WORD PRESS VULNERABILITY

- WordPress is an open-source content management system (CMS).
- It's a popular tool for individuals without any coding experience who want to build websites and blogs.
- The software doesn't cost anything. Anyone can install, use, and modify it for free.
- WordPress was mainly used to create blogs.
- Repository: core.trac.wordpress.org/browser.
- Operating system: Unix-like, Windows, Linux.

What are the vulnerabilities of WordPress?

- Cross-Site Scripting.
- DDoS Attack.
- Old WordPress and PHP versions.
- SQL Injection.
- Malware.
- Brute Force Attack.

How to identify whether the website is a word press website or not?

- To identify whether the website is a word press website or not we have to Use a tool called wappalyzer
- We have to add the wappalyzer tool extension to our browser.
- The Wappalyzer APIs provide instant access to website technology stacks, company and contact details, social media profiles, email verification and more.

How to capture the request and response of the server and client?

- We can capture the request and response of a server and client using burp Suite and foxy proxy.

Steps to check for WordPress vulnerability:

- Make sure that burp suite instance is on in proxy settings.
- Now enable the foxy proxy.
- Load the target website in the URL field along with the target path/folder of WordPress in any of the web browser.
- Now go back to the burp suite and right click on the response and select the option send to repeater.
- Next the intercept should be turned off and then select the send option in the top left corner.
- Now check for the POST http method in the repeater.

- The GET method refers to a Hyper Text Transfer Protocol (HTTP) method that is applied while requesting information from a particular source. It is also used to get a specific variable derived from a group.
- The HTTP POST asks for input of information from the supplying browser into the server's message system.
- For example: if the admin panel path is vulnerable, then hackers may try to perform credential brute force attack. This can be detected using the above-mentioned tools and analyzing the status codes and HTTP methods.
- Example of code: to escalate about the severity of the vulnerability.

  <methodCall>

  <methodName>system.listMethods</methodName>

  <params></params>

  </methodCall>

WordPress User Enumeration:

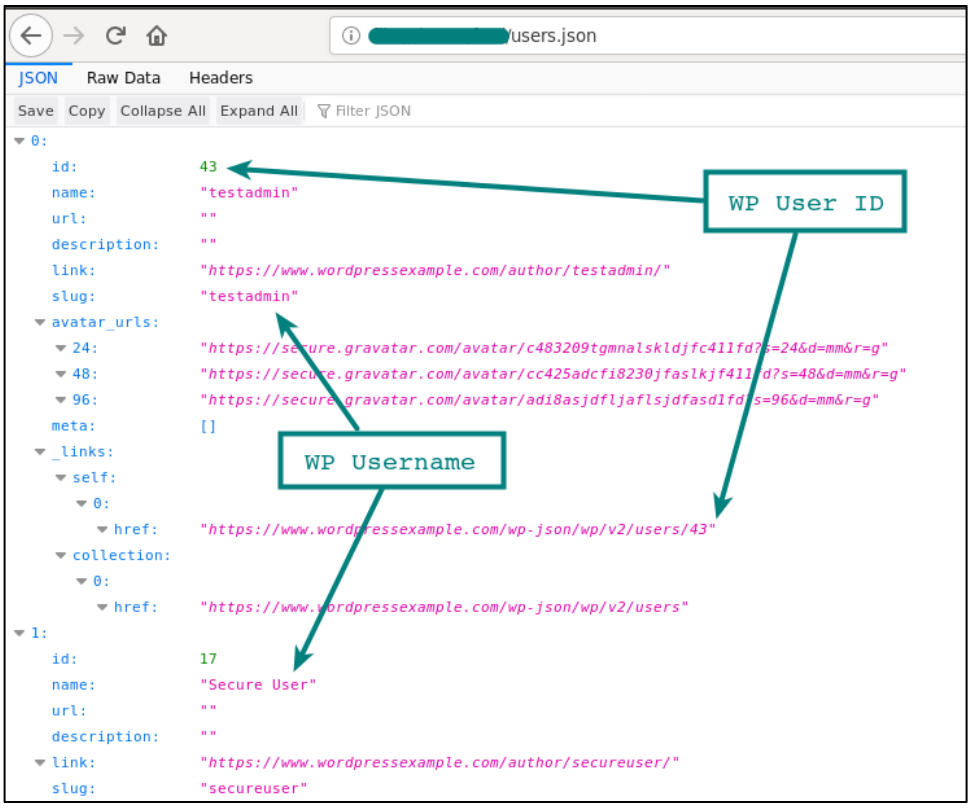
- These three enumeration techniques are a very fast way to identify users of a WordPress installation.
- With valid usernames effective brute force attacks can be attempted to guess the password of the user accounts.

WordPress User Enumeration via Author Archives

- Users have a unique user id that is used by the application in the database and for referencing the user account.
- By attempting to load the author archive for each user id, we quickly identify valid account id's and the username that matches the account.
- This includes the admin username. This is not a new trick and is available in a number of WordPress Security Testing tools.

WordPress Enumeration via JSON API:

- Using a Json endpoint, it may be possible to get a list of users on the site.
- This was restricted in version 4.7.1 to only show a user that has published a post and if configured, before that all users were shown by default.
- *https://wordpressexample.com/wp-json/wp/v2/users*



WordPress Enumeration via the Login Form:

- Brute forcing the user's name is possible using the login form as the response is different for a valid vs an invalid account.

- Using a tool such as Burp Intruder in Burp Suite, we would load a list of possible usernames and cycle through HTTP POST requests to the WordPress login form examining the response.
- A HTTP response that matches "invalid password" indicates the username is valid. We could then move onto attacking the password using the same process with a common password list.

References:

https://fossa.com/blog/open-source-software-licenses-101-gpl-v2/

https://www.wpbeginner.com/beginners-guide/beginners-guide-to-wordpress-file-and-directory-structure/

https://hackertarget.com/wp-content/uploads /2013/10/wordpress-login.png