IS YOUR WEBSITE HACKABLE?

VOQUZ IT SOLUTIONS

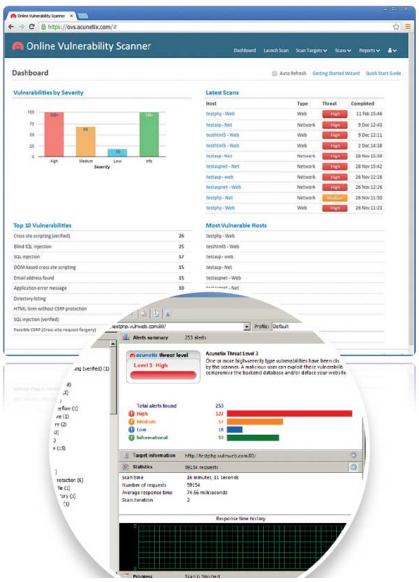
acunetix

CHECK WITH ACUNETIX WEB VULNERABILITY SCANNER

As many as 70% of websites have vulnerabilities that could lead to the theft of sensitive corporate data such ascredit 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 the operating system and network level security, and right into the heart of yourapplication and corporate data. Tailor-made web applications are often insufficiently tested, have undiscovered vulnerabilities and are therefore easy prey for hackers.

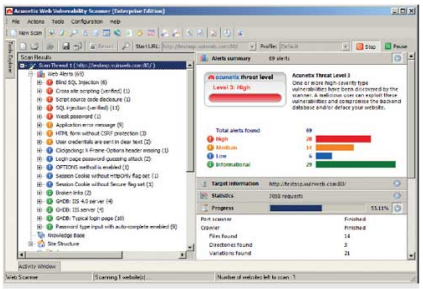


Find out if your website is secure before hackers download sensitive data, launch criminal activity from your website and endanger your business. Acunetix Web Vulnerability Scanner (WVS) crawls your website, automatically analyzes your web applications and finds perilous SQL injection, Cross-Site Scripting 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 - THE TECHNOLOGY LEADER IN WEB APPLICATION SECURITY

Acunetix has pioneered web application security scanning and has established an engineering lead in website analysis and vulnerability detection with the following innovative features:

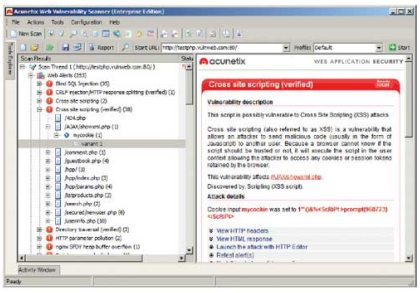
- AcuSensor Technology allows accurate scanning with low false positives, by combining black box scanning techniques with feedback from its sensors placed inside the source code.
- An automatic JavaScript analyzer for security testing of AJAX and Web 2.0 applications.
- Industry's most advanced and in-depth SQL injection and Cross-Site Scripting testing.
- Login Sequence 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 DeepScan understands complex web technologies such as SOAP, XML, AJAX and JSON.



Main WVS Interface

IN-DEPTH CHECKING FOR SQL INJECTION AND CROSS-SITE SCRIPTING (XSS) VULNERABILITIES

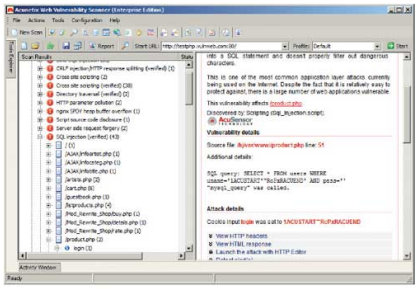
Acunetix WVS checks for all web vulnerabilities including SQL injection, Cross-Site Scripting and many others. SQL injection is a hacking technique which modifies SQL queries in order to gain access to data in the database. Cross-Site Scripting attacks allow a hacker to execute a malicious script on your visitor's browser. 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 them. Acunetix sophisticated scanning engine guarantees the highest rate of vulnerability detection including DOM-based XSS vulnerabilities.



XSS Vulnerability

INNOVATIVE ACUSENSOR TECHNOLOGY GUARANTEES

Acunetix includes unique AcuSensor Technology that analyzes code as it gets executed, resulting in higher detection rate, and importantly elimination of false positives. Furthermore, AcuSensor technology is able to indicate where the vulnerability is in the code and report debug information. AcuSensor not only finds more vulnerabilities, but will save valuable time for your security and development teams.



SQLi showing SQL Query (thanks to AcuSensor)

DEEPSCAN TECHNOLOGY SCANS MOST CONTENT

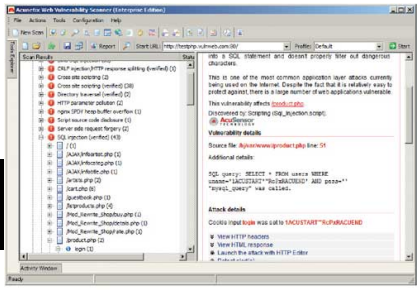
Acunetix DeepScan Technology, which includes the state-of-the-art CSA (Client Script Analyzer) Engine, crawls and scans the latest HTML5 and dynamic JavaScript web content. By being able to find the largest amount of web content and understand it (includingSingle Page Application sites) Acunetix can detect the highest number of vulnerabilities.

SCAN AJAX AND WEB 2.0 TECHNOLOGIES FOR VULNERABILITIES

The CSA Engine allows you to comprehensively scan the latest and most complex AJAX / Web 2.0 web applications. Acunetix WVS understands SOAP and XML, tests for vulnerabilities in AJAX and JSON request data, as well as web applications developed using Google Web Toolkit.

TEST PASSWORD PROTECTED AREAS AND WEB FORMS WITH AUTOMATIC FORM FILLER

Acunetix isable 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 Login Sequence Recorder macro recording tool, you can record a login sequence, form filling process or a specific crawling sequence. The scanner will replay this sequence during the scan process, fill in web forms and log on to password protected areas automatically.



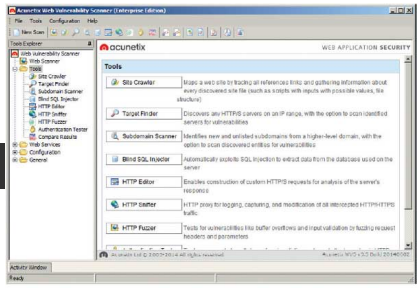
SQLi showing SQL Query (thanks to AcuSensor)

DETAILED REPORTS ENABLE YOU TO MEET LEGAL AND REGULATORY COMPLIANCE

Acunetix Web Vulnerability Scanner includes extensive reports which include: PCI DSS; OWASP Top 10; ISO 27001; NIST Special Publication 800-53 (for FISMA); HIPAA; Sarbanes-Oxley; Mitre CWE/SANS Top 25 Most Dangerous Software Errors, among others.

AUTO-CONFIGURATION OF WEB APPLICATION FIREWALL

Acunetix WVS can automatically create the appropriate Web Application Firewall rules to protect web applications 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 code level. Currently Acunetix supports the popular Imperva Web Application Firewall.



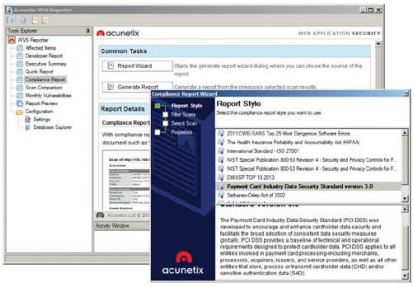
Acunetix Manual Testing Tools

ADVANCED NETWORK LEVEL SCANNING

Part of a Website audit is a network level audit against any operating system vulnerabilities. An online scanning engine integrates the popular OpenVAS scanner to identify the highest number of network level vulnerabilities. Acunetix will test forweak passwords, insecure web server configuration, directories with weak permissions, DNS server vulnerabilities, FTP access tests, badly configured Proxy Servers, weak SSL ciphers, and many other sophisticated security checks!.

WORDPRESS VULNERABILITY SCANNING

Acunetix identifies WordPress installations and will launch WordPress specific security checks to ensure your website is secure including detection of vulnerable plugins and themes, weak passwords, mal configuration of WordPress (username enumeration, WP config backup files), Malware disguised as plugins and old versions of plugins. Similar checks are also performed on other Content Management Systems such as Joomla and Drupal.



Reporter

ADVANCED PENETRATION TESTING TOOLS INCLUDED

Acunetix includes advanced tools for penetration testers to further their security audits:

- HTTP Editor - Construct HTTP/HTTPS requests to analyze the web server response.
- HTTP Sniffer - Intercept, log and modify HTTP/HTTPS traffic sent by web application.
- HTTP Fuzzer - Perform sophisticated fuzzing tests with thousands of input parameters using the rule builder and test input validation of web applications and handling of invalid/random data.
- Blind SQL Injector - An automated database data extraction tool.

MORE ADVANCED FEATURES

- Automatic Custom 404 Error Page & rewrite rule identification.
- HTTP Parameter Pollution (HPP) vulnerability detection.
- Supports custom HTTP headers in automated scans.
- Supports multiple HTTP authentication credentials.
- Support for CAPTCHA, Single Sign-On and Two Factor authentication mechanisms.
- Customize list of false positives & script custom web attacks.
- Automate File Upload Forms vulnerability testing.
- Locates CRLF injection, Code execution, Directory Traversal, File inclusion, Google Hacking Database and Authentication vulnerabilities.
- Scanning profiles to scan websites with different scan options and identities.
- Compare scans and find differences with previous scans.
- Easily re-audit vulnerability fixes with rescan functionality.

AVAILABLE AS A HOSTED OR ON PREMISE SOLUTION

Acunetix Web Vulnerability Scanner is available Online/Hosted or On Premise. The Online version can be licensed per year for any number of scan targets. The On Premise version is available as an Enterprise Edition to allow for scanning of an unlimited number of company owned websites and a Consultant Edition which allows you to use Acunetix WVS to perform penetration tests for third parties. Both editions can optionally scan up to 10 websites simultaneously.

CUSTOMER TESTIMONIALS

"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."

U.S. AIR FORCE

Mr Rodgers
IT Security Team
U.S. Air Force

"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."

ING

Petro Anduja
ING Direct, Spain

"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 vulnerabilities early in the SDLC."

betfair
The World's Biggest Betting Community

Jan Ettles
Betfair.com, UK

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.

Some of Acunetix clients:

SONY, AMERICAN EXPRESS, AVG, NHS, NATIONAL GEOGRAPHIC, FUJITSU, NASA, HSBC, NOKIA, SAMSUNG, Canon, Expedia

VOQUZ IT SOLUTIONS

Hamburg
T +49 40 675968-0

Frankfurt
T +49 69 6607680-0

München
T +49 89 925191-0

Zürich
T +41 52 62008-80

Düsseldorf
T +49 211 577996-0

Stuttgart
T +49 7195 92255-0

Wien
T +43 1 5222015 -10

kontakt@voquz.com
www.voquz.com