

WHAT MAKES A WEBSITE VULNERABLE?





A website vulnerability is a misconfiguration or weakness in the website's code that allows attackers to gain control and cause potential harm.

With over [30,000 website hacks happening daily](#), you may want to take care of any website vulnerabilities that expose your website to hackers.

Hackers exploit website vulnerabilities either through automated tools such as botnets or scanners. Hackers can create tools that seek out and exploit vulnerabilities on platforms such as Joomla, WordPress, etc.

In this article, you will learn more about what makes your website vulnerable and find ways to secure it.

Types of Website Vulnerabilities

While there are numerous ways for attackers to exploit your website, there are 5 common vulnerabilities that are used the most.

Direct Input of Malicious Code into Database (SQL Injections)

This is where hackers or tools exploit your website code to input malicious code directly into the database.

This is known as SQL Injection vulnerability as cybercriminals will input malicious “payloads” and gain access to your website.



Some of the injected payloads can include;

1. Injecting spam/ malicious posts onto a site
2. Stealing customers data and information
3. Overriding authentication to acquire full access to a website

An SQL injection happens mostly to websites that use open source content management systems such as Drupal, Joomla, and WordPress.

Cross-Site Request Forgery (CSRF)

CSRF attacks are not common, but they could jeopardize your website's security if utilized.

CSRF attacks work by tricking users or administrators into performing potentially harmful actions to a website unknowingly.

By exploiting CSRF vulnerabilities, an attacker can collect valid user information to perform the following actions;

1. Change the value of orders and product prices on ecommerce websites
2. Move funds from one account to another
3. Hijack accounts by changing passwords

These attacks are often executed on banking and ecommerce websites where attackers can gain sensitive financial information.

File Inclusion (RFI/LFI)

This vulnerability involves attackers using the “include functions” on web application languages such as PHP on the server backend to execute code from a remotely stored file.

An attacker will host malicious files and then exploit compromised user input to modify or insert and include functions on the PHP code of the victim’s side.

Once the files have been included, the attacker can then;

1. Include malicious shell files on websites that are available publicly
2. Assume control over a host server or website admin panel
3. Add malicious payloads that add phishing and attack pages to a visitor’s browser

Cross-Site File Scripting (XSS)

This vulnerability takes advantage of improper/failed input sanitization or other input fields to inject malicious scripts and execute code on a website.

Cross-site scripting targets web users without taking over/ harming the website or server. The malicious code only executes on the browser of your web visitors as the browsers cannot tell if the malicious script is a part of the website.

This vulnerability causes the following;

- 
1. Session hijacking
 2. Stealing of session data
 3. Distribution of spam content to an unsuspecting web visitor

WordPress has experienced large-scale cross-site scripting attacks in the past.

Security Misconfigurations

Misconfigurations make your website an easy target for hackers. Security misconfigurations are easy to detect and exploit.

These misconfigurations happen when the security settings of your website are not defined or implemented the right way. Attackers can gain control of your website if the security of the web server, database, and web application platforms and frameworks are not appropriately implemented.

How to Prevent and Manage Website Vulnerabilities

You can implement actions to prevent and manage website vulnerabilities and prevent attackers from gaining access to your website. Here are some of the steps you should take to minimize vulnerabilities on your website.

Update Your Website Applications

The first step to ensuring that your website is safe is to ensure that all website applications and plugins that you are using are up-to-date.

Vendors regularly release security patches for their applications, and it's necessary that you take these updates promptly.

Attackers will use news updates on security patches as a blueprint for finding vulnerable websites.

You can activate automatic updates for your applications to ensure that you stay ahead of malicious attackers.

Use a Web Application Firewall (WAF)

Web application firewalls act as the initial defence against attackers looking for vulnerabilities on your website.

WAFs block and eliminate lousy traffic such as; bots, IP addresses known for spam or cyberattacks, attack-based user input, and automated scanners.

Use a Malware Scanner

Malware scanners from reputable companies are the final step to eliminate vulnerabilities on your website. Use a malware scanner that automatically detects and eliminates malware.



You can also employ the expertise of a skilled programmer to go through your website's code manually and implement solutions to vulnerabilities.

While these vulnerabilities may sound techy for most people, it's necessary that you understand ways in which attackers could exploit your website.

Understanding the various types of vulnerabilities will help you keep your website safe and prevent any attacks.

References

<https://www.sitelock.com/blog/what-is-a-website-vulnerability/>

<https://www.toptal.com/security/10-most-common-web-security-vulnerabilities>

<https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref>