WEB SECURITY CONCERNS THAT WEB VULNERABILITY SCANNING CAN IDENTIFY

www.alliancetechpartners.com

Alliance Technology Partners

WEB SECURITY CONCERNS THAT WEB VULNERABILITY SCANNING CAN IDENTIFY

More than 70% of all websites have vulnerabilities that could put your business at risk. More than 20% of those vulnerabilities are classified as critical, which has the potential to bring business operations to a screeching halt.

Doing nothing about those security concerns will practically guarantee disaster for your business. Web vulnerability scanning tools are available to identify those issues, though.

Web Vulnerability Scanning

Web Vulnerability Scanning is a method that uses tools to automatically scan web applications for known security vulnerabilities and deliver a report on the findings. The scans can be scheduled to run when it's convenient and reports are broken down in a way that is easy to understand, thus enabling you to protect your business more effectively.

The 10 Most Common and Significant Web Security Pitfalls, according to the Open Web Application Security Project (OWASP):

Injection

Injection flaws, such as OS, SQL, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. Hostile data from an attacker can trick the interpreter into executing unintended commands or accessing data without proper authorization.

Broken Authentication and Session Management

Application functions related to authentication and session management are not implemented correctly much of the time, which allows attackers to steal keys, passwords, or session tokens. Attackers could also exploit other implementation flaws to assume other users' identities.

Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser, which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization

Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, an attack could facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and negative consequences.

Unvalidated Redirects and Forwards

Web applications will often redirect and forward users to other pages and websites, all while using untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Acunetix, a Pioneer in Web Vulnerability Scanning

With the threat landscape continually evolving, it's important to take steps to prevent would-be attacks and protect sensitive data.

Web Vulnerability Scanning tools, as those provided by Acunetix, has pioneered web application security scanning. Acunetix has done so by developing and enhancing technology and scanning methods which provide:

- Acunetix 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 (XSS) 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 REST, SOAP, XML, AJAX and JSON

With these built-in scanning methods and the more advanced features available, businesses are better able to protect themselves from some of the more common web security concerns around. These tools can also help businesses protect themselves against the security concerns that aren't quite as common, but can be just as devastating – if not more so.

Web Vulnerability Scanning Training Matters

However, having the tools handy are not enough. You must also be trained in how to utilize the full power and capabilities of web scanning technology. Alliance Technology Partners offers a basic training 3-hour course led by Alliance security engineers, trained directly by Acunetix.

Alliance's expert security consultants help customers take full advantage of Acunetix and its innovative technologies. Alliance clients include the United States Government, State and Local Government, as well as, Fortune 1000 organizations.

GET IN TOUCH

CORPORATE HEADQUARTERS
18102 Chesterfield Airport Rd. Suite E
Chesterfield, MO 63005

314 649 8888
314 649 8889
888 891 8885

sales@alliancetechpartners.com

St. Louis
Fax
Toll Free