Cyber Security Scans

Protect Your Business and Your Clients

Malicious actors are out to cause damage, steal personal and proprietary information, and commit fraud. Our software helps protect you from these actors by running security scans and showing you the vulnerabilities we find.

What Vulnerabilities Does Our Software Find?

When our software scans a website, it identifies the following five types of security threats:

- **Cross Site Request Forgery (CSRF)** is a type of attack in which the perpetrator is able to trick a web browser into performing an unwanted action. Typically, an email or link with a forged request makes the victim think he or she is responding to a legitimate one. Common examples of CSRF attacks include unauthorized fund transfers, changed passwords, and stolen data.
- **Cross-Site Scripting (CSS)** targets the users of web applications. It injects a malicious code into the application and can be stored on the application or activated when a user clicks on a link. These attacks can cause serious harm by compromising accounts, impersonating valid users, activating Trojan horse programs, modifying content, and tricking users into giving away personal data.
- **SQL Injection (SQLi)** attacks are common and dangerous attacks because most websites use an SQL database. Here, the attacker injects malicious code that manipulates the database to allow access to information not meant for display. The attacker might view user lists, steal personal data (like addresses and credit card numbers), delete information, or even gain administrative privileges over the entire database.
- **SSL certificates** allow websites to go from HTTP to the more secure HTTPS. The lack of an SSL certificate is not in itself an attack, and a site lacking one is not necessarily compromised. However, an SSL certificate does provide users assurance that the site is valid and that personal information is protected.
- **Subdomain Takeover** is an attack where the perpetrator uses a non-existing domain (such as an expired subdomain of another site) to take over another domain. When this happens, the attacker can engage in CSS, send phishing emails from what looks to be a legitimate domain, or cause damage to the principal domain's reputation.

What Can I Expect from a Cyber Security Scan?

When we scan your site, our software will provide the following information to you:

- All results will be displayed in a dashboard.
- From the dashboard, you can see the site's security errors on a page-by-page basis.
- Data about the errors will include how many there are in all, how many errors of each type exist, which pages have the highest number of errors, which errors are the most frequent, and more.

The Importance of Having a Secure Website

Sure, making certain that your website is secure might cost a bit more, but it more than pays for itself in several ways. In fact, any site not taking strong security precautions is going to struggle to stay going as consumers become more aware of the risks out there.

- **Users know you're authentic.** As we've seen, bad actors sometimes impersonate sites or sources you trust, gaining access to data or tricking users into transferring funds. Secure websites that have an SSL certificate let visitors know it's safe to enter and safe to make transactions.
- **Sensitive information is protected.** Websites store all kinds of sensitive information about employees and customers alike. Secure websites help prevent identity theft and online fraud, ever-growing problems today.
- **Your Google ranking will improve.** Google now penalizes sites that aren't encrypted; perhaps you've seen the "This is not a trusted site" message on some websites. You don't want that on your website because it will turn users away and damage your rankings in search results, harming your website's visibility.
- **Customers will trust you and return.** When there's a security breach, it can cause irreparable harm to a business's reputation. On the other hand, customers who know their accounts, credit card numbers, addresses, phone numbers, and other sensitive information are secure will feel safe returning for future purchases.

Your business's reputation and viability depend on your website's security. Contact us today to get started on identifying and addressing security errors on your site!

SOURCES USED:

XSS: https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/
SQLi: https://www.imperva.com/learn/application-security/sql-injection-sqli/
CSRF: https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/
SSL: https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/
Subdomain: https://0xpatrik.com/subdomain-takeover-basics/