent for .NET

1. Locate the AcuSensor installation files for the website where the AcuSensor will be injected. Copy **Setup.exe** to the remote server hosting the target website.
2. **Install Prerequisites:** The AcuSensor injector application requires Microsoft .NET Framework 3.5. 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 able listing of all .NET applications running on server.



Acunetix WVS .NET AcuSensor Installer

Installation details

Installation directory : C:\Program Files\Acunetix\AcuSensorInjector

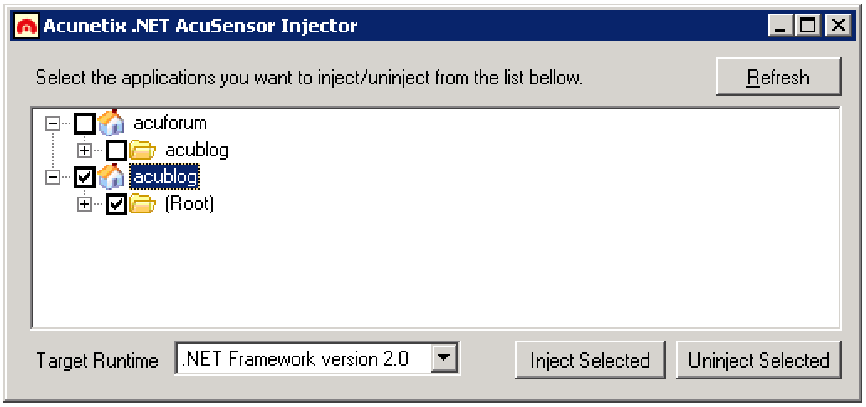
☑ Create shortcut on Desktop

☑ Create shortcut on Start Menu (Programs folder)

☑ Start application after the installation is completed

Screenshot 6 – Acunetix .NET AcuSensor Injector installation

1. Double click **Setup.exe** to install Acunetix .NET AcuSensor 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.



Acunetix .NET AcuSensor Injector

Select the applications you want to inject/uninject from the list bellow.

```
⊟ □ acuforum
   ⊞ □ acublog
⊟ ☑ acublog
   ⊞ ☑ (Root)
```

Target Runtime: .NET Framework version 2.0

Screenshot 7 – Acunetix .NET AcuSensor Technology Injector

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

If your web application is written in PHP:

1. Locate the PHP AcuSensor file of the website you want to install AcuSensor on. Copy the **acu_phpaspect.php** file to the remote webserver hosting the web application. The AcuSensor agent file should be in a location where it can be accessed by the web server software. Acunetix

AcuSensor Technology works on PHP version 5 or newer. Previous PHP versions are not supported.

2. You can use one of 2 methods to activate the sensor: Method 1 can be used to install the AcuSensor on Apache only, and Method 2 can be used to install the AcuSensor on both Apache and IIS. Both methods are explained below.

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 AcuSensor is working properly on the target website:

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 on 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**.

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

Disabling and uninstalling AcuSensor

To uninstall and disable the sensor:

AcuSensor for .NET

1. Run the Acunetix .NET AcuSensor Technology Injector from the program group and select the already injected code. Click on **Uninject Selected** to remove the AcuSensor Technology code

from the .NET applications. On success confirmation, close the confirmation window and the Acunetix .NET AcuSensor Technology Injector.

2. Run uninstall.exe from the application's installation directory.

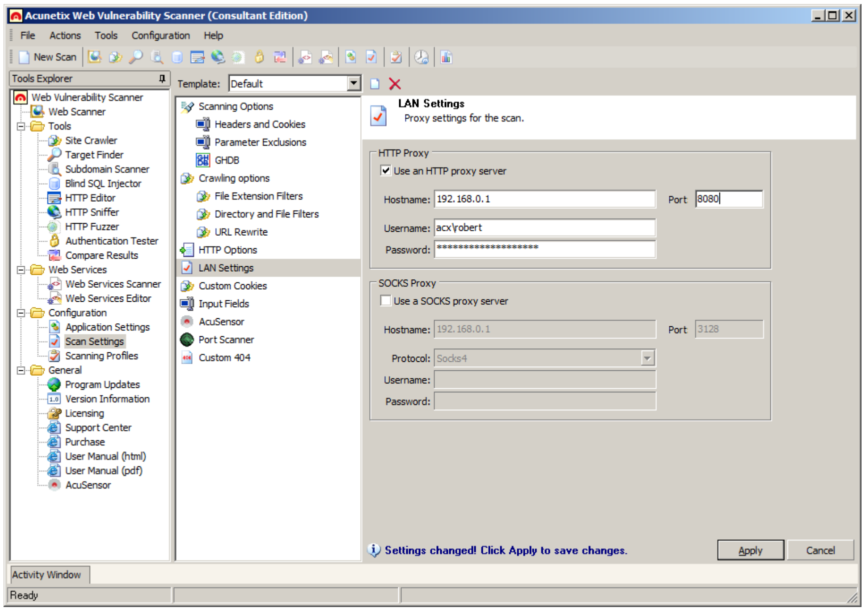
Note: If you uninstall the Acunetix .NET AcuSensor Technology Injector without un-injecting the .NET application, then the AcuSensor Technology code will not be removed from your .NET application.

AcuSensor for PHP

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

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

Configuring an HTTP Proxy or SOCKS proxy Server



Template: Default

LAN Settings
Proxy settings for the scan.

HTTP Proxy
☑ Use an HTTP proxy server
Hostname: 192.168.0.1 Port 8080
Username: acx\robert
Password: ********************

SOCKS Proxy
☐ Use a SOCKS proxy server
Hostname: 192.168.0.1 Port 3128
Protocol: Socks4
Username:
Password:

Settings changed! Click Apply to save changes.

Screenshot 8 - LAN HTTP Proxy Settings

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

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

HTTP Proxy Settings

- **Use an HTTP proxy server** - Tick the check box to configure Acunetix WVS to use a HTTP proxy server.

- **Hostname and Port** - Hostname (or IP address) and port number of the HTTP proxy server.
- **Username and Password** - Credentials used to access the proxy. If no authentication is required, leave these options empty.

SOCKS Proxy Settings

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

Upgrading from WVS 7

Acunetix WVS 7 and WVS 8 can run in parallel on the same computer. Therefore you can install both versions on the same computer without having any conflicts. Automatic importing of application settings from version 7 to version 8 is not possible because of the major changes in application settings between the two versions. Though you can copy the recorded login sequences and reporting database from the version 7 to version 8 installations by following the instructions below.

Copy recorded login sequences

1. Switch off both versions of Acunetix WVS.
2. Navigate to 'C:\Program Files (x86)\Acunetix\Web Vulnerability Scanner 7\Data\General\LoginSequences'.
3. Copy all recorded login sequences (e.g. testphp.vulnweb.com_login.loginseq) to 'C:\Users\Public\Documents\Acunetix WVS 8\LoginSequences'.

When you restart the Acunetix Web Vulnerability Scanner and navigate to Login Sequence Recorder, the list of recorded login sequences would be populated with the new login sequences which were imported from version 7.

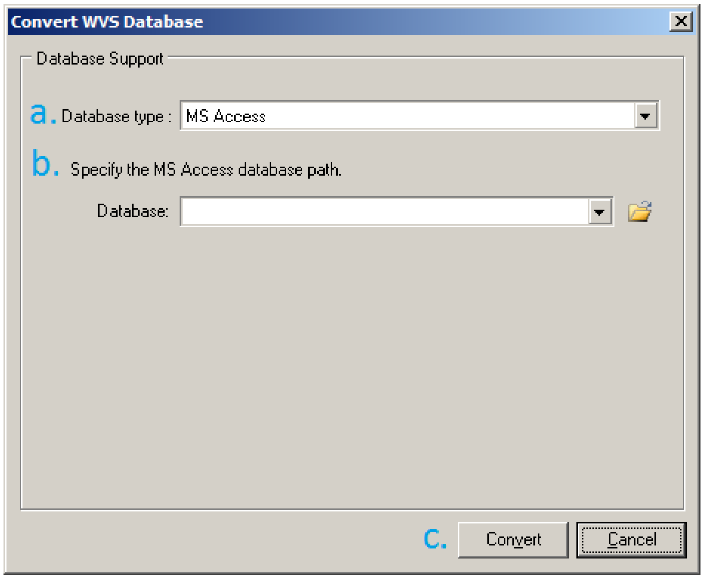
Migrate reporting database

1. Switch off both versions of Acunetix WVS.
2. Download the 'Convert WVS Database' tool from http://www.acunetix.com/download/tools/ConvertWVSDatabase.zip.
3. Extract the ZIP file and run 'Convert WVS Database'.
4. Configure the following in the 'Convert WVS Database' tool:
    a. The type of the database from the drop-down menu 'Database type' field e.g. MS Access (default) or SQL database.

b. Specify the location of the version 7 reporting database. By default, the database is located in ‘C:\Program Files (x86)\Acunetix\Web Vulnerability Scanner 7\Data\Database’.

c. If you are converting an SQL database, enter the IP of the server and the credentials used to access the SQL database.

d. Click Convert and wait until the conversion is complete. Once complete you will be alerted.



Database type : MS Access

Screenshot 9 – Reporting Database migration tool

5. If you converted a SQL database, all you need to do is configure Acunetix WVS 8 with the new connection details. If you converted a MS Access database, proceed with the below procedures.
6. Navigate to ‘C:\Program Files (x86)\Acunetix\Web Vulnerability Scanner 7\Data\Database’ directory.
7. Copy the file ‘vulnscanresults.mdb’ to ‘C:\ProgramData\Acunetix WVS 8\Data\Database’.

Once you launch Acunetix WVS 8, it will use the converted database which also includes all saved reports from version 7.

3. Scanning A Website

Introduction

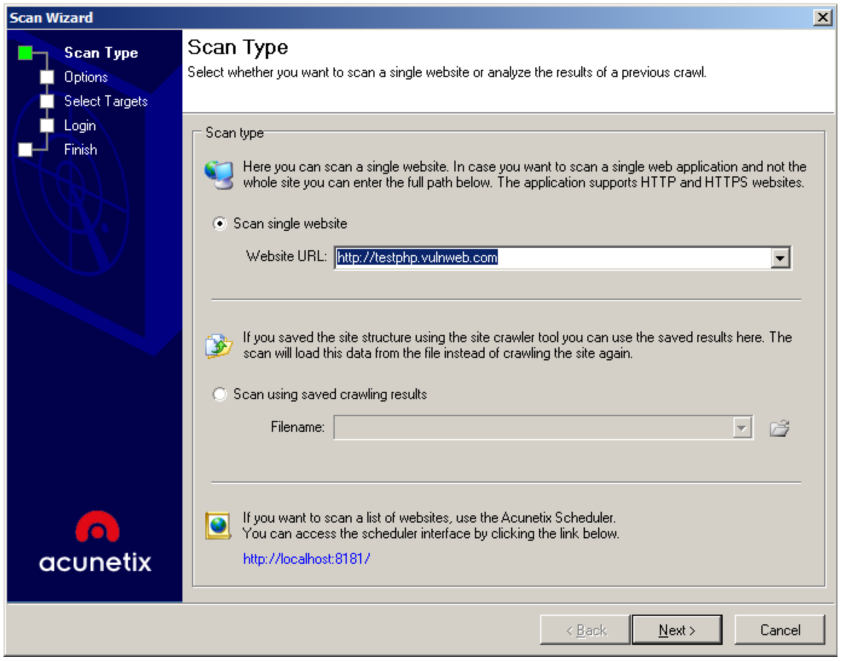
The Scan Wizard provides a quick and easy way to configure and launch a new scan.

NOTE: DO NOT SCAN A WEBSITE WITHOUT PROPER AUTHORIZATION!

The web server logs will show the scans and any attacks made by Acunetix WVS. If you are not the sole administrator of the website please make sure to warn other administrators before performing a scan. Some scans might cause a website to crash, requiring a restart of the website.

Step 1: Select Target(s) to Scan

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



Scan Type

Select whether you want to scan a single website or analyze the results of a previous crawl.

Scan type

Here you can scan a single website. In case you want to scan a single web application and not the whole site you can enter the full path below. The application supports HTTP and HTTPS websites.

● Scan single website

Website URL: http://testphp.vulnweb.com

If you saved the site structure using the site crawler tool you can use the saved results here. The scan will load this data from the file instead of crawling the site again.

○ Scan using saved crawling results

Filename:

If you want to scan a list of websites, use the Acunetix Scheduler.
You can access the scheduler interface by clicking the link below.
http://localhost:8181/

Screenshot 10 – Scan Wizard Select Scan Type

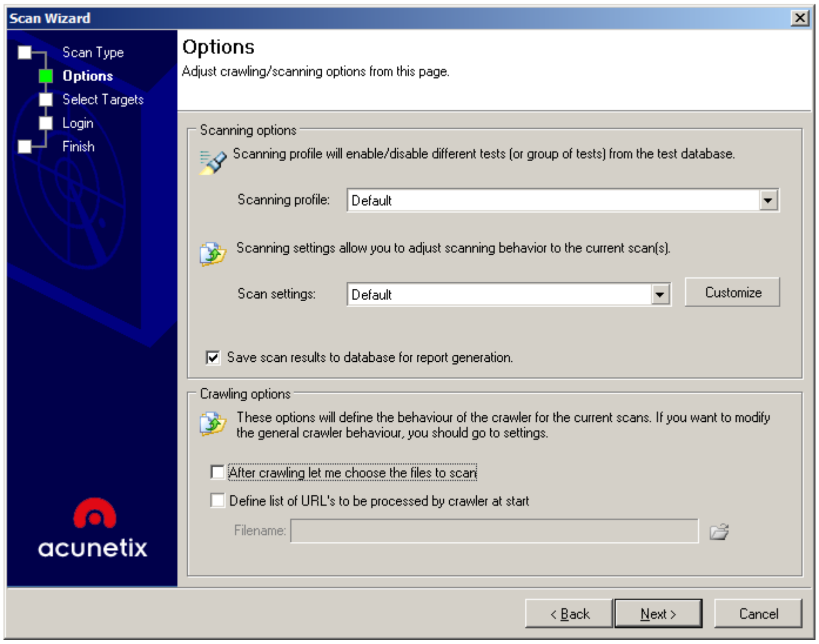
2. Specify the website(s) to be scanned. The scan target options are:

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

Note: The **Acunetix WVS Scheduler** can be used to scan multiple websites at the same time since it launches an instance of Acunetix WVS per each simultaneous scan. You can read more about the Acunetix WVS scheduler in page 74 of this manual.

3. Click **Next** to continue.

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



Scan Wizard

Options

Adjust crawling/scanning options from this page.

Scanning options

Scanning profile will enable/disable different tests (or group of tests) from the test database.

Scanning profile: Default

Scanning settings allow you to adjust scanning behavior to the current scan(s).

Scan settings: Default

☑ Save scan results to database for report generation.

Crawling options

These options will define the behaviour of the crawler for the current scans. If you want to modify the general crawler behaviour, you should go to settings.

☐ After crawling let me choose the files to scan

☐ Define list of URL's to be processed by crawler at start

Filename:

Screenshot 11 – 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 any known web vulnerability. Refer to the 'Scanning Profiles' section on page 88 for more information on how to customize or create scanning profiles.

Scan Settings template

The Scan Settings template will determine what Crawler (HTTP protocol, advanced crawling) and Scanner settings are to be used during a scan. Refer to the 'Scan Settings templates' section on page 88 for more information on how to customize or create new Scan Settings templates.

Save scan Results

If you want to automatically save the scan results to the reporting database, enable the **Save scan results to the database for report generation** option. You can read more about the Acunetix Reporter from page 37 of this user manual.

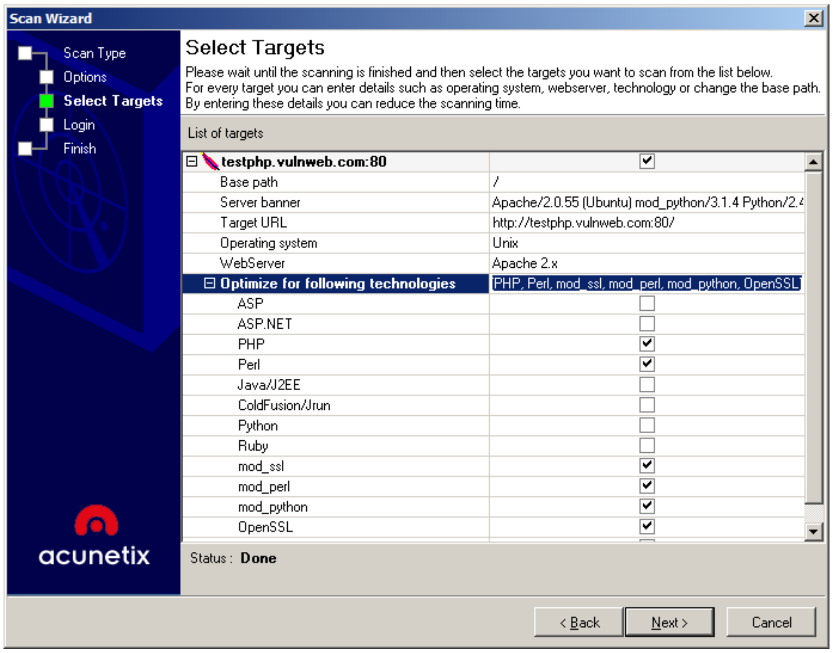
Crawling Options

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

Tick the option **Define list of URLs to be processed by crawler at start** if you would like a specific URL to be crawled before any other.

Note: If the scan is being launched from a saved crawl result, the **Define list of URLs…** option will be greyed out because an automated scan will start immediately without the crawl.

Step 3: Confirm Targets and Technologies Detected



Select Targets

Please wait until the scanning is finished and then select the targets you want to scan from the list below.
For every target you can enter details such as operating system, webserver, technology or change the base path.
By entering these details you can reduce the scanning time.

List of targets

⊟ testphp.vulnweb.com:80	☑
Base path	/
Server banner	Apache/2.0.55 (Ubuntu) mod_python/3.1.4 Python/2.
Target URL	http://testphp.vulnweb.com:80/
Operating system	Unix
WebServer	Apache 2.x
⊟ Optimize for following technologies	PHP, Perl, mod_ssl, mod_perl, mod_python, OpenSSL
ASP	☐
ASP.NET	☐
PHP	☑
Perl	☑
Java/J2EE	☐
ColdFusion/Jrun	☐
Python	☐
Ruby	☐
mod_ssl	☑
mod_perl	☑
mod_python	☑
OpenSSL	☑

Status : **Done**

Screenshot 12 – Scan Wizard Selecting Targets and Technologies

Acunetix WVS will automatically fingerprint the target website(s) for basic details such as the server's operating system and web server, web server technologies, and custom 404 error page in use. If a custom 404 error-page is being used, Acunetix WVS will automatically detect it and determine a pattern for it, removing the need for manual configuration. For more details on Custom 404 Error Pages refer to page 92 of this manual.

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

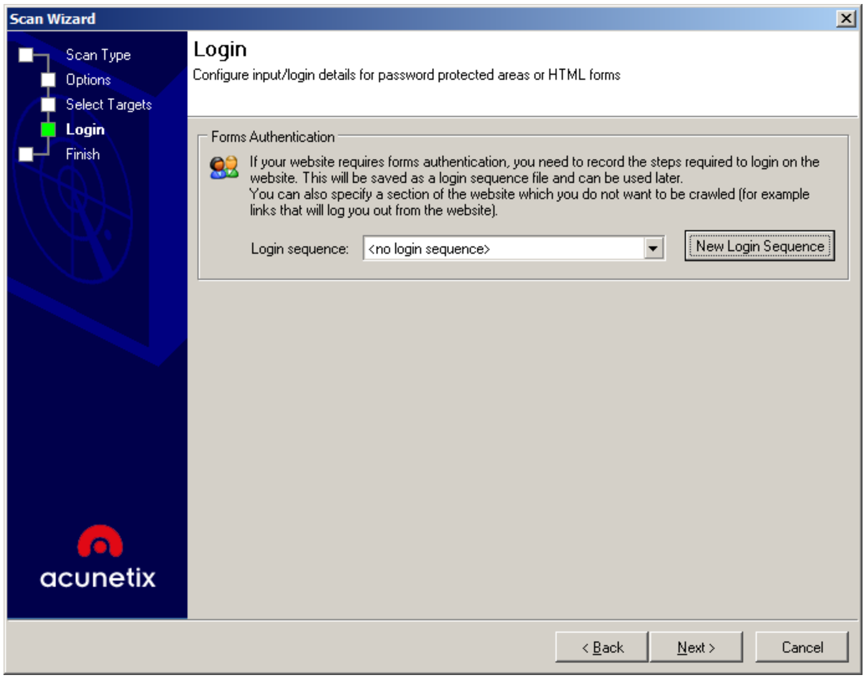
Note: if a specific web technology is not listed under **Optimize for the following technologies**, it does not mean that it is unsupported by WVS, but that there are no vulnerability tests exclusive to that technology.

Step 4: Configure Login for Password Protected Areas

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

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

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



Login

Configure input/login details for password protected areas or HTML forms

Forms Authentication

If your website requires forms authentication, you need to record the steps required to login on the website. This will be saved as a login sequence file and can be used later.
You can also specify a section of the website which you do not want to be crawled (for example links that will log you out from the website).

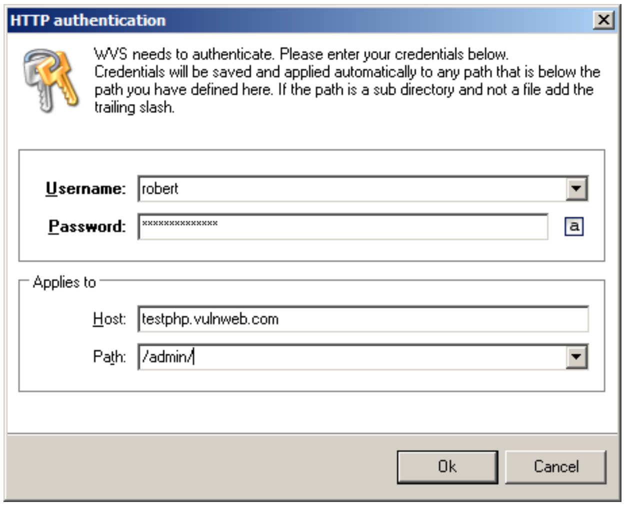
Login sequence: <no login sequence>

Screenshot 13 - Login Details Options

Scanning a HTTP password protected area:

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

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



WVS needs to authenticate. Please enter your credentials below.
Credentials will be saved and applied automatically to any path that is below the path you have defined here. If the path is a sub directory and not a file add the trailing slash.

Username: robert
Password: ***************

Applies to

Host: testphp.vulnweb.com
Path: /admin/

Screenshot 14 – HTTP Authentication

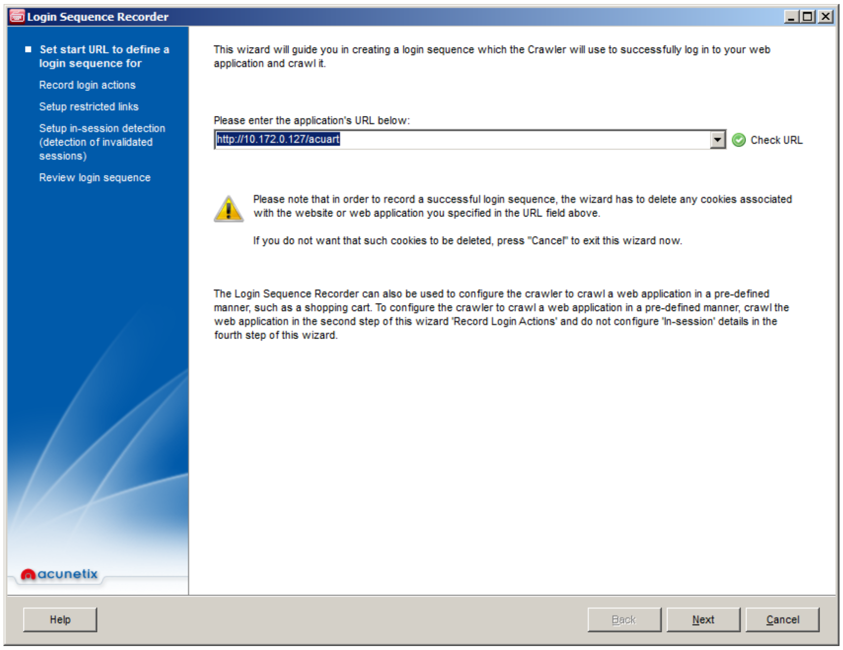
3. Enter the Username and Password. In the ‘Host’ text box field specify the main website URL, e.g. testphp.vulnweb.com. In the ‘Path’ text box, specify the path for where the credentials should be used, e.g. protected. Do not specify a path if the credentials are used site wide.

HTTP authentication options

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

Scanning a form based password protected area:

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



This wizard will guide you in creating a login sequence which the Crawler will use to successfully log in to your web application and crawl it.

Please enter the application's URL below:

http://10.172.0.127/acuart

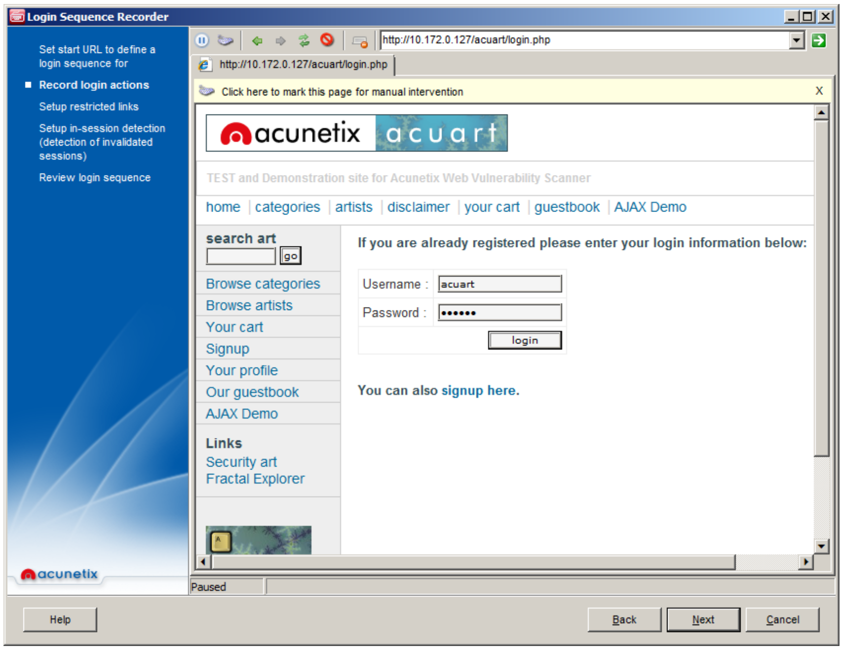
Please note that in order to record a successful login sequence, the wizard has to delete any cookies associated with the website or web application you specified in the URL field above.

If you do not want that such cookies to be deleted, press "Cancel" to exit this wizard now.

The Login Sequence Recorder can also be used to configure the crawler to crawl a web application in a pre-defined manner, such as a shopping cart. To configure the crawler to crawl a web application in a pre-defined manner, crawl the web application in the second step of this wizard 'Record Login Actions' and do not configure 'In-session' details in the fourth step of this wizard.

Screenshot 15 – Login Sequence Wizard

2. Enter the URL of the website for which you would like to record a login sequence. By default the URL of the target website is automatically populated. Click **Next** to proceed


Login Sequence Recorder
Set start URL to define a login sequence for
■ Record login actions
Setup restricted links
Setup in-session detection (detection of invalidated sessions)
Review login sequence
http://10.172.0.127/acuart/login.php
http://10.172.0.127/acuart/login.php
Click here to mark this page for manual intervention
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
Fractal Explorer
login
Paused
acunetix
Help
Back
Next
Cancel

If you are already registered please enter your login information below:

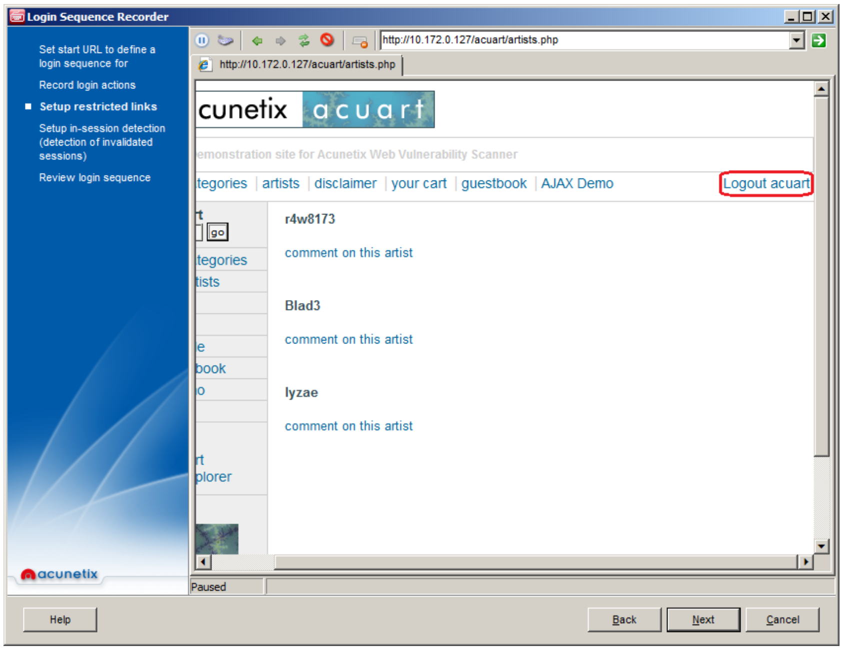
Username : acuart

Password : ••••••

You can also signup here.

Screenshot 16 – Login Sequence Recorder

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

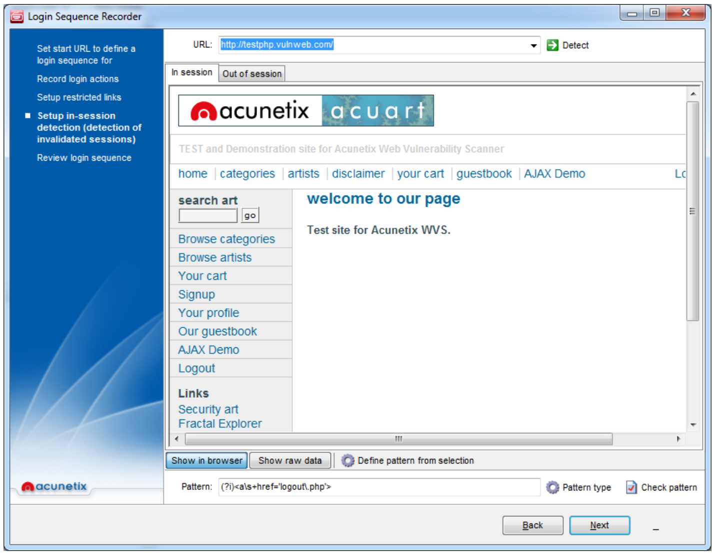


URL: http://10.172.0.127/acuart/artists.php

Login Sequence Recorder
Set start URL to define a login sequence for
Record login actions
Setup restricted links
Setup in-session detection (detection of invalidated sessions)
Review login sequence
http://10.172.0.127/acuart/artists.php
cunetix acuart
emonstration site for Acunetix Web Vulnerability Scanner
tegories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout acuart
r4w8173
comment on this artist
Blad3
comment on this artist
lyzae
comment on this artist
Paused
acunetix
Help
Back
Next
Cancel

Screenshot 17 – Specify an excluded link

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



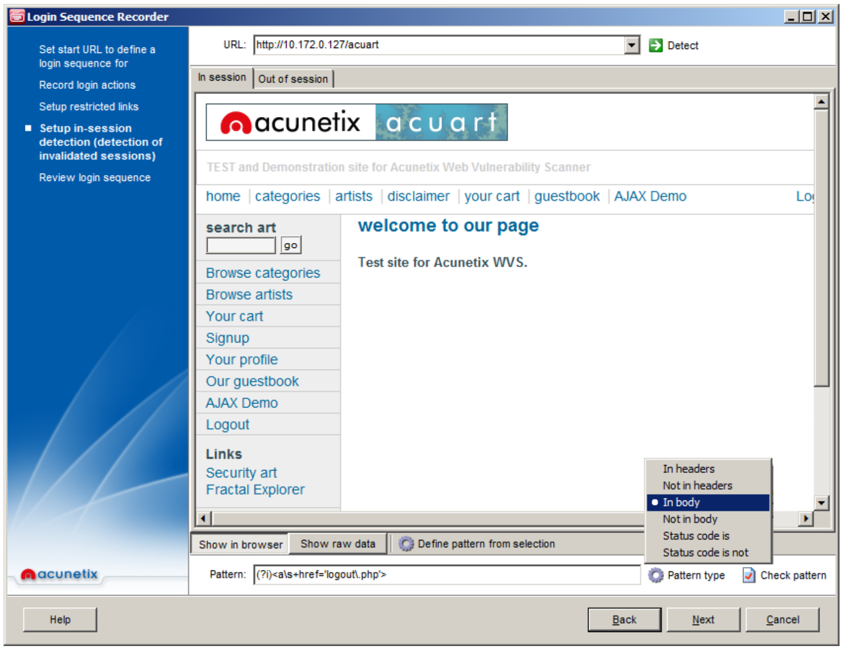
URL: http://testphp.vulnweb.com/

Pattern: (?i)<a\s+href='logout\.php'>

Screenshot 18 – Specify an 'In session' or 'Out of session' pattern

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

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

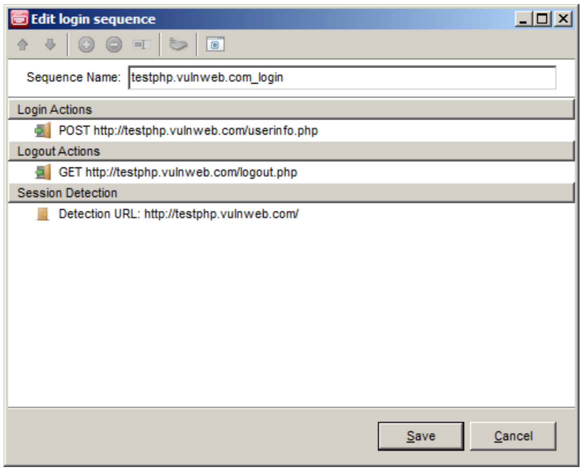


URL: http://10.172.0.127/acuart

Pattern: (?i)<a\s+href='logout\.php'>

Screenshot 19 – Specify an 'In session' or 'Out of session' pattern - Drop down menu

You also have to specify where the pattern can be found in the response. From the **Pattern Type** drop down menu select if the pattern is **In headers**, **Not in headers**, **In body**, **Not in body**, **Status code is** and **Status code is not**. Click on **Check Pattern** to verify that the crawler is able to recognize the difference between a logged in session and a logged out session. Click **Next** to proceed with the wizard.



Sequence Name: testphp.vulnweb.com_login

Login Actions
POST http://testphp.vulnweb.com/userinfo.php

Logout Actions
GET http://testphp.vulnweb.com/logout.php

Session Detection
Detection URL: http://testphp.vulnweb.com/

Screenshot 20 – Recorded login sequence review

6. In the last step of the wizard, you can review the recorded sequence. You can change priority of URL's using the up and down arrows, edit requests and add or remove requests. Click 'Finish' to finalize the session recording.

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

The Login Sequence Recorder can also be used to configure Acunetix WVS to crawl a web application in a pre-defined manner, such as a shopping cart or to automatically input data into a web form. For more information on the Login Sequence Recorder and its uses, see the section **Login Sequence Recorder** on page 80 of this manual or refer to the following URL; http://www.acunetix.com/blog/docs/acunetix-wvs-login-sequence-recorder/.

Step 6: Final wizard options

In the final step of the scan wizard, you are presented with an overview of the scan options and alerted if further actions are required. Below is a list of all possible options you might be presented with:

- If there an error is encountered while connecting to the target server, you will be alerted with the complete details of the error.
- If the target website is using Custom 404 error pages, they will be detected automatically, therefore no further action is required. If Acunetix WVS is unable to automatically detect a custom 404 error page and a pattern to recognize it automatically, you will have to configure a custom 404 error page rule by clicking the **Customize** button. You can read more about Custom 404 error pages from page 92 of the manual.
- If the target server is using CASE insensitive URLs, you will also be alerted with the option to force case insensitive crawling.
- If AcuSensor Technology is enabled and the target server is PHP or .NET, you will be prompted with the option to configure AcuSensor technology. Click the **Customize** button to install AcuSensor on the target server. You can read more about AcuSensor on page 13 of this manual.
- Acunetix WVS will also alert you if additional hosts have been discovered; i.e. other websites which your website links to. By default, Acunetix WVS will not crawl and scan additional hosts / FQDN's which are linked from your website. Tick the host(s) which Acunetix WVS should automatically crawl and scan.
- If you have made changes to the Scan Settings template, you can also save the modifications to the existing or new template. Refer to page 88 of this user manual to read more about the Scan Settings templates.

Step 7: Completing the scan

Click on **Finish** to start the automated scan. Depending on the size of the website, scanning profile, and the server response time, a scan may take up to several hours. These factors cannot be controlled by Acunetix WVS.

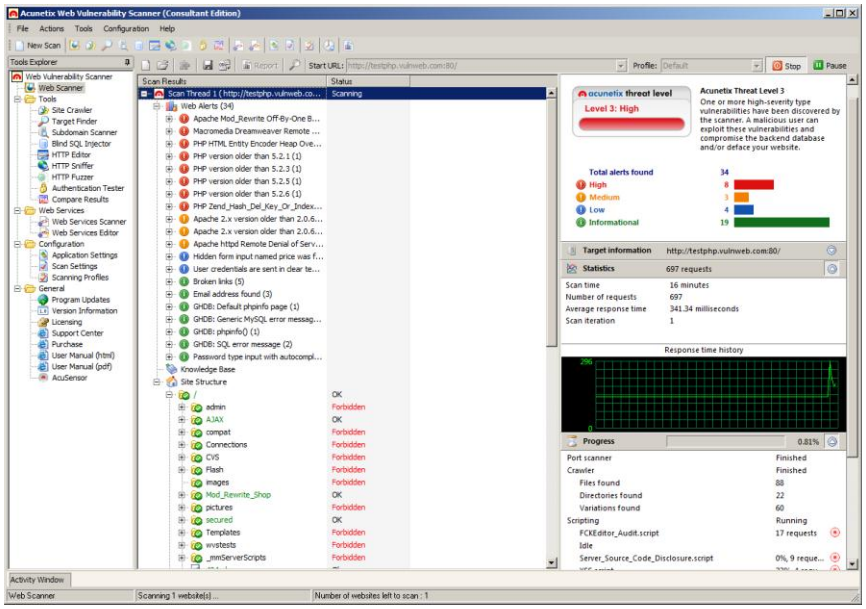
Step 8: Select the Files and directories to Scan

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

4. Analyzing the Scan Results

Introduction

All the security alerts that are discovered during the scan of a website are displayed in real-time under the Alerts node in the **Scan Results** window. A ‘Site Structure’ node is also shown and lists the files and folders discovered.



```
Scan Results                                   Status
Scan Thread 1 (http://testphp.vulnweb.co...    Scanning
  Web Alerts (34)
    Apache Mod_Rewrite Off-By-One B...
    Macromedia Dreamweaver Remote ...
    PHP HTML Entity Encoder Heap Ove...
    PHP version older than 5.2.1 (1)
    PHP version older than 5.2.3 (1)
    PHP version older than 5.2.5 (1)
    PHP version older than 5.2.6 (1)
    PHP Zend_Hash_Del_Key_Or_Index...
    Apache 2.x version older than 2.0.6...
    Apache 2.x version older than 2.0.6...
    Apache httpd Remote Denial of Serv...
    Hidden form input named price was f...
    User credentials are sent in clear te...
    Broken links (5)
    Email address found (3)
    GHDB: Default phpinfo page (1)
    GHDB: Generic MySQL error messag...
    GHDB: phpinfo() (1)
    GHDB: SQL error message (2)
    Password type input with autocompl...
  Knowledge Base
  Site Structure
    /                                          OK
      admin                                    Forbidden
      AJAX                                     OK
      compat                                   Forbidden
      Connections                              Forbidden
      CVS                                      Forbidden
      Flash                                    Forbidden
      images                                   Forbidden
      Mod_Rewrite_Shop                         OK
      pictures                                 Forbidden
      secured                                  OK
      Templates                                Forbidden
      wvstests                                 Forbidden
      _mmServerScripts                         Forbidden
```

```
acunetix threat level
Level 3: High

Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by
the scanner. A malicious user can exploit these vulnerabilities and
compromise the backend database and/or deface your website.

Total alerts found        34
High                       8
Medium                     3
Low                        4
Informational             19

Target information        http://testphp.vulnweb.com:80/
Statistics                697 requests
Scan time                 16 minutes
Number of requests        697
Average response time     341.34 milliseconds
Scan iteration            1

Response time history

Progress                                        0.81%
Port scanner                                    Finished
Crawler                                         Finished
   Files found                                  88
   Directories found                            22
   Variations found                             60
Scripting                                       Running
   FCKEditor_Audit.script                       17 requests
   Idle
   Server_Source_Code_Disclosure.script         0%, 9 reque...

Web Scanner        Scanning 1 website(s) ...        Number of websites left to scan : 1
```

Screenshot 21 - Scan Result and Information window

Web Alerts node

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

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

If a vulnerability is detected by the AcuSensor Technology, (AS) is displayed next to the vulnerability group. More information about the vulnerability is shown when you click on an alert category node:

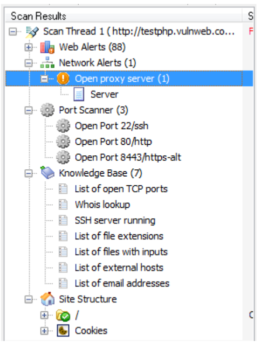
- **Vulnerability description** - A description of the discovered vulnerability.
- **Affected items** - The list of files vulnerable to the discovered vulnerability.
- **The impact of this vulnerability** – Level of impact on the website or web server if this vulnerability is exploited.
- **Attack details** - Details about the parameters and variables used to test for this vulnerability. E.g. for a Cross Site Scripting alert, the name of the exploited input variable and the string it was set to will be displayed. You can also find the HTTP request sent to the web server and the response sent back by the web server (including the HTML response). The attack can be inspected and re-launched manually by clicking **Launch the attack with HTTP Editor**. For more information, please refer to the HTTP Editor chapter on page 84.
- **How to fix this vulnerability** - This section provides recommendations on how to fix the vulnerability.
- **Detailed information** - This section provides detailed 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 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 Node



Screenshot 22 - Network, Port Scanner and Knowledge base nodes

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

Note: You can disable network security checks by un-ticking the **Enable Port Scanning** option in the Scan Wizard.

Port Scanner Node

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

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

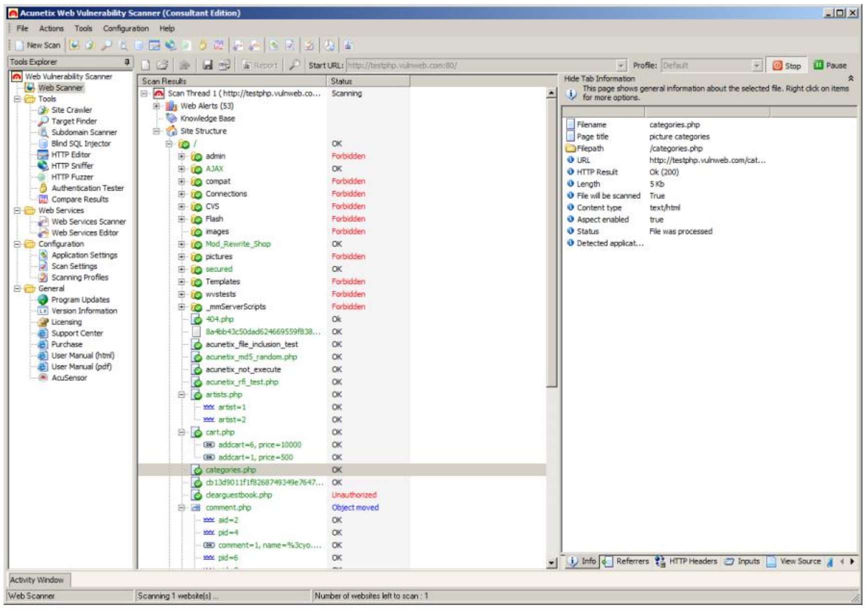
Knowledge Base Node

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

- List of open TCP ports found on the server, including the port banner.
- List of Network Services running on the web server and their response.
- List of files with inputs found on the website. Number of inputs per file are also shown.
- List of links to external hosts found on the website. E.g. testphp.vulnweb.com contains a link to www.acunetix.com.
- List of Client and Server HTTP error responses together with the HTTP requests that generated them. An example would be the response code Server Internal Error – HTTP 500. Check the response for information exposure.

Site Structure Node

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



Scan Results	Status
Scan Thread 1 (http://testphp.vulnweb.co...	Scanning
Web Alerts (53)	
Knowledge Base	
Site Structure	
/	OK
admin	Forbidden
AJAX	OK
compat	Forbidden
Connections	Forbidden
CVS	Forbidden
Flash	Forbidden
images	Forbidden
Mod_Rewrite_Shop	OK
pictures	Forbidden
secured	OK
Templates	Forbidden
wvstests	Forbidden
_mmServerScripts	Forbidden
404.php	Ok
8a4bb43c50dad624669559f838...	OK
acunetix_file_inclusion_test	OK
acunetix_md5_random.php	OK
acunetix_not_execute	OK
acunetix_rfi_test.php	OK
artists.php	OK
artist=1	OK
artist=2	OK
cart.php	OK
addcart=6, price=10000	OK
addcart=1, price=500	OK
categories.php	OK
cb13d9011f1f8268749349e7647...	OK
dearguestbook.php	Unauthorized
comment.php	Object moved
aid=2	OK
pid=4	OK
comment=1, name=%3cyo....	OK
pid=6	OK

This page shows general information about the selected file. Right click on items for more options.

Filename	categories.php
Page title	picture categories
Filepath	/categories.php
URL	http://testphp.vulnweb.com/cat...
HTTP Result	Ok (200)
Length	5 Kb
File will be scanned	True
Content type	text/html
Aspect enabled	true
Status	File was processed
Detected applicat...	

Scanning 1 website(s) ...

Number of websites left to scan : 1

Screenshot 23 - Scan Result and Information window

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

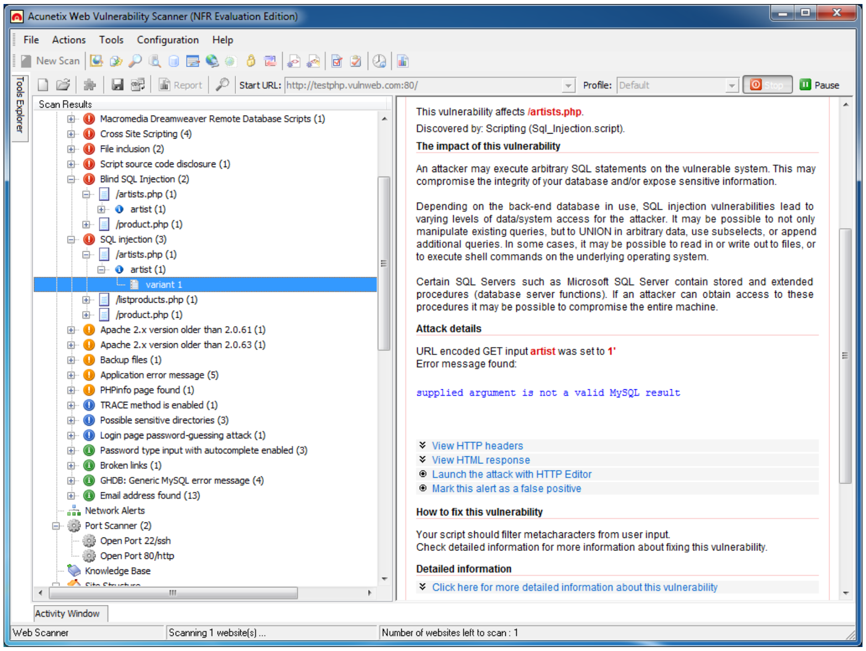
- **Green** – These files will be tested with AcuSensor Technology, resulting in more advanced security checks and less false positive alerts. From the AcuSensor data tab, the user can see what data related to these files is being returned from the AcuSensor. Such information is useful if a user wants to know what SQL queries were executed or if the file in question is using some functions which are monitored.
- **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 to avoid launching vulnerabilities against the computer on which Acunetix WVS is running.
- **HTML Structure Analysis** - HTML structure information such as
    - A list of links discovered on the file.
    - Comments discovered in the selected object. The information contained in the comments cannot be automatically analyzed but may reveal interesting information about the construction and coding of the website.
    - Any client side scripts (JavaScript, VBscript etc.) and their source code discovered in the selected object. The client web browser will execute these scripts. Such information might reveal information about the logic of the web application.
    - Any forms discovered in the selected object are shown in the top window. A list of parameters and their possible values are shown in the middle and bottom window.
    - A list of META tags discovered in the selected object. META tags contain information about the website, e.g. the description and keywords META tags used by search engines. META tags with an HTTP-EQUIV attribute are equivalent to HTTP headers. Typically, such META tags control the action of browsers and may be used to refine the information provided by the actual headers. Tags using this form should have an equivalent effect when specified as an HTTP header, and in some servers may be translated to actual HTTP headers automatically or by a pre-processing tool.
- **AcuSensor Data** – Any AcuSensor Technology data returned for the file.
- **Alerts** – A list of alerts this item is vulnerable to can be found in this tab.

Grouping of Vulnerabilities


Acunetix Web Vulnerability Scanner (NFR Evaluation Edition)
File
Actions
Tools
Configuration
Help
New Scan
Report
Start URL: http://testphp.vulnweb.com:80/
Profile: Default
Stop
Pause
Tools Explorer
Scan Results
Activity Window
Web Scanner
Scanning 1 website(s) ...
Number of websites left to scan : 1

- Macromedia Dreamweaver Remote Database Scripts (1)
- Cross Site Scripting (4)
- File inclusion (2)
- Script source code disclosure (1)
- Blind SQL Injection (2)
  - /artists.php (1)
    - artist (1)
  - /product.php (1)
- SQL injection (3)
  - /artists.php (1)
    - artist (1)
      - variant 1
  - /listproducts.php (1)
  - /product.php (1)
- Apache 2.x version older than 2.0.61 (1)
- Apache 2.x version older than 2.0.63 (1)
- Backup files (1)
- Application error message (5)
- PHPinfo page found (1)
- TRACE method is enabled (1)
- Possible sensitive directories (3)
- Login page password-guessing attack (1)
- Password type input with autocomplete enabled (3)
- Broken links (1)
- GHDB: Generic MySQL error message (4)
- Email address found (13)
- Network Alerts
- Port Scanner (2)
  - Open Port 22/ssh
  - Open Port 80/http
- Knowledge Base
- Site Structure

This vulnerability affects /artists.php.

Discovered by: Scripting (Sql_Injection.script).

The impact of this vulnerability

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use subselects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Attack details

URL encoded GET input artist was set to 1'
Error message found:

```
supplied argument is not a valid MySQL result
```

- View HTTP headers
- View HTML response
- Launch the attack with HTTP Editor
- Mark this alert as a false positive

How to fix this vulnerability

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

Detailed information

- Click here for more detailed information about this vulnerability

Screenshot 24 – Grouping of vulnerabilities

If the same vulnerability is detected on multiple pages, the scanner will group them under one alert node. Expanding the alert node will reveal the vulnerable pages. You can expand further to find the vulnerable parameters for that page. Grouping of vulnerabilities makes it easier to keep track of vulnerable pages and which vulnerabilities need to be fixed. Vulnerability data can also be grouped in reports by selecting the Vulnerability Report template in the reporting application.

Saving a Scan Result

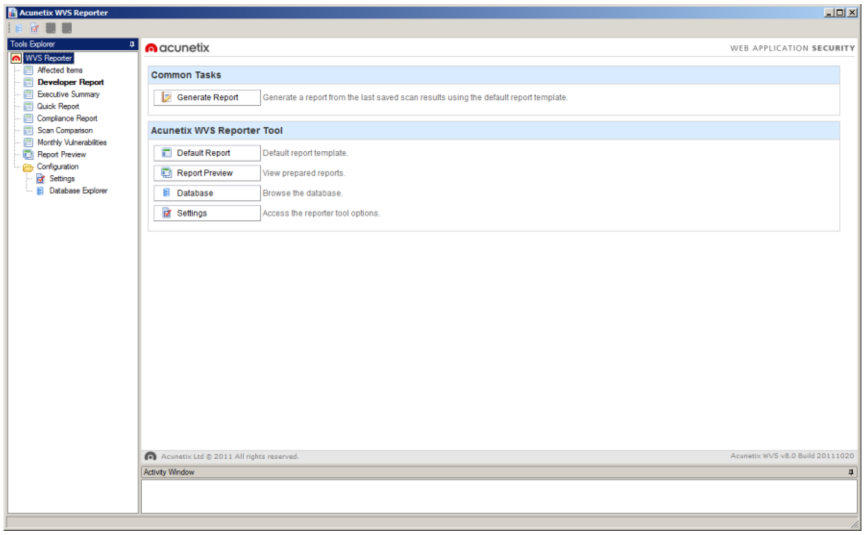
When a scan is completed you can save the scan results to an external file for analysis and comparison at a later stage. The saved file will contain all the scans from the current session including alert information and site structure.

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

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

5. Generating a Report from the results

Introduction to the Reporter



Generate Report — Generate a report from the last saved scan results using the default report template.

Default Report — Default report template.

Report Preview — View prepared reports.

Database — Browse the database.

Settings — Access the reporter tool options.

Acunetix Ltd © 2011 All rights reserved.

Acunetix WVS v8.0 Build 20111020

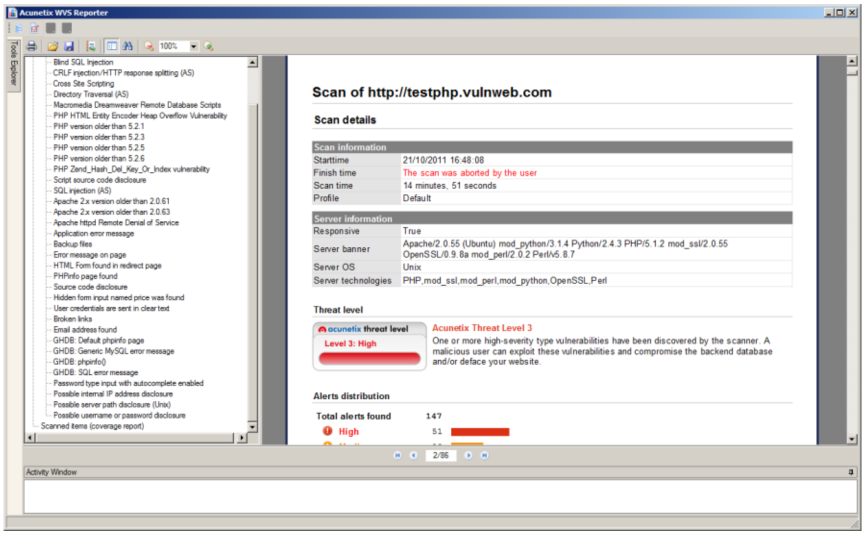
Screenshot 25 – The Reporter Application

The Reporter Application is a separate tool that allows you to generate reports from security scans performed. The results of a completed scan can be used to launch the Reporter directly from the Acunetix WVS, or from the Acunetix WVS program group. The following groups of reports can be produced:

- **Affected Items** – Organized by affected items on the website with detailed specifics of vulnerabilities found on each item.
- **Developer Report** – Used by developers of the website to easily fix discovered security issues.
- **Executive Report** – Useful for a management team to review a summary of a website's security status.
- **Quick Report** – A basic listing of single vulnerabilities per vulnerable file or affected parameter.
- **Compliance Standard Report** – Vulnerability reports designed to comply with regulatory and other standards bodies such as PCI DSS, OWASP and WASC
- **Scan Comparison Report** – Allow a comparison with previous scans to easily determine if issues were fixed or not.
- **Monthly vulnerabilities Report** – Statistical report of vulnerabilities found in scans from a given month.

Generating a Report from the Scan Results

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



Blind SQL Injection
CRLF injection/HTTP response splitting (AS)
Cross Site Scripting
Directory Traversal (AS)
Macromedia Dreamweaver Remote Database Scripts
PHP HTML Entity Encoder Heap Overflow Vulnerability
PHP version older than 5.2.1
PHP version older than 5.2.3
PHP version older than 5.2.5
PHP version older than 5.2.6
PHP Zend_Hash_Del_Key_Or_Index vulnerability
Script source code disclosure
SQL injection (AS)
Apache 2.x version older than 2.0.61
Apache 2.x version older than 2.0.63
Apache httpd Remote Denial of Service
Application error message
Backup files
Error message on page
HTML Form found in redirect page
PHPinfo page found
Source code disclosure
Hidden form input named price was found
User credentials are sent in clear text
Broken links
Email address found
GHDB: Default phpinfo page
GHDB: Generic MySQL error message
GHDB: phpinfo()
GHDB: SQL error message
Password type input with autocomplete enabled
Possible internal IP address disclosure
Possible server path disclosure (Unix)
Possible username or password disclosure
Scanned items (coverage report)

Scan of http://testphp.vulnweb.com

Scan details

Scan information	
Starttime	21/10/2011 16:48:08
Finish time	The scan was aborted by the user
Scan time	14 minutes, 51 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.0.55 (Ubuntu) mod_python/3.1.4 Python/2.4.3 PHP/5.1.2 mod_ssl/2.0.55 OpenSSL/0.9.8a mod_perl/2.0.2 Perl/v5.8.7
Server OS	Unix
Server technologies	PHP,mod_ssl,mod_perl,mod_python,OpenSSL,Perl

Threat level

acunetix threat level
Level 3: High

Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	147
High	51

Screenshot 26 – Default Generated Report from Scan Results

To generate a report;

1. Select the type of report template you would like to generate and click on 'Report Wizard' to launch a wizard to assist you in generating the report.
2. In the case of Compliance report, select the type of report you want to generate. Click 'Next'.
3. Configure the scan filter to list a number of specific saved scans, or leave the default selection to display all scan results. Click 'Next' to proceed and select the specific scan for which to generate a report.
4. Select what properties and details should the report include. Click 'Generate' button to finalize the wizard and generate the report.
5. Once the report is generated, it can be exported to various formats including PDF and HTML.

Affected Items Report

The **Affected Items Report** groups scan results based on affected files and includes both the request and response HTTP Headers. Included is also a coverage report, which is a list of all the URLs that have been automatically scanned.

Developer Report

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

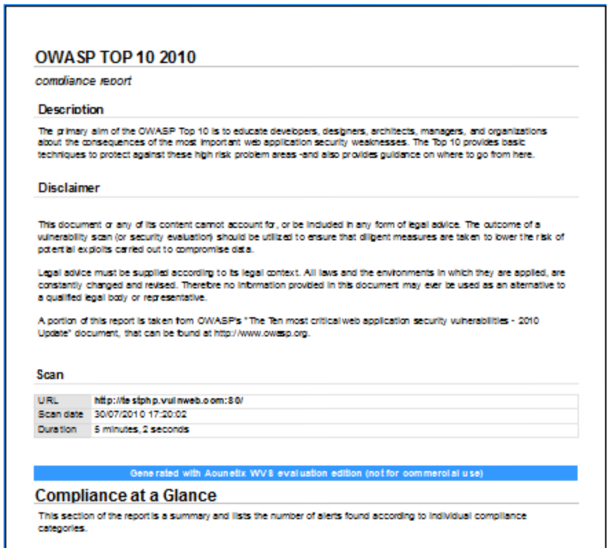
Executive Report

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

Quick Report

The Quick Report lists the individual vulnerabilities and the affected items without any type of grouping or sorting. From this report you can have a generic idea of what type of vulnerabilities can be exploited on your website.

Compliance Reports



OWASP TOP 10 2010

compliance report

Description

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

Disclaimer

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

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

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

Scan

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

Generated with Acunetix WVS evaluation edition (not for commercial use)

Compliance at a Glance

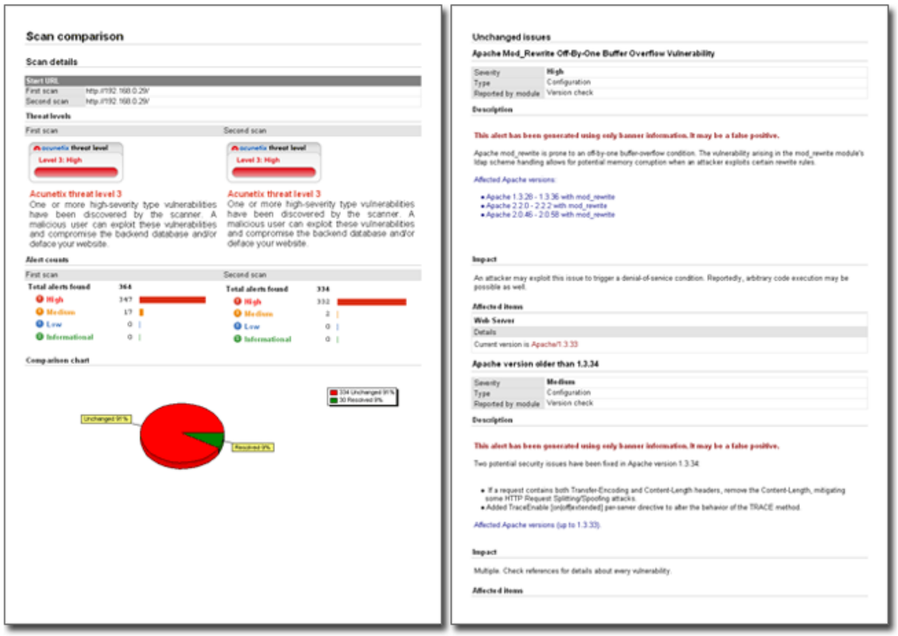
This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

Screenshot 27 – Compliance Report

The compliance feature allows you to generate reports based on various compliance standard specifications. An easy to use wizard will prioritize and report specific vulnerabilities according to the standardized format as specified by the following compliance bodies;

- The Health Insurance Portability and Accountability Act (HIPAA)
- OWASP Top10
- Payment Card Industry (PCI) standards
- Sarbanes Oxley Act of 2002
- Web Application Security Consortium (WASC) Threat Classification
- NIST Special Publication 800-53
- DISA STIG Web Security

Scan Comparison Report



Scan comparison

Scan details

Start URL	
First scan	http://192.168.0.29/
Second scan	http://192.168.0.29/

Threat levels

First scan	Second scan
acunetix threat level Level 3: High	acunetix threat level Level 3: High
Acunetix threat level 3 One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.	Acunetix threat level 3 One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alert counts

First scan		Second scan	
Total alerts found	364	Total alerts found	334
High	347	High	332
Medium	17	Medium	2
Low	0	Low	0
Informational	0	Informational	0

Comparison chart

Unchanged issues

Apache Mod_Rewrite Off-By-One Buffer Overflow Vulnerability

Severity	High
Type	Configuration
Reported by module	Version check

Description

This alert has been generated using only banner information. It may be a false positive.

Apache mod_rewrite is prone to an off-by-one buffer-overflow condition. The vulnerability arising in the mod_rewrite module's ldap scheme handling allows for potential memory corruption when an attacker exploits certain rewrite rules.

Affected Apache versions:

- Apache 1.3.28 - 1.3.36 with mod_rewrite
- Apache 2.2.0 - 2.2.2 with mod_rewrite
- Apache 2.0.46 - 2.0.58 with mod_rewrite

Impact

An attacker may exploit this issue to trigger a denial-of-service condition. Reportedly, arbitrary code execution may be possible as well.

Affected items

Web Server
Details
Current version is Apache/1.3.33

Apache version older than 1.3.34

Severity	Medium
Type	Configuration
Reported by module	Version check

Description

This alert has been generated using only banner information. It may be a false positive.

Two potential security issues have been fixed in Apache version 1.3.34:

- If a request contains both Transfer-Encoding and Content-Length headers, remove the Content-Length, mitigating some HTTP Request Splitting/Spoofing attacks.
- Added TraceEnable [on|off|extended] per-server directive to alter the behavior of the TRACE method.

Affected Apache versions (up to 1.3.33).

Impact

Multiple. Check references for details about every vulnerability.

Affected items

Screenshot 28 – Comparison Report

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

Monthly Vulnerabilities Report

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

Customizing the Report Layout

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

Report Options

This configuration node consists of 2 sections that can be used to customize the layout, titles, and images in the headers of the report.

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

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

You can use these settings to customize the report layout and to apply corporate branding. These settings are global, therefore any changes made will appear across all the reports generated by the WVS Reporter.

Page Settings

The Page Settings node allows you to configure the default page size, orientation and margins of your reports.

The Report Viewer

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

Using Microsoft SQL

The Acunetix Reporter uses a backend database to store the scan results and generate reports from. Microsoft Access (included in Microsoft Windows) is used as the default database engine when Acunetix is installed, however you can also choose to use Microsoft SQL server to store scan results. To change the Reported database:

1. 1. Navigate to the ‘Configuration > Application Settings > Database’ node in the Acunetix WVS interface. Select MS SQL Server from the ‘Database Type’ drop down menu.
2. 2. Enter the Server IP or FQDN in the ‘Server’ text box and the credentials to connect to the server in the ‘Username’ and ‘Password’ text box.
3. 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.

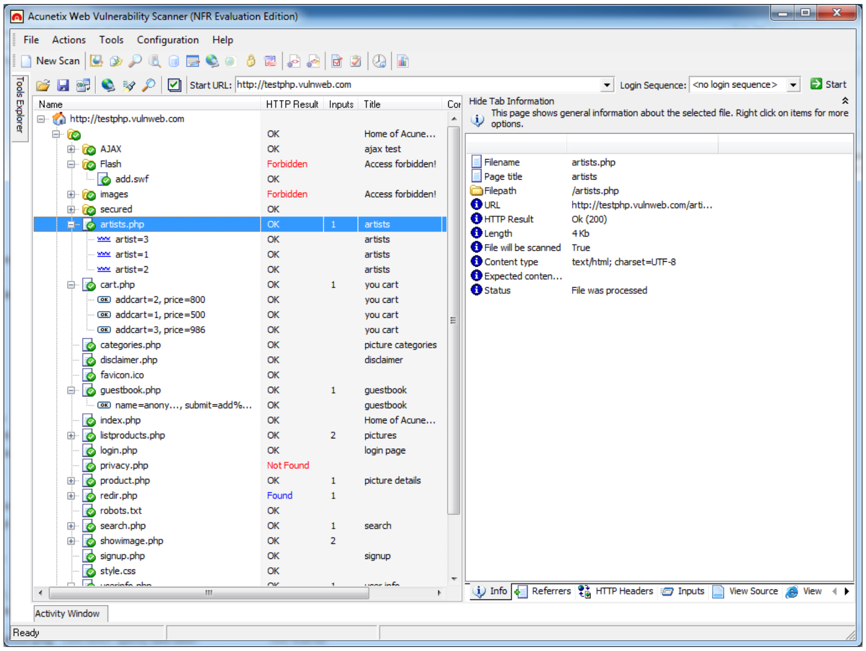
Note: To create a new database, a user with SQL Administrator privileges must be specified. If an existing database is specified, a user with Administrator privileges on the specified database ONLY is required. Once the database is created, a user account with only read and write permissions can be used to access 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.

6. Site Crawler Options

Introduction

The Site Crawler analyses a target website and builds the site structure using the information collected, including the site’s directories and files / objects. You can also use the site Crawler tool to analyze the structure of a website without automatically launching the attacks.



Start URL: http://testphp.vulnweb.com

Login Sequence: <no login sequence>

Start

Name	HTTP Result	Inputs	Title
http://testphp.vulnweb.com			
	OK		Home of Acune…
AJAX	OK		ajax test
Flash	Forbidden		Access forbidden!
add.swf	OK		
images	Forbidden		Access forbidden!
secured	OK		
artists.php	OK	1	artists
artist=3	OK		artists
artist=1	OK		artists
artist=2	OK		artists
cart.php	OK	1	you cart
addcart=2, price=800	OK		you cart
addcart=1, price=500	OK		you cart
addcart=3, price=986	OK		you cart
categories.php	OK		picture categories
disclaimer.php	OK		disclaimer
favicon.ico	OK		
guestbook.php	OK	1	guestbook
name=anony…, submit=add%…	OK		guestbook
index.php	OK		Home of Acune…
listproducts.php	OK	2	pictures
login.php	OK		login page
privacy.php	Not Found		
product.php	OK	1	picture details
redir.php	Found	1	
robots.txt	OK		
search.php	OK	1	search
showimage.php	OK	2	
signup.php	OK		signup
style.css	OK		

This page shows general information about the selected file. Right click on items for more options.

Filename	artists.php
Page title	artists
Filepath	/artists.php
URL	http://testphp.vulnweb.com/arti…
HTTP Result	Ok (200)
Length	4 Kb
File will be scanned	True
Content type	text/html; charset=UTF-8
Expected conten…	
Status	File was processed

Screenshot 29 – The crawler tool interface

The interface of the Crawler tool consists of:

- **Site structure window** (left hand side) – Displays target site information fetched by the crawler, e.g., cookies, robots, files and directories.
- **Details window** (right hand side) – Displays general information about a file selected in the site structure window (e.g., filename, file path etc.). A series of tabs at the bottom of the Details window display further information about the selected object.

It is also possible to load the results of a previously saved crawl or save the results of a completed crawl. If you use the option **choose files to be scanned** to select / deselect a number of, these changes will also be saved along with the crawl results.

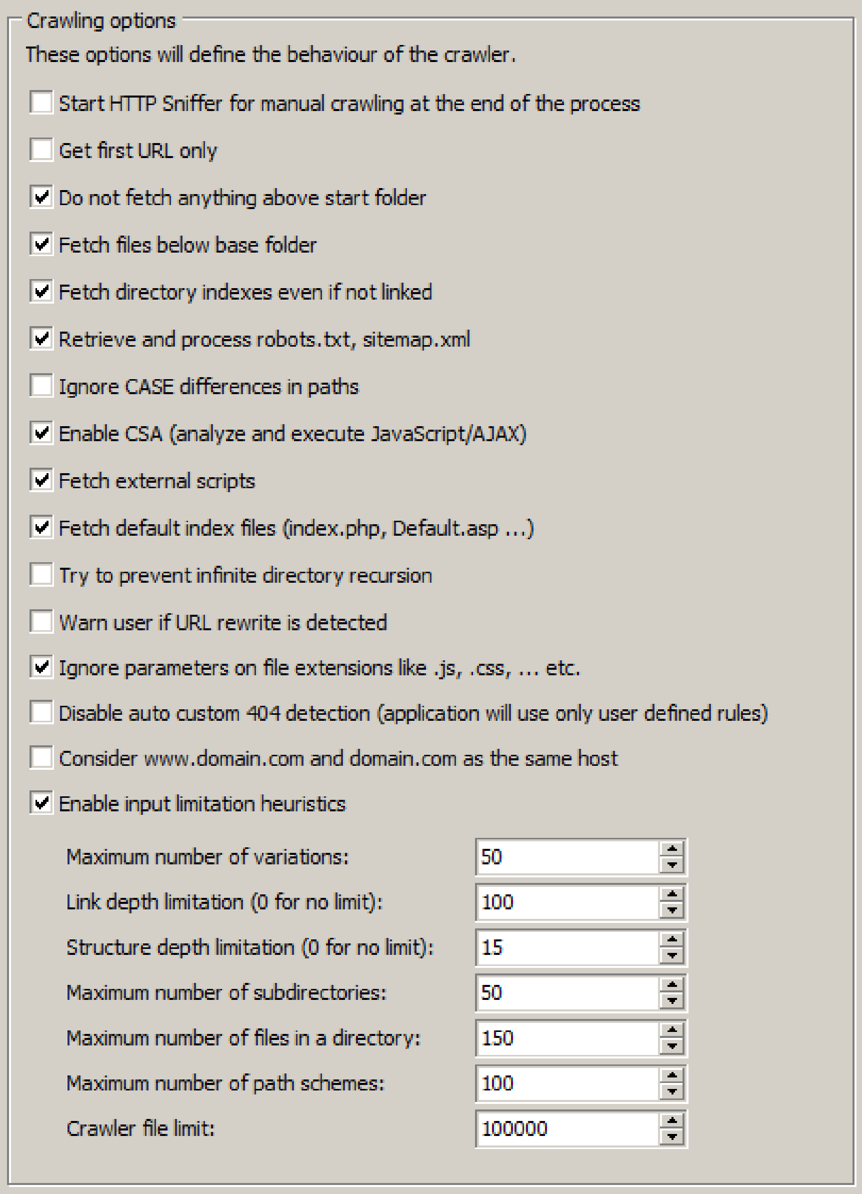
Starting a Website Crawl

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

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

Once a crawl is complete, you can specify which of the crawled files should be scanned for vulnerabilities. By default all files are scanned.

Crawler options



Crawling options

These options will define the behaviour of the crawler.

☐ Start HTTP Sniffer for manual crawling at the end of the process

☐ Get first URL only

☑ Do not fetch anything above start folder

☑ Fetch files below base folder

☑ Fetch directory indexes even if not linked

☑ Retrieve and process robots.txt, sitemap.xml

☐ Ignore CASE differences in paths

☑ Enable CSA (analyze and execute JavaScript/AJAX)

☑ Fetch external scripts

☑ Fetch default index files (index.php, Default.asp ...)

☐ Try to prevent infinite directory recursion

☐ Warn user if URL rewrite is detected

☑ Ignore parameters on file extensions like .js, .css, ... etc.

☐ Disable auto custom 404 detection (application will use only user defined rules)

☐ Consider www.domain.com and domain.com as the same host

☑ Enable input limitation heuristics

Maximum number of variations:	50
Link depth limitation (0 for no limit):	100
Structure depth limitation (0 for no limit):	15
Maximum number of subdirectories:	50
Maximum number of files in a directory:	150
Maximum number of path schemes:	100
Crawler file limit:	100000

Screenshot 30 –Site crawler options

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

- **Start HTTP Sniffer for manual crawling at the end of the scan process** - This option will start the HTTP Sniffer at the end of the crawl to allow manual crawling by enabling the user to browse to parts of the site that were not discovered by the crawler. Typically the Acunetix WVS crawler is able to crawl every web application though there are some specific scenarios were it fails to do so automatically. The crawler will update the website structure with the newly discovered links and pages.

- **Get first URL only** - Scan only the index or first page of the target site and do not crawl any links.
- **Do not fetch anything above start folder** - By enabling this option the crawler will not traverse any links that point to a location above the base link. E.g. if http://testphp.vulnweb.com/wvs/ is the base URL, the crawler will not crawl to links which point to a location above the base URL like http://testphp.vulnweb.com.
- **Fetch files below base folder** - By enabling this option the crawler will follow links that point to locations outside the base folder. E.g. if http://testphp.vulnweb.com/ is the base URL, it will still traverse the links which point to an object which resides in a sub directory below the base folder, like http://testphp.acunetix.com/wvs/. With this option disabled, the crawler will not crawl any objects from the root's sub directories.
- **Fetch directory indexes even if not linked** – When enabled the crawler will try to request the directory index for every discovered directory even if the directory index is not directly linked from another source.
- **Retrieve and process robots.txt, sitemap.xml** - By enabling this option the crawler will search for a robots.txt or sitemap.xml file in the target website, and follow all the links specified if robots or sitemap are detected..
- **Ignore CASE differences in paths -** By enabling this option the crawler will ignore any case difference in the links found on the website. E.g. "/Admin" will be considered the same as "/admin".
- **Enable CSA (analyze and execute JavaScript/AJAX) –** The Client Script Analyzer (CSA) is enabled by default during crawling. This will execute JavaScript/AJAX code on the website to gather a more complete site structure.
- **Fetch external scripts –** With this option enabled, the CSA engine will fetch all external resources linked through client scripts running on the target. The external resources will only be crawled and will not be scanned. If this option is not enabled and a client script uses external resources, the CSA engine will not be able to analyze the client script correctly, which might result in an incomplete crawl.
- **Fetch default index files (index.php, Default.asp …) -** If this option is enabled, the crawler will try to fetch common default index filenames (such as index.php, Default.asp) for every folder, even if not directly linked.
- **Try to prevent infinite directory recursion –** In certain website structures, there is an uncommon probability that the scanner will start looping when trying to fetch the same directory recursively (e.g. /images/images/images/images/…). Enabling this setting will instruct the scanner to try to prevent this situation by identifying repeated directory names in recursion.
- **Warn user if URL rewrite is detected –** Enable this option to be notified if URL rewrite is detected during the crawling stage of a scan.
- **Ignore parameters on file extensions like .js, .css etc–** When enabled, Acunetix WVS will not scan parameters on files which are not typically accessed directly by a user, such as js, css etc.

- **Disable auto custom 404 detection –** By default Acunetix WVS will automatically try to detect custom 404 error pages and detect a recognition pattern. With this option enabled, Acunetix WVS will not automatically detect 404 error pages, thereby requiring 404 recognition patterns to be configured manually. You can read more about Custom 404 Error Page rules from page 92 of this manual.
- **Consider www.domain.com and domain.com as the same host –** If this option is enabled, Acunetix WVS will scan both sites www.domain.com and domain.com and treat them as one instead of separate hosts.
- **Enable input limitation heuristics –** If this option is enabled and more than 20 identical input schemes are detected on files in the same directory, the crawler will only crawl the first 20 identical input schemes.
- **Maximum number of variations –** In this option you can specify the maximum number of variations for a file. E.g. index.asp has a GET parameter ID of which the crawler discovered 10 possible values from links requesting the page. Each of these links is considered a variation and each variation will appear under the file in the Scan Tree during crawling.
- **Link Depth Limitation –** This option allows you to configure the maximum number of links to crawl from the root URL.
- **Structure Depth Limitation –** This option allows you to configure the maximum number of directories to crawl from the root URL.
- **Maximum number of sub directories –** This option allows you to configure the maximum number of sub directories Acunetix WVS should crawl in a website. Upon reaching the configured limit, Acunetix WVS will stop crawling further sub directories.
- **Maximum number of files in a directory –** In this option you can configure the maximum number of files in a directory. Upon reaching the configured limit, Acunetix WVS will stop crawling a directory and proceed to the next one.
- **Maximum number of path schemes –** In this option you can specify the maximum number of path schemes that should be detected by the crawler. You should only tweak this setting if you are crawling a very large website and notice that some path schemes are not being crawled.
- **Crawler file limit –** This option allows you to configure the maximum number of files the crawler should crawl during a website crawl.

File Extension Filters

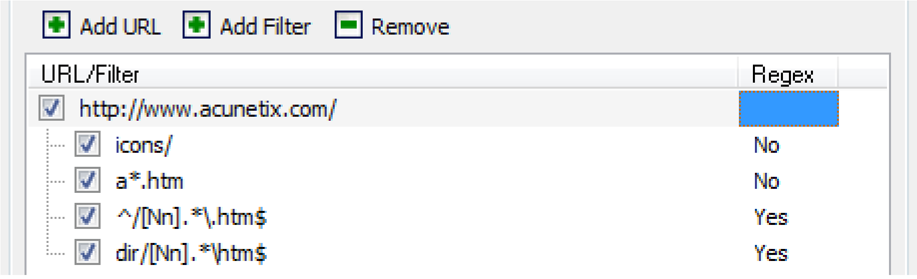
It is possible to configure a list of file extensions to be included or excluded during a crawl. This is done by matching the respective extension of the files specified in any of the columns listed below.

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

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

Directory and File Filters

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



URL/Filter	Regex
☑ http://www.acunetix.com/	
☑ icons/	No
☑ a*.htm	No
☑ ^/[Nn].*\.htm$	Yes
☑ dir/[Nn].*\htm$	Yes

Screenshot 31 – Directory and File Filter rules

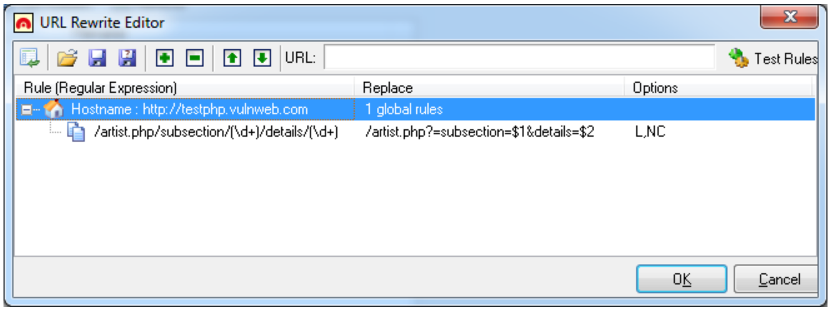
To add a directory or file rule:

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

Note: Directory and file filters specified for the root or any other directory of a website are not inherited by their sub directories, therefore a filters must be specified separately for sub-directories, as shown in the screen shot above.

URL Rewrite rules

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



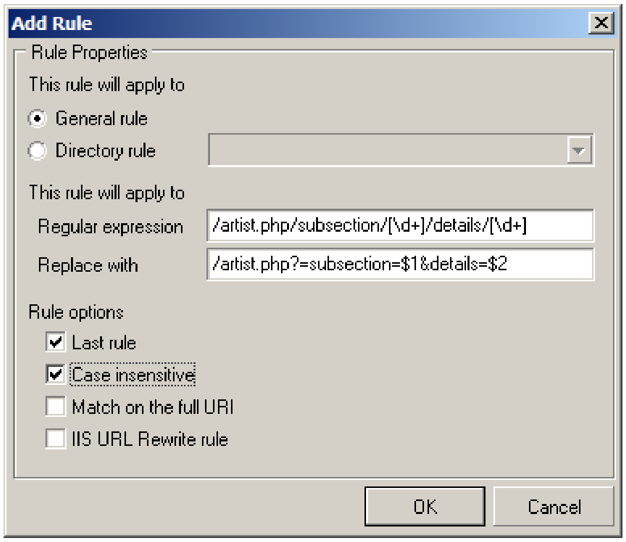
Rule (Regular Expression)	Replace	Options
Hostname : http://testphp.vulnweb.com	1 global rules	
/artist.php/subsection/(\d+)/details/(\d+)	/artist.php?=subsection=$1&details=$2	L,NC

Screenshot 32 – URL Rewrite Configuration

Adding a URL rewrite rule manually

1. Navigate to the 'Configuration > Scan Settings > Crawling Options > URL rewrite' node.

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



Add Rule

Rule Properties

This rule will apply to

● General rule

○ Directory rule

This rule will apply to

Regular expression: /artist.php/subsection/[\d+]/details/[\d+]

Replace with: /artist.php?=subsection=$1&details=$2

Rule options

☑ Last rule

☑ Case insensitive

□ Match on the full URI

□ IIS URL Rewrite rule

Screenshot 33 – URL Rewrite Rule

1. Specify if the rule-set is generic for the whole website by ticking **General rule**. If for a specific directory only, tick **Directory rule** and specify the directory name.
2. In the **Regular Expression** input field, specify a part of the URL including regular expressions (or a group of Regular expressions) which Acunetix WVS should use to recognize a rewritten URL. E.g. “Details/.*/(\d+)” indicates that everything must be matched after the Details/ directory, as well as subsequent strings beginning with digits.
3. In the **Replace with** input field, specify the URL Acunetix WVS should request instead of the rewritten URL. E.g. /Mod_Rewrite_Shop/details.php?id=$1. The $1 will be replaced with the value retrieved from the first regular expression group specified in the **Regular Expression** input field, in this case (\d+). For example, if Acunetix finds this URL; /Mod_Rewrite_Shop/Details/network-storage-d-link-dns-313-enclosure-1-x-sata/1, it will request the following; /Mod_Rewrite_Shop/details.php?id=1.
4. Tick the **Last rule** option to indicate that no more rules should be executed after this one.
5. Tick **Case insensitive** if the URLs are not case sensitive.
6. Tick **Match on the full URI** option so that the regular expression is executed on the whole URI with the query, instead of the path only.
7. Tick **IIS URL rewrite rule** if the target website is using Microsoft Windows IIS URL rewrite rules (http://www.iis.net/download/urlrewrite).
8. To test the URL rewrite rule, enter a URL and click **Test Rule**.

Importing a URL Rewrite rule configuration from an Apache web server

To import the rewrite rule logic for Apache web servers:

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

Importing a URL Rewrite rule configuration from an IIS web server

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

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

Note: Every Scan Settings template can have different crawler settings. Refer to page 88 of this user manual to read more on how to modify or create new Scan Settings templates.

Custom Cookies

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

To add a custom cookie:

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

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

Traversing Web Form pages

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

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

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

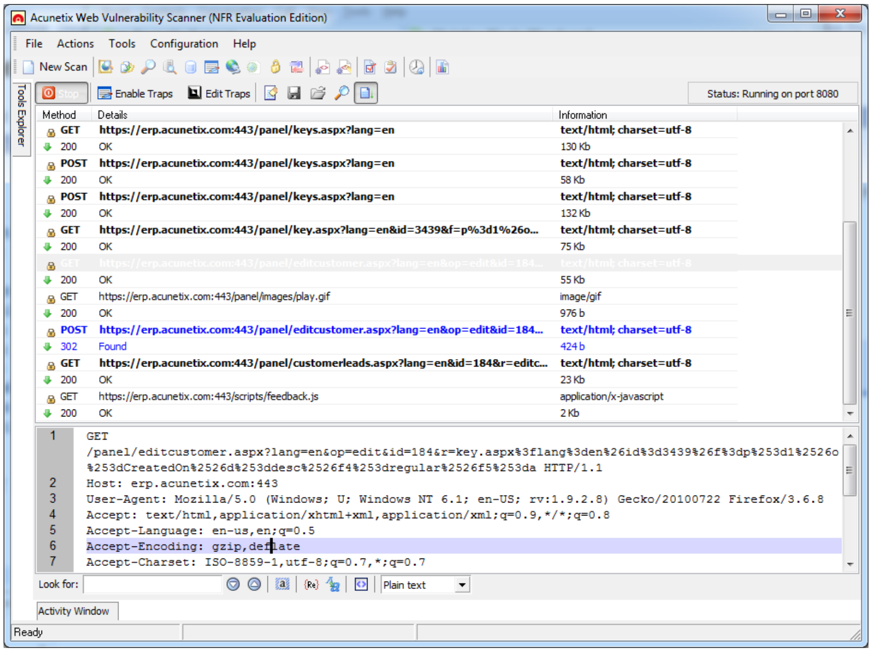
1. Navigate to the Configuration > Scan Settings > Input Fields node.
2. Enter the URL of the webpage or web service containing the specific form or list of operations to which pre-defined values must be passed, and click **Parse from URL** button.
3. The resulting list will then be automatically completed with the form fields found in the given URL.
4. Enter the values for the required fields by double clicking the respective value column. Click **Apply** to save changes.
5. Input fields also support wildcards to match a broad range of data. Below you can find a number of examples:
    - **cus** is used to match any number of characters before and after the pattern 'cus'
    - **cus* is used to match any number of characters before the pattern 'cus'
    - *cus** is used to match any number of characters after the pattern 'cus'
    - *?cus* is used to match a single character before the pattern 'cus'
    - *c?us* is used to match a single character as a second character in the pattern specified
6. Alternatively, you can configure Acunetix WVS to automatically randomize the values for each input field by entering the bolded variable names below in the parameter's value field:
    - **${alpharand}** – Automatically submit random alphabetical characters (a –z)
    - **$[numrand}** – Automatically submit random numeric characters (0 - 9)
    - **${alphanumrand}** – Automatically submit random alphabetical and numeric characters (a – z, 0 – 9)

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

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

7. Manual crawling with the HTTP Sniffer

Introduction



Method	Details	Information
GET	https://erp.acunetix.com:443/panel/keys.aspx?lang=en	text/html; charset=utf-8
200	OK	130 Kb
POST	https://erp.acunetix.com:443/panel/keys.aspx?lang=en	text/html; charset=utf-8
200	OK	58 Kb
POST	https://erp.acunetix.com:443/panel/keys.aspx?lang=en	text/html; charset=utf-8
200	OK	132 Kb
GET	https://erp.acunetix.com:443/panel/key.aspx?lang=en&id=3439&f=p%3d1%26o...	text/html; charset=utf-8
200	OK	75 Kb
GET	https://erp.acunetix.com:443/panel/editcustomer.aspx?lang=en&op=edit&id=184...	text/html; charset=utf-8
200	OK	55 Kb
GET	https://erp.acunetix.com:443/panel/images/play.gif	image/gif
200	OK	976 b
POST	https://erp.acunetix.com:443/panel/editcustomer.aspx?lang=en&op=edit&id=184...	text/html; charset=utf-8
302	Found	424 b
GET	https://erp.acunetix.com:443/panel/customerleads.aspx?lang=en&id=184&r=editc...	text/html; charset=utf-8
200	OK	23 Kb
GET	https://erp.acunetix.com:443/scripts/feedback.js	application/x-javascript
200	OK	2 Kb

```
GET
/panel/editcustomer.aspx?lang=en&op=edit&id=184&r=key.aspx%3flang%3den%26id%3d3439%26f%3dp%253d1%2526o
%253dCreatedOn%2526d%253ddesc%2526f4%253dregular%2526f5%253da HTTP/1.1
Host: erp.acunetix.com:443
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
```

Screenshot 34 – The HTTP Sniffer

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

The HTTP Sniffer can be used to manually crawl sections of a website that cannot be crawled automatically by Acunetix WVS. Using the HTTP Sniffer, sections of the website that cannot be crawled automatically can be loaded in a web browser for HTTP traffic to be captured in real-time as various objects are clicked. The captured data can then be loaded into the Crawler and used to launch a scan.

To capture live traffic, your web browser must be configured to proxy through the HTTP Sniffer and then export the logs to the Site Crawler.

You can read more about this process from the following URL;
http://www.acunetix.com/blog/docs/manual-crawling-http-sniffer/

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

Configuring the HTTP Sniffer

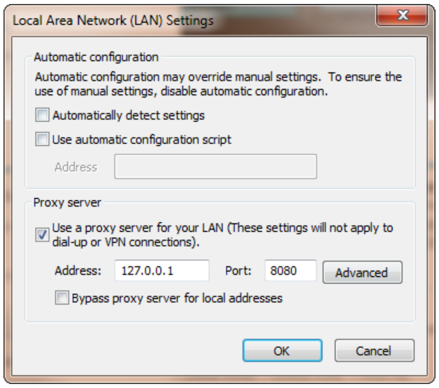
To start capturing traffic, you must first configure your browser to use the Acunetix HTTP Sniffer as proxy server:

Mozilla Firefox

1. From the Tools drop down menu select **Internet Options**
2. Select **Lan Settings** from the **Connections** tab

3. In the Connection section click on Settings and tick Manual proxy configuration
4. Set **HTTP Proxy** to 127.0.0.1 and **Port** to 8080
5. If you also need to capture SSL traffic, configure the **SSL Proxy** to 127.0.0.1 and **Port** to 8080
6. Click **OK** to save all options and close all configuration windows.

Internet Explorer



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 127.0.0.1 Port: 8080

□ Bypass proxy server for local addresses

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

Google Chrome

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

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

The HTTP Sniffer options in Acunetix WVS can be accessed from the Configuration > Application Settings > HTTP Sniffer node.

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

Capturing HTTP traffic

To capture HTTP traffic:

7. Go to the Tools > HTTP sniffer node
8. Click on the **Start** button to enable the HTTP Sniffer. All HTTP requests and responses will be listed in the main window.

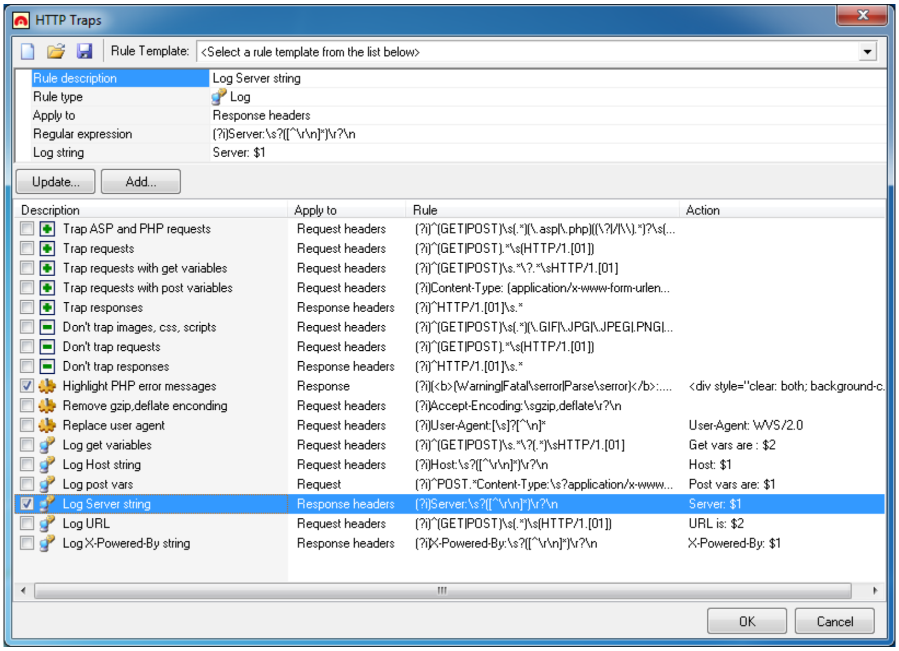
9. Click on a request or response to view the complete details. All the requests/responses will be displayed in the lower window pane.
10. Click **Stop** when browsing is complete. Keep in mind that when the HTTP Sniffer is stopped, the web browser will lose its connection to the target URL.
11. You can then save the browsing logs, and load them into the crawler. Click **Save** to store the logs.
12. Go to Tools > Site Crawler and click on the **Build structure from HTTP sniffer log** button. Browse to the sniffer log you just saved.
13. The crawler will build the structure. You can then right click on the site and scan it from within the Crawler, or save the crawl results and load them into the web scanner.

For more information about using the HTTP sniffer:

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

HTTP Sniffer Trap Filters

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



Rule Template: <Select a rule template from the list below>

Rule description	Log Server string
Rule type	Log
Apply to	Response headers
Regular expression	(?i)Server:\s?([^\r\n]*)\r?\n
Log string	Server: $1

Description	Apply to	Rule	Action
☐ Trap ASP and PHP requests	Request headers	(?i)^(GET|POST)\s(.*)(\.asp|\.php)((\?|/|\\).*)?\s(...	
☐ Trap requests	Request headers	(?i)^(GET|POST).*\s(HTTP/1.[01])	
☐ Trap requests with get variables	Request headers	(?i)^(GET|POST)\s.*\?.*\sHTTP/1.[01]	
☐ Trap requests with post variables	Request headers	(?i)Content-Type: (application/x-www-form-urlen...	
☐ Trap responses	Response headers	(?i)^HTTP/1.[01]\s.*	
☐ Don't trap images, css, scripts	Request headers	(?i)^(GET|POST)\s(.*)(\.GIF|\.JPG|\.JPEG|.PNG|...	
☐ Don't trap requests	Request headers	(?i)^(GET|POST).*\s(HTTP/1.[01])	
☐ Don't trap responses	Response headers	(?i)^HTTP/1.[01]\s.*	
☑ Highlight PHP error messages	Response	(?i)(<b>(Warning|Fatal\serror|Parse\serror)</b>:....	<div style="clear: both; background-c.
☐ Remove gzip,deflate enconding	Request headers	(?i)Accept-Encoding:\sgzip,deflate\r?\n	
☐ Replace user agent	Request headers	(?i)User-Agent:[\s]?[^\n]*	User-Agent: WVS/2.0
☐ Log get variables	Request headers	(?i)^(GET|POST)\s.*\?(.*)\sHTTP/1.[01]	Get vars are : $2
☐ Log Host string	Request headers	(?i)Host:\s?([^\r\n]*)\r?\n	Host: $1
☐ Log post vars	Request	(?i)^POST.*Content-Type:\s?application/x-www...	Post vars are: $1
☑ Log Server string	Response headers	(?i)Server:\s?([^\r\n]*)\r?\n	Server: $1
☐ Log URL	Request headers	(?i)^(GET|POST)\s(.*)\s(HTTP/1.[01])	URL is: $2
☐ Log X-Powered-By string	Response headers	(?i)X-Powered-By:\s?([^\r\n]*)\r?\n	X-Powered-By: $1

Screenshot 35 - HTTP Sniffer Edit Trap window

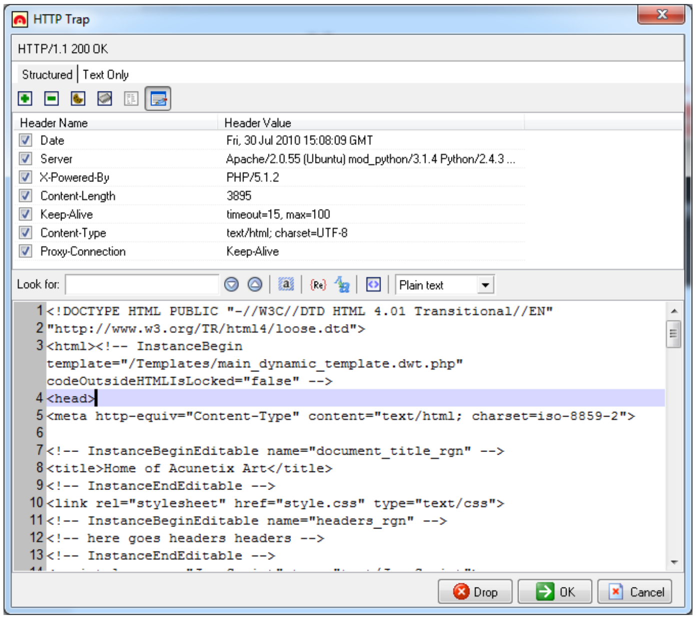
Creating a HTTP Sniffer Trap Filter

1. In the HTTP Sniffer toolbar, click on the **Edit traps** button to launch the HTTP Traps window.
2. Select a trap rule template, e.g. trap requests, and trap ASP or PHP requests. This will load up a preconfigured trap which you can edit.
3. Alternatively you can create a new trap by first entering a description for the rule.
4. Specify the rule type from the following 4 options:

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

5. The type of traffic that will be captured by the trap must also be configured. Traps can be set to capture all traffic, HTTP requests only, request headers only, etc.
6. In the Regular expression option, enter a regular expression that matches the data you would like to trap.
7. Once the new trap is ready, click on the ‘Add…’ button to save the new trap. This will add the trap and automatically enable it. You can enable/disable traps by clicking on the tick box in front of the trap rule.
8. Click the ‘OK’ button to return to the HTTP Sniffer dialog and click on the ‘Enable traps’ button to activate the traps in the HTTP Sniffer.

The Trap Form



HTTP/1.1 200 OK

	Header Name	Header Value
☑	Date	Fri, 30 Jul 2010 15:08:09 GMT
☑	Server	Apache/2.0.55 (Ubuntu) mod_python/3.1.4 Python/2.4.3 ...
☑	X-Powered-By	PHP/5.1.2
☑	Content-Length	3895
☑	Keep-Alive	timeout=15, max=100
☑	Content-Type	text/html; charset=UTF-8
☑	Proxy-Connection	Keep-Alive

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin
template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
```

Screenshot 36 - HTTP Sniffer Trap form

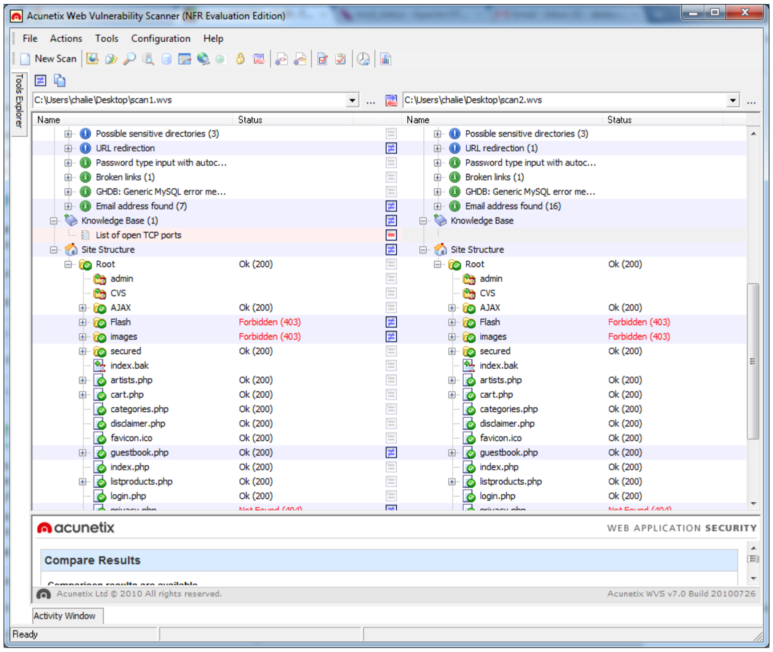
When an HTTP request or a response is trapped by the HTTP Sniffer, the **HTTP Trap** window will automatically appear to allow you to edit the captured data. Similarly to the HTTP Editor, the Trap Form editor allows you to edit headers, cookies, queries, and post variables. Click **OK** to allow the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

Editing a HTTP Request without a Trap

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

8. Compare Results Tool

Introduction



C:\Users\chalie\Desktop\scan1.wvs

C:\Users\chalie\Desktop\scan2.wvs

Name	Status		Name	Status
Possible sensitive directories (3)		=	Possible sensitive directories (3)	
URL redirection		≠	URL redirection (1)	
Password type input with autoc...		=	Password type input with autoc...	
Broken links (1)		=	Broken links (1)	
GHDB: Generic MySQL error me...		=	GHDB: Generic MySQL error me...	
Email address found (7)		≠	Email address found (16)	
Knowledge Base (1)		≠	Knowledge Base	
List of open TCP ports		−		
Site Structure		≠	Site Structure	
Root	Ok (200)	=	Root	Ok (200)
admin		=	admin	
CVS		=	CVS	
AJAX	Ok (200)	=	AJAX	Ok (200)
Flash	Forbidden (403)	≠	Flash	Forbidden (403)
images	Forbidden (403)	≠	images	Forbidden (403)
secured	Ok (200)	=	secured	Ok (200)
index.bak		=	index.bak	
artists.php	Ok (200)	=	artists.php	Ok (200)
cart.php	Ok (200)	=	cart.php	Ok (200)
categories.php	Ok (200)	=	categories.php	Ok (200)
disclaimer.php	Ok (200)	=	disclaimer.php	Ok (200)
favicon.ico	Ok (200)	=	favicon.ico	Ok (200)
guestbook.php	Ok (200)	≠	guestbook.php	Ok (200)
index.php	Ok (200)	=	index.php	Ok (200)
listproducts.php	Ok (200)	=	listproducts.php	Ok (200)
login.php	Ok (200)	=	login.php	Ok (200)
privacy.php	Not Found (404)	≠	privacy.php	Not Found (404)

acunetix WEB APPLICATION SECURITY

Compare Results

Comparison results are available

Acunetix Ltd © 2010 All rights reserved. Acunetix WVS v7.0 Build 20100726

Screenshot 37 – Compare Results Tool

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

Comparing Results

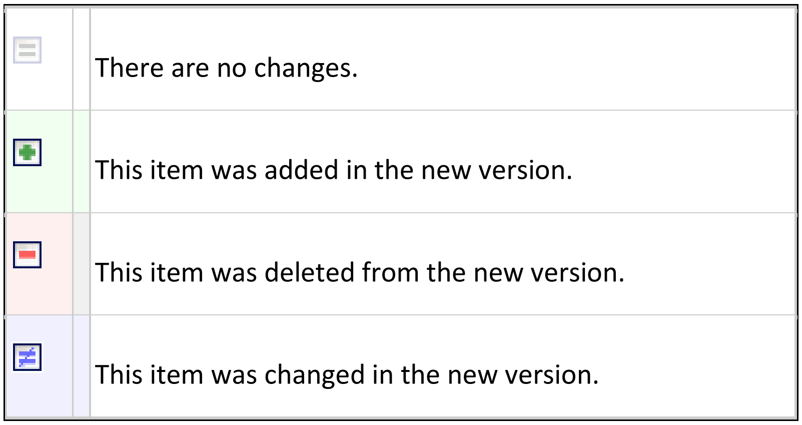
To compare two saved scan results;

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

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

Analyzing the Results Comparison

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



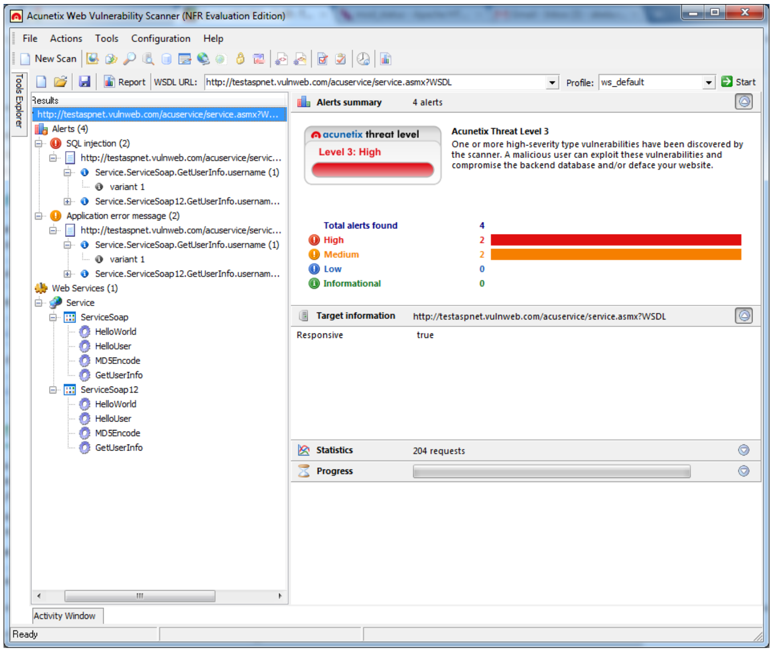
=		There are no changes.
+		This item was added in the new version.
−		This item was deleted from the new version.
≠		This item was changed in the new version.

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

9. Scanning Web Services

Introduction

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



WSDL URL: http://testaspnet.vulnweb.com/acuservice/service.asmx?WSDL
Profile: ws_default

Results
http://testaspnet.vulnweb.com/acuservice/service.asmx?W...
Alerts (4)
SQL injection (2)
http://testaspnet.vulnweb.com/acuservice/servic...
Service.ServiceSoap.GetUserInfo.username (1)
variant 1
Service.ServiceSoap12.GetUserInfo.usernam...
Application error message (2)
http://testaspnet.vulnweb.com/acuservice/servic...
Service.ServiceSoap.GetUserInfo.username (1)
variant 1
Service.ServiceSoap12.GetUserInfo.usernam...
Web Services (1)
Service
ServiceSoap
HelloWorld
HelloUser
MD5Encode
GetUserInfo
ServiceSoap12
HelloWorld
HelloUser
MD5Encode
GetUserInfo

Alerts summary 4 alerts

acunetix threat level
Level 3: High

Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Total alerts found	4
High	2
Medium	2
Low	0
Informational	0

Target information http://testaspnet.vulnweb.com/acuservice/service.asmx?WSDL
Responsive true

Statistics 204 requests
Progress

Screenshot 38 – Web Services Scanner

Starting a Web Service Scan

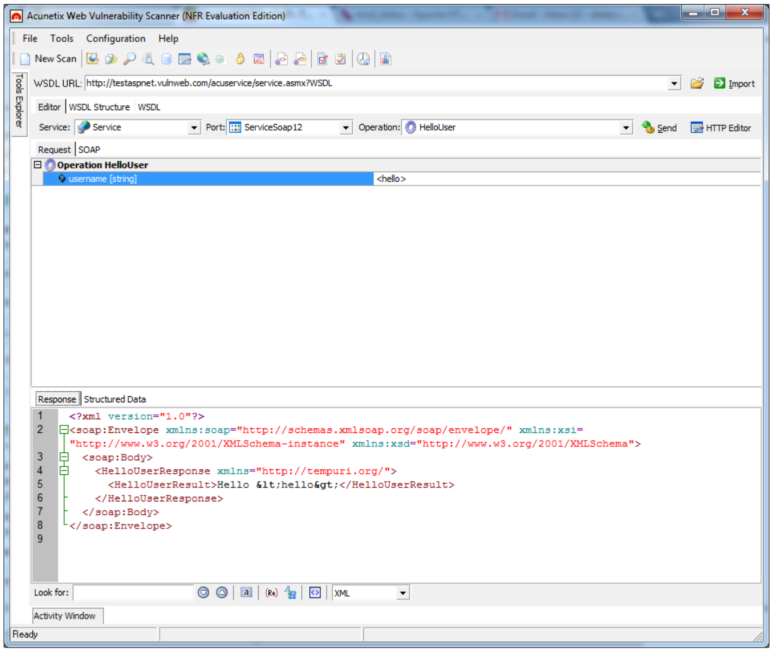
1. From the ‘Tools Explorer’ select **Web Services Scanner** and click the **New Scan** button in the toolbar to launch the Web Service Scan Wizard. Specify the URL of an online or local WSDL and choose a scanning profile. Click **Next** to proceed.

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



WSDL URL: http://testaspnet.vulnweb.com/acuservice/service.asmx?WSDL

Service: Service Port: ServiceSoap12 Operation: HelloUser

Operation HelloUser

username [string]	<hello>

```
<?xml version="1.0"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi=
"http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <HelloUserResponse xmlns="http://tempuri.org/">
      <HelloUserResult>Hello &lt;hello&gt;</HelloUserResult>
    </HelloUserResponse>
  </soap:Body>
</soap:Envelope>
```

XML

Screenshot 39 – Web Services Editor

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

Importing WDSL and Sending Request

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

Response Tab

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

Structured Data Tab

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

WSDL Structure Tab

Presents a detailed view of the web service data as provided by the WSDL Structure.

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

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

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

WSDL Tab

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

HTTP Editor Export

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

10. Command Line Operation

Introduction

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

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

C:\Program Files\Acunetix\Web Vulnerability Scanner 8\wvs_console.exe

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

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

WVS Console Scanner Command Line Parameters

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

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

	/scanlist [path and file name] Example: /scanlist c:\lists\sites.txt
/scanwsdl	Starts a web services scan. Syntax: /scanwsdl [wsdlurl] Example: /scanwsdl http://testaspnet.vulnweb.com/acuservice/service.asmx?WSDL
/profile	Uses specified scanning profile during the scan. Syntax: /profile [profile name] Example: /profile default
/Settings	Uses specified scan settings template during the scan. Syntax: /settings [Template name] Example: /settings test
/loginseq	Uses specified login sequence during the scan. Syntax: /loginseq [filename] Example: /loginseq testphp_seq
/save	Saves scan once scan is finished. The file will be saved in the location specified by the "/savefolder" switch. Syntax: /save
/savefolder	Specify the folder were all the scans and other scan related files will be saved. Syntax: /savefolder [directory]

	Example: /savefolder c:\Acunetix\Scans
/GenerateZIP	Compress all the saved scan data into a zip file. Syntax: /GenerateZIP
/exportxml	Exports scan results to XML file. The file will be saved in the location specified by the “/savefolder” switch. Syntax: /exportxml
/exportavdl	Exports results as AVDL format. The file will be saved in the location specified by the “/savefolder” switch. Syntax: /exportavdl
/savetodatabase	Saves scan results to reporting database. If this option is not specified, reports cannot be generated after the scan unless scan results are manually imported to reporting database. Syntax: /savetodatabase
/savelogs	Saves scan log files to the non-default location. The file will be saved in the location specified by the “/savefolder” switch. Syntax: /savelogs
/sendmail	Sends an email alert that the scan is finished to the user using the details configured in the scheduler settings. Syntax: /sendmail
/verbose	Enables verbose mode; the log file entries will also be displayed in the command line window. Syntax: /verbose
/Password	Application password if user interface password is

	enabled. Password can be enabled from the Application settings > General node. Syntax: /Password [password string] Example: /Password TestPass123!

WVS Console Scanner Command Line Options

Option	Description
--GetFirstOnly	Specifies to get the first URL only. Syntax: --GetFirstOnly=[true | false]
--RestrictToBaseFolder	Specifies if crawler should fetch anything above start directory. Syntax: --RestrictToBaseFolder=[true | false]
--FetchSubdirs	Specifies if the crawler should fetch files discovered in sub directories below base directory. Syntax: --FetchSubdirs=[true | false]
--ForceFetchDirindex	Specifies if the crawler should fetch directory indexes even if not linked. Syntax: --ForceFetchDirindex=[true | false]
--RobotsTxt	Retrieves and processes robots.txt and sitemap.xml during crawl to discover more links. Syntax: --RobotsTxt=[true | false]
--CaseInsensitivePaths	Specifies if the crawler should cater for case insensitive / sensitive paths. Syntax: --CaseInsensitivePaths=[true | false]

--UseCSA	Enable Client Script Analyzer engine to analyze JavaScript and other client side scripts during crawling. For all kind of web 2.0 applications this option should always be enabled. Syntax: --UseCSA=[true | false]
--scanningMode	Specify which scanning mode to use for this scan. Options available are Quick, Heuristic or extensive. Syntax: --scanningMode=[Quick | Heuristic | Extensive]
--TestWebAppsInAllDirs	Tests for well-known web applications vulnerabilities in all directories. Enable only if popular web applications are installed on the target website, such as Wordpress, Joomla etc. Syntax: --TestWebAppsInAllDirs=[True | False]
--ManipHTTPHeaders	Manipulate HTTP headers during scan. Syntax: --ManipHTTPHeaders=[True | False]
--UseAcuSensor	Enable AcuSensor technology for this scan. AcuSensor Technology sensor files must be installed on the target website. Syntax: --UseAcuSensor=[True | False]
--EnablePortScanning	Port scan target and run network alerts tests against target during web security scan. Syntax: --EnablePortScanning=[True | False]
--UseSensorDataFromCrawl	You can specify to use the AcuSensor data from a saved crawl to proceed with scan or to re-crawl the target. Syntax: --UseSensorDataFromCrawl=[Yes | No | Revalidate]

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

The Acunetix WVS Console Reporter

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

C:\Program Files\Acunetix\Web Vulnerability Scanner 8\reporter_console.exe

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

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

The Acunetix WVS console Reporter command line options

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

/k or /Kind	This parameter may be used only for compliance type reports. In fact, such parameter should only be used when the /r or /Report switches are set to WVSComplianceReport.rep. CWE.xml HIPAA.xml NIST_SP800_53.xml OWASP_Top_10_2004.xml OWASP_Top_10_2007.xml OWASP_Top_10_2010.xml PCI.xml PCI12.xml PCI20.xml Sarbanes_Oxley.xml STIG_DISA.xml WASC_Threat_Classification.xml To see a list of compliance templates available, run the following command 'reporter_console.exe /?' in the command prompt. Syntax: /r WVSComplianceReport.rep /k [compliance type template] Example: /r WVSComplianceReport.rep /k PCI12.xml
/p or /Password	Application password if user interface password is enabled. Password can be enabled from the Application settings > General node. Syntax: /p [password]
/c or /Console	Do not load Acunetix Reporter user interface. If this option is not specified, by default the user interface of the Acunetix Reporter will automatically pop up. Syntax: /c

/a or /Action	Specify the file type in which the generated report should be exported to. File types available: PDF, RTF, HTML, REP (Acunetix WVS proprietary format). Syntax: /a [format type] Example: /a PDF
/p or /Parameters	For each type or report template, there are different parameters. If no parameters are specified, the default parameter settings will be used. To specify the parameters to be passed to the reporter, us the “name=value” format delimited by “;”. To find out what parameters are available for each type report template, use the following syntax: Reporter_console.exe /r [ReportTemplate] /? Syntax: /r [report template] /p [parameter=True/False] Usage Example: /r WVSSingleScan.rep /p "ShowHTTP=False "
/t or /Target	Scan identifiers from the database to use as a report source. From the Acunetix WVS reporter, in the Configuration > WVS Database node, you can find the ID for each scan stored in the reporting database. The identifier can be one integer for single target template, two integers for comparison templates delimited by “;”. Can also be omitted for reports without specific scan target. For single scan templates, you can use “last” as target to indicate the last saved scan from the database. Syntax: /t [report ID] Example: /t 24

11. The Scheduler

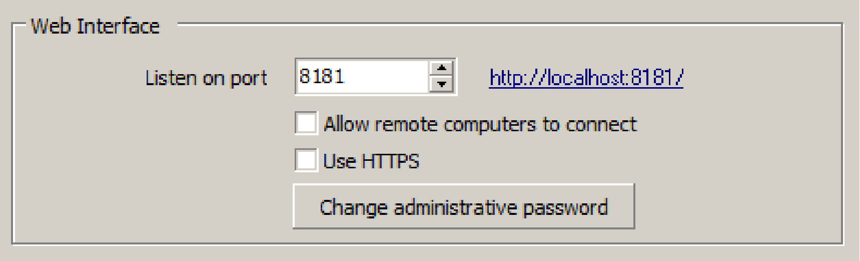
Introduction

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

Configuring the Scheduler service

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

Configuring the Scheduler web interface


Web Interface

Listen on port: 8181

http://localhost:8181/

□ Allow remote computers to connect

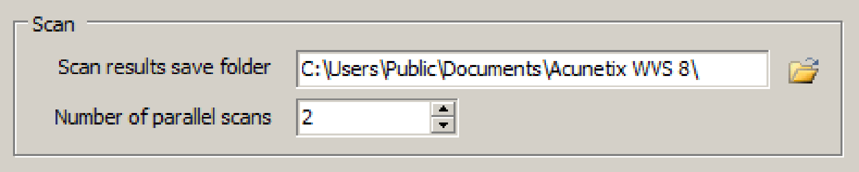
□ Use HTTPS

Screenshot 40 – 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 Scheduler web interface to be accessible from other remote computers, tick the **Allow remote computers to connect** option. When enabled, you will be prompted to specify a username and password for HTTPS to be automatically enabled. For security reasons, login credentials must always be defined when the scheduler web interface is configured to be accessed remotely.

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

Scan Options


Scan

Scan results save folder: C:\Users\Public\Documents\Acunetix WVS 8\

Number of parallel scans: 2

Screenshot 41 – Scheduler scan options

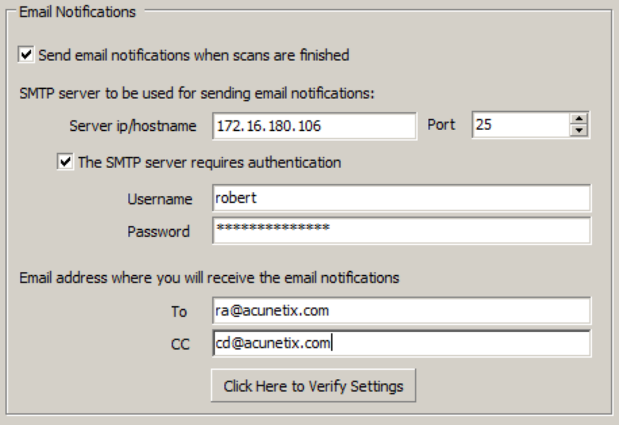
In this section you can specify the path where the Acunetix WVS scan results should be saved. By default, the scan results are saved in the My Documents folder of the Windows Public user profile in the Acunetix WVS 8 sub directory.

Scanning multiple websites

From this section you can also configure the number of parallel scans launched in Acunetix WVS. E.g. if you want to scan 4 websites and their scan schedule overlaps, instead of the scans being queued, another instance of Acunetix WVS 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 of 10 if you have the x10 instances license.

Note: The maximum number of scheduled scans that can be configured in the Acunetix WVS scheduler is of 500. To schedule more than 500 scans, you have to do this partially by waiting for other scans to finish, and replace them with the new scans.

Configuring Email notifications



Email Notifications

☑ Send email notifications when scans are finished

SMTP server to be used for sending email notifications:

Server ip/hostname: 172.16.180.106 Port: 25

☑ The SMTP server requires authentication

Username: robert

Password: ***************

Email address where you will receive the email notifications

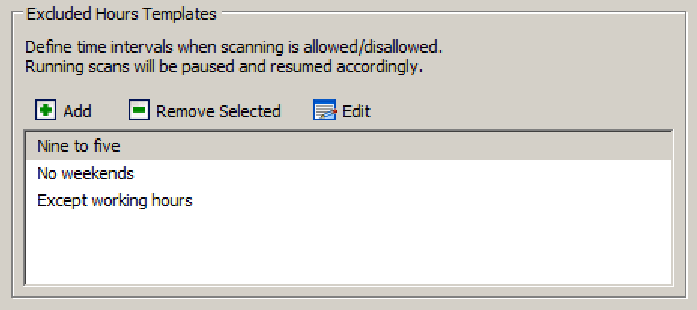
To: ra@acunetix.com

CC: cd@acunetix.com

Screenshot 42 – 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



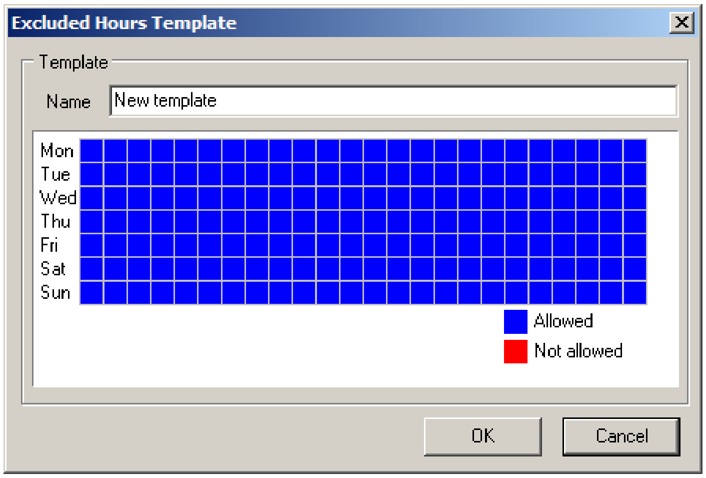
Excluded Hours Templates

Define time intervals when scanning is allowed/disallowed.
Running scans will be paused and resumed accordingly.

Nine to five
No weekends
Except working hours

Screenshot 43 – 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.



Name: New template

Screenshot 44 – Excluded Hours Configuration

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

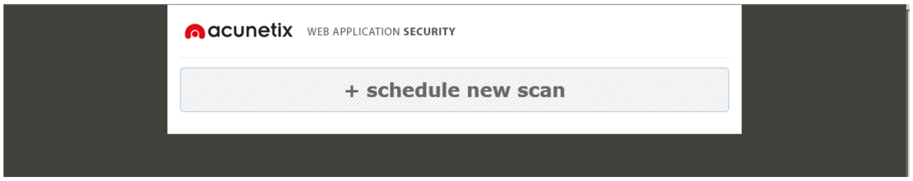
1. Specify a name of the template in the Name input field.
2. Highlight the hours of the day when scans should not run.
3. Click **OK** to save the new template.

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 WVS interface, or browse http://127.0.0.1:8181 using a web browser.

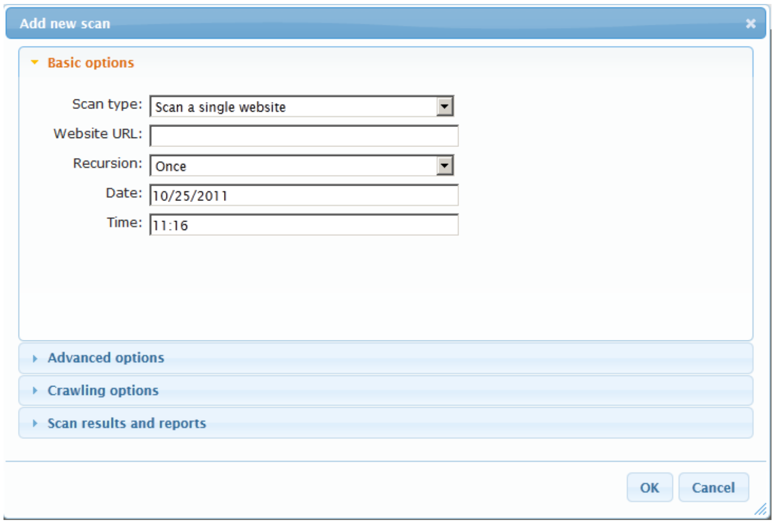
Note: JavaScript should be enabled to access the Acunetix Scheduler web interface.



Screenshot 45 – Acunetix Scheduler web interface

2. Click on **+ schedule new scan** 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 WVS application settings.

Scheduled Scan Basic Options

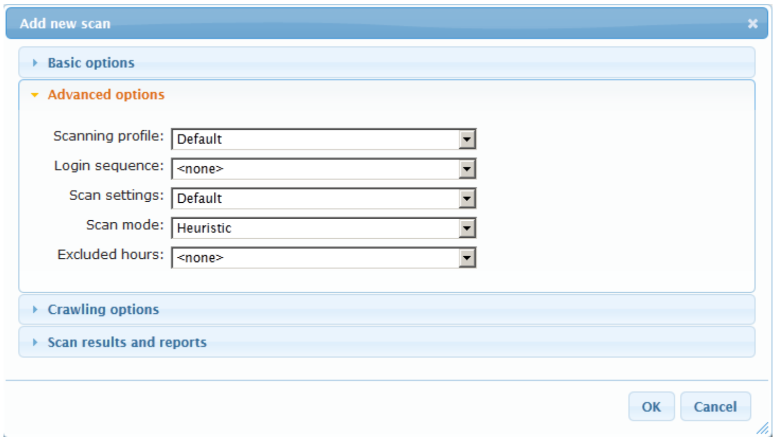


Scan type: Scan a single website
Website URL:
Recursion: Once
Date: 10/25/2011
Time: 11:16

Screenshot 46 – Acunetix Scheduler Basic options

The Basic Options allow you to specify what target/s to scan as well as the scan recursion. The recursion option gives you the option to configure the Scheduler to run a scan Once, Every Day, Every Week, Every Month or Continuous. Set a specific day number if schedule is set to weekly or monthly, e.g. 2nd day of the week or 21st day of the month.

Scheduled Scan Advanced Options



Scanning profile: Default

Login sequence: <none>

Scan settings: Default

Scan mode: Heuristic

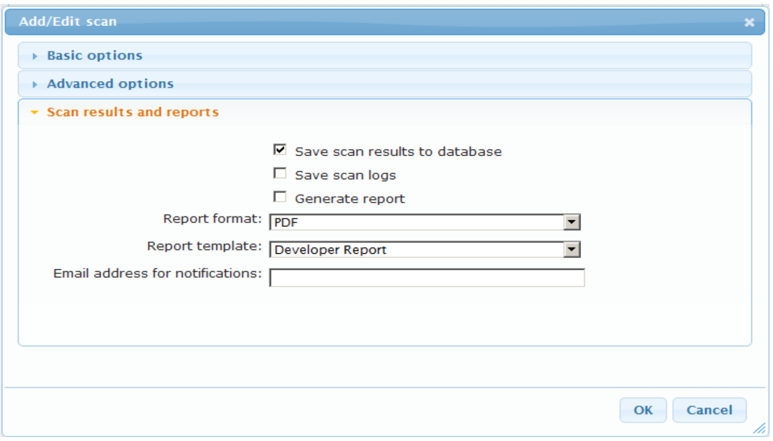
Excluded hours: <none>

Screenshot 47 – 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



☑ Save scan results to database

□ Save scan logs

□ Generate report

Report format: PDF

Report template: Developer Report

Email address for notifications:

Screenshot 48 – Acunetix Scheduler Scan results and Reports

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

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

12. Other Acunetix WVS tools

The Target Finder

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

More information about the target finder can be found here:

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

The Subdomain Scanner

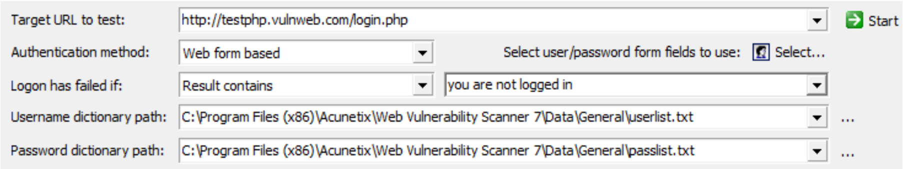
The Subdomain Scanner scans a top-level domain to discover any sub domains configured in its hierarchy, by using the target domain's DNS server, or any other DNS server specified by the user.

More information about the Subdomain scanner can be found here:

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

The Authentication tester

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



Target URL to test: http://testphp.vulnweb.com/login.php

Authentication method: Web form based

Select user/password form fields to use: Select...

Logon has failed if: Result contains — you are not logged in

Username dictionary path: C:\Program Files (x86)\Acunetix\Web Vulnerability Scanner 7\Data\General\userlist.txt

Password dictionary path: C:\Program Files (x86)\Acunetix\Web Vulnerability Scanner 7\Data\General\passlist.txt

Screenshot 49 – Authentication Tester

More information about the Authentication tester can be found here:

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

Login Sequence Recorder

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

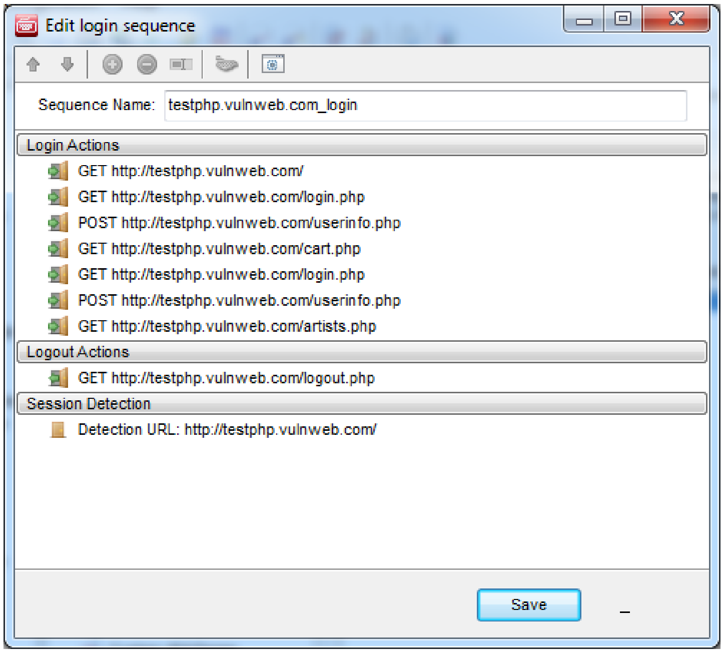
- To configure Acunetix WVS to access a form based password protected section
- To create a pre-defined crawling sequence, such as a shopping cart
- To mark pages that require human / manual intervention each time they are accessed, such as pages with CAPTCHA, One-Time password, Two-Factor authentication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

Creating or editing login sequences

1. Navigate to Configuration > Application Settings > Login Sequence Manager
2. In this configuration screen you can create or edit the login sequences used by Acunetix WVS to access website areas protected by form-based authentication. Login sequences allow Acunetix WVS to replicate all events that are manually performed to access the area secured by a login page.
3. Click on the 🗋 button to open up the Login Sequence Recorder. Enter the URL of the website and click on **Next**. One can also click **Check URL** to confirm that the URL entered is reachable from the Acunetix Login Sequence Recorder.
4. Record the login sequence. For more information refer to the section 'Scanning a form based password protected area' on page 26 in this user manual.

Editing a Login Sequence

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



Sequence Name: testphp.vulnweb.com_login

GET http://testphp.vulnweb.com/
GET http://testphp.vulnweb.com/login.php
POST http://testphp.vulnweb.com/userinfo.php
GET http://testphp.vulnweb.com/cart.php
GET http://testphp.vulnweb.com/login.php
POST http://testphp.vulnweb.com/userinfo.php
GET http://testphp.vulnweb.com/artists.php

GET http://testphp.vulnweb.com/logout.php

Detection URL: http://testphp.vulnweb.com/

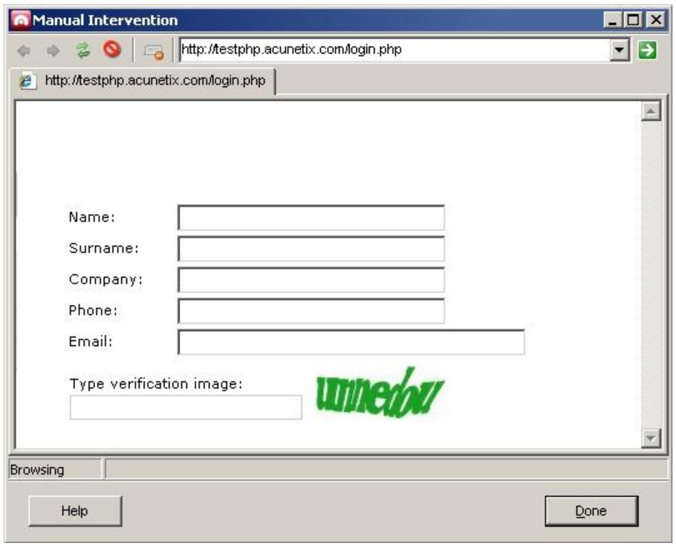
Screenshot 50 – Login Sequence Editing

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

Marking Pages for Manual Intervention (human input is required)

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

1. Launch the Login Sequence Recorder and enter the web application URL in the first step.
2. In the second step of the wizard 'Record Login Sequence', click on the **Pause** button to pause the recording, and enter the URL of the page which requires human input in the URL input field.



Screenshot 51 – Manual browser window

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

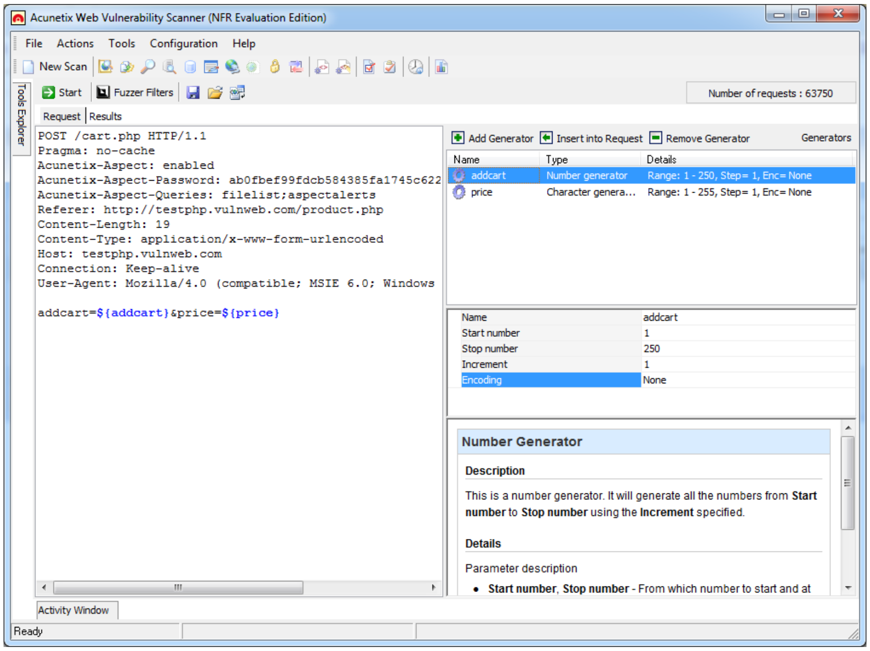
Once a scan is launched, a browser window will automatically pop up when the application page is reached. You can now perform the required action. Click **Done** once the action is complete.

Note: Only one page has to be marked for manual intervention. If you have more than one page that requires manual intervention, specify these URLs the first time the browser window automatically appears during the crawl and perform the action on those pages as well. This allows the crawler to automatically process those pages without you having to wait for another dialog to appear.

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

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

The HTTP Fuzzer



Number of requests : 63750

```
POST /cart.php HTTP/1.1
Pragma: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: ab0fbef99fdcb584385fa1745c622
Acunetix-Aspect-Queries: filelist;aspectalerts
Referer: http://testphp.vulnweb.com/product.php
Content-Length: 19
Content-Type: application/x-www-form-urlencoded
Host: testphp.vulnweb.com
Connection: Keep-alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows

addcart=${addcart}&price=${price}
```

Name	Type	Details
addcart	Number generator	Range: 1 - 250, Step= 1, Enc= None
price	Character genera...	Range: 1 - 255, Step= 1, Enc= None

Name	addcart
Start number	1
Stop number	250
Increment	1
Encoding	None

Number Generator

Description

This is a number generator. It will generate all the numbers from **Start number** to **Stop number** using the **Increment** specified.

Details

Parameter description

- **Start number**, **Stop number** - From which number to start and at

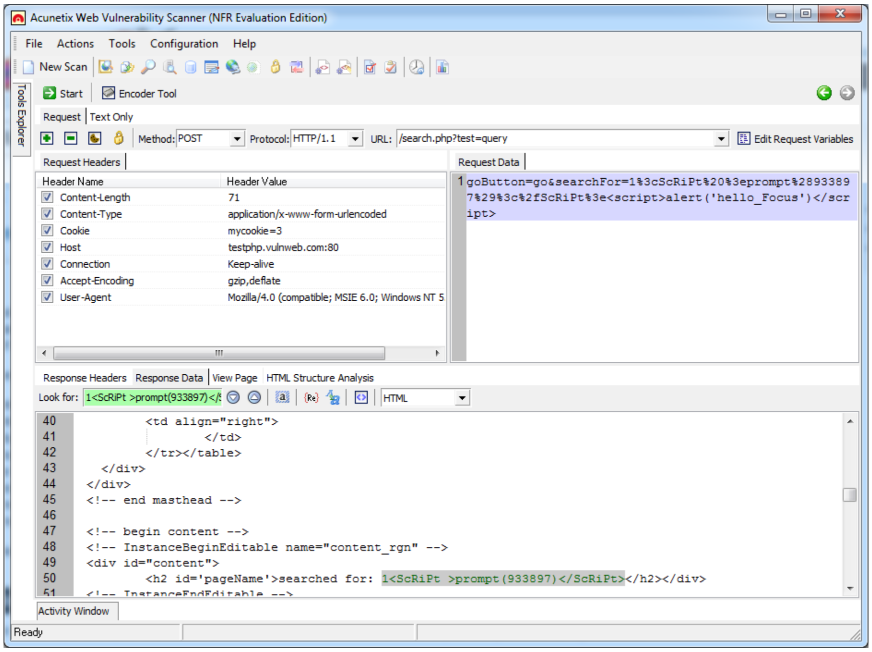
Screenshot 52 – The HTTP Fuzzer

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

More information about the HTTP Fuzzer can be found here:

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

The HTTP Editor



Method: POST

Protocol: HTTP/1.1

URL: /search.php?test=query

Header Name	Header Value
☑ Content-Length	71
☑ Content-Type	application/x-www-form-urlencoded
☑ Cookie	mycookie=3
☑ Host	testphp.vulnweb.com:80
☑ Connection	Keep-alive
☑ Accept-Encoding	gzip,deflate
☑ User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5

```
goButton=go&searchFor=1%3cScRiPt%20%3eprompt%2893389
7%29%3c%2fScRiPt%3e<script>alert('hello_Focus')</scr
ipt>
```

Look for: 1<ScRiPt >prompt(933897)</

HTML

```
            <td align="right">
                    </td>
            </tr></table>
      </div>
    </div>
    <!-- end masthead -->

    <!-- begin content -->
    <!-- InstanceBeginEditable name="content_rgn" -->
    <div id="content">
            <h2 id='pageName'>searched for: 1<ScRiPt >prompt(933897)</ScRiPt></h2></div>
    <!-- InstanceEndEditable -->
```

Screenshot 53 - The HTTP Editor

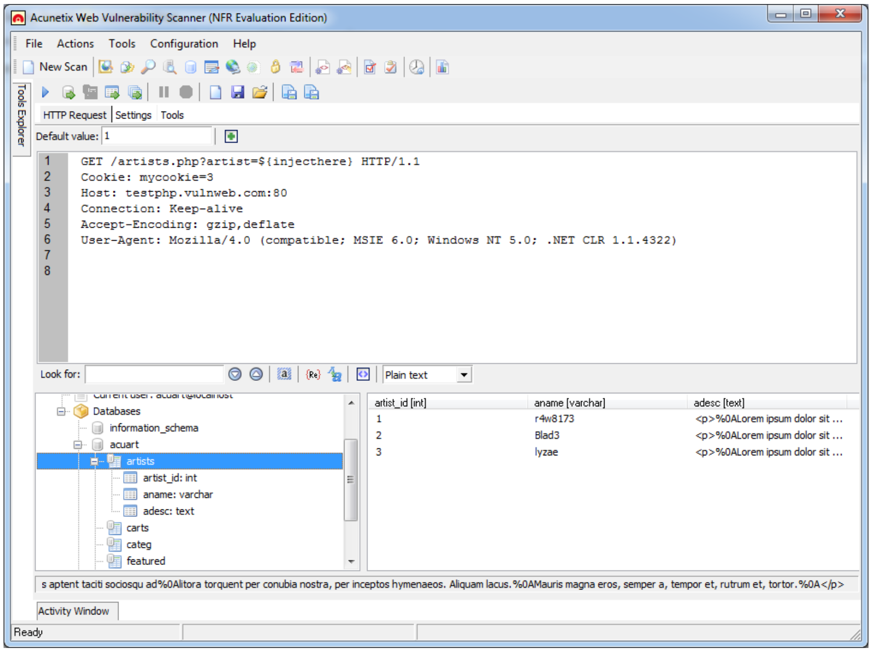
The HTTP Editor allows you to create, analyze, and edit client HTTP requests and server responses. This allows you to further fine tune attacks and confirm if vulnerabilities were solved.

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/

The SQL Injector



Default value: 1

```
GET /artists.php?artist=${injecthere} HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com:80
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
```

artist_id [int]	aname [varchar]	adesc [text]
1	r4w8173	<p>%0ALorem ipsum dolor sit ...
2	Blad3	<p>%0ALorem ipsum dolor sit ...
3	lyzae	<p>%0ALorem ipsum dolor sit ...

s aptent taciti sociosqu ad%0Alitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.%0AMauris magna eros, semper a, tempor et, rutrum et, tortor.%0A</p>

Screenshot 54 - SQL Injector

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

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

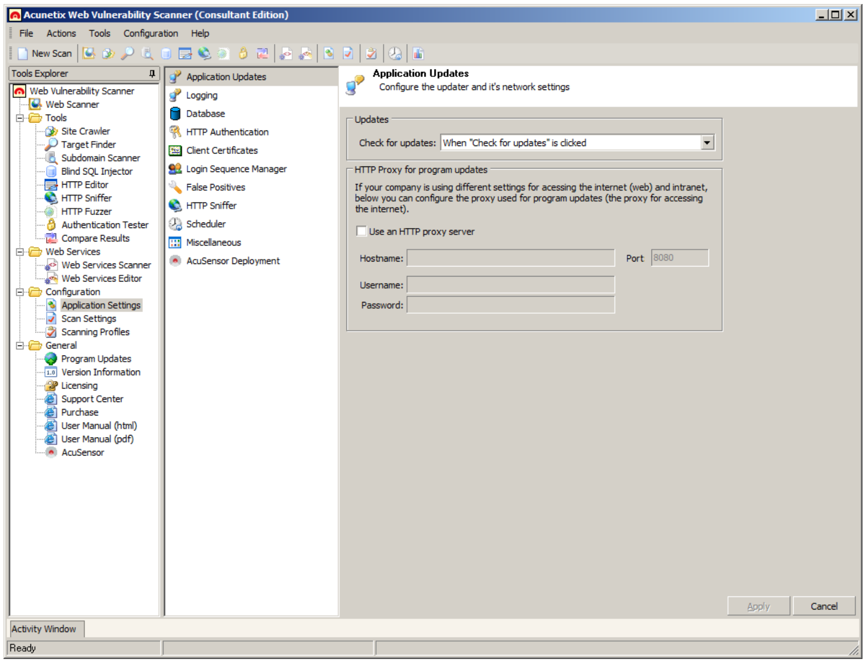
More information about the blind SQL injector can be found here:

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

13. Advanced Configuration

Application Settings

Acunetix WVS configuration settings can be accessed from the ‘Configuration > Application Settings’ node in the Tools Explorer window pane.



Application Updates

Configure the updater and it's network settings

Updates

Check for updates: When "Check for updates" is clicked

HTTP Proxy for program updates

If your company is using different settings for acessing the internet (web) and intranet, below you can configure the proxy used for program updates (the proxy for accessing the internet).

☐ Use an HTTP proxy server

Hostname: Port 8080

Username:

Password:

Screenshot 55 – Application Settings

Application Updates

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

Logging

You can configure different logging levels in Acunetix WVS from:

Configuration > Application Settings > Logging

HTTP Authentication

Refer to page 24 of this manual for information about the HTTP Authentication options.

Client Certificates

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

Navigate to ‘Configuration > Application Settings > Client Certificates’

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

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

False Positives

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

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

Miscellaneous

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

Memory Optimization

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

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

Display Options

- **Display custom HTTP status information** - Display the full HTTP response status line header and the corresponding status string.
- **Display HTTPS status icon** – Enable this option to show a padlock icon next to files or directories that are accessed via HTTPS and not HTTP.

Password Protection

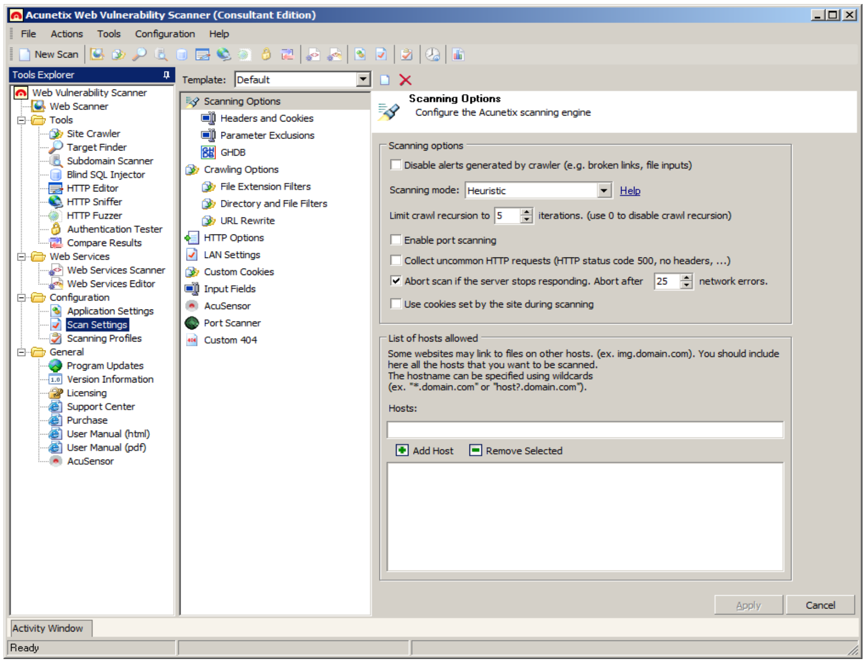
In this section the user can set a password to restrict access to the Acunetix WVS main interface and all the other Acunetix WVS applications, such as the Reporter.

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

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

Scan Settings Templates

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



Template: Default

Scanning Options
Configure the Acunetix scanning engine

Scanning options

☐ Disable alerts generated by crawler (e.g. broken links, file inputs)

Scanning mode: Heuristic

Limit crawl recursion to 5 iterations. (use 0 to disable crawl recursion)

☐ Enable port scanning

☐ Collect uncommon HTTP requests (HTTP status code 500, no headers, ...)

☑ Abort scan if the server stops responding. Abort after 25 network errors.

☐ Use cookies set by the site during scanning

List of hosts allowed

Some websites may link to files on other hosts. (ex. img.domain.com). You should include here all the hosts that you want to be scanned.
The hostname can be specified using wildcards
(ex. "*.domain.com" or "host?.domain.com").

Hosts:

Screenshot 56 – Scan Settings templates

Creating, modifying, or deleting Scan Settings templates

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

Scanning Options

- **Disable Alerts generated by crawler** - Select this option to disable crawler related alerts – such as broken links, file inputs and files which their name indicates that they can be dangerous etc. – from being reported.
- **Scanning Mode** - From this section you can select the **Scanning Mode** which will be used during both the crawling and scanning stage of the target website. The scan mode will determine how both the crawler and the scanner will treat website parameters (also known as inputs), which will affect the number of security checks launched against the website. The following scanning mode options are available:
  - **Quick** - In this mode, the crawler will only fetch a very limited number of variations of each parameter, because they are not considered to be actions

parameters. Action parameters are designed to control the execution flow of the server scripts. Such scanning mode should only be used with small and static websites.

  - **Heuristic** - In this mode, the crawler will try to make heuristic decisions on which parameters should be considered as action parameters. It will try to fetch the most possible values of each parameter. This will result in a larger number of different variations, and therefore the scanner will launch more security checks against the website. This scanning mode is the most efficient and accurate one, and is recommended as the scanning mode of choice unless there are specific reasons to use other scanning modes.
  - **Extensive** - In this mode, the crawler will fetch all possible values and combinations of all parameters. This will lead to a much larger number of variations, and therefore the scanner will launch an extensive amount of security checks against the website. This scanning mode should only be used for specialized security audits since it can take a considerable amount of time to finish.

- **Limit crawl recursions to X iterations** - After a site is crawled and vulnerability scanning has started, the scanner can still discover new objects – for which a new crawl will be started. This is called iteration. Configure the maximum number of crawl iterations that can happen during a website scan.
- **Enable Port Scanning –** Enable this option to port scan the web server on which the target website is hosted during a web security scan by default. For more information about the Port Scanner and Network Alerts, refer to page 6 of this manual.
- **Collect uncommon HTTP Requests -** Acunetix WVS can report any uncommon server response that might include sensitive data, such as internal server errors. These alerts are reported under the 'Knowledge Base' node in the Scan Results window.
- **Abort Scan if the server stops responding** - Configure the maximum number of network errors the scanner must encounter before completely aborting the scan.
- **Use cookies set by the site during scanning** – By default, Acunetix WVS ignores the cookies sent by the website during the scan but uses the ones discovered during the crawling process. Enable this option to always use the latest cookies provided by the website; ignore the cookies discovered in the crawl and use the ones the website is sending during the scan.
- **List of hosts allowed -** By default, Acunetix WVS will not crawl links outside the target URL. However, some links on some websites link to external locations outside the target URL and may require being included in the scan. Configure Acunetix WVS to include and follow these links in the 'list of hosts allowed' field. Enter the host name or IP address of the domain to be included in a crawl / scan and click the **+** button to add the entry. E.g. when scanning testphp.vulnweb.com there are links which link to www.acunetix.com.

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

Headers and Cookies

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

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

Parameter Exclusions

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

Note: Parameters specified in the Parameter Exclusions list will only be excluded from a scan but will still be crawled.

Adding a parameter to the exclusion list

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

GHDB (Google Hacking Database) Options

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

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

Crawling Options

Refer to page 45 of this manual for more information on the crawling options.

HTTP Options

HTTP General

- **User agent string** – Configure what user agent header string Acunetix WVS should use when accessing a target website. You can click on ✕ to use a predefined user agent string or you can specify your own custom user agent string by manually typing it in.
- **Maximum number of parallel connections** – Specify the maximum number of HTTP connections made to a target website. If overloaded with requests, some target servers might crash or reject new connections.
- **HTTP request timeout in seconds** – Specify how long Acunetix WVS must wait for a HTTP response before considering it as timed out.
- **Delay between consecutive requests in milliseconds** – Configure the delay between each HTTP request Acunetix WVS sends to the target website.
- **HTTP response size limit in kilobytes** - Maximum HTTP response size accepted by the crawler. Larger HTTP responses than the specified size will not be crawled (with this option you are controlling the maximum size of the requested files).

Custom HTTP Headers

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

LAN Settings

For more details on configuring LAN and proxy settings refer to page 17 of this manual.

Custom Cookies

For more details on configuring custom cookies refer to page 50 of this manual.

Input Fields

For more details on configuring input fields refer to page 50 of this manual.

AcuSensor

For more details on configuring AcuSensor refer to page 13 of this manual.

Port Scanner

While scanning a website you can also choose to launch a port scan against the web server hosting the site. The port scanner will scan the web server using a specific list of ports. If a port is found to be open, the port scanner will identify what network service is running on that port and will launch a number of security checks specifically targeting the discovered network service.

Therefore if a DNS server is discovered, tests such as DNS open zone transfer and DNS open recursion tests are run against the network service. The Port Scanner configuration options are:

- **Number of sockets used for scanning** – Specify the amount of network sockets to be used by the Port Scanner module. The larger the number the faster the scan will be, but it will also increase the load on the web server.

- **Connection timeout (in seconds)** – Specify the timeout in seconds, i.e. if there is no response when trying to connect to a port within the specified amount of seconds, the port will be considered as closed.
- **List of scanned ports** – The list of specified ports for which the Port Scanner will check. Use the **+** button to add a port and a description and use the **-** button to remove selected ports from the list.

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

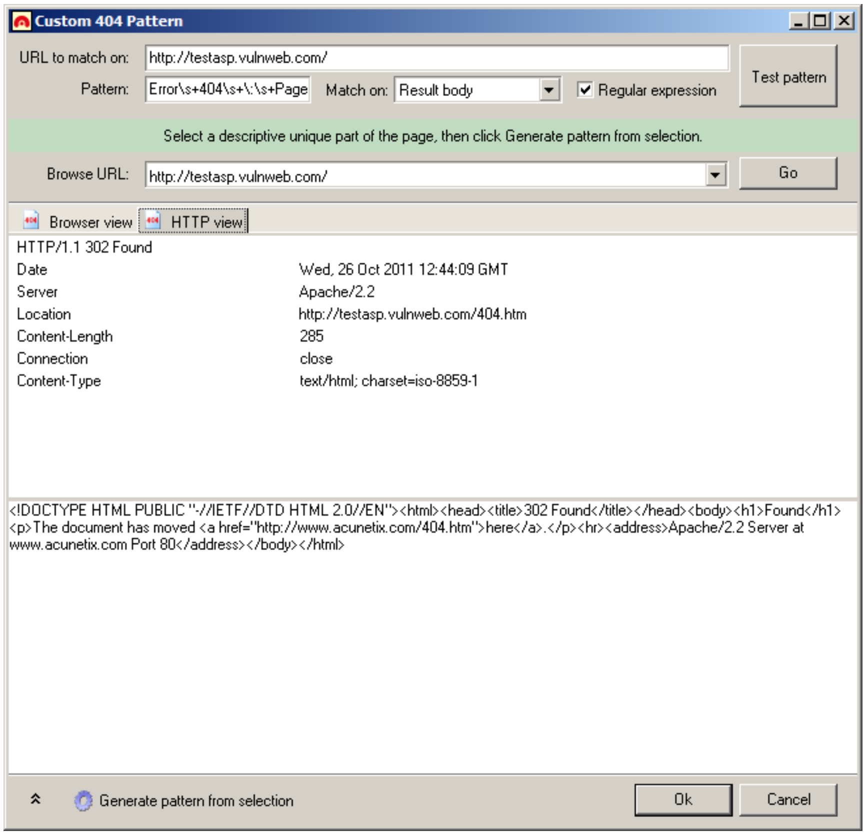
Note: The Network Alert Scripts (Network security checks) are fully scriptable thereby allowing you to write new ones. The Acunetix Web Vulnerability Scanner Network Alert scripting reference is available from the following URL;

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

Custom 404 Error Pages

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

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


Custom 404 Pattern
Test pattern
Select a descriptive unique part of the page, then click Generate pattern from selection.
Go
Browser view
HTTP view
Generate pattern from selection
Ok
Cancel

URL to match on: http://testasp.vulnweb.com/

Pattern: Error\s+404\s+\:\s+Page

Match on: Result body

☑ Regular expression

Browse URL: http://testasp.vulnweb.com/

```
HTTP/1.1 302 Found
Date                    Wed, 26 Oct 2011 12:44:09 GMT
Server                  Apache/2.2
Location                http://testasp.vulnweb.com/404.htm
Content-Length          285
Connection              close
Content-Type            text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body><h1>Found</h1>
<p>The document has moved <a href="http://www.acunetix.com/404.htm">here</a>.</p><hr><address>Apache/2.2 Server at
www.acunetix.com Port 80</address></body></html>
```

Screenshot 57 – Custom 404 Error page configuration

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

You can also generate such pattern automatically:

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

Scanning Profiles

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

Default Scanning Profiles

A number of default scanning profiles are included with Acunetix WVS. Below is a list of all the scanning profiles and a summary of the security checks they perform. For a detailed list of the vulnerability checks that are included in each scanning profile, navigate to the ‘Configuration > Scanning Profiles’ node in the Tools Explorer, and select the profile name from the ‘Profile’ drop down menu. The tests selected with a checkbox will be launched when the scanning profile is used.

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

Web_Applications	Well known web applications e.g. Joomla, Wordpress security checks
Ws_default	Web services vulnerability checks only
XSS	Cross-site scripting vulnerability checks only

Creating/Modifying Scanning Profiles

Creating a new Scanning Profile

4. Select the Empty scanning profile from the 'Profile' drop down menu.
5. Check all the vulnerability checks / security checks you would like to include in the scanning profile.
6. Click on **save** 💾 button to save the profile.

Modifying a Scanning Profile

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

Creating custom vulnerability checks

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

More information about creating vulnerability checks can be found here:

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

14. Troubleshooting

Obtaining support

User Manual

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

Support

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

The Acunetix Support Center

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

Acunetix Forums

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

Request Support via E-Mail

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

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

Acunetix Blog

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

Acunetix Facebook page

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

Knowledge base / Help / Support page

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