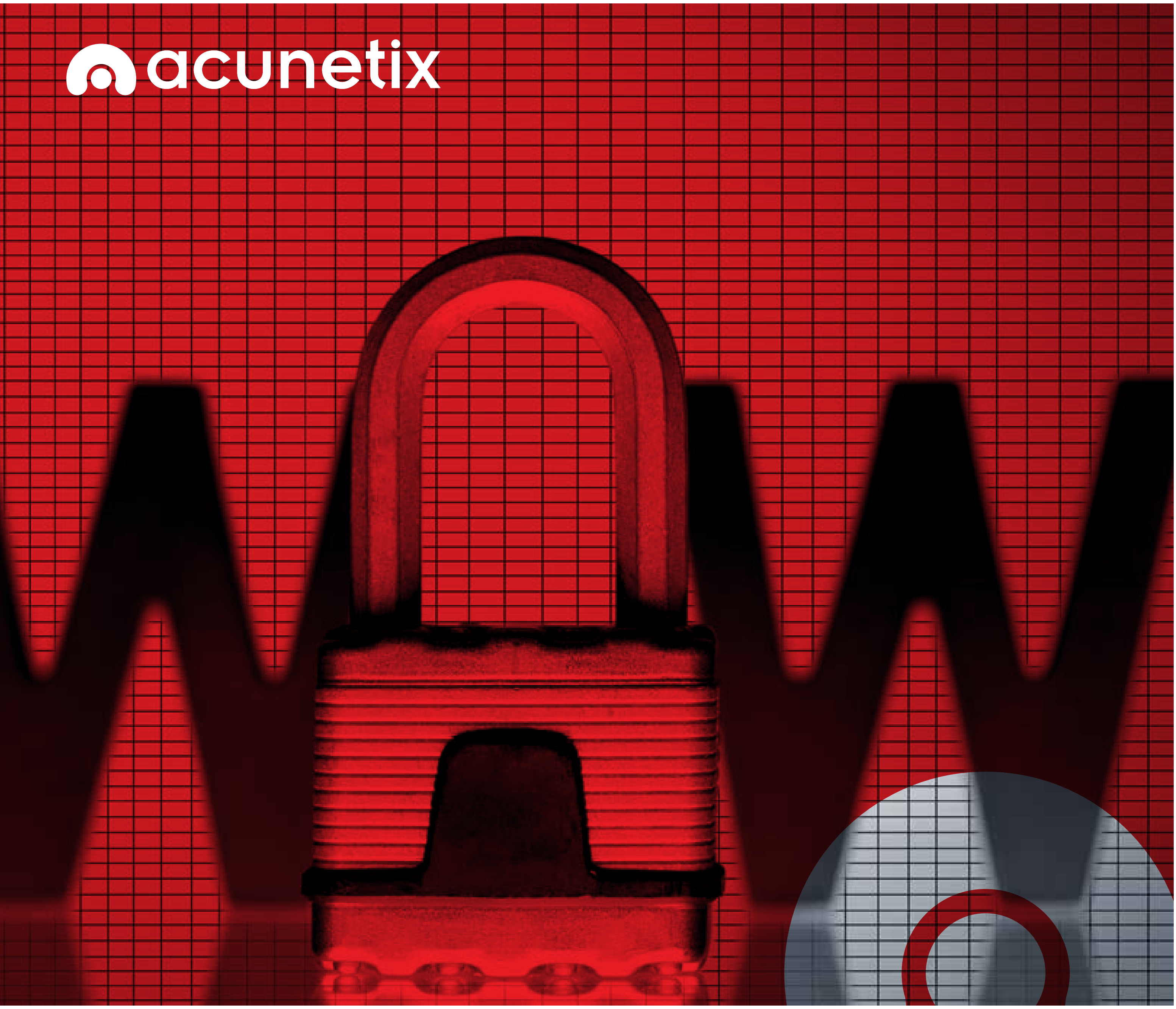
acunetix



IS YOUR WEBSITE HACKABLE?

Audit your Web Applications with Acunetix

As many as 70% of websites have vulnerabilities which could be exploited by hackers, leading to theft of sensitive corporate data such as credit card information and customer lists.

Hackers concentrate their efforts on web-based applications such as shopping carts, forms, login pages, dynamic content and plain-and-simple human error. Accessible 24/7 from anywhere in the world, insecure web applications and web servers provide easy access to backend corporate databases and allow hackers to perform illegal activities using the compromised server.

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 WEBSITES, WEB APPLICATIONS AND WEB SERVERS ARE SECURE BEFORE HACKERS download sensitive data, use your servers as a launch pad for criminal activities, or endanger your business. Acunetix Vulnerability Scanner crawls your web-based business-critical assets, automatically analyzing them for perilous SQL injection, Cross Site Scripting, flaws in the underlying operating system, misconfiguration of the web server software and other vulnerabilities that expose your online business. Concise reports identify where web applications and servers need to be fixed, thus enabling you to protect your business from impending hacker attacks!

COMPREHENSIVE SCANNING for SQL Injection and Cross Site Scripting (XSS) Vulnerabilities

Acunetix is the market leader in the detection of SQL Injection and XSS vulnerabilities. Acunetix has a very high detection rate for the 2 major web security flaws - SQL Injection and Cross Site Scripting; together with very low false positives, leaving more time for your security analysts to discuss the real threats.

A WORLD-WIDE LEADER IN WEB APPLICATION SECURITY

Acunetix has pioneered web application security scanning: Its engineers focused on web security as early as 1997 and developed an engineering lead in website analysis and vulnerability detection.

Not everyone can boast the detection of the latest XSS security threats such as Blind XSS and DOM based XSS. The detection of these vulnerabilities requires a sophisticated engine. Traditional crawling and scanning technologies simply don't cut it anymore. Acunetix makes use of **AcuMonitor** to keep one step ahead of hackers and detect sophisticated vulnerabilities such as Blind XSS and Mail Header Injection..

QUICKER REMEDIATION with the Innovative AcuSensor Technology

This proprietary state-of-the-art security technology guarantees a higher level of vulnerability detection and reduction in false positives together with the precise pinpointing of where in the source code the vulnerability is located. The result is much quicker remediation of the vulnerability compared to other commercial scanners.

FULL HTML5 SUPPORT with Acunetix DeepScan

Powered by the same rendering engine used in Chrome and Safari, Acunetix DeepScan allows our scanners to fully interpret websites, web applications and mobile friendly websites, including those implemented using HTML5 and JavaScript-based technologies, such as AJAX and Single Page Applications. Through its advanced JavaScript interpretation, Acunetix DeepScan is also used automatically detect DOM-based XSS vulnerabilities.

SCAN PASSWORD PROTECTED AREAS Automatically

Acunetix is able to automatically fill in web forms and authenticate against web logins. Most 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 and fill in web forms and log on to password protected areas automatically.

SCAN MULTIPLE WEBSITES Anytime, Anywhere

Launch scans to all your websites even while on the go. With both Acunetix' on-premise and online solutions you can perform immediate scans or schedule the scans for a later period, and retrieve the results from anywhere, at any time.

COMPREHENSIVE REPORTS for Legal and Regulatory Compliance

Do your web application and perimeter servers meet your industry's compliance and regulatory requirements? Let Acunetix help you with its extensive and detailed reporting modules that cover a wide range of standards including:

- CWE/SANS Top 25 Most Dangerous Software Errors
- The Health Insurance Portability and Accountability Act (HIPAA)
- International Standard - ISO 27001
- NIST Special Publication 800-53 - Recommended Security Controls for Federal Information Systems
- OWASP TOP 10 2013
- Payment Card Industry Data Security Standard version 3.0
- Sarbanes-Oxley Act
- DISA STIG Web Security
- Web Application Security Consortium: Threat Classification

STOP SEARCH ENGINE HACKERS

Acunetix launches queries from the Google Hacking Database (GHDB) onto the crawled content of your website, identifying sensitive data or exploitable targets before a search engine hacker does.

AUTOMATIC CUSTOM 404 Error Page Identification

Automatically determine if a custom error page is in use, and identify it without needing any recognition patterns to be configured before the scan.

PERIMETER SERVER SECURITY

Acunetix runs port scans against the web server hosting the website and automatically identifies network services running on open ports and launches a series of network security tests against that network services. 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,
- FTP access tests such as if anonymous access is allowed, and list of writeable 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.

In addition, the online solution makes use of OpenVAS - the leading network vulnerability scanner, thereby drawing on a database of tens of thousands of network level checks.

ADVANCED PENETRATION Testing Tools

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 the browser and by the 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.

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.
- Detect directories with weak permissions and if dangerous HTTP methods are enabled.
- Generate 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.

DOWNLOAD OR REGISTER YOUR FREE 14-DAY TRIAL AT
www.acunetix.com

acunetix

WHERE TO FIND US:

Stay up to date with the latest web security news:
Website: www.acunetix.com
Acunetix 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) 404 990 3280
Fax: (+1) 404 990 3279
Email: salesusa@acunetix.com