Jose Barrios

Anastacia Webster

IST-590

5/17/18

**Five Vulnerabilities Report**

**Denial of Service Attack-(DDOS)**

One of the main attacks hackers can use to disrupt a company’s data or service is a Denial of Service attack. A denial of service attack is one the most common attacks hackers can use to disrupt business operations. Essentially, it happens when a system is flooded by a high amount of systems up to the point where the targeted system is unresponsive. A good example, of a Denial of Service attack is when a hacker uses zombie bots which then floods the targeted system with a high volume of packets. In addition, this is one type of vulnerability that many websites currently have. For instance, Word Press is a one of the most popular open source websites used by many individuals and companies. To better clarify the website provides users with a service to efficiently manage content. As a matter of fact, many websites use the open source for the simple matter of creating websites and blogs. Although, word press is used by many websites a (DoS) vulnerability has been discovered on it. Furthermore, according Kumar (2018) the online article the Word Press “CMS platform that could allow anyone to take down most WordPress websites even with a single machine hitting with a massive amount of bandwidth” (p.1). This brings a great concern to the company due to the vulnerability that researches discovered. Moreover, the according to the research found the attacker can simply “force load scripts’ calling all possible JavaScript in one go by passing their names into the above URL, making the targeted website slight slow by consuming high CPU and server memory” (kumar,2018, p.1). Despite the fact a vulnerability has been found on the company’s website, WordPress has denied in patching the issue. In regard to the vulnerability Word Press has not really paid much interest on the issue due to the fact a single request would not be enough to take down the entire website.

**SQL Injections**

Another popular attack and perhaps one of the most commonly used is a SQL injection attack. In fact, one of the major cyber-attacks today are SQl Injections. This type of attack is performed when a malicious user creates a statement that can take control over a web application or database. These attacks can be performed by a high skilled hacker with malicious intentions. In addition, many companies and web applications have experience such an attack in the past years due to flaws in their web applications. Likewise, WordPress has discovered a flaw that could give unauthorized user access to sensitive information. According to Lieskovsky (2010), “An improper input sanitization flaw was found in the way WordPress performed trace backs maintenance remote attacker with Author-level privilege could use this flaw to conduct SQL injections attacks” (p.1) Meaning researchers discovered a flaw to conduct SQL attacks by performing a maintenance trace back. Together with this the author also stated the severity of this issue that was discovered was classified as a medium severity issue. Furthermore, a scheduled update of the version was then recommended to resolve the flaw that was discovered. Consequently, constant updates are a good way to fix any flaws or bugs any application may have. Therefore, constant patches are recommended to fix issues that may arise. Moreover, this goes to show how a simple research and analyzing can help discover flaws which can ultimately prevent unauthorized access. In the situation of WordPress, the flaw was discovered and then the company patched it by issuing the latest version of word press which essential solve the issue/flaw.

**Cross Site Scripting (XSS)**

Cross site scripting is a type of attack that can be used by hackers to inject malicious data or code into a web application by editing the HTML. These attacks are also commonly referred to as forgery attacks. Additionally, attackers use this type of attack to gain sensitive information by targeting certain users. Many individuals as well as website have fallen victim to this type of attack due the sophistication of the attack. To better explain users who are not well aware of these attacks can easily be targeted and fall victim to this attack by clicking a link or file. Another example, of a forgery attack is when attacker inputs malicious code and then victim downloads onto his or her computer. These a few of many examples many users can fall victim to such an attack. Comparatively, this type of vulnerability has also been discovered in Word Press. According to word press (2017) “A remote use can create a specially crafted HTML page or URL file that, when loaded by the target authenticated user, will take actions on the target interface acting as the target user” (p.1). This means that a malicious user can be authenticated as a legitimate user when performing such attack. As a result of this a hacker can then take control of sensitive information without being noticed. Consequently, this a hacker can bypass security measures when this type of attack is executed making it difficult for security professionals to detect it. This type of vulnerability was discovered in versions 4.7 and prior versions of WordPress. Furthermore, the vendor resolved the issue through updates of later versions. Though the versions of Word Press were essentially updated it still necessary for the website to take necessary precautions to prevent such a vulnerability from happening.

**Cross-site Request Forger(CSRF)**

Cross-site request forgery works by making an authenticated user perform forced actions. For instance, an authenticated user can long into his or her account and when a token is requested a hacker use that same token session to perform malicious actions. In addition, this is a type of attack that web developers were not aware of. Although, web developers were not aware of this type of attacks it has now becomes one of the top three cyber-attacks. The reason why web developers were not aware of this attack was due to the fact that a malicious user could potentially use the same session token to bypass security measures. This vulnerability has been found in many websites that have this issue. In addition, WordPress has found this type of vulnerability as well. According to Manideep (2018) “this plugin is vulnerable to a combination of CSRF/XSS attack meaning that if an admin user can be tricked to visit a crafted URL created by the attacker” (p.1). In addition, to this after the attacker exploit the attack he or she can potentially take over the session cookie giving the malicious user the permission to anything he or she wants. The version of WordPress on in which the vulnerability was discovered was version 0.3.1. Consequently, lower versions of the site could possibly have the same vulnerability. Moreover, the website has patched this vulnerability by realizing new updates and providing new versions of WordPress. This patch has essentially fixed the vulnerability issue.

**Insecure Direct Object Reference**

This type of vulnerability happens when a malicious user provides direct access to objects that is based on user input and authentication. This security vulnerability is commonly referred to as (IDOR). In addition, many web applications can be vulnerable to this type of attack. To clarify how this attack is executed imagine that some individual logs into a web application in which he or she can modify data. Furthermore, a malicious user can copy the URL the authenticated users provided and therefore, editing it. This is where trouble arises as the vulnerability here is that the user gave the unauthorized user an opportunity to edit the page file. This type of attack can be a vulnerability Many companies have faced this vulnerability issue. For instance, yahoo was one of the main companies that had a critical hack due to this type of attack. According to Paganini (2014) “a vulnerability in Yahoo allowed Egyptian hacker to delete more than one million and half records from Yahoo database” (p.1) This is a clear example on how the company Yahoo experience a dramatic attack in which the attacker gained access to sensitive information which eventually enabled him to delete up to one million user’s records. This is one clear example on how a malicious user can cause severity in a company. Although these types of attacks are becoming more common in today’s world there are ways in preventing such of attack from occurring. For instance, one way from preventing this attack from occurring is by having the application perform an access control check to make sure the user is in fact an authorized user. Overall this type of attack among one of the top ten cyber security attacks that are being executed by malicious users all across the world. Therefore, it is essential for companies to take initiative in making sure their web applications are secure by taking the necessary actions to prevent these types of attacks from happenin

Reference

Kumar. (2018) Unpatched Dos Flaw Could Help Anyone Take Down WordPress Websites. The Hacker News. Retrieved from <https://thehackernews.com/2018/02/wordpress-dos-exploit.html>

Lieskovsky.J.(2010) SQL injection Flaw by processing trackbacks.buzilla.redhat.com. Retrieved from <https://bugzilla.redhat.com/show_bug.cgi?id=659265>

Security. (2017). Word Press Bugs let Remote Users Conduct Cross-site Scripting. Security Tracker.com Retrieved from <https://securitytracker.com/id/1037591>

Manideep.K. WordPress Pict Browser 0.3.1q/xss.packetstormsecurity.com.Retrieved from <https://packetstormsecurity.com/files/129638/WordPress-PictoBrowser-0.3.1-CSRF-XSS.html>

Paganini. Vulnerability in Yahoo allowed Egyptian hacker to delete more than one million records.Securityaffairs.com.Retrieved from <https://securityaffairs.co/wordpress/22687/hacking/critical-flaw-yahoo.html>