



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 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
- Intelligent crawler detects web server type and application language
- 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 Muilwijk,
member of the Quality
& Testing Team,
Joomla!

Acunetix Customers:

US Army
US Air Force
Bank of China
Fujitsu
Hewlett Packard
AmSouth Bank
San Diego County Credit Union
US Department of Agriculture
US Department of Energy
California Department of Justice
Wescom Credit Union
State of Virginia Gov Department
State of North Carolina
US Geological Service
France Telecom
ActionAid UK
University of Reading
Virginia Tech
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 commands 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 and Authentication vulnerabilities.

Scan AJAX and Web 2.0 Technologies for vulnerabilities

The state of the art JavaScript analyzer 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 Data 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

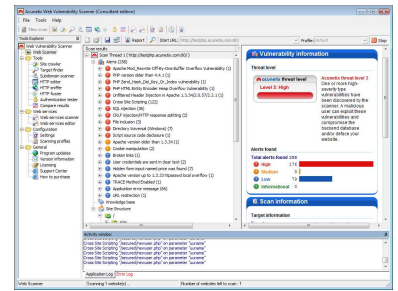
Acunetix Web Vulnerability Scanner includes an extensive reporting module which can generate reports that show whether your web applications meet the new VISA PCI Data Compliance requirements amongst others.

Analyzes your site against the Google Hacking Database

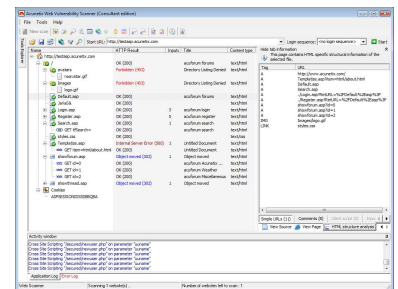
The Google Hacking Database (GHDB) is a database of queries used by hackers to identify sensitive data on your website such as portal logon pages, logs with network security information, and so on. Acunetix launches the Google hacking database queries onto the crawled content of your web site and identifies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

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

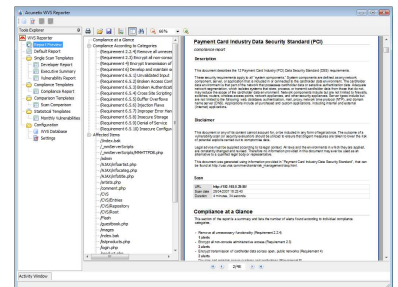
Acunetix Web Vulnerability Scanner is able to automatically fill in web forms and authenticate against web logins. Most web vulnerability scanners are unable to do this or require complex scripting to test these pages. Not so with Acunetix: Using the macro recording tool you can record a logon or form 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.



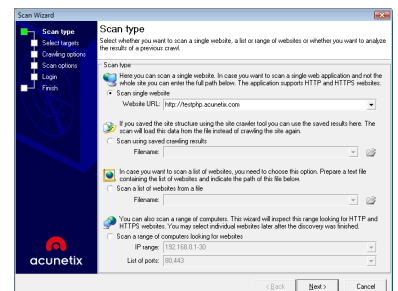
Acunetix performs automated attacks and displays vulnerabilities found.



Acunetix crawls web site automatically and displays web site structure.



Extensive reporting including VISA PCI compliance.



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.

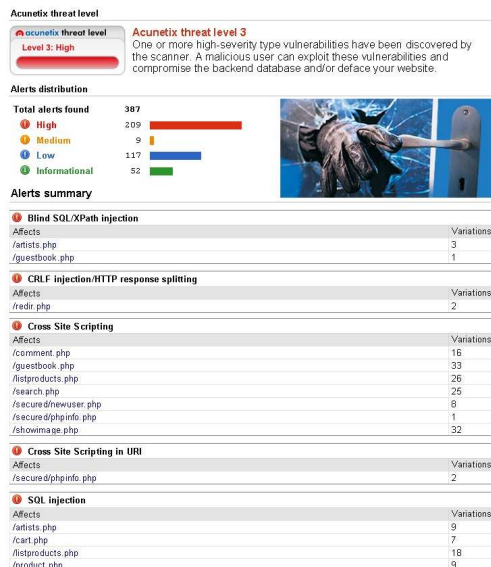
Many more advanced features

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
- Discovers directories with weak permissions
- Detects popular web applications (e.g. forums, shopping carts) and detects vulnerable versions
- Detects if dangerous HTTP methods are enabled on your web server
- 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.



Example of scan results

© 2008 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 professional and server or Windows 2003 server
- Internet Explorer 5.1 or higher
- 200 Mb of hard disk space



Acunetix Ltd

6th Floor
Portomaso Tower
PTM 01, Portomaso
Malta

Tel: (+356) 2316 8000
Fax: (+356) 2138 3396
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) 0845 6126712
Fax: (+44) 0845 612716
Email: sales@acunetix.com

