

1

# Auditing Your Web Site Security

# A practical "how to" using Acunetix Web Vulnerability Scanner

Auditing the security of your website with Acunetix WVS is easy. Acunetix WVS performs most of the steps in an automated manner and therefore giving you a good idea of your website security simply by launching a scan and reviewing the alerts. This White Paper walks you through the process of launching a security audit of your website using the Scan wizard

#### Starting a Scan

NOTE: DO NOT SCAN A WEBSITE WITHOUT AUTHORISATION! The web server logs will show the scans and attacks being made by Acunetix WVS. If you are not the sole administrator of the website ensure that you warn other administrators before performing a scan. Furthermore some attacks can cause a web site to crash requiring a restart of the web site.

Starting a Scan	2
Step 1: Select target(s) to scan	2
Step 2: Confirm targets and technologies detected	
Step 3: Specify scanning profile and crawler options	4
Step 4: Configure login/input for password protected areas or HTML forms	5
Step 5: Configuring custom 404 error pages	8
Analyzing the Scan Results	
Saving the Scan Results	13
Generating a report	
Google hacking vulnerability detection	14

# Step 1: Select target(s) to scan

You will need to enter the IP or the URL of the website that you wish to scan. To begin a new scan:

1 Click on File > New Scan. The Scan Wizard will start, which guides you through the process of launching a website audit.



Screenshot 1 - Select type of scan

- 2 Specify the target(s) to be scanned. The scan target options are:
- Scan single website Scans a single website. Enter a URL, e.g. <u>http://testphp.acunetix.com</u>, <u>https://www.test.com</u> or http:// 80.237.145.112.
- Scan using saved crawling results If you performed a crawl/scan on a website previously and saved the results, you can analyze these results directly without having to crawl the site again. Specify the 'Saved crawler results' file by clicking on the folder button.
- Scan List of Websites Scans a list of target web sites specified in a plain text file (one target per line). Every target in the file is to be specified in the format <URL> / <URL:port> / <IP> / <IP:port>, For example <u>http://80.237.145.112:80/</u>. Ensure that the port is included in each line, even if it's a default port.
- Scan Range of Computers This will scan a specific range of IP's (e.g. 192.168.0.10-192.168.0.200) for target sites which are open on the specified ports (Default 80, 81 and 443).

ican tuna	Select targets				
Folget Second	Plants weit that the appear to is interest and table scloot the targets for weat to appe itst. the list below				
	For every facet you can enter details such as operating system, webserver, technolog, or chance the tase				
Seen options	bath Sylanta ng Illeba detaro you ban laduba tha scan <b>ng</b> tine.				
Lbar Charles	Tier of migers				
	🗉 🔪 test acunctiz com:80	2			
	Ease pall	1			
	Cerver panner	Apache/20.40 (Linux/ScCC)			
	Thigs: IBI	http://dest.acuneticom/80/			
	Uperating system	Lhx			
	WebGerver	Apache 2.x			
	Peterted exercit 404 circl page	to			
	±l flachnologies	[FHF]			
	ASE .				
	ASE NET				
	P-IP	<b>v</b>			
	Per				
	mod_cal				
	mod_pet				
	OpenSCL				
	FictiPhge				
acunetix	Status: Done				

# Step 2: Confirm targets and technologies detected

Screenshot 2 - Selecting Targets and Technologies

3 Acunetix WVS will automatically probe the website(s) target(s) for some basic details such as operating system, web server, web server technologies and whether a custom error page is used. The web vulnerability scanner will use these details in order to reduce the number of tests performed which are not applicable (e.g. Acunetix WVS will not probe IIS tests on a UNIX system). This will reduce scanning time. If you already know what technologies the website is running, you can check whether Acunetix WVS identified them correctly. Click on the relevant field and change its setting from the provided dropdown list or check box. After you have confirmed the technologies, click **Next** to proceed.

# Step 3: Specify scanning profile and crawler options



Screenshot 3 - Scan Options setup

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

# Scanning profile

The scanning profile will determine which tests are to be done on the target site. For example, if you only want to test your website(s) for SQL injection, you would select the sql\_injection profile and no additional tests would be performed. Refer to the 'Scanning Profiles' chapter for further information on how to customize existing and create new scanning profiles.

#### **Crawling options**

The crawler traverses the entire website and identifies its structure. The following crawling options can be configured:

Start HTTP sniffer for manual crawling at the end of the scan process – this option will start the HTTP sniffer automatically at the end of the crawl process, so that you can browse (with the browser configured to use the Acunetix WVS proxy) to parts of the site that the crawler could not reach or did not find. Frequently these are pages are linked via javascript menus or other methods. The crawler will updated the site structure with the newly discovered links & pages.

Get first URL only - Scan index/first page only.

- Do not fetch anything above start folder Select this option to instruct the crawler not to follow any links above the start folder. E.g. if you specify <u>http://testphp.acunetix.com/wvs/</u> as a start URL it will not traverse the links which point to a location above the base link e.g. <u>http://testphp.acunetix.com/</u>. However it will traverse all links to pages located in the wvs folder or any of its subfolders.
- Fetch files below base folder Select this option to also follow links which are contained outside the base folder. E.g. if you specify <u>http://testphp.acunetix.com/</u> as a start URL it will

traverse the links which point to a location below the base link e.g. <u>http://testphp.acunetix.com/wvs/</u>.

- Fetch directory indexes even if not linked Select this option to instruct the crawler to request the directory index for every discovered directory even if the directory index is not directly linked.
- Submit forms Select this option to automatically fill in & submit HTML forms with information that you have previously configured in the scan settings > HTML forms node.
- Retrieve & process robots.txt Select this option to have Acunetix WVS look for a robots.txt file and follow all the links in it.

Click Next.

# Step 4: Configure login/input for password protected areas or HTML forms

If the website has password protected areas or pages behind an HTML feedback form (e.g. visitor registration required to download whitepapers, files etc.) which you want Acunetix WVS to scan, then you will have to configure Acunetix WVS to authenticate to the password protected area or fill in the HTML form details so that it can scan the pages contained within/behind the page.

Password protected areas on Websites are protected using either HTTP authentication or HTML forms authentication.

HTML forms authentication is not handled via HTTP, but rather via a web form which asks the user for a username and password. This information is sent back to the server for validation by a custom script.

HTTP authentication is part of the HTTP specification. If a site uses HTTP authentication, then the browser will pop up a password dialog. The web server validates the logon against a database of users. (in the case of IIS these are local windows user accounts, and in the case of Apache these are stored in a file)

Scan Wizard		×
Scan type Select targets Scan options	Login If your website requires authentication (HTTP or HTM	L)
Enor pages	HTTP authentication  If your websites requires HTTP authentication you need to provide the credentials bellow  Authenticate with this usemane and password c Usemane: Password:	x (Basic or NTLM). combination :
	HTML authenticstion (Login sequence) HTML authenticstion (Login sequence) Website, This will be saved as a login sequency You can also specify a section of the website links that will log you out from the website  Login sequence one login sequence>	n, you need to record the steps sequired to login in the ce file and can be used later. which you do not want to be crawled (for example
acunetix	Record new login sequence	
		< Back Next> Carcel

Screenshot 4 - Login Details Options

To test a HTTP password protected area:

- 1 Tick the box "Authenticate with this user name and password combination"
- 2 Enter the username and password
- 3 Click next. When Acunetix WVS encounters a HTTP password dialog, it will enter the details you entered.

To test a HTML form password protected area:

1 Click on Record new login sequence. The record login sequence window starts. The Login Sequence Recorder allows you to 'record' the login process.

🗋 🛃 🔐 End login seq	puences 🔝 Select restricted links 📑 🥥 🝙 🔹 😰 Addeess: [http://test.acumitis.com/agin.php.	0.6
ACUNETIX A	RT	2
TEST and Doministratio	n alto fur Adamittic Web Velicarability Scalenar	
home   categories   ;	artists   disclaimer   your cart   guestbook	
search art	If you are already registered please enter your login information below:	
Browse categories	Username : tect	
Browse artists	Passwort	
Your cart	i domara.	
Signup	Tegin	
Your profile		
Our guestbook	You can also signup here.	
Logout		
Links Security art Fractal Explorer		
· WKA		
About Us   Privacy Policy	ContactUs ( 60/00) Asumetal Les	
Recording login sequence	4	EW

2 Browse to the HTLM forms login page, enter username and password and authenticate by clicking login. Note that on your website the names of the fields and the submit button might be different. Now click on the 'End login sequence' button at the top of the dialog.

🔄 🛃 😫 Start login se	quence 🍱 Select restricted	Baka 📑 🔾 🔄 🔹 🛛 Addeess Hit	p://text.acurretie.com/usein/siph 🛛 🔂 G
C user into			
ACUNETIX A	RT		1
TEST and Documentation	ni situ fur Acientitis Vykia S	Adminutability Scalence	-
home categories	artists   disclaimer   yo	our cart   guestbook	(Logout test)
search art	test account (	test)	$\sim$
90			
Browse categories	On this page you can	visualize or edit you user information.	
Browse artists			
Your cart			
Signup	Manual		
Your profile	Name.	test account	
Our guestbook	Credit card number:	test	
Logout	E-Mail:	test@test.com	
Links	Phone number:	PT1.250.4155	
Fractal Explorer	Address:	hhf 📄	
		-1	
		update	
****			
are st			
	March 1997 March 1997		

Screenshot 6 - Login Sequence Recording Logout

3 After you have authenticated, you also need to identify the logout link – otherwise Acunetix WVS will try to crawl the logout link and logout of the password protected area. Click on the logout link and 'select restricted link'

edit login see	quence and restricted lir	iks	
ogin sequence			1
Action	URL	POST data	
👌 Navigate 👌 Post data	/login.php /userinfo.php	uname=test&pass=test	
estricted links			[
Action	UBI	POST Data	
Action ∂ Navigate	URL /logout.php	POST Data	
Action 🤌 Navigate	URL /logout.php	POST Data	

Screenshot 7 - Login Sequence Editing

- 4 You can review the login sequence that you recorded by clicking on the Edit login sequence button:
- 5 When you are done, click on the save icon and click on the exit button to exit the login sequence editor. The wizard will save the login sequence.



Screenshot 8 - Login Sequences configuration

You can reuse the login sequence for future scans. Login sequences can be edited from the Configuration > Settings > Automation Settings > Login sequences node.

Note: You can choose to configure HTML form input directly, without the login sequence editor, from the Configuration > Scanner settings> HTML forms node. For more information see the chapter "Configuring Acunetix WVS"

# Step 5: Configuring custom 404 error pages

A custom 404 error page is a page that appears when the browser enters an invalid URL. Rather then displaying error 404, many websites show a formatted page informing the user that the page does not exist. Acunetix WVS needs to know about custom 404 error pages, since your webserver will respond with an OK (200) for every query that WVS makes and therefore it can not detect the difference between an invalid URL and a valid web page.



Screenshot 9 – Custom Error Page Configuration

The scan wizard will automatically try to detect whether your site uses custom error pages. If your website uses custom error pages, it will display the custom error page and try to automatically find the part that uniquely identifies an error page.

To configure the custom error page:

- 1 Highlight the text that is unique to this page. This text should not be found on any other page on your website. Example: "Sorry, the page you have requested cannot be found".
- 2 Click on the "Generate pattern" button to generate a regular expression from the highlighted text. The highlighted text will be copied to the "Error message pattern" box and changed into a regular expression that Acunetix WVS can understand.
- 3 Click on the "Text pattern" button to verify the generated pattern.
- 4 Click Next.

Once the custom error page is configured, it will be saved in the Configuration > Settings > Automation settings > Custom 404 error pages node.



Screenshot 10 - Scan Wizard - Finish window

5 If you want to save the scan results to a database, enable 'Save scan results to the database for report generation'. Click on the Finish button to start the scan.

Note: It may take several hours to complete a scan for a large website!

# Analyzing the Scan Results

After the scan completes, the results can be expanded by clicking on the scan in the Scan results window. Two main nodes, Alerts & Site structure, will be shown.



Screenshot 11 - Scan Result and Information window

# **Alerts Node**

The alerts node displays all vulnerabilities found and how to fix them. Alerts are sorted into four severity levels: High, Medium, Low & Informational. The number of vulnerabilities detected is displayed in brackets () next to the alert categories.

Hide toolbar				ź
🗋 🧭 🛃 Start URL   test.acunetix.com		2010 T	· Profiler default	💌 🔛 Start
Scan lesults	Stake	A dcune	ətix	All Street of the
Scan Thread 1 ( http://blat.acunatic.com/80/ )	Finished (67 alerts)		24174	IC APPENDENCE
E 4erts (67)		<ul> <li>DMD module is</li> </ul>	and the second state of the	
E - D PHP multiple vulnerabilities (1)		Visue months	vinite annues	
		Affects	PHP	2014220
EE- 😍 SQL Intection (9)		Details	Current version is PH	PV4.3.3
B - 4 Script source code disclosure (1)		Severity	high	
Hacronecia Dreamweaver Remote Databas		Type	Configuration	a a a a a
Apache 2.x version older than 2.0.49 (1)		Description	Nultiple vulnerabilities	s have been reported
B 4 Apache Error Log Escape Sequence Injection			in PHP, which can be	exploited to gain
III- (1) Apache version older than 2.0.51 (1)			escalated privileges,	hypass certain
III- PHP version older 4.3.8 (1)			security restrictions, g	an knowledge of
PHP unspecified remote arbitrary file upload			vulnerable system.	or compromise a
Cross Site Scripting (8)			and the state of t	
⊕-			Affected PHP versions	a (up to 4.3.9/5.0.2).
EII- ( Backup Files (1)				
🖽 🐠 PtiFinfa page found (2)			Note:	state states below
③ ④ Source code disclosure (1)			batcer information	enerated using only
🛞 🐠 Broken links (2)			It may be a false posi	liva:
Hidden form input named price was found (1)		Impact	Possible local and re-	mate execution of
III- (I) TRACE Nethod Enabled (I)		1000000	arbitrary code. Check	references for more
III I Apache manual directory (1)			information.	
B- I CVS files found (9)		Recommendati	en Upgrade PHP to the I	allest version.
Possible sensitive directories (1)		Reported by	Manager at and	
Enal address found (22)		mandate	Version check	
🗄 📸 Site Structure		References		
曲·100 /	OK (200)	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Handened-PHP Artes	intre .
- Se Cookies			Converting of the Party	MALE.
			addunia Advisiony	*

Screenshot 12 - Scan Results – Vulnerability information

By clicking on an alert category node more information will be shown:

• Affects – The object affected by this vulnerability.

- **Details** Detailed information about the current alert. For example, for a SQL injection alert the parameters used to test for this vulnerability will be displayed.
- Severity The severity of the alert.
- **Type** The type of vulnerability.
- **Description** A description of the current vulnerability.
- Impact What impact this vulnerability may have.
- Recommendation A short recommendation on how to fix the problem.
- Reported by module The module that reported this vulnerability.
- References A list of references where you could gather more information about the current vulnerability and/or how to fix it.
- View HTTP headers Display HTTP headers for the request and response.
- View HTML response Display the HTML response as a frame in the current document.

**NOTE:** For further investigation, click on Edit with HTTP editor at the bottom of the pane. This will load the current HTTP request and response in the HTTP editor for manual inspection. For more information, please refer to the 'HTTP Editor' chapter.

# Site Structure Node

The site structure node displays the layout of the target site including all files and directories discovered during the crawling process. For every item retrieved more detailed information is available in the right information pane.



Screenshot 13 - Site Structure details

Summary information for a file or directory includes:

- Filename The name of this file/directory.
- Page Title The page title of this file/directory.
- File path The file/directory location.
- URL The file/directory URL location.
- HTTP Result The file/directory HTTP Get Response Code.
- Length The file/directory size in bytes.
- Input Variable Count Number of inputs used for collecting and processing data usually gathered within HTML forms.
- Status File status.

#### Saving the Scan Results

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

To save the scan results go on File > Save Scan Results.

To load the scan results go on File > Load Scan Results.

#### Generating a report

NOTE: To generate a report, a database must be configured (either MDB or SQL). This can be done from The Configuration > Settings node, under Application options > Database.

To create a report:

1 From the tools node, right Click on Reporter and select New Report, to start the report generation wizard.

Genera	ate report wizard	92 M			×
	Report source Report settings	Report source Please select one or more scans/scan g This scans will be used as source for thi	groups from the list is report.	bellow.	
		List of scan groups			
		Name	Profile default	Saved on 15/7/2005, 11:14	
		두 🗹 😼 Scan Thread 1 ( http://	/test.acunetix.com:	807)	
a	cunetix				
			< <u>B</u> ack	<u>N</u> ext > Cano	el

Screenshot 14 - Report Source selection

- 2 Select the report source from the database which contains the information to be displayed in the report and click on Next.
- 3 Now follow the steps of the wizard to create a report on the vulnerability scan.

# Google hacking vulnerability detection

Google hacking is the term used when a hacker tries to find exploitable targets and sensitive data by using search engines. The Google Hacking Database (GHDB) is a database of queries that identify sensitive data. Although Google blocks some of the better known Google hacking queries, nothing stops a hacker from crawling your site and launching the Google Hacking Database queries directly onto the crawled content.

Acunetix WVS Google hacking feature will launch all the queries found in the Google hacking database, onto the crawled content of your website thus finding any sensitive data or exploitable targets before a "search engine hacker" does. The Google hacking feature is a unique, industry first feature.

Information that the Google Hacking Database looks for:

- Advisories and server vulnerabilities
- Error messages that contain too much information
- Files containing passwords
- Sensitive directories
- Pages containing logon portals
- Pages containing network or vulnerability data such as firewall logs.

The Google Hacking Database is located at <u>http://johnny.ihackstuff.com</u>. More information can be found on: <u>http://www.informit.com/articles/article.asp?p=170880&rl=1</u>

#### Google hacking vulnerabilities node



Screenshot 15 - Scanner results with GHDB node

The GHDB vulnerability detection is performed as part of the automated scanning process and the results will be displayed as a separate node in the Scanner results.

© 2005 Acunetix Ltd. All rights reserved. The information contained in this document represents the current view of Acunetix on the issues discussed as of the date of publication. Because Acunetix must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Acunetix, and Acunetix cannot guarantee the accuracy of any information presented after the date of publication. This White Paper is for informational purposes only. Acunetix MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. Acunetix, Acunetix Web Vulnerability Scanner and their product logos are either registered trademarks or trademarks of Acunetix Ltd. in the United States and/or other countries. All product or company names mentioned herein may be the trademarks of their respective owners.