acunetix

Is your website hackable?

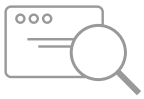
Check with **Acunetix Web Vulnerability Scanner**

As many as 70% of websites have vulnerabilities that could lead to the theft of sensitive corporate data such 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 Hardened Networks 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 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, launch criminal activity from your website and endanger your business. Acunetix Vulnerability Scanner automatically crawls and scans off-the-shelf and custom-built websites and web applications for SQL Injection, XSS, XXE, SSRF, Host Header Attacks & over 500 other web vulnerabilities.



Crawl & Scan

What you can't crawl you can't scan. Acunetix can crawl complex web application architectures including JavaScript-heavy HTML5 Single Page Applications while being able to scan restricted areas automatically, with ease.

Detect & Alert

With vulnerability detection, it's accuracy that counts. Acunetix detects over 500 types of web app vulnerabilities alerting according to severity, but its ability to scan accurately, guaranteeing low false positives, is what places it above the rest.

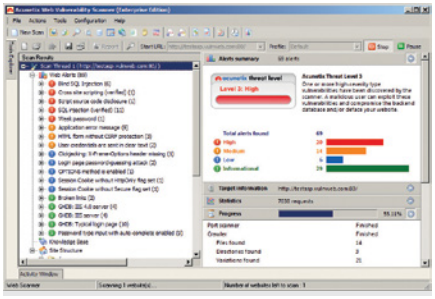
Report & Remediate

A wide variety of reports help developers and business owners alike to quickly identify a web application's threat surface, detect what needs to be fixed, and ensure conformance with several compliance standards.

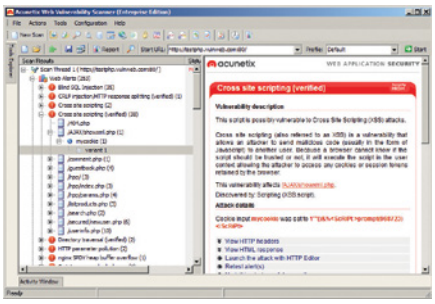
Acunetix - The Technology Leader in Web Application Security

Acunetix are the pioneers in Automated Web Application Security Testing with an engineering lead in website structure analysis and vulnerability detection. The Acunetix innovative technologies include

- DeepScan Technology allows accurate crawling of AJAX-heavy client-side Single Page Applications (SPAs) that leverage complex technologies such as SOAP/WDSL, SOAP/WCF, WADL, XML, JSON, Google Web Toolkit (GWT) and CRUD operations.
- Industry's most advanced and robust SQL Injection and Cross-site Scripting testing, including advanced detection of DOM-based Cross-site Scripting.
- A Login Sequence Recorder that allows the automatic crawling and scanning of complex password protected areas including multi-step, Single Sign-On (SSO) and OAuth-based websites.
- AcuSensor Technology allows accurate scanning further reducing the false positive rate, by combining black box scanning techniques with feedback from its sensors placed inside the source code.
- Highest detection of WordPress vulnerabilities - scans WordPress installations for over 1200 known vulnerabilities in WordPress' core, themes and plugins.
- Multi-threaded, lightning fast crawler and scanner that can crawl hundreds of thousands of pages without interruptions.
- Easily generate a wide variety of technical and compliance reports aimed towards developers and business owners alike.



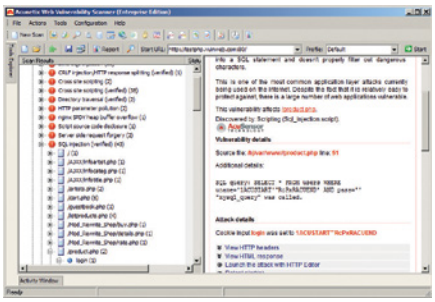
Main WVS Interface



XSS Vulnerability

In-depth checking for SQL Injection and Cross-Site Scripting (XSS) Vulnerabilities

Acunetix Vulnerability Scanner rigorously tests for hundreds of web application vulnerabilities including SQL Injection and Cross-site Scripting. SQL Injection is one of the oldest and most prevalent of software bugs; it allows attackers to modify SQL queries in order to gain access to data in the database. Cross-Site scripting attacks allow attackers to execute malicious scripts inside your visitors' browser; possibly leading to impersonation of that user. Acunetix is the industry leader in detecting the largest variety of SQL Injection and XSS vulnerabilities, including Out-of-band SQL Injection and DOM-based XSS.



SQLi showing SQL Query (thanks to AcuSensor)

AcuSensor Technology Guarantees Low False Positives

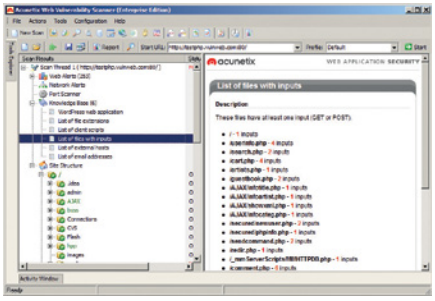
Acunetix includes unique AcuSensor Technology that analyzes code as it gets executed, resulting in higher detection rate, and importantly elimination of false positives. Furthermore, AcuSensor technology is able to indicate where the vulnerability is in the code and report debug information. AcuSensor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

Test Authenticated Web Applications with Login Sequence Recorder

Testing authenticated areas of your web applications is absolutely crucial to ensure full testing coverage. Acunetix Vulnerability Scanner can automatically test authenticated areas by recording a Login Sequence using the Login Sequence Recorder. The Login Sequence Recorder makes it quick and easy to record a series of actions the scanner can re-play to authenticate to a page. The Login Sequence Recorder can also record a series of Restrictions; making it trivial to granularly limit the scope of a scan in a few clicks.

DeepScan Technology Scans Most Content

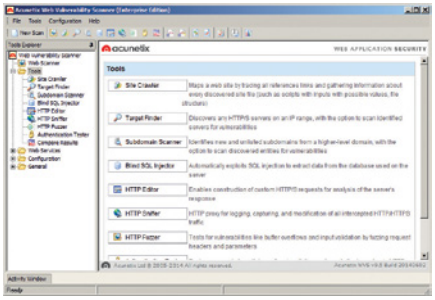
A fundamental process during any scan is the scanner's ability to properly crawl an application, no matter what web technology it's written in. Acunetix Vulnerability Scanner features DeepScan Technology; an HTML5 crawling and scanning engine that fully replicates user interaction inside of a browser by executing and analyzing JavaScript. DeepScan allows accurate crawling of AJAX-heavy client-side Single Page Applications (SPAs) that leverage technologies such as AngularJS, EmberJS and Google Web Toolkit. It can understand and interact with complex web technologies such as: AJAX, SOAP/WDSL, SOAP/WCF, WADL, XML, JSON, Google Web Toolkit (GWT) and CRUD operations. In addition, DeepScan has been further optimized to analyze websites and web applications developed in Ruby on Rails and Java Frameworks including Java Server Faces (JSF), Spring and Struts.



Knowledge Base showing List of files with inputs

Advanced Network Level Scanning

Comprehensive security audits require detailed inspection of the perimeter of your public-facing network assets. Acunetix has integrated the popular OpenVAS scanner within Acunetix Online Vulnerability Scanner to provide a comprehensive perimeter network security scan that integrates seamlessly with your web application security testing, all from an easy to use simple cloud-based service. Acunetix will test for weak 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.



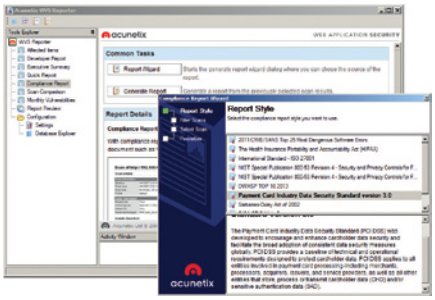
Acunetix Manual Testing Tools

Detailed Reports Enable you to Meet Legal and Regulatory Compliance

In order to keep track of the vulnerabilities detected in your web applications, Acunetix Vulnerability Scanner includes extensive reports to help manage escalation and remediation of vulnerabilities while assisting in task prioritization. It also includes a range of Compliance and Classification reports including: 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.

WordPress Vulnerability Scanning

Acunetix Vulnerability Scanner identifies WordPress installations, and will launch security tests for over 1200 popular WordPress plugins, as well as several other vulnerability tests for WordPress core vulnerabilities. In addition, Acunetix Vulnerability Scanner will also conduct other WordPress-specific configuration tests such as weak WordPress admin passwords, WordPress username enumeration, wp-config.php backup files, malware disguised as plugins and old versions of plugins.



Reporter

Advanced Penetration Testing Tools

Acunetix Web Vulnerability Scanner includes advanced tools for penetration testers to further automated testing, integration with external tools, as well as tools to aid in testing business-logic web applications:

- 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 - Fuzz HTTP/HTTPS requests to test validation and handling of invalid or random data.
- Perform automated database data extraction using Blind SQLi vulnerabilities.

More Advanced Features

- Flexible Scan Settings - Scan websites and web applications with different Scan Settings and Login Sequences.
- Easily Customize Scan Scope - Leverage Scanning Profiles and Directory and File Filters (support for wildcard and regular expression-based filters) to customize tests and pen-test scope.
- Schedule Scans with Ease - Schedule scans to run at a given time, or setup recurring scans based on a customized schedule, set-up custom Excluded Hours templates to pause scans during specific hours.
- Import Crawl Data from Third-Party Tools - Import manual crawl data from the built-in Acunetix HTTP Editor, third-party tools such as Telerik Fiddler, Portswigger BurpSuite, and HAR (HTTP Archive) files.
- Dynamic Crawl Pre-Seeding - Dynamically pre-seed automated crawls using external or custom-built tools and scripts.
- Business Logic Testing with Selenium IDE - Support for crawling and scanning complex Business Logic-driven applications through consumption of Selenium IDE test cases.
- Auto-configuration of Web Application Firewalls.

Available as a Hosted or On Premise Solution

Acunetix 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.

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 Vulnerability Scanner, is designed to replicate a hacker's methodology to find dangerous vulnerabilities like SQL injection and Cross-Site Scripting, before hackers do.

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

Some of Acunetix clients

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

acunetix

WHERE TO FIND US

Stay up to date with the latest web security news.

Website. www.acunetix.com
Acunetix Web Security Blog. www.acunetix.com/blog
Facebook. www.facebook.com/acunetix
Twitter. twitter.com/acunetix

CONTACT INFORMATION

Acunetix (Europe and ROW)
Tel. +44 (0) 330 202 0190
Fax. +44 (0) 30 202 0191
Email. sales@acunetix.com

Acunetix (USA)
Tel. (+1) 917 7228550
Fax. (+1) 917 7228552
Email. salesusa@acunetix.com