acunetix

IS YOUR WEBSITE HACKABLE?

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 into 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.

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

CERN, Switzerland

Panasonic Asia Pacific

The Armed Forces of Norway

Credit Suisse

In the press:

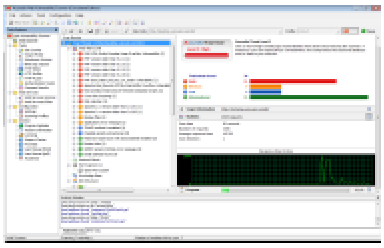
"Acunetix WVS doesn't just let you see how your website is vulnerable. It also provides information and tools that allow you to test your web applications. It is an important tool for web developers. It's very customizable and, therefore, lends itself to in-depth testing beautifully ." *Help Net Security*

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

Acunetix WVS checks for all web vulnerabilities including SQL injection, Cross site scripting and many 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.

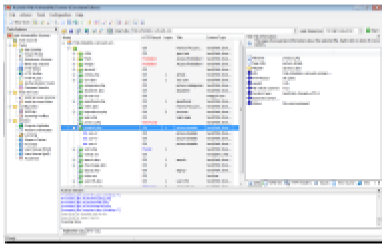
Acunetix has a state of the art vulnerability detection engine that comes with the pioneering **AcuSensor Technology**. This is a unique security technology that quickly finds vulnerabilities with a low number of false positives, indicates where the vulnerability is in the code and reports debug information.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



Acunetix performs automated attacks and displays vulnerabilities found.

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 web vulnerabilities.

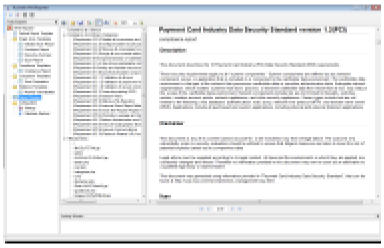


Acunetix crawls web site automatically and displays web site structure.

Port Scanning and Network Alerts

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



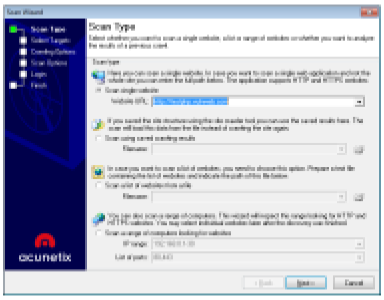
Extensive reporting including VISA PCI compliance.

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 PCI DSS Data Compliance requirements amongst many 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 information 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.



Wizard makes launching scans quick and easy.

Test password protected areas and web forms with Automatic web 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 such pages. Not so with Acunetix: Using the macro recording tool Login Sequence Recorder, you can record a login sequence, form filling process or a specific crawling sequence. The scanner will replay this sequence during the scan process and fill in web forms and log on to password protected areas automatically.

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 audits:

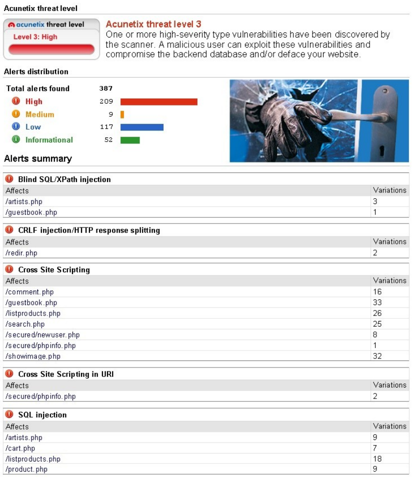
- HTTP Editor - Construct HTTP/HTTPS requests and analyze the web server response.
- HTTP Sniffer - Intercept, log and modify all HTTP/HTTPS traffic and reveal all data sent by a web application.
- HTTP Fuzzer - Perform sophisticated fuzzing tests to test web applications input validation and handling of unexpected and invalid random data. Test thousands of input parameters 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.
- Script your own custom web vulnerability attacks with the WVS Scripting tool. A scripting SDK documentation is available from the Acunetix website.
- 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 with rescan functionality.
- 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.

Editions available - Small Business, Enterprise, and Consultant

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



Acunetix 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	387
High	209
Medium	9
Low	117
Informational	52

Alerts summary

Blind SQL/XPath injection

Affects	Variations
/artists.php	3
/guestbook.php	1

CRLF injection/HTTP response splitting

Affects	Variations
/redir.php	2

Cross Site Scripting

Affects	Variations
/comment.php	16
/guestbook.php	33
/listproducts.php	26
/search.php	25
/secured/newuser.php	8
/secured/phpinfo.php	1
/showimage.php	32

Cross Site Scripting in URI

Affects	Variations
/secured/phpinfo.php	2

SQL injection

Affects	Variations
/artists.php	9
/cart.php	7
/listproducts.php	18
/product.php	9

Example of scan results

"Acunetix WVS has played a very important role in identification and mitigation of web apps vulnerabilities. Acunetix has proven itself and is worth the cost."

Mr Rodgers
IT Security Team
U.S. Air Force

"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!

"The use of Acunetix WVS has allowed us to scheduler regular automated scans on a host of sites under the Betfair Group umbrella, providing invaluable visibility in capturing website vulnerabilities early in the SDLC."

Jan Ettles
Betfair.com, UK

Acunetix is a key point in our application's security strategy, it's integrated with the QA process, allowing us a cost effective way of detecting flaws that can be solved early within the development life cycle.

Petro Anduja
ING Direct
Spain

"As a penetration tester, Acunetix WVS makes the most tedious and recurring tasks a breeze, cutting down on time requirement and raising the quality of the test."

Thierry Zoller
Telindus PSF
Luxembourg

What's new in Acunetix Web Vulnerability Scanner Version 7

In Acunetix WVS Version 7, most of the core components have been rewritten. It is 75% faster, and ships with a more intelligent and faster scanning engine. In Version 7 you can also script your own web and network vulnerability checks since the vulnerability database has been migrated to scripts. Scripting also allows more advanced and flexible security checks, while reducing false positives. Version 7 also includes many more meticulous web security tests, some of which were not possible before.

Summary of new features:

- New revolutionary scanning engine detects a wider range of web vulnerabilities.
- Less false positives and false negatives; human like vulnerability verifying techniques!
- Improved web 2.0 applications support; better handling and parsing of JSON and XML.
- Improved handling and detection techniques of links and input parameters.
- Consolidation of vulnerabilities to facilitate coordination of vulnerability remediation.
- Less chances of breaking down a website; advanced analysis of website presentation layer.
- Improved Web 2.0 web applications Session management handling.
- New graphical Scan Status Interface presents user with granular scanning details.
- Ability to rescan a specific vulnerability to verify remediation.
- HTTP Authentication settings node; support for multiple HTTP authentication credentials.
- Support for a wider range of content-types.
- Faster and better handling of network traffic; support for DNS caching, keep-alive etc.
- Improved old and added new web server security auditing techniques.
- Drastically improved file upload security checks.
- Support for a wider variety of communication mechanisms.
- New 'Acunetix Scripting tool' to assist you with scripting of new vulnerabilities.
- Ability to automatically submit correct and relevant data in web forms.

For more information about Acunetix Web Vulnerability Scanner visit:

Web: www.acunetix.com

Web Application Security Blog: www.acunetix.com/blog

Connect with us:

Twitter: twitter.com/acunetix

Facebook: www.facebook.com/acunetix

System Requirements

- Windows XP, Vista, 2000, 2003 and 2008 server, Windows 7
- Internet Explorer 6 or higher
- 250 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: (+1) 877 260 8931
Fax: (+1) 425 650 6873
Email: salesusa@acunetix.com

Acunetix (UK)

Unit 2, St John Mews
St John Road, Hampton Wick
KT1 4AN
Kingston upon Thames
United Kingdom

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

WindowSecurity.com READERS' CHOICE WINNER

Microsoft CERTIFIED Partner

OWASP Member The Open Web Application Security Project

Compatible with Windows 7