International Journal of Scientific & Engineering Research, Volume 9, Issue 11, November-2018
ISSN 2229-5518

Detection of WordPress User Enumeration Vulnerability

Isrg Rajan[1]

Abstract – WordPress is one of the highly popular content management system (CMS) with estimated at over 172 million active websites including e-Commerce, Personal, News and e-Magazines [1]. The WordPress is popular because of its distributed system support, multi-user, and capacity for easy accessibility. With the popularity of WordPress usability thousands of websites are attacked with DoS, DDoS where user enumeration vulnerability is very common which assist the attackers to completely bring a website to unavailability status [2]. The user-enumeration also assist the hackers in user account cracking. Thousands of websites are relying on the WordPress and therefore it is important to detect such critical vulnerability from time to time. In this paper, we have discussed the loopholes and the root cause of WordPress DDoS, DoS and user enumeration. SSH Script, Python and CGI scripts were used to conduct the examination on more than 100 WordPress powered website including 3 locally hosted websites. We achieved 95% of success in generating the list of user accounts created on the WordPress powered website 80% of success in bringing a WordPress website to unavailable status.

Index Terms – WordPress, CMS, WordPress Security, WordPress User Enumeration, WordPress Vulnerability, PHP, CMS Vulnerability

1 INTRODUCTION

Today more 3.2 billion people across the world are accessing and interacting with the Internet through various devices including laptop, PC, smartphones, featured phones, Point of Sale (PoS) Machines, Smart Gadgets and cars etc. while they are generating 2.5 quintillion bytes of data each day which is not only challenging to store, but also to protect it from data bleach. At present, we are struggling with data storage, performance & availability issues, data encryption, bugs & vulnerabilities with web-applications [3].

Websites and web applications has become a compulsory requirement of any business where WordPress standalone has powered nearly 172 million web-applications, websites, iOS and Android apps which is nearly 30% of the websites at present on the Internet [1]. Here upon, the WordPress has become the major target of the hackers & attackers to exploit the web-applications, apps and websites developed using WordPress content management software (CMS). According to the Open Web Application Security Project (OWASP) Injection, Broken Authentication, SQL-injection, Sensitive Data Exposure, XML External Entities (XXE), Distributed Denial of Service Attack (DDoS) & Denial of Service Attack (DoS), Broken Access Control, Security Misconfiguration, Cross-site scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring etc. are the common vulnerabilities with web-applications [4].

In past few decades, thousands of attempts were made to deal with these common vulnerabilities where open source organisations such as OWASP has proposed some guidelines and solutions to manage with these problems. However, implementing necessary steps to secure the web-applications is possible, but implementing all these solutions will bring performance issues with these web-applications especially when there are millions of users interacting with these applications every day [5].

According to wordfence.com, the most of vulnerabilities in WordPress powered websites are found in the plugins which are used to increase the working of the WordPress and add more features to it. After plugin the second most common attack is made through brute force attempts [6].

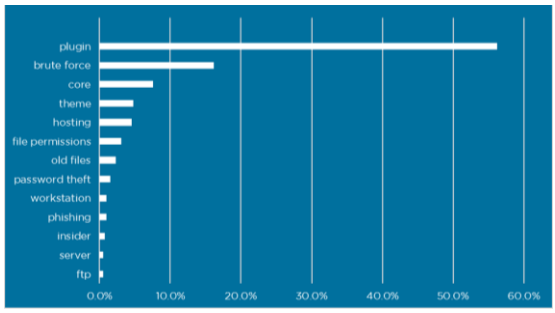

Figure 1 Statistics of root cause of WordPress hacks

When it comes to maintenance of web-applications developed using WordPress most of people fail to keep the plugins and WordPress core up to date which sometime contains vulnerable codes where the exploiters and attackers crawls for the WordPress web-applications using

[1] *Isrg Rajan, entrepreneur and an scholar of Masters in Computer Applications at BPIBS, IP University, New Delhi, isrgrajan@outlook.com*

International Journal of Scientific & Engineering Research, Volume 9, Issue 11, November-2018
ISSN 2229-5518

Python and other programming languages scripts to detect the WP-core version, plugin versions and common WordPress vulnerabilities. Once they find the vulnerability they set the target and begin with attacking and exploiting processing in-bulk using tools and custom made scripts. Thus, time to time maintenance of these web-applications are needed [7].

Despite, adopting these security measures there are no permanent solution for the brute force attacks, DDoS & DoS. For instance, in past few years, the giant tech companies like Cloudflare, Facebook, Twitter and YouTube has faced the similar attacks even after high-tech and multi-layer security deployments which is not affordable by small and medium sized businesses and organisations [8].

According to the Kaspersky Labs, HTTP-DDoS is the second most common target of the attackers after SYN-DDoS and there is increase in numbers of attacks in 2015 as compared to the 2014 [9].

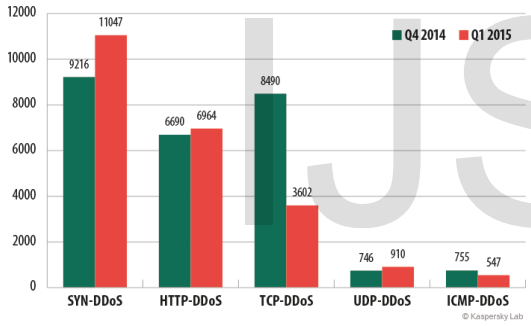

Figure 2 DDoS/DoS Attacks Statistics- between 2014-2015 in Quadrillion

There are many automated and manual methodology to find the vulnerabilities with these web-applications proposed by many freelance developers, open-source companies and platforms like GitHub for the purpose of scanning and detecting the vulnerability, WP-Core version, Plugin and Plugin version etc.

In our research we have developed a tool using an SSH script with the combination of PHP & Python programming languages to scan WordPress web-application, detect WordPress version, Installed Plugins, plugin version, common WordPress vulnerabilities and run the exploitation including user-enumeration and DDoS. Using the tool developed by us we have tested more than 100 WordPress web-applications to validate the accuracy and rate of success.

This paper is organized in ten sections. After the Introduction we included the Background & related work in second section where the third section tells about the proposed model, WordPress DDoS and user enumeration vulnerability exploitation processes.

2. BACKGROUND AND RELATED WORKS

The introduction and invention of content management software also known as content management system has created the new opportunities not only for the web-application developers, but also for the small and medium sized businesses to own a website which is easy to maintain, update, create new contents, pages and release regular updates. It has also given employment to the millions of bloggers and birth to the thousands of e-magazine and news companies where trillions of blog posts are made every month. The content management software has also assist the e-commerce industry using which advanced and high quality of e-commerce web-portal can be developed by installing some plugins and configuring it as per the requirement. Especially, when we talk of WordPress a variety of web-application can be developed for example forum, e-commerce website, html5 based iOS and Android apps, blogging websites, news and magazine website, social networking and community platforms, matrimony and classified portals etc [10].

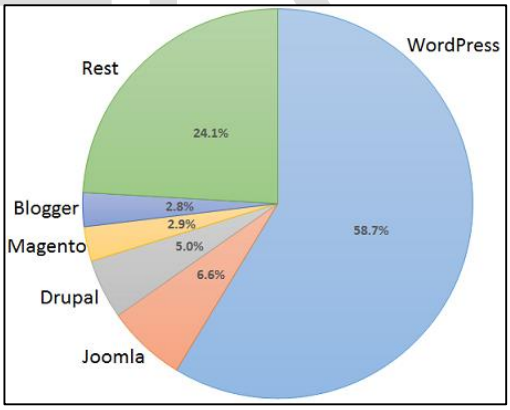

Figure 3 Shares of CMS on the Internet (Report: w3techs.com)

According to the statistics released by w3techs.com for the websites using content management software, 58.7% websites on the Internet are powered by WordPress alone as compared to the Blogger (2.8%), Magento (2.9%), Drupla (5.0%), Joomla (6.6%) and other (24.1%) [11].

3. OUR PROPOSED MODEL

A tool developed using SSH script, Python and PHP has been implemented on our proposed model to detect WordPress websites, find the WordPress version, fetch the list of user accounts created on the website, and exploit the website with DDoS attack, brute force and common WP-vulnerabilities.

The list of user account created on the website fetched using *$_GET* method where the DDoS attack, brute force and WP-vulnerabilities was implemented using *$_GET* and *$_POST* both the methods. The technique allow the user to fetch the list of user accounts (usernames) created on the website and launch "login-attempts" with common passwords and fetched usernames as well as to launch the DDoS attempts.

The process and our proposed model architecture is given below:

Step 1:

Using the tool developed by us the script will check whether the entered URL running is WordPress or not.

Step 2:

If the entered URL is running WordPress, it will return the WordPress version and will prompt for the step 3.

Step 3: The tool will check if user-enumeration is vulnerable, if it is vulnerable then it will start generating the list of user accounts created on the website else it will return "error: not vulnerable".

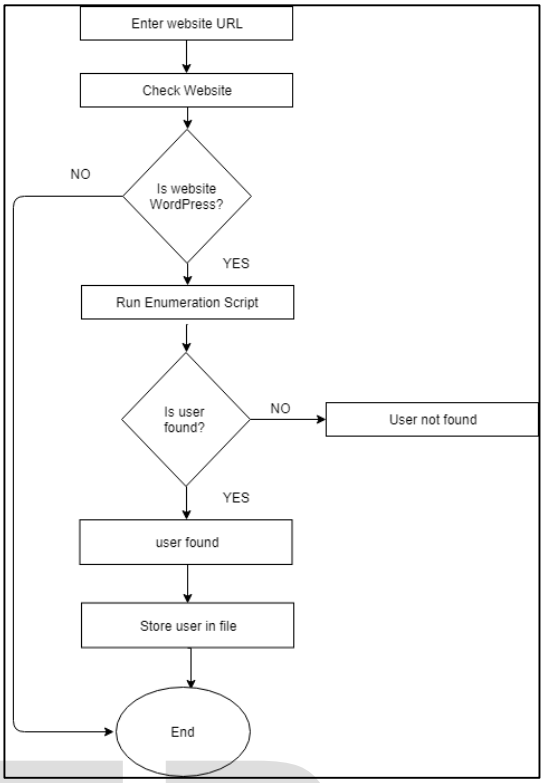

Figure 4 Proposed Model for user-enumeration vulnerability

4. GENERAL PREVENTION TECHNIQUE

According to the methodology the content management system should be identified first, nonetheless, the user enumeration vulnerability process should be executed.

If WordPress is detected, then:

https://anywpwebsite.com/?author={i}

OR

https://anywpwebsite.com/?author={num:i}

Where 'i' is the integer value that can be incremented or decremented to fetch more user accounts.

```
$urla='https://www.shoutmeloud.com';
$max_limt=10;
$user_list=array();
$flag=0;
function get_http_response_code($urla) {
   $headers = get_headers($urla);
   return substr($headers[0], 9, 3);
}
for($i=1;$i<=$max_limt;$i++) {
```

International Journal of Scientific & Engineering Research, Volume 9, Issue 11, November-2018
ISSN 2229-5518


```
if(get_http_response_code($urla.'/?author={num:'.$i.'}')
== "200") {
$url=$urla.'/?author='.$i;
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_HEADER, true);
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, true);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
$a = curl_exec($ch);
$url = curl_getinfo($ch, CURLINFO_EFFECTIVE_URL);
array_push($user_list,basename($url));
curl_reset($ch);
$flag++;
} else {
break; }
}
print_r($user_list);
echo '<br />User accounts found:'.$flag;
```

Output of the above code will be in an array format with list of usernames

```
Array ( [0] => admin )
User accounts found:1
```

5. EFFECT OF WP USER ENUMERATION

Wordpress user enumeration could have worse effect on the WordPress including DDoS, Brutal Force attack and website compromisation.
Sometime this could also lead to data bleach and effect on the website's performance, unnecessary resource utilisation.

6. GENERAL PREVENTION TECHNIQUE

There are several possible ways to detect and stop the user enumeration, brutal force attack and website compromisation.

a. Using .htaccess in Apache

```
RewriteCond %{REQUEST_URI} !^/wp-admin [NC]
RewriteCond %{QUERY_STRING} ^author=\d+ [NC,OR]
RewriteCond %{QUERY_STRING} ^author=\{num
RewriteRule ^ - [L,R=403]
```

b. Using PHP

```
if ( ! is_admin() ) {
   add_filter(
      'query_vars',
      function ( $public_query_vars ) {

         foreach ( array( 'author', 'author_name' ) as $var ) {
            $key = array_search( $var, $public_query_vars );
            if ( false !== $key ) {
               unset( $public_query_vars[$key] );
            }
         }

         return $public_query_vars;
      }
   );
}
```

7. CONCLUSION

Internet, web applications, mobile and computer applications are daily to daily usable utilities that as automated the entire process. The content management system like WordPress is powering nearly millions of websites, blogs and e-commerce websites and shockingly most of people who are operating these websites are from non-technical background and this became possible just because of ease of usability, integrability and manageability.

When millions of people are using these applications they not only invest money, but also trust in that which could be compromised with loopholes and bugs.

8. ACKNOWLEDGEMENT

We are thankful to the management of Bhai Parmanand Institute of Business Studies, authorities that gave permission to test the project.

9. REFERENCES

[1] Quality Nonsense Ltd, "Shocking WordPress Stats 2017," Nov 09 2018. [Online]. Available: https://www.whoishostingthis.com/compare/wordpress/stats/.

[2] M. Maunder, "Breaking: Aggressive WordPress Brute Force Attack Campaign Started Today, 3am UTC," Wordfence, 18 December 2017. [Online]. Available: https://www.wordfence.com/blog/2017/12/aggressive-brute-force-wordpress-attack/. [Accessed 09 Nov 2018].

[3] J. DAVIDSON, "Here's How Many Internet Users There Are," Time, 26 May 2015. [Online]. Available: http://time.com/money/3896219/internet-users-worldwide/. [Accessed 09 Nov 2018].

[4] Rapid7, "Common Types of Cybersecurity Attacks," Rapid7, 09 Nov 2018. [Online]. Available: https://www.rapid7.com/fundamentals/types-of-attacks/.

[5] OWASP, "Code Reviews and Compliance," OWASP ORG, 09 Nov 2018. [Online]. Available: https://www.owasp.org/index.php/Code_Reviews_and_Compliance. [Accessed 09 Nov 2018].

[6] M. Veenstra, "Privilege Escalation Flaw In WP GDPR Compliance Plugin Exploited In The Wild," Wordfence.com, 08 Nov 2018. [Online]. Available: https://www.wordfence.com/blog/category/vulnerabilities/. [Accessed 09 Nov 2018].

[7] wpbeginner.com, "11 Top Reasons Why WordPress Sites Get Hacked (and How to Prevent it)," Wpbeginner.com, 09 Sept 2018. [Online]. Available: https://www.wpbeginner.com/beginners-guide/reasons-why-wordpress-site-gets-hacked/. [Accessed 09 Nov 2018].

[8] E. Darrell and C. Kate, "Large DDoS attacks cause outages at Twitter, Spotify, and other sites," Tech Crunch, 2016. [Online]. Available: https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/. [Accessed 09 Nov 2018].

[9] Kaspersky Labs USA, "Distributed Denial of Service: Anatomy and Impact of DDoS Attacks," Kaspersky Labs, 09 Nov 2018. [Online]. Available: https://usa.kaspersky.com/resource-center/preemptive-safety/how-does-ddos-attack-work.

[10] WordPress, "Getting Started with WordPress," 09 Nov 2018. [Online]. Available: https://codex.wordpress.org/Getting_Started_with_WordPress.

[11] W3Techs, "Market share trends for content management systems for websites," W3Techs, 09 Nov 2018. [Online]. Available: https://w3techs.com/technologies/history_overview/content_management.