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 websites 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 compromised site.

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 website is secure before hackers download sensitive data, commit a crime using your website as a launch pad, and endanger your business. Acunetix Web Vulnerability Scanner (WVS) crawls your website, automatically analyzes your web applications and finds perilous SQL injection, Cross site scripting and other vulnerabilities that expose your online 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 website analysis and vulnerability detection.

Acunetix Web Vulnerability Scanner includes many innovative features:

- Innovative AcuSensor Technology that allows accurate scanning with low false positives, by combining black box scanning techniques with feedback from its sensors placed inside the source code.
- 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.
- Multi-threaded and lightning fast scanner able to crawl hundreds of thousands of pages without interruptions.
- Acunetix WVS understands complex web technologies such as SOAP, XML, AJAX and JSON.

Acunetix Customers:

NASA · U.S. AIR FORCE · THE PENTAGON · DEPARTMENT OF ENERGY · U.S.ARMY · AMERICAN EXPRESS · NORWEGIAN ARMED FORCES · CISCO · London Stock Exchange · ING · BANK OF CHINA · CREDIT SUISSE · SONY · Deloitte. · HSBC · KPMG · PRICEWATERHOUSECOOPERS · Deutsche Bank · CERN · BARCLAYS · Panasonic · FUJITSU · WALT DISNEY PICTURES · france telecom

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 and Cross Site Scripting (XSS) Vulnerabilities

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 which the scanner launches SQL injection, Cross Site scripting and other attacks.

Innovative AcuSensor Technology Guarantees Low False Positives

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 much more.

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. Acunetix WVS understands SOAP, XML, AJAX and JSON.

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.

Schedule Scans of Multiple Websites at Anytime, Anywhere

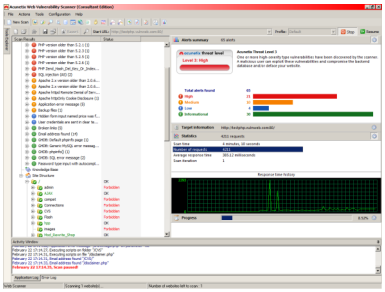
Acunetix offers you the possibility of scanning up to 10 websites simultaneously, by launching multiple instances of the scanner, on the same computer. The scanning performance is therefore significantly increased. You may decide to schedule the scans when the website is less busy, for example at night. Furthermore, a web portal allows you to log in, schedule the scans and retrieve the results from anywhere at any time.

Detailed Reports Enable You to Meet Legal and Regulatory Compliance

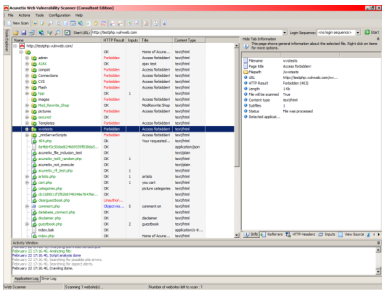
Acunetix Web Vulnerability Scanner includes an extensive reporting module which can generate reports that show whether your web applications meet the PCI DSS Data Compliance requirements. It also reports whether any vulnerabilities from the OWASP Top 10 are found. OWASP is a web application security organisation that publishes the top 10 web vulnerabilities on the internet. Acunetix checks if your web application is compliant with the NIST Special Publication 800-53, as well as the DISA Application Security and Development STIG guidelines. There is also a report which shows whether you website has any errors listed in the CWE/SANS Top 25 Most Dangerous Software Errors.

Analyzes Your Website Against the Google Hacking Database

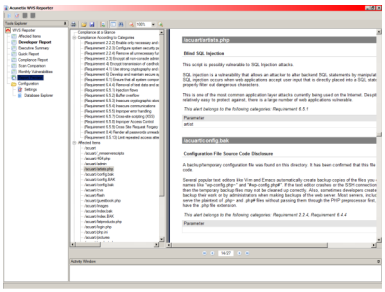
The Google Hacking Database (GHDB) is a database of queries used by hackers to identify sensitive information on your website such as portal logon pages, logs with network security information, and so on. Acunetix launches the Google hacking database queries onto the crawled content of your website and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



Acunetix performs automated attacks and displays vulnerabilities found.

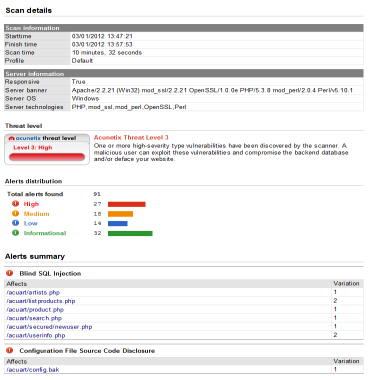


Acunetix crawls website automatically and displays website structure.



Extensive reporting including VISA PCI compliance.

Wizard makes launching scans quick and easy.



Example of scan results.

Automatic Custom 404 Error Page Identification

Acunetix WVS 8 can automatically determine if a custom error page is in use, and identifies it without needing any recognition patterns to be configured before the scan.

Auto-configuration of a Web Application Firewall

Acunetix WVS can automatically create the appropriate Web Application Firewall rules to protect your web application against attacks targeting vulnerabilities that Acunetix finds. This allows you to continue using your web application in a secure manner until you are able to fix the vulnerabilities at the code level. Currently Acunetix supports the popular Imperva Web Application Firewall.

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!

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, in order 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.

More Advanced Features

- Detect HTTP Parameter Pollution (HPP) vulnerabilities.
- Support for custom HTTP headers in automated scans.
- Support for multiple HTTP authentication credentials.
- 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 website changes with rescan functionality.
- Support for CAPTCHA, Single Sign-On and Two Factor authentication mechanisms.
- Detects directories with weak permissions and if dangerous HTTP methods are enabled.

"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 schedule 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
United Kingdom

''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

"In addition to traditional web application security testing, Acunetix has proven its power and flexibility to quickly identify major risks in an environment such as SharePoint, PKI and Citrix.''

Serge Faller
Datalynx AG
Switzerland

- Generates a list of uncommon HTTP responses such as internal server error, HTTP 500, etc.
- Customize list of false positives.
- Security audit of the web server configuration.
- Auto importation of IIS 7 rewrites rules directly from web.config.file.
- Ability to rescan a specific vulnerability in order to verify remediation.
- Automate File Upload Forms vulnerability testing.

Editions Available

Acunetix Web Vulnerability Scanner is available in five Editions: a Small Business Edition for one nominated website, an Enterprise Edition to allow for scanning of an unlimited number of company own websites and a Consultant Edition which allows you to use Acunetix WVS to perform penetration tests for third parties. Both the Enterprise and Consultant Editions are available with the optional function to scan up to 10 websites simultaneously.

About Acunetix

Acunetix was founded in 2004 to combat the alarming rise in web attacks and today is a market leader in web application security technology. Its flagship product, Acunetix Web Vulnerability Scanner (WVS), is designed to replicate a hacker's methodology to find dangerous vulnerabilities -- like SQL injection and cross site scripting -- before hackers do.

Contact Information

Acunetix (Head office)
Office 303, Engomi Business Center
No 1, 28th October Street
2414 Nicosia
Cyprus
Tel: +44 (0)330 202 0192
Fax: +44 (0)330 202 0191
Email: sales@acunetix.com

Acunetix (UK)
Unit 2, St John Mews
St John Road, Hampton Wick
KT1 4AN, Kingston upon Thames
United Kingdom
Tel: +44 (0)330 202 0190
Fax: +44 (0)330 202 0191
Email: sales@acunetix.com

Acunetix (USA)
Tel: (+1) 888 593 5285
Fax: (+1) 888 367 4512
Email: salesusa@acunetix.com

Stay up to date with the latest web security news:
Read the Acunetix Blog: **www.acunetix.com/blog**
Like the Acunetix Facebook Page: **www.facebook.com/acunetix**
Follow us on Twitter: **twitter.com/acunetix**
Interact with the Acunetix online community on the forums: **www.acunetix.com/forums**

System Requirements

- Windows XP, 2008 server, Windows7
- Internet Explorer 8, Google Chrome, Mozilla Firefox
- 512 Mb of hard disk space
- 2GB of RAM

Acunetix's Customers Include