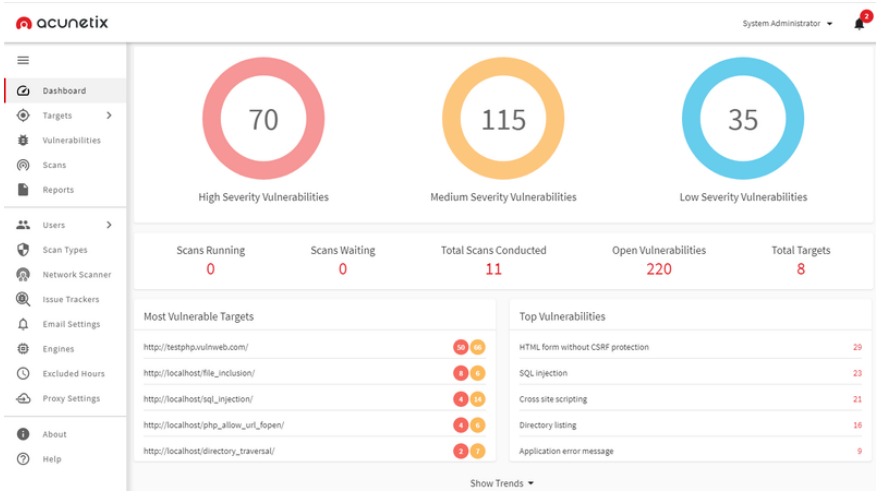
What is Acunetix? How to check website vulnerabilities with Acunetix

Acunetix is ??an effective website vulnerability scanner, designed to detect and fix security vulnerabilities in web applications.

Security vulnerabilities such as SQL Injection or Cross Site Scripting can become doors for network security intrusions. And to deal with these threats, many businesses today have used security vulnerability scanning tools such as Acunetix. But how to check and detect security vulnerabilities with Acunetix? Let's find out with ***TipsMake in the following article.***

What is Acunetix?

Acunetix is ??an effective website vulnerability scanner designed to detect and fix security vulnerabilities in web applications. Acunetix provides automated tools to scan and identify security issues, helping to prevent cyber attacks such as SQL Injection and Cross Site Scripting (XSS).



What is Acunetix?

The need for using Acunetix

Web application security is a neglected issue in the enterprise, while 75% of cyber attacks take place through websites. Many companies focus on network data security but ignore web application protection, making them easy targets for hackers.

Acunetix software is developed to automatically scan web applications, identify and fix security vulnerabilities. Launched in July 2005, Acunetix Web Vulnerability Scanner replicates hackers' attack methods to detect serious vulnerabilities such as SQL injection and cross site scripting. This tool has become the first choice for many fields such as banking, military, education, e-commerce, .

Acunetix is ??capable of detecting vulnerabilities across multiple platforms such as WordPress, PHP, and Java. It also provides security analysis and reporting for efficient application management and development. Acunetix's development team is made up of experienced cybersecurity experts.

In addition, many businesses' websites are now required to integrate security standards such as PCI DSS or GDPR and are regularly audited. Therefore, it is necessary to use Acunetix to have detailed reports, thereby easily meeting the standards.

Outstanding features of Acunetix

Automated security vulnerability scanning

Firewalls and SSL certificates both help to enhance web application security, but these are just the basics. When Acunetix was deployed, the application scanned 4,500 website vulnerabilities.

Acunetix is ??equipped with DeepScan to help collect SPA data from the client side to AJAX. At the same time, the AcuSensor feature scans the black box from sensors inside the source code. Acunetix can also automatically scan even high-security, password-protected areas.

Pentest Software

Manual penetration testing tools help businesses conduct more thorough security assessments, but they are time-consuming and expensive. That's why many businesses have turned to automated testing tools like Acunetix.

Users can test for SQL injection, Cross-Site Scripting, and other security vulnerabilities with Acunetix. The software scans automatically on a pre-set schedule. It also provides full support for modern SPAs. The penetration testing tools are capable of scanning and assessing applications using JavaScript frameworks such as Angular and React, from legacy to modern web applications.

Acunetix software also provides useful reporting features for businesses, allowing reports to be generated according to standards such as PCI DSS, HIPAA, OWASP Top 10. If vulnerabilities are detected, users can export information for monitoring through tools such as Atlassian JIRA, GitHub and Microsoft Team Foundation Server.

Web Application Security

Acunetix scans and identifies vulnerabilities quickly, even on websites written in HTML5 or JavaScript Single Page Applications, which are difficult to scan. Acunetix includes unlimited black-box testing techniques including AcuSensor gray-box scanning technology. Users can automatically evaluate executed Java, ASP.NET, and PHP server code.

Network Security Scan

Many of today's data breaches are caused by unsecured network perimeters (both the devices on the 'outer' and 'inner' perimeters of the network). Acunetix helps users discover open ports, running services, and check whether the network is vulnerable to one of 50,000 known network vulnerabilities or misconfigurations.

In addition, Acunetix is ??also equipped with a number of additional features such as:

1. Security analysis of routers, switches, load balancers, etc.
2. Check for weak passwords
3. Check if proxy server is configured properly
4. Check hidden FTP access and FTP writable folders
5. Check if TLS/SSL cipher is weak

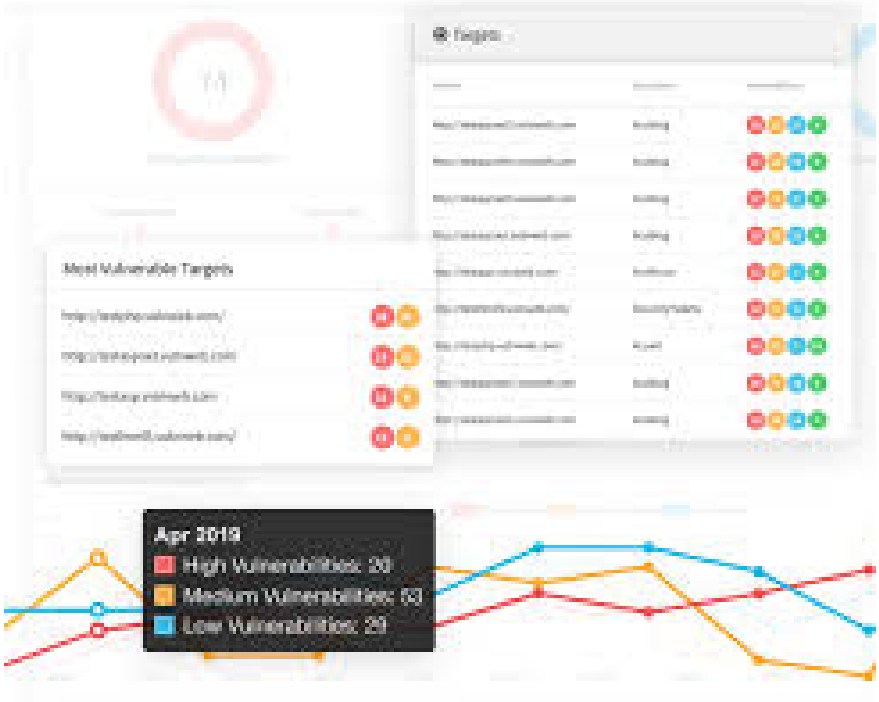
WordPress Vulnerability Scan

There are currently more than 75 million active WordPress websites. Thanks to its user-friendly plugins, themes, and content management systems, WordPress is the top choice. That is why WordPress has become the target of many hackers. Acunetix vulnerability scanner is a solution to help website owners prevent their websites from being attacked.

1. Detect Old WordPress Versions
2. Identify malware hidden under the guise of third-party themes and plugins
3. Detect WordPress usernames used to compromise accounts
4. Exploring the available wp-config.php files revealed
5. Predicting if WordPress is vulnerable to XML-RPC brute force attack

Should I use Acunetix?

Should you use Acunetix? The answer is yes. Acunetix is ??an automated tool that frees up security teams' resources, detecting vulnerabilities that other technologies often miss with a combination of static and dynamic scanning, along with a dedicated monitoring agent.



Should I use Acunetix?

Additionally, Acunetix offers vulnerability management and compliance reporting, allowing issues to be classified, ranked, and re-examined, and can integrate with trackers and continuous integration solutions.

How to check website vulnerabilities with Acunetix?

To check website vulnerabilities with Acunetix, do the following:

1. Step 1: Select a website you suspect has security vulnerabilities to test.
2. Step 2: Open the Acunetix scanner. In the Toolbar, select Button, then follow the Wizard instructions to go through the options.
3. Step 3: Select a scanning profile to customize the test, with or without Acunetix WVS enabled. The default Scanning Profile includes the Acunetix Web Vulnerability Scanner tests. If you want to check more pages, use the Advance option.

To remove unnecessary pages, select the "After crawling let me" checkbox and define the scan file. The test results will be compiled by Acunetix into detailed reports, helping users easily monitor and detect security vulnerabilities, thereby improving operational efficiency and information security on the website.

Conclude

With the ability to scan and detect more than 50,000 security vulnerabilities, Acunetix helps businesses and individuals protect their digital assets from potential threats. Hopefully, through the above article of TipsMake, readers have understood and know how to use this tool for their website.