



Check with Acunetix Web Vulnerability Scanner

#### Audit your website security with Acunetix Web Vulnerability Scanner

As many as 70% of web sites have vulnerabilities that could lead to the theft of sensitive corporate data such as credit card information and customer lists.

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 site. 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.

#### Firewalls, SSL and locked-down servers are futile against web application hacking!

Web application attacks, launched on port 80/443, go straight through the firewall, past operating system and network level security, and right in to the heart of your application and corporate data. Tailor-made web applications are often insufficiently tested, have undiscovered vulnerabilities and are therefore easy prey for hackers.

Find out if your web site is secure before hackers download sensitive data, commit a crime using your web site as a launch pad, and endanger your business. Acunetix Web Vulnerability Scanner crawls your web site, automatically analyzes your web applications and finds perilous SQL injection, Cross site scripting and other vulnerabilities that expose your on line business. Concise reports identify where web applications need to be fixed, thus enabling you to protect your business from impending hacker attacks!

#### Acunetix - a world-wide leader in web application security

Acunetix has pioneered the web application security scanning technology: Its engineers focused on web security as early as 1997 and developed an engineering lead in web site analysis and vulnerability detection.

Acunetix Web Vulnerability Scanner includes many innovative features:

- An automatic Javascript analyzer allowing for security testing of Ajax and Web 2.0 applications
- Industry's most advanced and in-depth SQL injection and Cross site scripting testing
- Visual macro recorder makes testing web forms and password protected areas easy
- Extensive reporting facilities including VISA PCI compliance reports
- Multi-threaded and lightning fast scanner crawls hundreds of thousands of pages with ease
- Automate File Upload Forms vulnerability testing
- Acunetix crawls and analyzes websites including flash content, SOAP and AJAX
- Innovative AcuSensor Technology that allows accurate scanning for many vulnerabilities
- Port scanning and network alerts against the web server for complex security checks

"The issues detected were of major impact; if hackers would have found the security holes, they could have hacked an entire Joomla! Site."



Robin Muilvijk, member of the Quality & Testing Team, Joomla!

#### **Acunetix Customers:**

NASA **US** Army US Air Force KPMG Disney Bank of China Fujitsu Hewlett Packard AmSouth Bank US Department of Energy California Department of Justice Wescom Credit Union Trend Micro State of North Carolina US Geological Service France Telecom ActionAid UK University of Reading PricewaterhouseCoopers Australia **IBM** Denmark Panasonic Asia Pacific

The Armed Forces of Norway



# In depth checking for SQL Injection, Cross Site Scripting (XSS) and Other Vulnerabilities with the innovative AcuSensor Technology

Acunetix checks for all web vulnerabilities including SQL injection, Cross site scripting and others. SQL injection is a hacking technique which modifies SQL queries in order to gain access to data in the database. Cross site scripting attacks allow a hacker to execute a malicious script on your visitor's browser.

Detection of these vulnerabilities requires a sophisticated detection engine. Paramount to web vulnerability scanning is not the number of attacks that a scanner can detect, but the complexity and thoroughness with the scanner launches SQL injection, Cross Site scripting and other attacks.

Acunetix has a state of the art vulnerability detection engine that comes with the pioneering **AcuSensor Technology**. This is a unique security technology that quickly finds vulnerabilities with a low number of false positives, indicates where the vulnerability is in the code and reports debug information. It also locates CRLF injection, Code execution, Directory Traversal, File inclusion, Authentication vulnerabilities and others.

## Scan AJAX and Web 2.0 Technologies for vulnerabilities

The state of the art CSA (client script analyzer) Engine allows you to comprehensively scan the latest and most complex AJAX / Web 2.0 web applications and find vulnerabilities.

## **Port Scanning and Network Alerts**

Acunetix Web Vulnerability Scanner also runs an optional port scan against the web server where the site is hosted and automatically identifies the network service running on an open port, launching a series of network security tests against that web service. Customized network alerts can also be developed by following detailed documentation provided by Acunetix.

The security checks that ship with the product are: Test for weak passwords on FTP, IMAP, SQL servers, POP3, Socks, SSH, Telnet and other DNS server vulnerabilities like Open Zone Transfer, Open Recursion, Cache Poisoning, as well as, FTP access tests such as if anonymous access is allowed and list of writable FTP directories, security checks for badly configured Proxy Servers, checks for weak SNMP Community String, checks for weak SSL ciphers, and many other sophisticated security checks!

#### Detailed reports enable you to meet Legal and Regulatory Compliance

Acunetix Web Vulnerability Scanner includes an extensive reporting module which can generate reports that show whether your web applications meet the new VISA PCI Data Compliance requirements amongst others.

#### Analyzes your site against the Google Hacking Database

The Google Hacking Database (GHDB) is a database of queries used by hackers to identify sensitive data on your website such as portal logon pages, logs with network security information, and so on. Acunetix launches the Google hacking database queries onto the crawled content of your web site and identifies sensitive data or exploitable targets before a "search engine hacker" does.

## Test password protected areas and web forms with Automatic HTML form filler

Acunetix Web Vulnerability Scanner is able to automatically fill in web forms and authenticate against web logins. Most web vulnerability scanners are unable to do this or require complex scripting to test these pages. Not so with Acunetix: Using the macro recording tool you can record a logon or form filling process and store the sequence. The scanner can then replay this sequence during the scan process and fill in web forms automatically or logon to password protected areas.

🔨 Acuretis Web Vulnerability 1	cenner (Consultant edition)	
Tools Explanar 0 Tools Explanar Tools Uniterability Scanner With Scanner Tools Tools	Image: Section 2	- Pule(Stat - @ s
Son cubic Son cubic So	••••••••••••••••••••••••••••••••••••	Weiter State       Weiter State
	Attraction watcher Dass Site Controls, Inscretely invester ally on paremeter fundame Dass Site Controls, Inscretely invester ally on paremeter fundame Dass Site Controls, Inscretely invester ally on paremeter fundame Dass Site Site Site Site Controls, Inscrete ally on paremeter fundame Analisation Site Site Site Controls, Inscrete ally on paremeter fundame Analisation Site Site Site Controls, Inscrete ally on paremeter fundame Analisation Site Site Site Controls, Inscrete ally on paremeter fundame Analisation Site Site Site Site Site Site Site Site	

Acunetix performs automated attacks and displays vulnerabilities found.

	🛛 🗟 📽 😵 🔎 Sectific 🗠						er sesuentet i fors lager sequences 💌 🖬
	ana contrast, (betago, accreto, com R may /	wTTF:Read	logate.	Tale and the second	Carbon type	Hide tab information of the page co	
7	resultar.gf	Perfektion (1603)	Drestory Unling/Deried	text/stel	704 4 4	1951 Mitje (Junum Journellin, com) Terrefacture: Januar Miterrahmi, Julya A Julya	
	P (2) Ineges	Forbidden (403)		Directory Listing Daried	toohtel	2	Defailt.ap Saidt.ap Juge.ap/testRLv1t/POefail1428ap143 Jeptier.ap?testRLv1270efail1428ap peorform.ap?d+l
	Defait.ap	0K (203) 0K (203) 0K (203) 1			southers southers		
	anda					A	
	3) S inginiero 31 S teoretariae	OK CRIER	2	acutarum legin	Sext/Head	1	menforum.apid=1 menforum.apid=2
	R in Search and	OK (200)	÷.	ection werds	heathead	240	
	H D SHI'CLAD	06 (200)	1	action march	sochists truthing	UNK .	styles an
	Contraction and Contraction	DK (200)		NOVEM IN SERVICE	Malifus		
	Contenting and	Internel Server Error (SEC)		Untitled Document	anapose anapose		
	and OT they shall do ut him	06 (200)		Unified Too ment	brathing		
	ri al conformati	Cline(1 moved (202)		Ditell swed	brabhied		
	L International	OK (2001		apple in Appendix	water		
	and OT days	06,0200		auto e litetre	brathing		
	NOR CET MIN2	DK (200)		atufarun Macelaneous Obiect moved	brack/steel		
	and an	Otherst mayed CRUD	4				
	Costies						
						×	
н						Smale URLs (10	
н.						tien Source	A Ven Page 🔄 HTM, sinchare analysis

Acunetix crawls web site automatically and displays web site structure.

Tools Dightner 0	8 2 8 5 0 M 9 44	Q.
Architer freet     Construction     Construction	• Internet of the sector of the sec	Property of the strate of
	A hand of the	Conjust to same of controls day screek per a provide the second providence of the second providence of the second per second pe
		N D 24 D X

Extensive reporting including VISA PCI compliance.

Wizard		6
Scan type	Scan type	
Select targets Crawling colions	Select whether you want to scan a single website, a list or range of web the results of a previous crawl.	billes or whether you want to anal
Scan options	Scan Mpe	
Login	Here you can scan a single website. In case you want to scan a whole site you can enter the full path below. The application sup	a single web application and not # pports HTTP and HTTPS website
r man	Scan single website	
	Website URL: http://testphp.acunetix.com	-
	If you saved the site structure using the site crawler tool you can scan will load this data from the Reinstead of crawling the site a	n use the saved results here. The
	C Scan using saved crawling results	
	Filenare:	× 23
	In case you want to scan a list of websites, you need to choose containing the list of websites and indicate the path of this lie by	this option. Prepare a test file
	C Scan a list of websites from a file	
	Filename:	- 2
	You can also scan a range of computers. This wizard will inspec HTTPS websites. You may select individual websites later after	t this range looking for HTTP and the discovery was finished.
	You can also scan a range of computers. This wised will inspec HTTPS websites. You may relect individual websites later after Scan a range of computers looking for websites	t this range looking for HTTP and the discovery was finished.
<b>n</b>	HTTPS websites. You may select individual websites later after	t this range looking for HTTP and the discovery was finished.

Wizard makes launching scans easy and quick.



# Advanced penetration testing tools included

In addition to its automated scanning engine, Acunetix includes advanced tools to allow penetration testers to fine tune web application security checks:

- HTTP Editor With this tool you can easily construct HTTP/HTTPS requests and analyze the web server response.
- HTTP Sniffer Intercept, log and modify all HTTP/HTTPS traffic and reveal all data sent by a web application.
- HTTP Fuzzer Performs sophisticated testing for buffer overflows and input validation. Test thousands of input variables with the easy to use rule builder of the HTTP Fuzzer. Tests that would have taken days to perform manually can now be done in minutes.
- Create custom attacks or modify existing ones with the Web Vulnerability Editor.
- Blind SQL Injector An automated database data extraction tool that is ideal for penetration testers who wish to make further tests manually.

#### Many more advanced features

Scanning profiles to easily scan websites with different scan options and identities

- Custom report generator
- Compare scans and find differences with previous scans
- Easily re-audit web site changes
- Support for CAPTCHA, Single Sign-On and Two Factor authentication mechanisms
- Detects popular web applications (e.g. forums, shopping carts) and detects vulnerable versions
- Detects directories with weak permissions and if dangerous HTTP methods are enabled
- Generates a list of uncommon HTTP responses such as internal server error, HTTP 500, etc
- Customize list of false positives

#### Versions available - Small Business, Enterprise, and Consultant

Acunetix Web Vulnerability Scanner is available in three versions: A Small Business Version for one nominated web site, an Enterprise version to allow for scanning of an unlimited number of websites, and a Consultant version, which allows you to use Acunetix WVS to perform penetration tests for third parties.

acunetix threat level	Acunetix threat level 3				
Level 3: High	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	387				
🕖 High	209				
O Medium	9				
O Low	117				
Informational	52				
Alerts summary					
Blind SQL/XPath injuge	ction				
Affects		Variations			
/artists.php		3			
/guestbook.php		1			
ORLF injection/HTTF	response splitting				
Affects		Variations			
/redir.php		2			
Oross Site Scripting					
Affects		Variations			
/comment.php		16			
/guestbook.php		33			
/listproducts.php		26			
/search.php		25			
/secured/newuser.php /secured/phpinfo.php		0			
/showimage.php		32			
Oross Site Scripting	000				
Affects	n uru	Variations			
/secured/phpinfo.php		2			
9 SQL injection					
Affects		Variations			
/artists.php		9			
/cart.php		7			
/listproducts.php		18			
/product.php		9			

Example of scan results

© 2009 Acunetix Ltd. All rights reserved. Acunetix, Acunetix Web Vulnerability Scanner and their product logos are either registered trademarks or trademarks of Acunetix Software Ltd. in the United States and/or other countries.

## **System Requirements**

- Windows XP, Vista, 2000 or Windows 2003 server
- Internet Explorer 6 or higher
- 200 Mb of hard disk space
  - 1GB of RAM



# **Acunetix Ltd**

6th Floor Portomaso Tower PTM 01, Portomaso Malta

Tel: (+356) 2316 8000 Fax: (+356) 2138 8099 Email: sales@acunetix.com

## Acunetix (USA)

Tel: 888 593 5285 Fax: (+1) 425 650 6873 Email: salesusa@acunetix.com

#### Acunetix (UK)

Communications House 26 York Street W1U 6PZ London United Kingdom

Tel: (+44) 0800 0517577 Fax: (+44) 0844 8732291 Email: sales@acunetix.com







