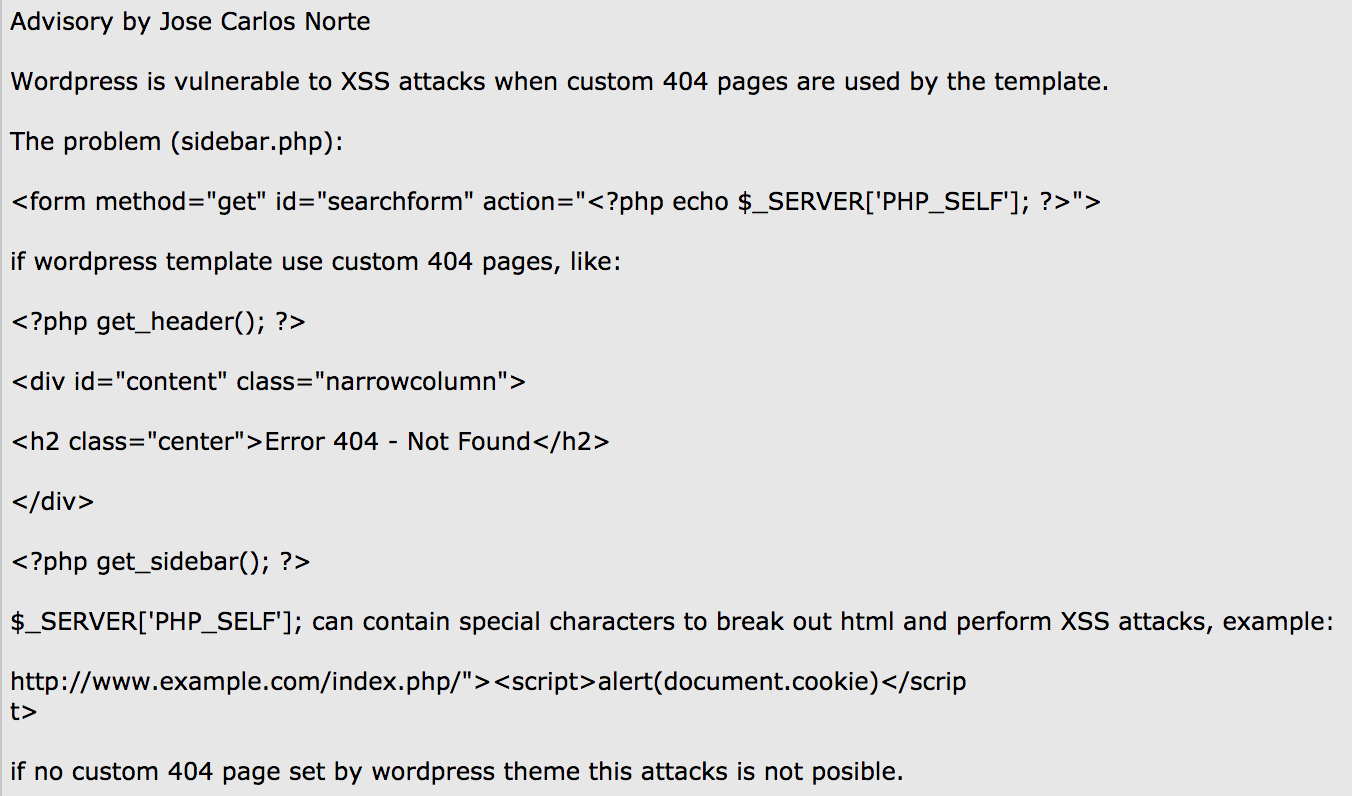
Kristen Trunnelle

IST 590

May 17, 2018

**5 WordPress Vulnerabilities**

The CVE Details website reports **CVE-2007-2627** as a “cross-site scripting (XSS) vulnerability in sidebar.php in WordPress” that affects custom 404 pages when they use get\_sidebar, allowing “remote attackers to inject arbitrary web script or HTML via the query string (PHP\_SELF).” It has a CVSS score of 6.8. It partially affects confidentiality, integrity, and availability, and it is considered a medium complex attack. Access is gained through the user. The vulnerability was discovered in May of 2005.



CVE Details. Vulnerability Details : CVE-2007-2627. Retrieved May 16, 2018, from <https://www.cvedetails.com/cve/CVE-2007-2627/>

#### The **CVE-2018-6389** vulnerability is a recent one that was just discovered on February 6th of this year. It was found on WordPress version 4.9.2. In this exploit, “unauthenticated attackers can cause a denial of service (resource consumption) by using the large list of registered .js files (from wp-includes/script-loader.php) to construct a series of requests to load every file many times.” It was discovered by Barak Tawily. It is an attack done by a remote user. It is reported as a simple denial of service vulnerability that has the power to take down most WordPress websites. The load-scripts.php can be forced to all JavaScript files which then slows a website, consumes high amount of CPU and server memory. If multiple concurrent requests are sent to slow down the website it can cause a denial of service attack. The attack can be prevented by disabling concatenation and by disabling load-scripts.php and load-styles.php. Its CVSS v2 base score is a 5, its impact score a 2.9, and exploit score a 10.

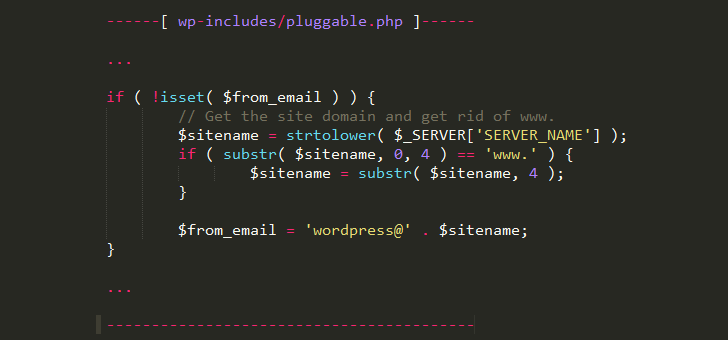
#### 

#### National Vulnerability Database. CVE-2018-6389 Detail. Retrieved May 16, 2018, from <https://nvd.nist.gov/vuln/detail/CVE-2018-6389>

Milla N. Prevent CVE-2018-6389 Exploit on Your WordPress Powered Website. Retrieved May 16, 2018, from https://www.dev4press.com/blog/tutorials/2018/prevent-cve-2018-6389-exploit-on-your-wordpress-powered-website/

Mohit Kumar. Unpatched DoS Flaw Could Help Anyone Take Down WordPress Websites. Retrieved May 16, 2018, from <https://thehackernews.com/2018/02/wordpress-dos-exploit.html>

The **CVE-2017–8295** vulnerability was discovered by security researcher David Golunski on May 4, 2017. It is a security-bypass vulnerability. WordPress up to version 4.7.4 “relied on the Host HTTP header for a password-reset e-mail message, which made it easier for remote attackers to reset arbitrary passwords by making a crafted wp-login.php?action=lostpassword request and then arranging for the message to bounce or be resent leading to transmission of the reset key to a mailbox on an attacker-controlled SMTP server.” For that vulnerability to be exploitable one of three things had to be achieved. With this vulnerability, it “allowed arbitrary code to be executed on the target server.” WordPress uses the variable called SERVER\_NAME to gather the hostname of a server to input values of the From/Return-Path fields. Attackers were able to spoof an HTTP request and change the hostname value (email address) while also setting up a password reset for an admin user. It is really like a phishing email, as the victim by interacting with the reset password email or not, automatically sends a reply back to the attacker’s email. This vulnerability has a CVSS score of 4.3. It does not affect confidentiality or availability. It partially affects integrity and is a medium complexity attack. It has an impact sub score of 2.9 and an exploitability sub score of 8.6. There have been no patches made to stop it.



National Vulnerability Database. CVE-2017-8295 Detail. Retrieved May 16, 2018, from <https://nvd.nist.gov/vuln/detail/CVE-2017-8295>

Tzury Bar Yochay. New Wordpress Vulnerabilities: CVE-2016–10033d and CVE-2017–8295. Retrieved May 16, 2018, from <https://blog.reblaze.com/new-wordpress-vulnerabilities-cve-2016-10033d-and-cve-2017-8295-8b442cd8eef9>

Mohit Kumar.Unpatched Wordpress Flaw Could Allow Hackers To Reset Admin Password. Retrieved May 16, 2018, from <https://thehackernews.com/2017/05/hacking-wordpress-blog-admin.html>

The **CVE-2017-16510** vulnerability is a SQL input validation error vulnerability. It was reported on November 2, 2017. It affects all versions of WordPress before 4.8.3 due to “an issue where $wpdb ->prepare() can create unexpected and unsafe queries leading to potential SQL injection (SQLi) in plugins and themes.” It partially affects confidentiality, integrity, and availability. This vulnerability has a low complexity meaning that practically anyone can do it as it is very easy and requires little knowledge to do so. It has a CVSS score of 7.5, an impact subscore of 6.4 and an exploitability subscore of 10. It was discovered by Anthony Ferrara. WordPress is prone to SQL- injection attacks because it “fails to sufficiently sanitize user-supplied data before using it in an SQL query.” An attacker can remotely view, modify, add, and delete information through the back-end of a database by exploiting this vulnerability. The fix was to upgrade to WordPress 4.8.3.

IBM X-Force Exchange. WordPress wpdb::prepare() method SQL injection CVE-2017-16510 Vulnerability Report. Retrieved May 17, 2018, from <https://exchange.xforce.ibmcloud.com/vulnerabilities/134488>

Security Focus. WordPress 'wpdb::prepare()' Method SQL Injection Vulnerability. Retrieved May 17, 2018, from <https://www.securityfocus.com/bid/101638/info>

CVE Details. Vulnerability Details : CVE-2017-16510. Retrieved May 17, 2018, from <https://www.cvedetails.com/cve/CVE-2017-16510/>

National Vulnerability Database. CVE-2017-16510 Detail. Retrieved May 17, 2018, from https://nvd.nist.gov/vuln/detail/CVE-2017-16510

## The **CVE-2017-5492** vulnerability is a cross-site request forgery vulnerability. It was found in the “widget-editing accessibility-mode feature” in WordPress versions prior to 4.7.1 and allowed for remote hijacking of authentication of “unspecified victims for requests that perform a widgets-access action, related to wp-admin/includes/class-wp-screen.php and wp-admin/widgets.php. It was reported on January 14, 2017 by Roni Skansing. It I classified as an input validation error that is done remotely. Once an attacker gains access through this attack, he/she can perform other attacks. An attacker gains access by getting a victim to open a malicious URI. Updates were made to WordPress as a solution for this vulnerability. It has a CVSS score of 6.8, an impact subscore of 6.4, and an exploitability subscore of 8.6.

National Vulnerabilities Database. CVE-2017-5492 Detail. Retrieved May 17, 2018, from <https://nvd.nist.gov/vuln/detail/CVE-2017-5492>

WordPress Prior to 4.7.1 Cross Site Request Forgery Vulnerability. (n.d.). Retrieved May 17, 2018, from https://www.securityfocus.com/bid/95407/exploit