
WordPress
Plugin Vulnerability

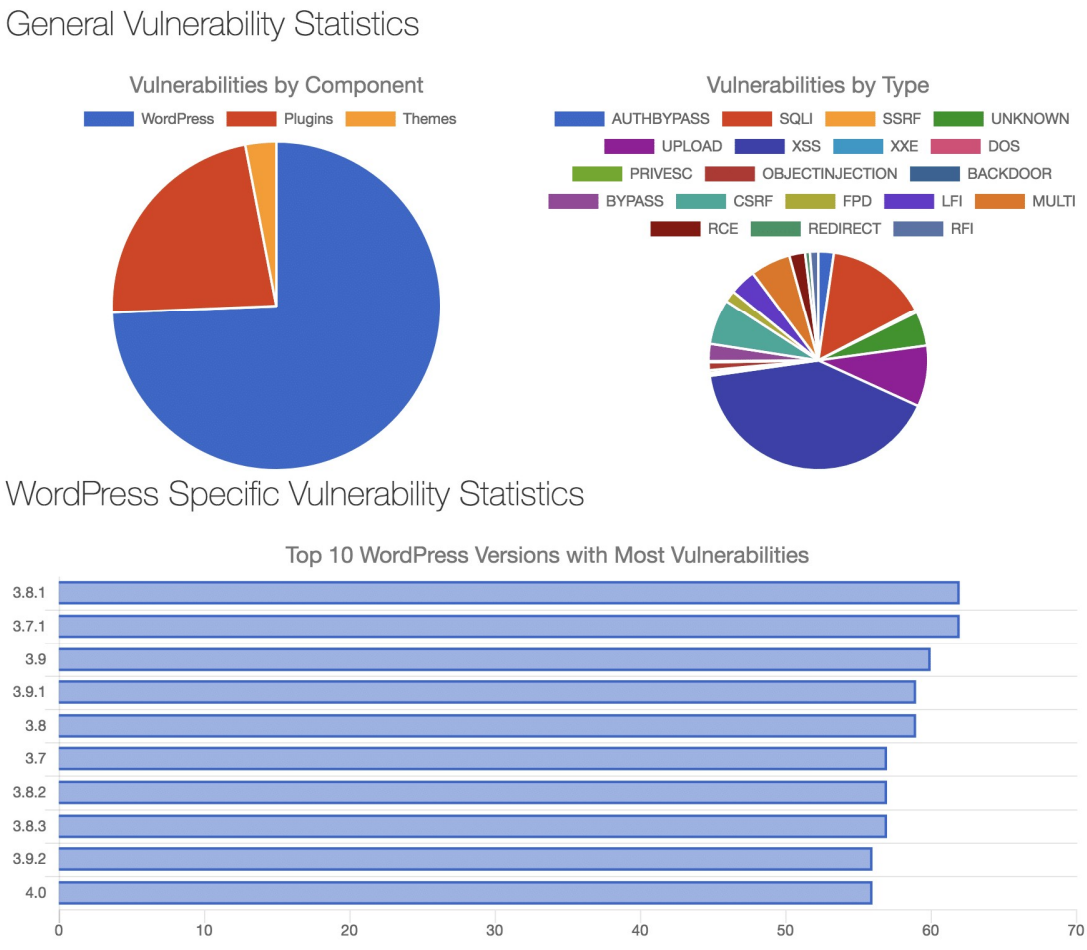
WORDPRESS

WordPress is a free and open-source content management system (CMS) written in php and paired with a MySQL or MariaDB database and supported HTTPS. WordPress was released on May 27, 2003, by American developer Matt Mullenweg and English developer Mike Little, as a folk of b2/cafelog. The software is released under the GPLv2 licence. Features like plugin architecture and template system are referred to within WordPress as Themes. It was created as a blog-publishing system but later it got evolved to support other web content types. This evolution of WordPress brought many changes to its core and made it more stable and secure than its previous versions. If WordPress has to be functioned is has to be installed on a web server, either part of an Internet hosting service like WordPress.com or a computer running the software package WorddPress.org in order to serve as a network host in its own right. A local computer may be used for single-user testing and learning purposes.

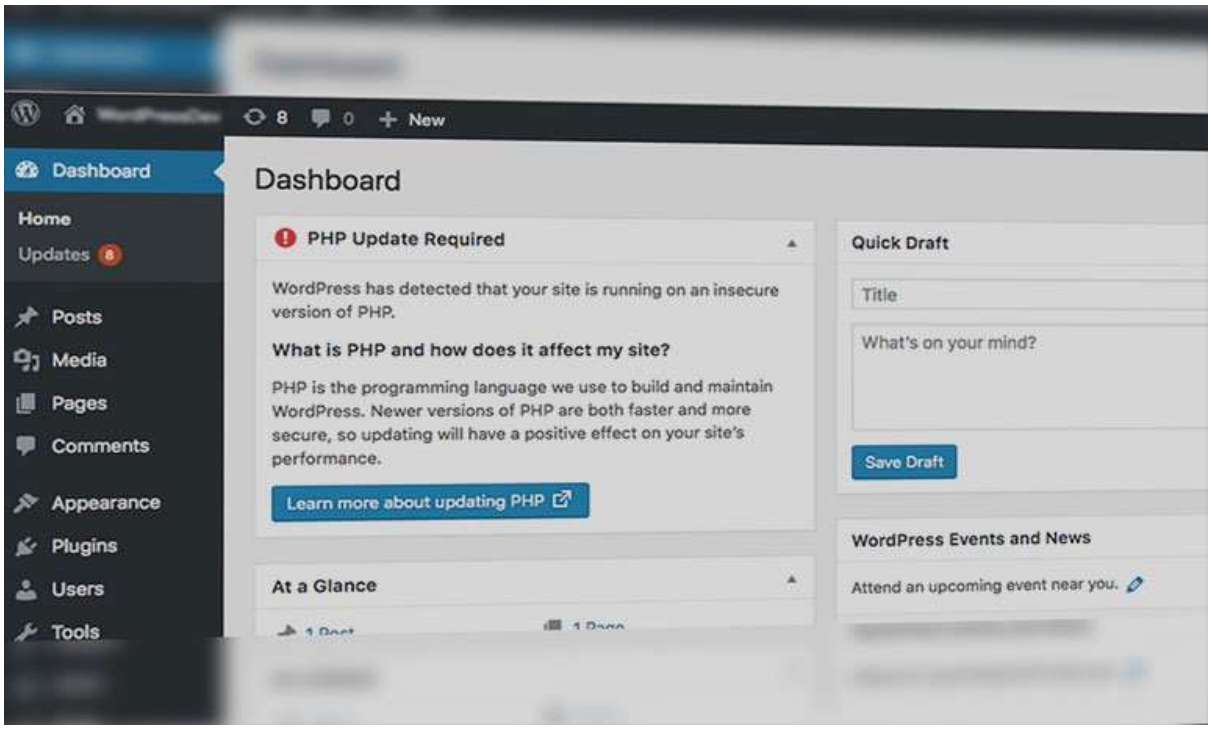
WORDPRESS VULNERABILITY

WordPress is the most popular CMS on the Internet and also the most hacked. In 2020, Wordfence reported more than 2800 attacks per second targeting WordPress. Here are few WordPress security issues and Vulnerabilities.

1. Outdated Core Software
2. Outdated Themes and Plugins
3. Malware
4. Credit Card Skimming
5. Unauthorized Logins
6. Undefined User Roles
7. Brute Force Attack
8. SQL Injections
9. SEO (Search Engine Optimization)
10. XSS
11. DDoS
12. Phishing
13. Supply Chain Attacks
14. Hotlinking
15. CSRF

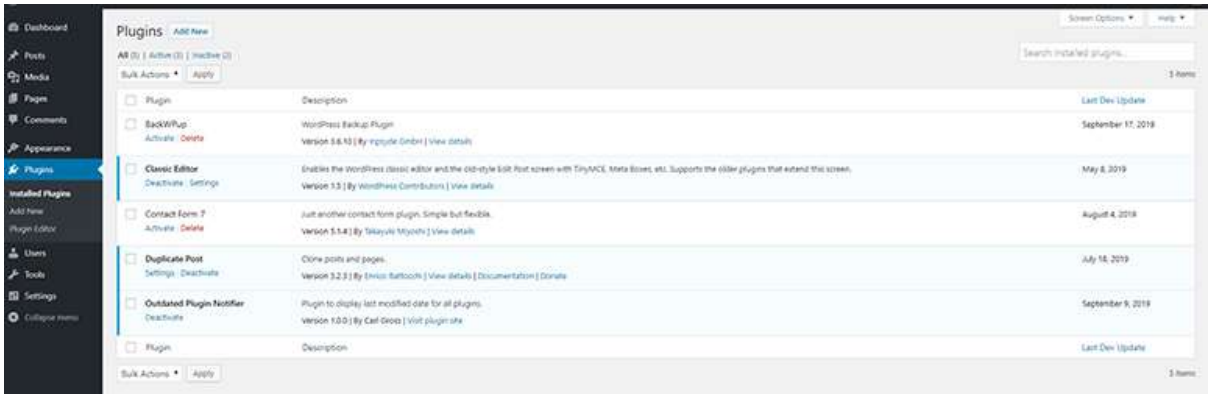


1. **<u>Outdated Core software</u>: -**



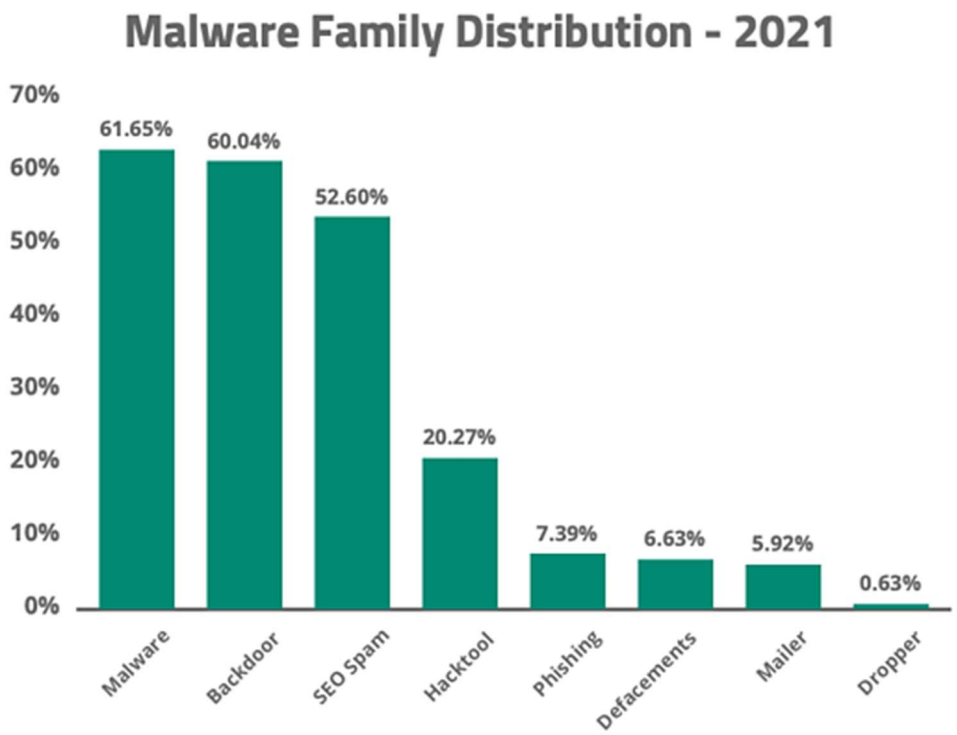
Outdated core WP software leaves sites vulnerable because updates are usually designed to address critical security issues. Users who don't download an update are then vulnerable to hackers. If the user's software is outdated, the user also enables to update the user's themes and plugins and thus his site becomes more vulnerable to many of the security threats.
To get rid of this vulnerability, WordPress offers automatic updates for new version of WordPress. The user can turn those on in his dashboard to ensure his core files remain up-to-date. If he doesn't then he is leaving his site vulnerable to known threats.

2. **<u>Outdated Themes and Plugins</u>: -**



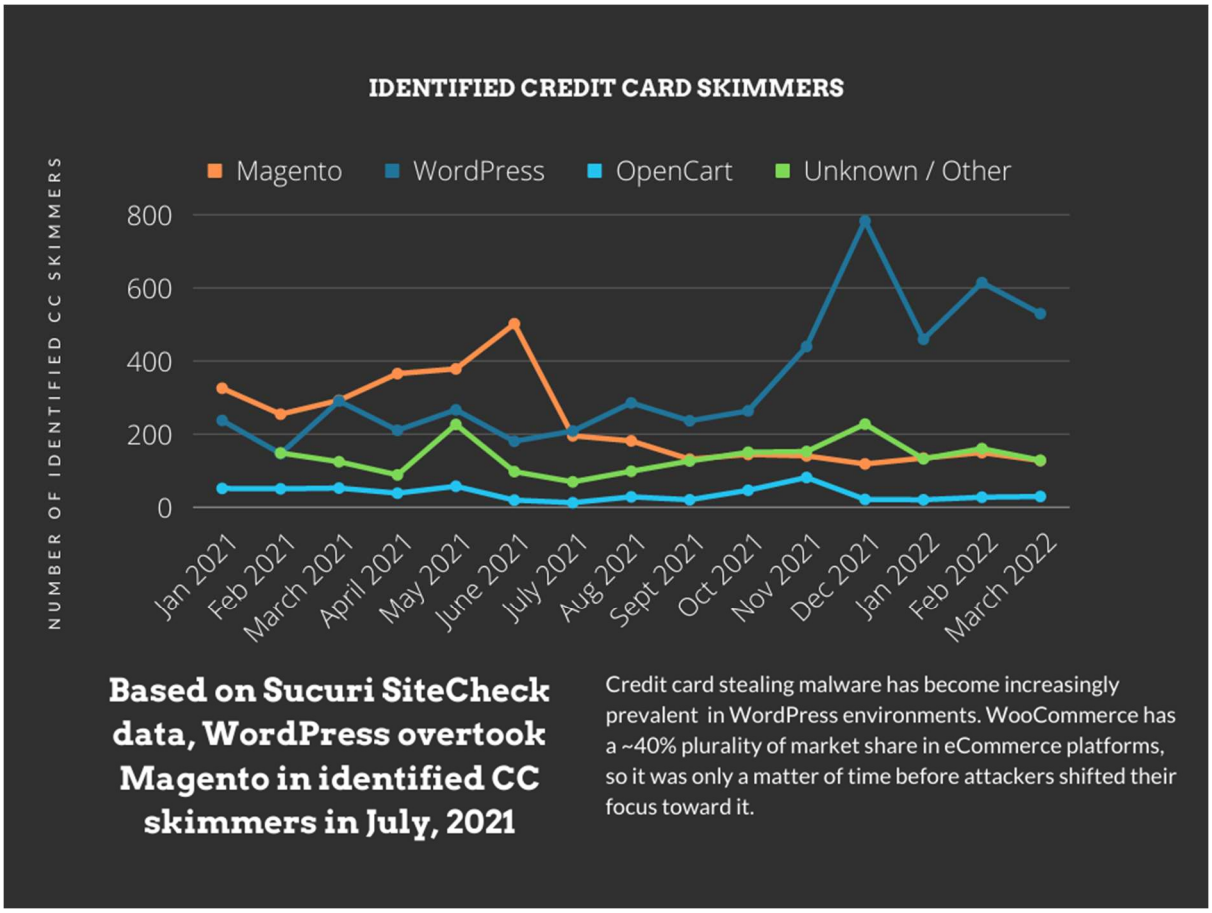
Themes and plugin developers often release updates with functionality enhancements and additional security measures. When the user doesn't do this, sites using these resources become vulnerable to hackers who can use outdated tools as entry points.
In order to patch this vulnerability, the user must update his software because, Updates serve to improve WordPress themes security and will protect the user's website. When updates are available for plugins and themes, the user can install them manually or use a plugin to automatically install them as they go live.

3. **<u>Malware</u>: -**



Malware usually enters WordPress sites through unauthorized and outdated themes and plugins. Hackers take advantage of security problems in plugins and themes, imitate existing ones, or even create entirely new add-ons for the sole purpose of placing harmful code on the user's site. AnonymousFox hack was the most popular type of malware infection in 2021.
To prevent this, by default, WP restricts the file types users can upload to the media library. If the user tries to upload a file that isn't included, the user will get and error message, and his file won't upload. Beyond that, he must vet every plugin and theme the user installed on his WordPress site. The user should also conduct regular security scans to find any potential malware hiding on this WordPress website. There are many strong security plugins that can scan for malware and fix damaged files.

4. **<u>Credit Card Skimming</u>: -**



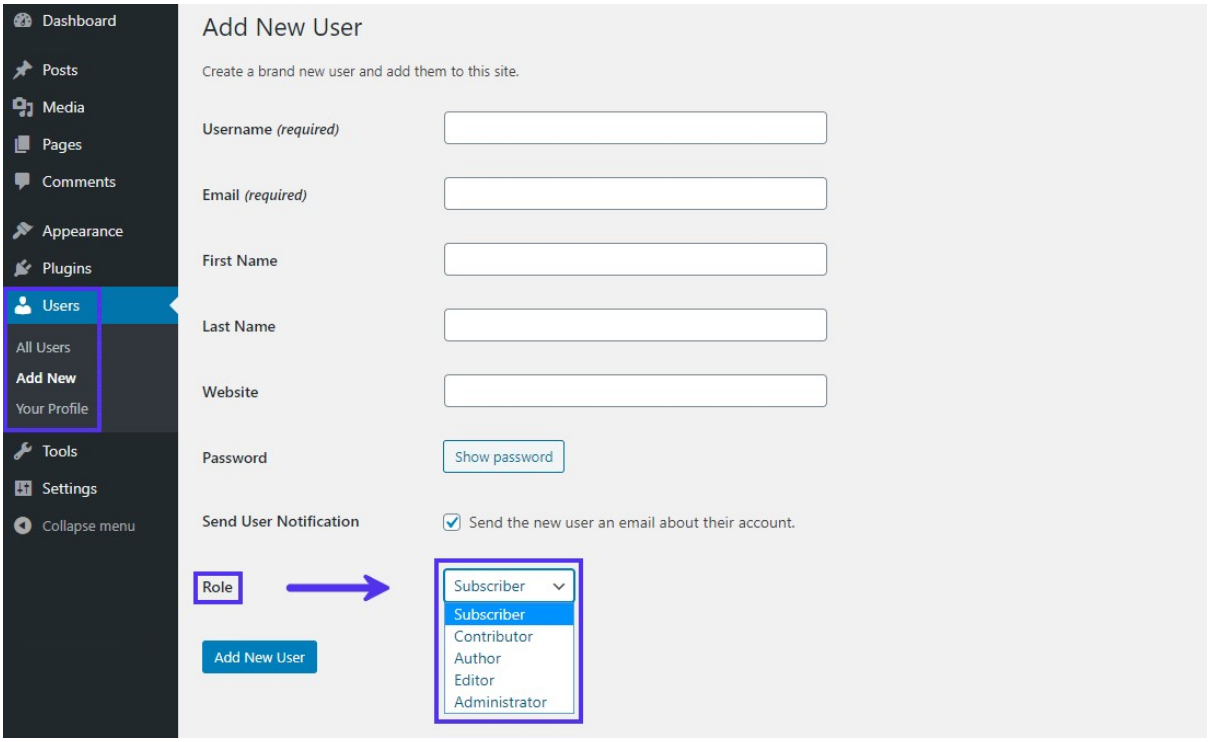
This is a type of malware designed to steal the user's costumer's credit card information. This exploit vulnerable software, weak passwords, and other points of entry. Once the hacker gets access to the user's admin areas, he will inject a malicious payload amongst a website's plugin, theme, or other legitimate files, and obfuscate it in order to harvest as many credit card details form the user's site as possible.
The solution for this vulnerability is a monitoring tool like Sucuri SiteCheck, which scans the user's website for known malicious content and malware injections and allows the user to see what attackers want his information for.

5. **<u>Unauthorized Logins</u>: -**

The two major reasons for this attack to happen is first, the default backend login page for any given WordPress site is relatively easy to find, Anyone can simply take the site's main URL and add keywords like /wp-admin, /wp-login.php at the end, and then the attacker gains access to the login page. In the case of unauthorized WordPress login incidents, the responsibility also falls on the WordPress user. Attackers can easily gain access by pairing the default "admin" username with a simple, common password.
The easiest and most effective defence against brute-force hacking is a strong password that will be difficult to discover, even with the powerful technology. In addition to strong passwords, there are additional measures the user can take crub unwanted entries.

- Two Factor Authentication
- Getting rid of WordPress account with the "admin" username.
- Several reputable WordPress plugins can limit login attempts.

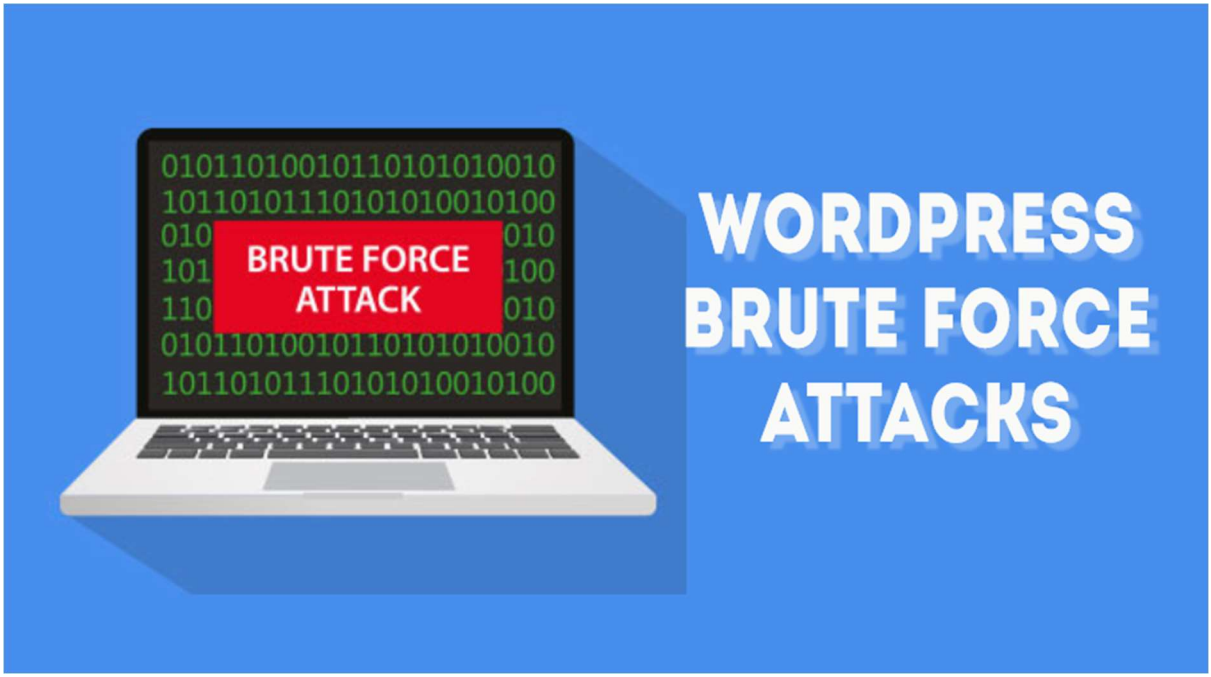
6. **<u>Undefined User Roles</u>: -**



If the user has multiple users and don't change the default settings, everyone is an admin, which would become an issue. This can make a hacker gain access to the user's site and make changes as an administrator. Poorly defined admin roles subject the user's site to increase risk if Brute-force attacks are successful. XSS also gives hackers access to front-end capabilities to obtain additional information form the user's site visitors.

To solve this the admin must ensure that the user have taken additional security measures to prevent hackers form entering his site, like two-factor authentication or longer passwords.

7. **<u>Brute-force Attacks</u>: -**



WordPress does not block a user form trying multiple fail attempts which let a human or bot try thousands of combinations per second. This attack involves a multiple try and error approach using hundreds of combinations to guess the right username or password. This is done using powerful algorithms and dictionaries which guess the password using some kind of context.
To avoid this attack, the user has to do is he must create a strong password that includes Uppercase, lowercase letters, numbers and special characters, because each character has different ASCII values and it would be difficult to guess a long and complex password. Two-factor Authentication is also a great plugin to use.

8. **SQL Injections: -**

WordPress sites are vulnerable to this kind of attack because most are designed to foster a sense of community. Attackers commonly use SQL inejctions through visitor-facing submission forms, like contact forms, payment info fields, and lead forms. Upon successful intrusion, a hacker can manipulate the MySQL database and quite possibly gain access to the user's WordPress admin or simply change its credentials for further damage.
In order to fix this vulnerability, The user must restrict the submission of special characters in visitor's submissions. Without symbols, the user reduces a string of malicious code into harmless gibberish.

9. **Search Engine Optimization (SEO): -**

WordPress websites are vulnerable to these attacks the same way as other security issues. The hackers will often gain access but wait to make any changes not to raise immediate suspicion. Since they're SEO-based theses spammy keyword additions are only placed on the user's high-ranking pages. SEO spam is most noticeable to SEO crawlers, as they'll index the user's site for the spammy keywords and users searching for spammy keywords.
Here, the first thing the user can do is follow the aforementioned security measures like updating on time and defining user roles. If the user is keen on identifying these hacks on his own, then he must pay close attention to the analytics data and note any sudden changes in SERP positions or increased site traffic for no apparent reason. It is essential to target and address these hacks early on because SEO crawlers will strike against the user's site for spammy tactics, and all the hard work he has put in will go to waste.

10. XSS: -

If an attacker finds and outdated or poorly-maintained plugin on the user's side, they can exploit it for access to files that dictate his front end. In this attack, the attacker loads a malicious JavaScript code which when loaded at client-side start collecting data and possibly redirecting to other malicious sites affecting the user experience.
To avoid this type of attack, proper data validation across the WordPress site is used. The output sanitization is made to ensure the right type of data is being inserted.
The user can also use the plugin like 'Prevent XSS Vulnerability'. Another helpful tool for preventing XSS is a web application firewall (WAF), which inspects traffic and prevents unapproved visitors form entering the user's system form outside networks.

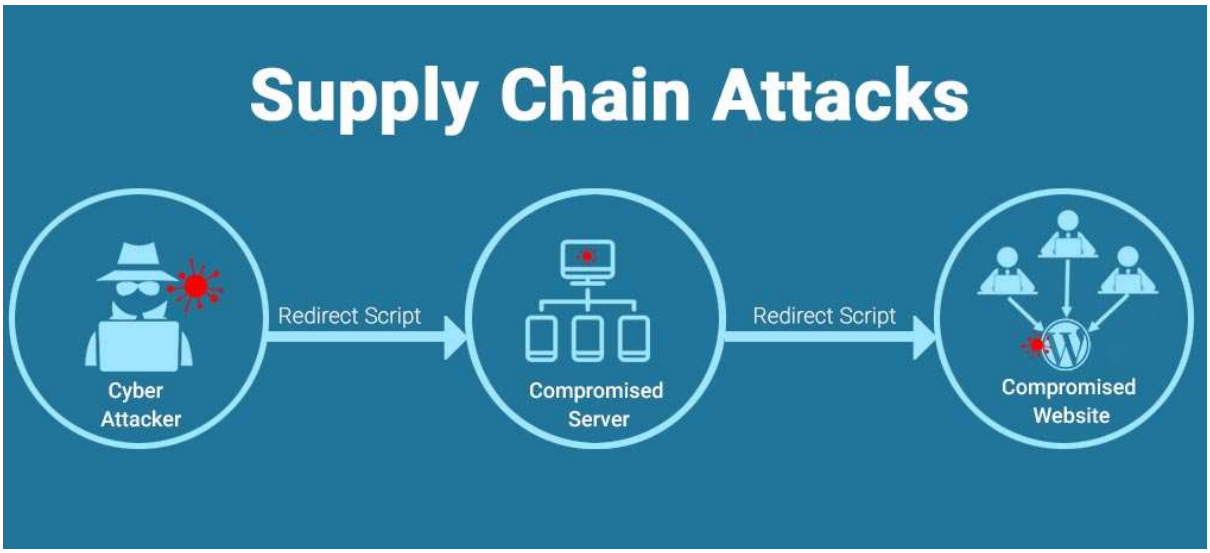
11. <u>DDOS Attack</u>: -

In this attack, a large volume of requests is made to a web server which makes it slow and ultimately crashes. DoS and DDoS attacks target hosting servers, namely those with limited security in place.
The best defence against DoS/DDoS attacks is secure WordPress hosting. DDoS attacks are difficult to prevent using conventional techniques.

12. <u>Phishing</u>: -

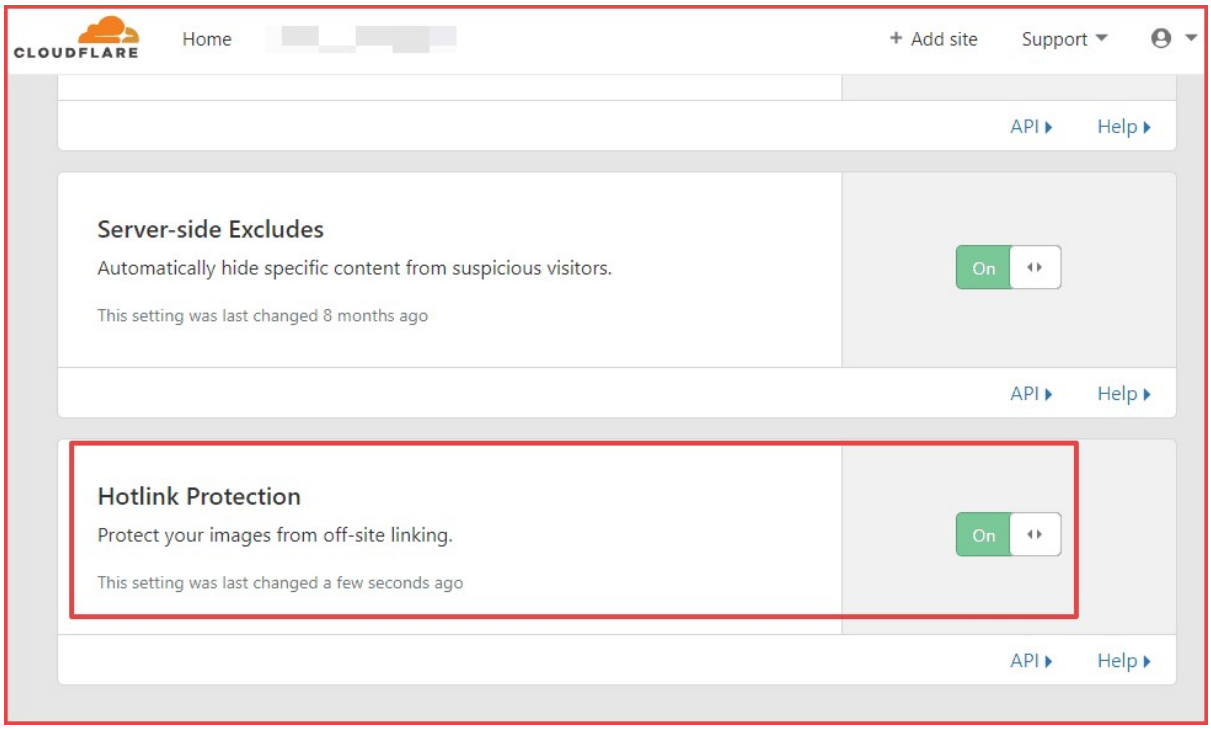
WordPress sites become vulnerable to phishing attempts through outdated plugins, themes, software, or lack of security checks for submission and comment forms. If a user with malicious intent gains access to the user's site with admin privileges, they can post spammy link for users to click that will compromise their information. Phishing capitalizes off of the trust that users have for the user and his content. Hackers can also leave comments on the user's site pages with links that may seemingly direct a user to additional resources that are spam.
To protect from phishing attacks the user must conduct regular updates, monitor site activity, and use secure passwords. The user should also download additional security measures for his site, like ReCAPTCHA, to protect against spammy phishing bots.

13. **<u>Supply Chain Attacks</u>: -**



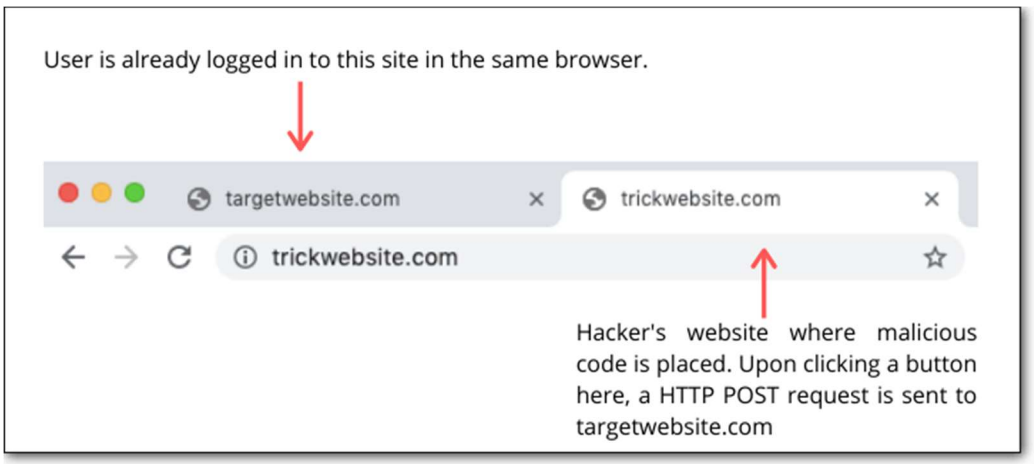
There are two ways to make this attack successful: a plugin owner installs malware a customer sites, or a hacker purchases a popular plugin and injects spammy code disguised as an update.
Supply chain attacks often have a short shelf life because WordPress developers actively identify these fake plugins and themes and quickly ban those affected. However, if one happens to fly under the radar, installing security plugins that run regular checks on the user's site will quickly identify any vulnerability. It's also worth backing up the user's WordPress site data, so that the user can save it If it becomes compromised. As always, this can be done manually or by downloading additional plugins.

14. **Hotlinking: -**



As a site owner, the user wants to share his high-quality content with site visitors. Hence, WordPress sites are vulnerable to hotlinking because people take advantage of this. Attackers simply copy and paste a link to an image or digital file from another site onto their site without giving credit. Many WordPress site owners might not have the time to take preventive measures against hotlinking, or even think to do so. There are a various ways to protect the user's content from hotlinkers, but an easy option is to add discernible watermarks. It's a user-friendly solution that won't necessarily stop all malicious parties, but it will require an additional step to remove the personal tag. A watermark can simply be his name, website domain, or a copyright trademark logo for registered content. The user can personally add this water mark to his content.

15. **Cross-site Request Forgery (CSRF): -**



Cross-site request forgery (CSRF) is a vulnerability that allows attackers to influence users to take actions they don't want to take. WordPress sites using some of the most popular plugins are particularly vulnerable to CSRF attacks. More specifically, plugins that use the function check_url(), like WP Fastest Cache, are vulnerable to CSRF attacks.
One can prevent CSRF attacks by keeping a close eye on his site's plugins. Although plugins are essential, don't blindly trust every plugin user come across. He can protect himself from cross-site request forgery by installing a robust WordPress security plugin. There are many great plugins out there, and these can keep the user safe from all types of attacks, including CSRF attacks. He can also prevent this attack by hardening the user's website via two-factor authentication and disabling file editor and PHP execution in untrusted folders.

WPSCAN

Wpscan , short form of WordPress Scan, is a black box WordPress vulnerability scanner. Wpscan is used to scan remote WordPress installations or websites to find security issues. WordPress can also be used to enumerate WordPress plugins and themes and brute-force logins. Approximately 35% of the internet runs on WordPress, WordPress is a free content management system. Which is used to build and maintain websites. It is the scanner to scan the WordPress websites for vulnerable plugins, themes, and security misconfigurations. It is the pre-installed tool in kali linux.

The other WordPress Vulnerabillity scanner tools are Malcare, Sucuri, Wordfence, Quttera.

1. **Malcare: -**

MalCare is an all-round WordPress security plugin that helps the user easily detect and fix vulnerabilities and hacks.

Highlights:

- Intelligent scanner
- Complete WordPress security scan
- Early detection of vulnerabilities
- Guaranteed malware removal
- Works without breaking the site

2. **Sucuri: -**

The Sucuri Security Plugin enables the user to stay on top of emerging website security threats. It offers a thorough check of the website not only on WordPress but also on Magento and Joomla!

Highlights:

- Traffic monitoring
- Bad bot blocking
- Virtual patching
- Zero-day exploit prevention

3. **Wordfence: -**

Wordfence is a popular WordPress Firewall and Security Scanner that enables the user to check if there are any security lapses on the website. It offers a way to repair the site as well but it isn't an easy automated solution.

Highlights:

- Extensive WordPress security scanner
- WordPress Malware detection
- WordPress Central
- Live traffic Monitoring

4. **Quttera: -**

Quttera's online web scanner helps detect threats on the WordPress site. The web scanner uses patented technology that is built on a multi-layered approach and self-learning mechanisms.

Highlights:

- Online scanner and plugin scanner
- Detailed investigation report
- Wide range of protection

Conclusion:

We got ourselves familiar with various WordPress vulnerabilities and their possible solutions. It is worth noticing that update plays an essential role in keeping the WordPress security intact. Even after implementing web security measures on your site, vulnerabilities can appear on your site every now and then. This happens because plugins and themes tend to develop security flaws over time. Hackers are aware of this and are constantly in search of vulnerable WordPress sites to exploit.

Reference links:

https://blogvault.net/wordpress-vulnerability-scanner/

https://blog.hubspot.com/website/wordpress-security-issues

https://www.websiterating.com/wordpress/most-common-wordpress-vulnerabilities/