WPScan

2021 Mid-Year

WordPress Security Report

Ryan Dewhurst, Founder & CEO, WPScan
Chloe Chamberland, Threat Analyst, Wordfence

Introduction

As of June 2021, the market share of sites using WordPress has grown to nearly 42% of all major sites. As WordPress continues to grow, more attackers are targeting sites created with WordPress. Meanwhile, more security researchers than ever before are analyzing WordPress-based software, including plugins and themes, for vulnerabilities. This in turn makes the WordPress ecosystem significantly more secure.

Organizations like WPScan and Wordfence play critical roles in securing the WordPress ecosystem. WPScan contributes to WordPress security by encouraging researchers to find vulnerabilities and submit findings to the WPScan vulnerability database. Wordfence, on the other hand, provides unparalleled security solutions and threat intelligence while contributing towards WordPress security education and best practices.

As a joint initiative between Wordfence and WPScan, this whitepaper was created to analyze the current threat and vulnerability landscape of WordPress using complementary data from both organizations. This year has already been an incredibly active year for both vulnerability research and threat actors, and we expect that this will only continue to increase as WordPress grows.

Over 86 Billion Password Attack Attempts Blocked in the First Half of 2021

One of the most common methods threat actors use to compromise WordPress sites is password attacks. Taking advantage of widespread password reuse across a variety of sites, threat actors targeting WordPress sites typically use lists of compromised passwords to attempt site access. Referred to as a “credential stuffing attack,” these attacks are often very successful due to individuals reusing passwords that have been compromised across sites.

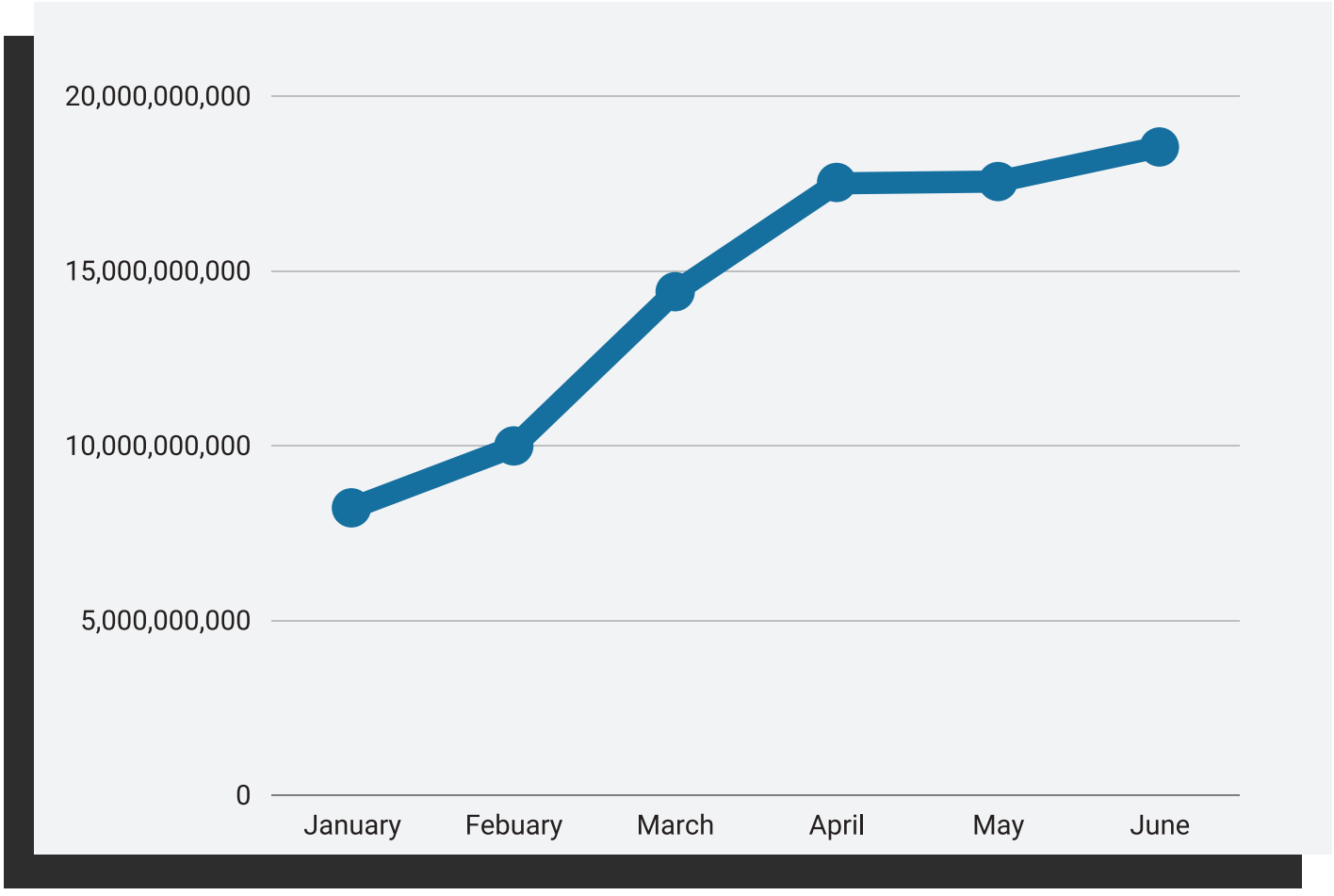
Another common password attack method that threat actors use to target WordPress sites is a dictionary attack. In this scenario, attackers use a list of dictionary words to guess a password. Moreover, hybrid attacks that use a combination of a dictionary attack and brute force methods are popular. These password attacks are often successful due to individuals using weak passwords containing dictionary words with minimal complexity.

More frequently, the term “brute force attack” describes a variety of password attacks. However, this is just another method threat actors use but it is more time consuming and resource intensive. Therefore it is less commonly used. This attack relies on random guessing of a password using a mix of characters, letters, and numbers to try and obtain a password and can take significantly longer to crack a password than the dictionary and credential stuffing attacks.

In the first 6 months of 2021, the Wordfence firewall has blocked over 86 billion password attack requests. Analysis of the data and trends indicates that the number of password attacks will continue to increase. In January 2021, Wordfence blocked just 8,227,887,615 brute force attempts. This volume has more than doubled with around 18,552,519,601 brute force attempts blocked in June 2021 alone.

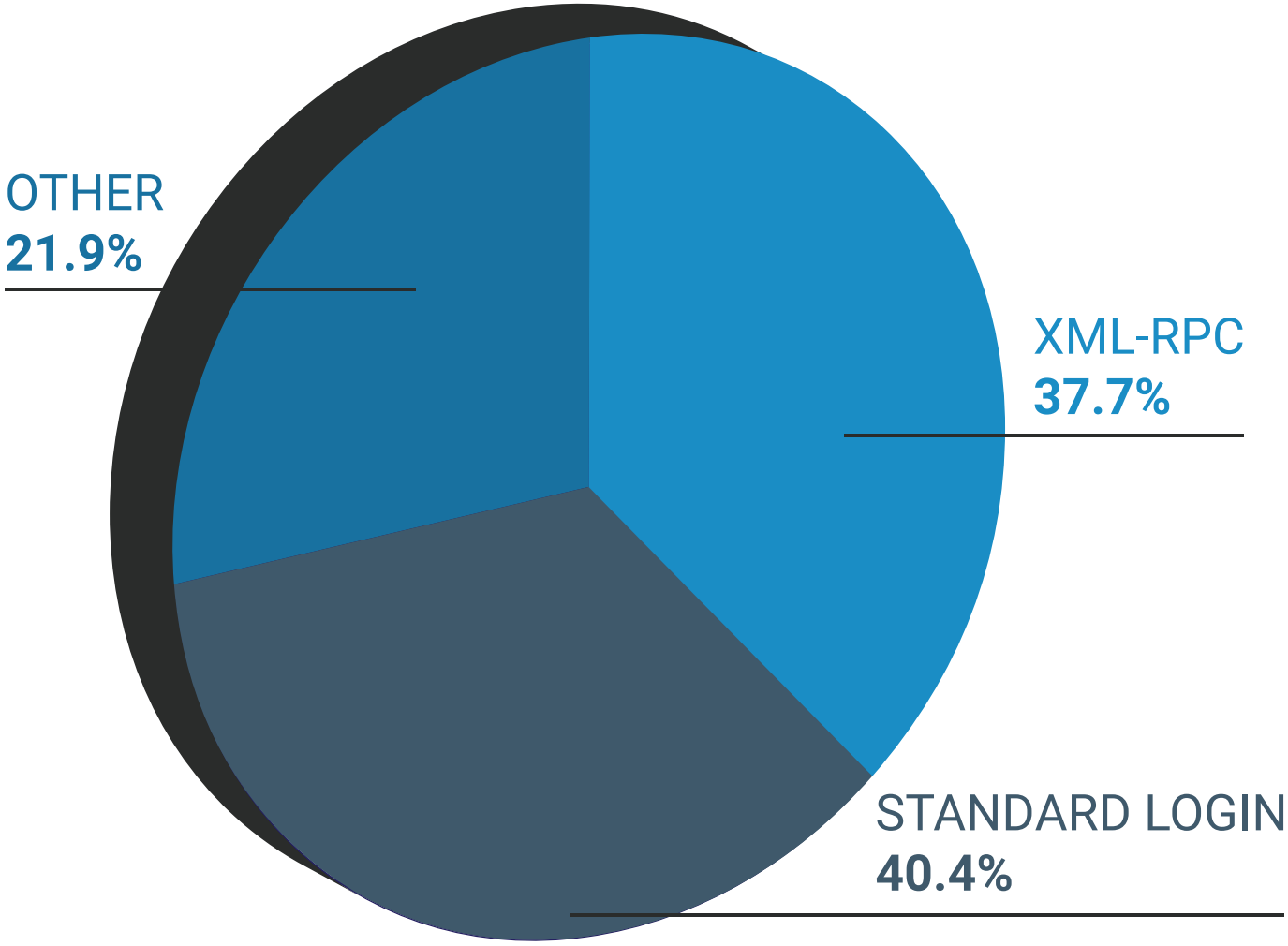
A password attack request blocked by Wordfence is any request that appears to be attempting to log in to a site unsuccessfully via the standard /wp-login.php page, via XML-RPC, or any other custom directory used for logging in.

Blocked Password Attack Requests



Our data also suggests that password attacks targeting XML-RPC and the standard /wp-login.php login page occur at nearly the same rate. This serves as an important reminder to disable XML-RPC if not in use on a WordPress site as attackers frequently target that method for brute force attacks. This can be done simply by using Wordfence and going to the Login Security Settings page, and checking the option to "Disable XML-RPC authentication." The "Other" category is representative of password attacks targeting non-standard login routes such as custom login URLs and AJAX endpoint login attempts.

Password Attack Targets



As password attacks appear to be on the rise, it is important that site owners continue to perform password hygiene best practices. This includes using 2-factor authentication on all available accounts, using strong secure passwords that are unique per account, and disabling XML-RPC when not in use.

In addition to maintaining good password hygiene, brute force protections on a WordPress site can help minimize the impact of password attacks and stop attackers in their tracks. We recommend using Wordfence's brute force protection settings that allow site owners to lockout users after a certain amount of unsuccessful login requests have been made. Wordfence provides several other security options to mitigate brute force attacks.

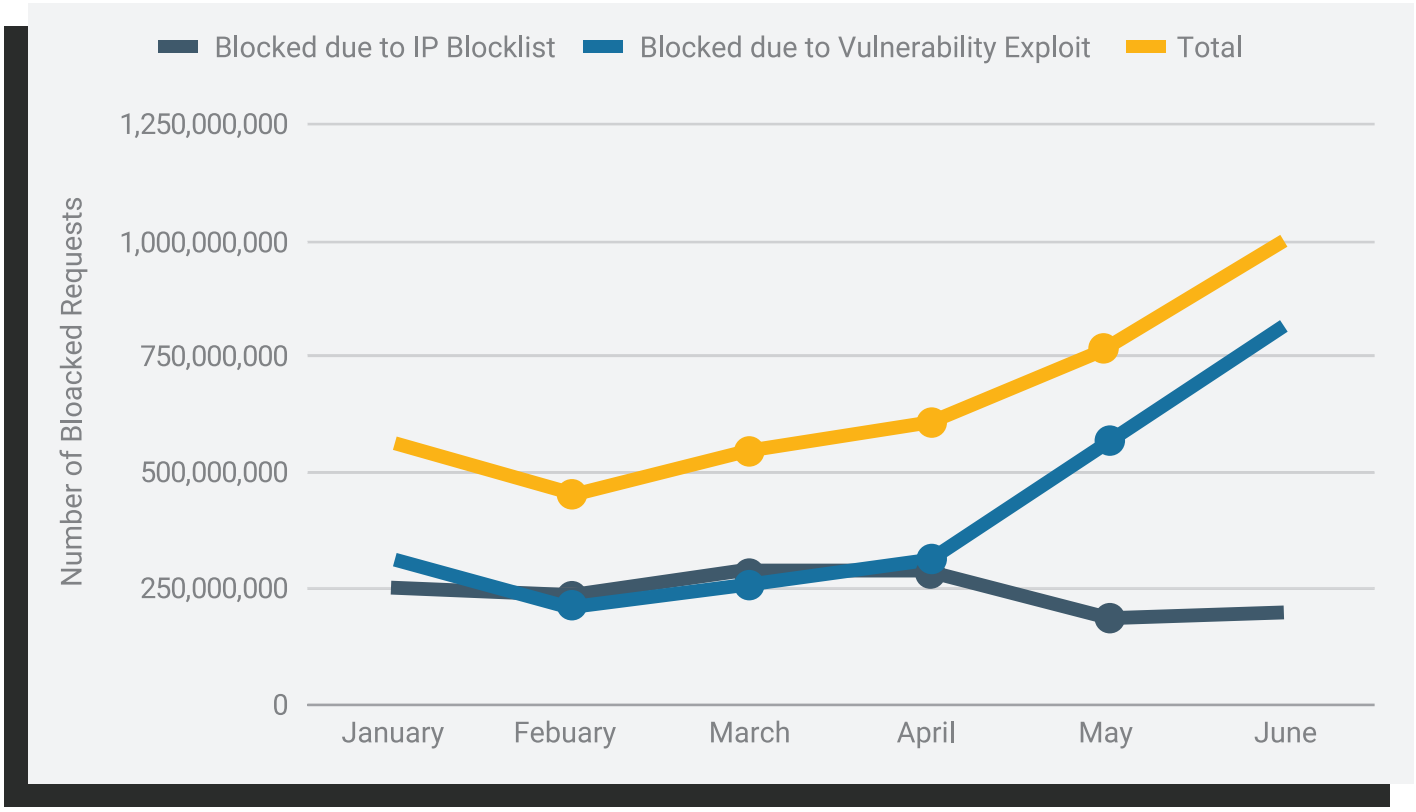
Over 4 Billion Requests Blocked by Wordfence Web Application Firewall in the First 6 Months of 2021

Vulnerabilities are frequently discovered in WordPress plugins and themes and therefore, continue to remain one of the top targets for threat actors targeting WordPress sites.

A vulnerability is a weakness in something, commonly a piece of software, that makes it possible for an unauthorized user to perform an action that they should not be able to perform under normal circumstances.

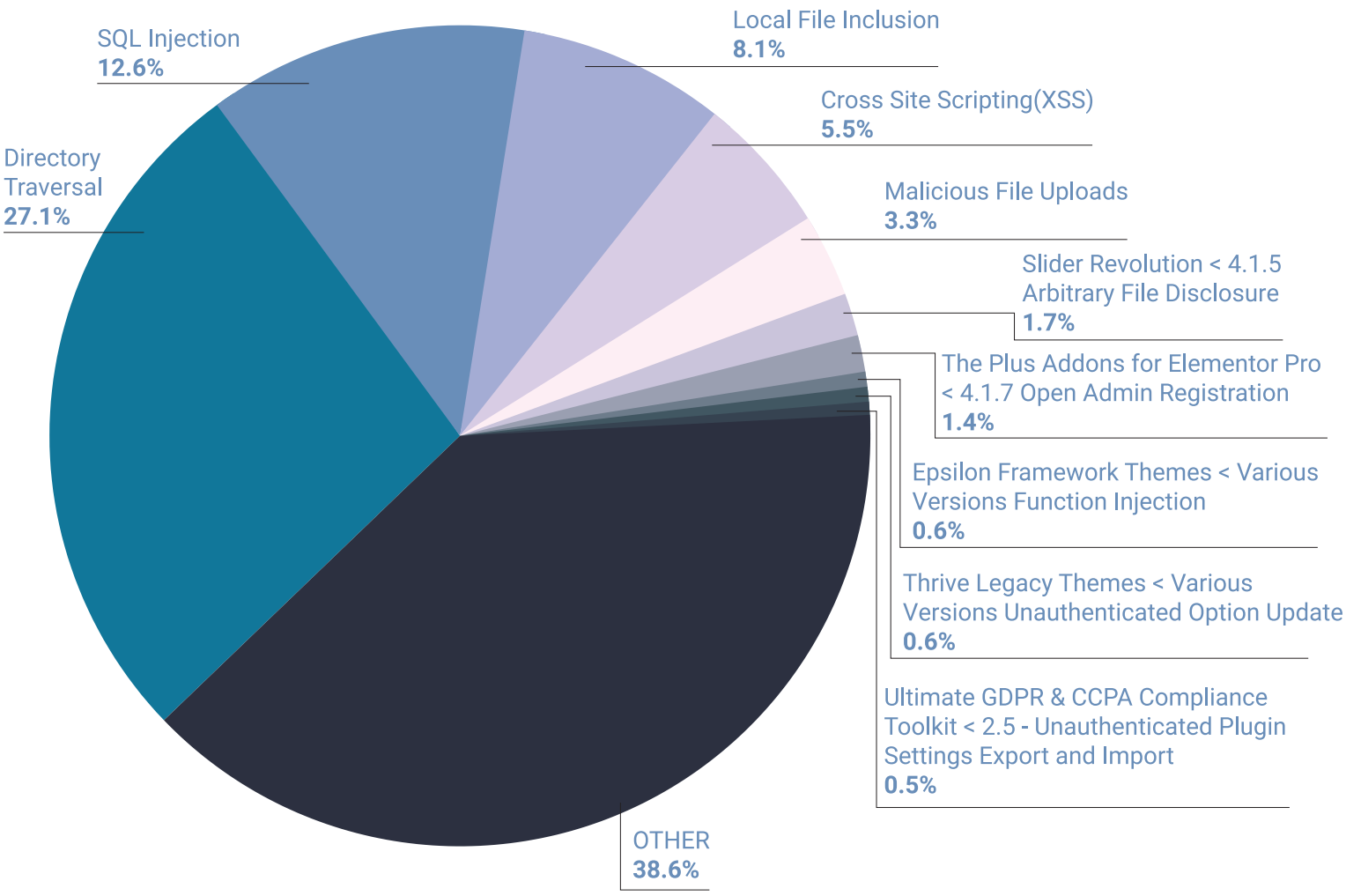
Between January - June 2021, WPScan recorded 602 new vulnerabilities across WordPress plugins, themes, and core, with only 3 of those found within WordPress core. This means that WPScan has already surpassed the 514 reported vulnerabilities during 2020. This trend indicates a rise in vulnerability researchers spending time finding vulnerabilities in WordPress software. This is an extremely positive trend for the security of the WordPress ecosystem which will result in fewer vulnerable plugins and themes available to attackers in the WordPress repository and on external sites.

Requests Blocked by the Wordfence Web Application Firewall



With that, the Wordfence Web Application Firewall has already blocked over 4 billion requests coming from blocklisted IPs and attackers attempting to exploit vulnerabilities during the first 6 months of 2021. As with password attacks, the data indicates that threat actor activity has nearly doubled since the beginning of the year which indicates that there is higher activity from threat actors targeting WordPress on all fronts. As more sites are using WordPress, the easier it will be for attackers to successfully compromise at least one victim when targeting many.

Percentage of Requests Blocked by Firewall Per Firewall Rule



The top 10 Wordfence web application firewall rules that provided the most protection to Wordfence users thus far in 2021 are as follows:

1. Directory Traversal: The firewall rule blocking directory traversal exploit attempts accounted for approximately 674,497,882, or 27.1%, of blocked requests from January 1st to July 1st of 2021. Directory Traversal vulnerabilities occur when an unauthorized user can access files outside of an intended directory and perform an action such as downloading, reading, or deleting a file. More commonly than not, attackers attempt to exploit these types of vulnerabilities to read or delete the /wp-config.php file.

2. SQL Injection[1]: The firewall rule blocking SQL Injection attempts accounted for 313,773,568, or 12.6%, of blocked requests from January 1st to July 1st of 2021. SQL Injection vulnerabilities occur when additional SQL commands or queries can be supplied to an already existing query in order to obtain additional information from the database. This vulnerability is likely number two on our list due to the large number of requests it can take to find out if a site is vulnerable and successfully extract information from the database.

[1] https://www.wordfence.com/learn/how-to-prevent-sql-injection-attacks/

3. Local File Inclusion: The firewall rule blocking local file inclusion attempts accounted for approximately 202,503,671, or 8.1%, of blocked requests from January 1st to July 1st of 2021. Local File Inclusion vulnerabilities occur when locally hosted files can be included on a page and execute the code or display the contents of the file. Attackers frequently try to find ways to read and download sensitive files, so it is not surprising to see this close to the top of the list.

4. Cross Site Scripting(XSS)[2]: The firewall rule blocking XSS attempts accounted for approximately 135,803,425, or 5.5%, of blocked requests from January 1st to July 1st of 2021. This is one of the most commonly discovered vulnerabilities in the WordPress ecosystem as it is quite easy to introduce a XSS vulnerability. WPScan saw that over 52% of the vulnerabilities reported to them so far during the first half of 2021 have been XSS vulnerabilities, so it makes sense that these vulnerabilities are frequently targeted by attackers. Further, cross-site scripting vulnerabilities can be exploited to perform a plethora of malicious actions like redirecting site visitors, uploading malicious files, and adding new administrative users.[3]

5. Malicious File Uploads[4]: The firewall rules blocking malicious file uploads accounted for approximately 81,432,302, or 3.3%, of blocked requests from January 1st to July 1st of 2021. Malicious file upload vulnerabilities are frequently a target of threat actors considering the significant impact they can have on an affected site. If an attacker can upload a PHP file to a WordPress site, then they have the ability to execute arbitrary commands that allow further infection of a site.

6. Slider Revolution < 4.1.5 - Arbitrary File Disclosure: The firewall rule blocking requests to exploit this vulnerability accounted for approximately 41,735,30, or 1.7%, of blocked requests from January 1st to July 1st of 2021. Though this vulnerability is significantly older than all the rest with it's discovery back in 2014, it continues to remain an active target for attackers looking for old abandoned WordPress instances and sites that haven't updated. This vulnerability makes it possible for attackers to download any of a site's sensitive files, like the wp-config.php file.

7. The Plus Addons for Elementor Pro < 4.1.7 - Open Admin Registration:[5] The firewall rule blocking requests to exploit this vulnerability accounted for approximately 35,854,180, or 1.4%, of blocked requests from January 1st to July 1st of 2021. In March of this year, this zero-day vulnerability was discovered being actively exploited and wreaked havoc on WordPress sites for months due to its simplicity to exploit and the fact that it gave attackers administrative access to vulnerable sites. It is not surprising to see this on our top ten list for the first half of 2021.

8. Epsilon Framework Themes < Various Versions - Function Injection:[6] The firewall rule blocking requests to exploit this vulnerability accounted for approximately 14,804,299, or .6%, of blocked requests from January 1st to July 1st of 2021. This was a vulnerability discovered in late 2020, and it made it possible for unauthenticated users to execute arbitrary functions and effectively achieve remote code execution.

9. Thrive Legacy Themes < Various Versions Unauthenticated Option Update:[7] The firewall rule blocking requests to exploit this vulnerability accounted for approximately 14,464,469, or .6%, of blocked requests from January 1st to July 1st of 2021. This was another vulnerability we saw actively exploited during the first half of 2021 just after it was patched. This vulnerability

[2] https://www.wordfence.com/learn/how-to-prevent-cross-site-scripting-attacks/
[3] https://www.youtube.com/watch?v=5BCeXubHegw
[4] https://www.wordfence.com/learn/how-to-prevent-file-upload-vulnerabilities/
[5] https://www.wordfence.com/blog/2021/03/critical-0-day-in-the-plus-addons-for-elementor-allows-site-takeover/
[6] https://www.wordfence.com/blog/2020/11/large-scale-attacks-target-epsilon-framework-themes/
[7] https://www.wordfence.com/blog/2021/03/recently-patched-vulnerability-in-thrive-themes-actively-exploited-in-the-wild/

made it possible for attackers to update options on a site to upload a malicious file that would ultimately allow them to achieve remote code execution, which is why it has been heavily targeted.

10. Ultimate GDPR & CCPA Compliance Toolkit < 2.5 - Unauthenticated Plugin Settings Export and Import: The firewall rule blocking requests to exploit this vulnerability accounted for approximately 12,811,481, or .5%, of blocked requests from January 1st to July 1st of 2021. This is another vulnerability that was discovered this year by a security researcher, and it allowed unauthenticated attackers to update the plugin's settings to redirect site visitors to external sites. Attackers likely targeted this vulnerability to redirect innocent site visitors to spam sites for monetary gain.

Attackers continue to target older vulnerabilities hoping to exploit abandoned WordPress sites to host their malicious content or infect unaware site visitors. This serves as a reminder that attackers will target any site regardless of the content, age, and type as they are looking to steal a site's resources for their own monetary gain.[8]

However, 2021 has also seen several new vulnerabilities that have been high-value targets for attackers. It is evident that attackers have used that to their advantage to try and take over sites that have missed updating their plugins or themes. Attackers targeting WordPress will use any critical vulnerabilities they can find to target as many WordPress sites as possible.

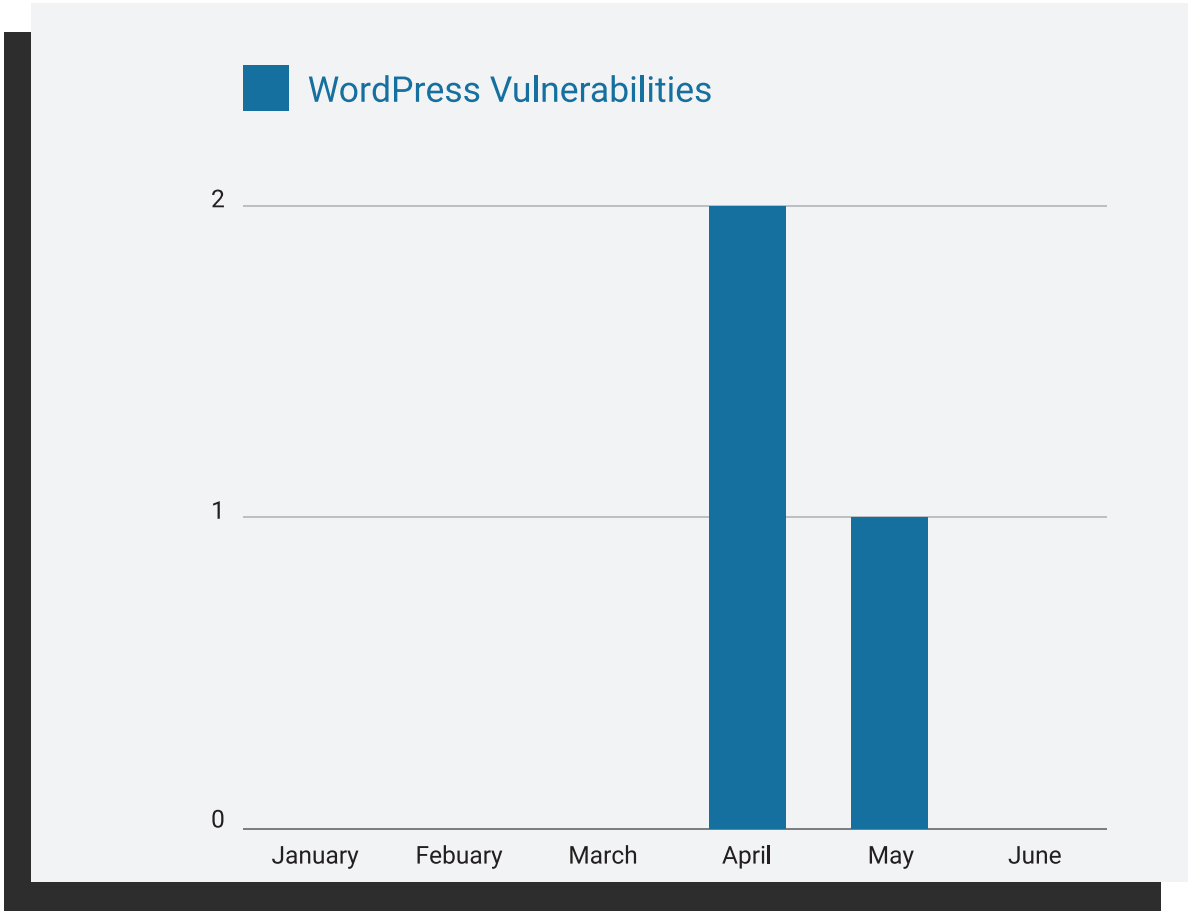
Fortunately, there are many measures site owners can take to protect themselves against WordPress vulnerabilities, one of which includes running a web application firewall (WAF) that will block vulnerability exploit attempts and known malicious IP addresses. Just in 2021 alone, Wordfence has added 61 new firewall rules to provide supplemental protection to the already existing firewall rules that catch a vast majority of exploit attempts targeting WordPress. This ensures that those running the Wordfence Firewall receive up-to-date wholesome protection.

In addition to running a WAF, ensuring that plugins, themes, and core remain up to date, while following security hardening guidelines,[9] will ensure a site safe from virtually all WordPress vulnerabilities. It is also recommended to stay in tune with the latest WordPress vulnerabilities, therefore, we recommended subscribing to the WPScan newsletter that provides monthly digests of all vulnerabilities published in their database, in addition to subscribing to the Wordfence mailing list for the latest news on WordPress security and vulnerabilities.

[8] https://www.wordfence.com/blog/2020/09/the-hacker-motive-what-attackers-are-doing-with-your-hacked-site/
[9] https://wordpress.org/support/article/hardening-wordpress/

A Breakdown of WordPress Vulnerabilities Recorded by WPscan Between January 1st and July 1st 2021

Number of WordPress Core Vulnerabilities by Month

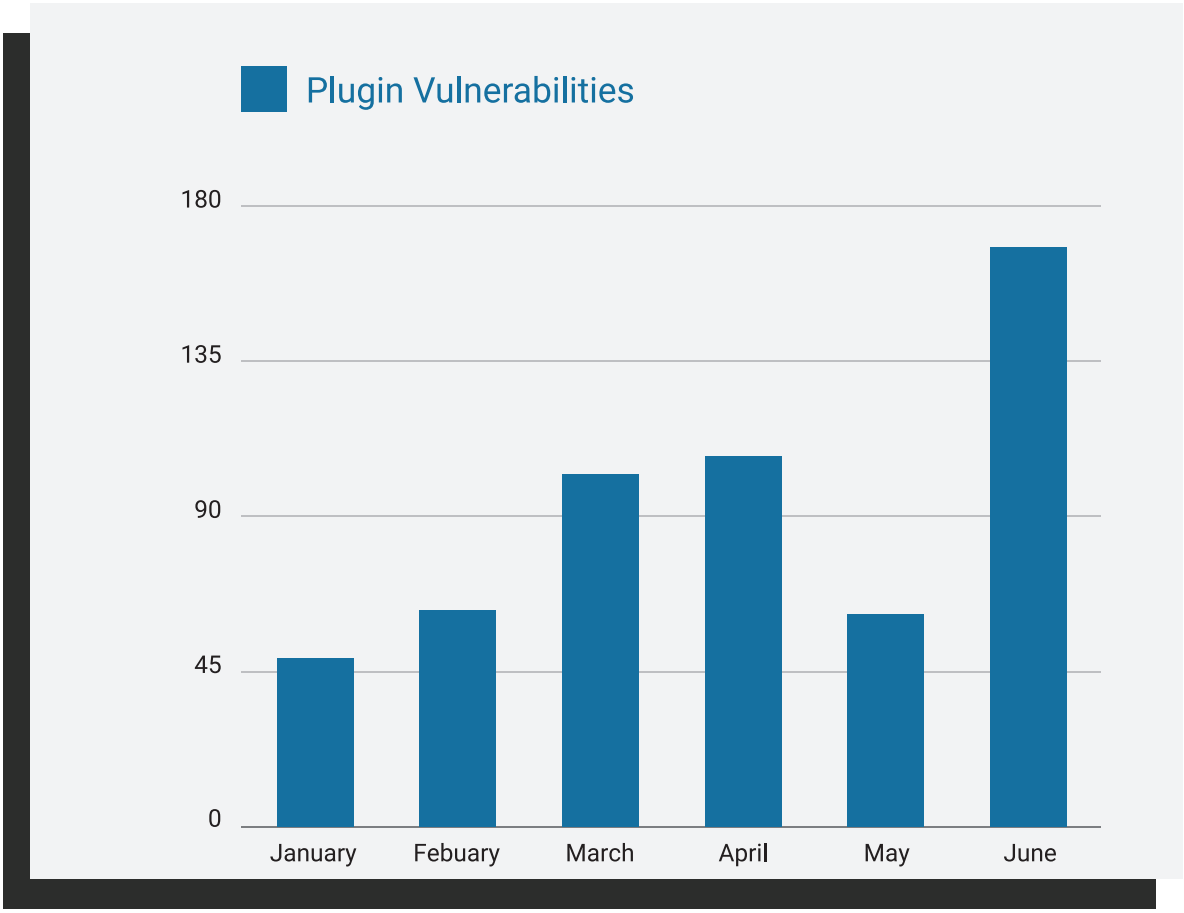


This year so far there have only been three known security vulnerabilities patched in WordPress core. Two were patched in April, with the release of WordPress version 5.7.1, and one in May with the release of WordPress version 5.7.2. Those vulnerabilities were:

- WordPress 3.7 to 5.7.1 - Object Injection in PHPMailer CVSS 6.6 (medium)
- WordPress 4.7-5.7 - Authenticated Password Protected Pages Exposure CVSS 4.3 (medium)
- WordPress 5.6-5.7 - Authenticated XXE Within the Media Library Affecting PHP 8
- 7.5 (high)

The Object Injection vulnerability in PHPMailer (CVE-2020-36326 & CVE-2018-19296) would have been difficult to exploit and would have required authentication in most configurations. The Password Protected Pages Exposure vulnerability (CVE-2021-29450) allowed authenticated users to expose the contents of password protected pages by using the “Latest Posts” block. The XML External Entity (XXE) vulnerability (CVE-2021-29447) affected a third-party audio parsing library used by WordPress called ID3. Given the complexity required to exploit these vulnerabilities, the minimal impact exploitation of these vulnerabilities would have on WordPress sites, and the fact that only three vulnerabilities have been discovered in core this year indicates that WordPress core is on a positive trend as it is more foundationally secure than ever before.

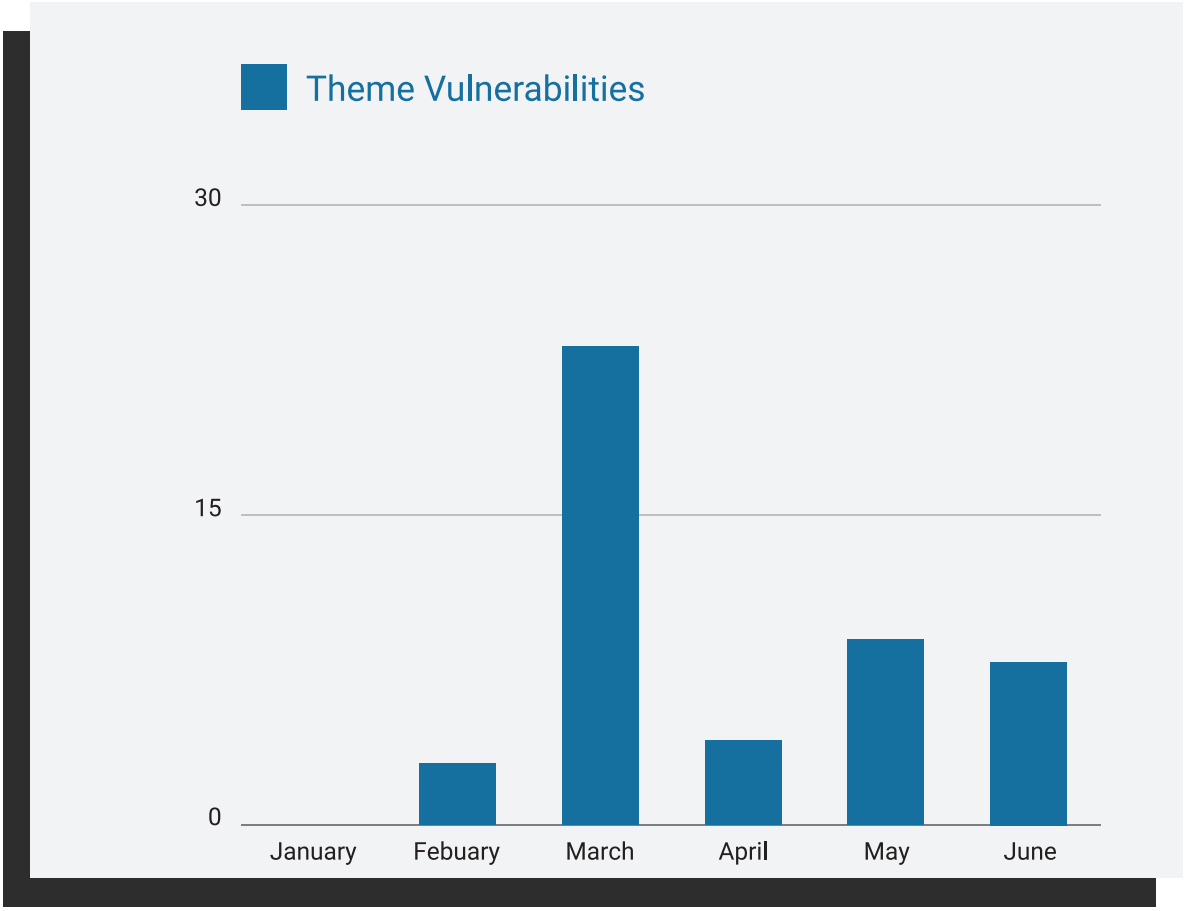
Over 550 Plugin Vulnerabilities Recorded by WPScan WordPress Vulnerability Database



The bar chart shows an upwards trend in the number of discovered WordPress plugin vulnerabilities. The month with the lowest number of plugin vulnerabilities discovered was January 2021, with a total of 49 plugin vulnerabilities. The highest number of plugin vulnerabilities were discovered in June, totalling 176. From January to June 2021, the WPScan WordPress vulnerability database catalogged a total of 552 WordPress plugin vulnerabilities.

Although the chart shows an upwards trend in plugin vulnerabilities, this does not indicate that WordPress plugins are becoming more vulnerable over time. Instead, this just means that more people are discovering and reporting more plugin vulnerabilities. We could attribute the increased number of discovered vulnerabilities to WordPress' continual market growth, the growing increase in interest in cyber security and WPScan's efforts in encouraging security researchers to discover and report vulnerabilities in the WordPress ecosystem. For example, in June, to encourage more security researchers to discover vulnerabilities in the WordPress ecosystem, WPScan's vulnerability disclosure competition awarded a winner with an OSCP voucher, a prestigious cyber security certification. WPScan also does monthly giveaways to security researchers who submit valid vulnerabilities to them. In June, over 49 independent security researchers contributed to the WPScan WordPress vulnerability database.

Number of WordPress Theme Vulnerabilities by Month



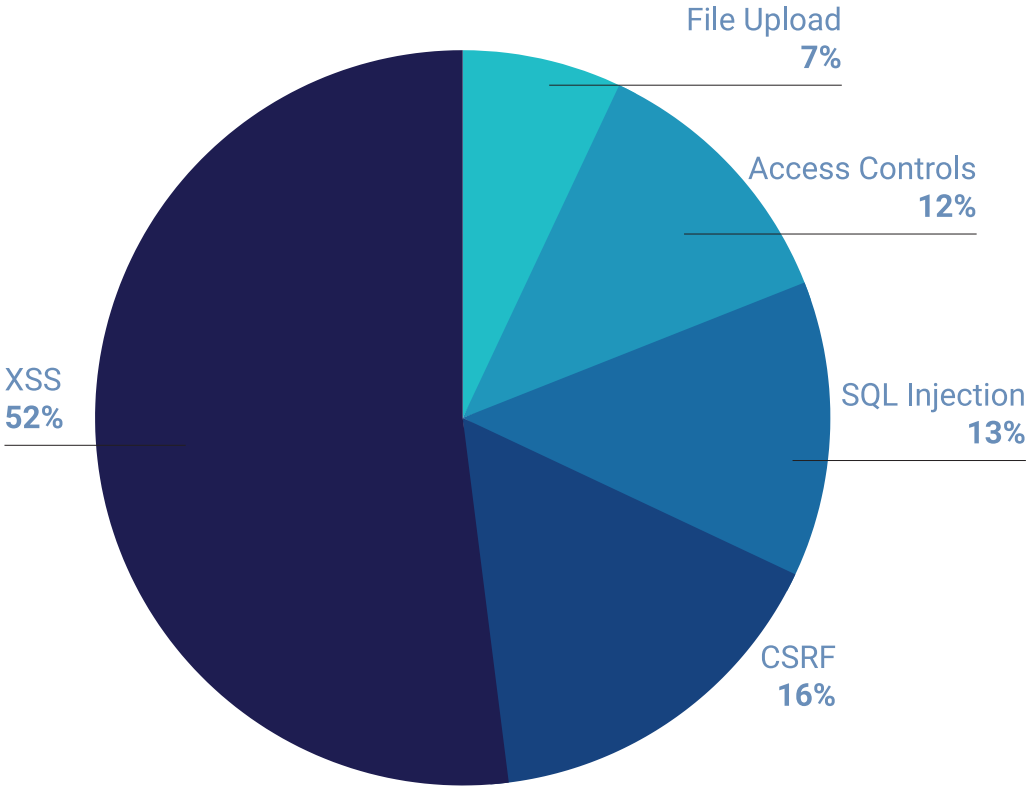
During this time period, the WPScan WordPress vulnerability database catalogued 47 WordPress theme vulnerabilities, compared to the 552 plugin vulnerabilities. WPScan usually sees fewer WordPress theme vulnerabilities discovered than plugin vulnerabilities. As there are fewer themes compared to plugins, and their functionality is generally more basic, there is naturally a lower attack surface. There were no theme vulnerabilities discovered in January, whereas there were 23 discovered in March. The increase in March was due to Wordfence's Threat Intelligence Team discovering two patched vulnerabilities being actively exploited in Thrive Themes, which affected multiple themes.

Note: The monthly total vulnerability counts were counted as non-unique vulnerabilities, with the exception of WordPress core vulnerabilities. That is to say, if one vulnerability affected ten WordPress plugins, here we have counted them as ten individual vulnerabilities, rather than just one vulnerability. Whereas if a vulnerability affected multiple WordPress versions, we have counted them as one vulnerability.

Cross-Site Scripting (XSS) Vulnerabilities Accounted for Over Half of Plugin Vulnerabilities

The top five vulnerability types recorded were Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection, Access Control issues and File Upload issues.

Top Reported Vulnerabilities by Type



As the pie chart shows, Cross-Site Scripting (XSS) is by far the most commonly discovered vulnerability affecting WordPress plugins. Cross-Site Request Forgery (CSRF) vulnerabilities comes in second at 16% of the top five. There were 216 Cross-Site Scripting and 68 Cross-Site Request Forgery (CSRF) vulnerabilities cataloged by the WPScan WordPress vulnerability database in the given time period.

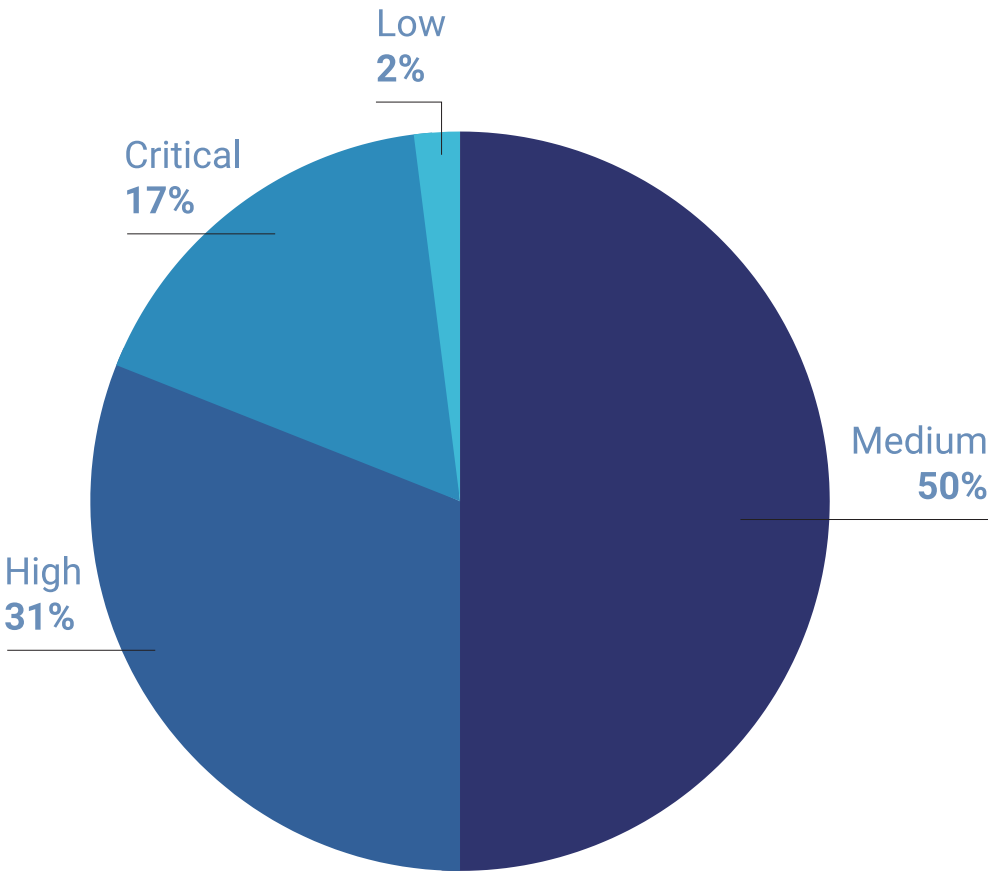
It is not surprising that Cross-Site Scripting (XSS) is the most common vulnerability affecting WordPress plugins. This has been the trend across the internet for many years now, with it making a consistent appearance in the OWASP Top 10. XSS vulnerabilities can be inadvertently incorporated rather easily by plugin developers into their source code. The developer needs to remember to validate all input and encode all output for the correct output context. This can be a hefty task if there are hundreds of potential ways for the plugin to accept untrusted input. To help combat XSS vulnerabilities, the following WordPress functions can be used to encode output esc_html(), esc_attr(), esc_url() and others.

Note: The reason the vulnerability type numbers are lower than the monthly total vulnerability counts is because WPScan assigns a vulnerability type to a unique vulnerability, rather than individual WordPress versions, plugins or themes. For example, if a vulnerability affects ten WordPress versions, WPScan will assign just one vulnerability type, rather than ten individual vulnerability types.

17% of WordPress Plugin Vulnerabilities Were of Critical Risk

The WPScan WordPress vulnerability database uses the Common Vulnerability Scoring System (CVSS) to give risk scores to vulnerabilities so that they can be better prioritised. These scores are Critical, High, Medium and Low.

Reported Vulnerabilities by Severity



As we can see from the pie chart above, 50% of the vulnerabilities discovered within the WordPress ecosystem (mainly WordPress plugins) were of Medium severity. This number closely correlates with the percentage of Cross-Site Scripting (XSS) vulnerabilities, which are generally of Medium severity. What is concerning is that 17% of the vulnerabilities were of Critical risk. This usually indicates that the vulnerability can be immediately exploited by an attacker to take over the website. Some example vulnerabilities that were given a Critical risk rating were vulnerabilities such as unauthenticated SQL Injection and unauthenticated Remote Code Execution.

Note: The reason the vulnerability severity numbers are lower than the monthly total vulnerability counts is because WPScan assigns a vulnerability type to a unique vulnerability, rather than individual WordPress versions, plugins or themes. For example, if a vulnerability affects ten WordPress versions, WPScan will assign just one vulnerability type, rather than ten individual vulnerability types.

WordPress Plugin Vulnerabilities Top 10

The top 10 WordPress plugin vulnerabilities catalogued by the WPScan vulnerability database are listed below.

- W1. Cross-Site Scripting (XSS)
- W2. Cross-Site Request Forgery (CSRF)
- W3. SQL Injection
- W4. Access Controls
- W5. File Uploads
- W6. Remote Code/Command Execution
- W7. Object Injection
- W8. Insecure Direct Object Reference (IDOR)
- W9. Sensitive Data Disclosure
- W10. Insecure Redirects

Conclusion

The first half of 2021 has been an incredibly active year not only for the growth of WordPress sites but also for the attackers who target them. With this growth, we're also seeing an increasing number of security researchers turn their attention to WordPress core, themes, and plugins, increasing the number of vulnerabilities identified and responsibly disclosed to developers.

The trends identified by both WPScan and Wordfence indicate a healthy growth of attention on WordPress security that will lead to more robust software for WordPress users and a more mature security landscape for web publishers.