WordPress Exploitation Lab

Summary of Lab

In this lab I installed WordPress as a content management system for my website hosted by Apache2. I installed a plugin from Sonaar that allows clients to listen to music and leave comments. Version 4.7 of this plugin has a Cross-Site Scripting vulnerability, where users can leave comments with code that the server executes when loading the page. I installed this version of the plugin, and created a page that is vulnerable to this attack. I then used WPScan to emulate an attacker enumerating the webpage for potential vulnerabilities. This scan revealed the out-of-date plugin, which would prompt an attacker to look for discovered vulnerabilities. The attacker would likely find the XSS vulnerability using and exploit database (like exploit-db), and carry out the attack like in my example.

If this was a real scenario, this specific vulnerability could be mitigated by updating the plugin. The opportunity for Cross-Site Scripting can be removed with proper server-side and client-side user-input validation.

Step-By-Step Documentation

WordPress Installation

I used the commands provided in the assignment to get WordPress up and running on a new Ubuntu virtual machine.

Plugin Installation

For selecting the plugin to use, I looked at exploit-db and selected the Sonaar Music Plugin. Specifically, version 4.7, which has a stored XSS vulnerability that was found by Furkan Karaarslan (https://www.exploit-db.com/exploits/51739). Since I was starting from a new ubuntu install, I had to delete the index.html file, so Apache would serve my index.php file. I then traversed to this page (http://192.168.27.5/wp-admin/post-new.php?post_type=sr_playlist) to add the mp3 file for the music, which completes the plugin integration for my use.

WPScan Results

Notable Scan Results:

- **Apache Server Version Disclosed:** The server is identified as Apache/2.4.52 (Ubuntu)
- **XML-RPC Enabled:** The xmlrpc.php file is accessible, posing a risk for brute-force attacks and DDoS amplification.
- **Upload Directory Listing Enabled:** The /wp-content/uploads/ directory allows listing of files, which could expose sensitive or private uploads.
- **External WP-Cron Potentially Enabled:** The wp-cron.php file might be accessible externally, which could be abused for resource exhaustion or unauthorized task execution.
- **Outdated mp3-music-player-by-sonaar Plugin (4.7):** It found the plugin we installed, as well as the version.

Full scan results below:

```
Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.52 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.27.5/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.27.5/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.27.5/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.27.5/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.7.2 identified (Latest, released on 2025-02-11).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.27.5/index.php/feed/, <generator>https://wordpress.org/?v=6.7.2</generator>
 |  - http://192.168.27.5/index.php/comments/feed/, <generator>https://wordpress.org/?v=6.7.2</generator>

[+] WordPress theme in use: twentytwentyfive
 | Location: http://192.168.27.5/wp-content/themes/twentytwentyfive/
 | Last Updated: 2025-02-11T00:00:00.000Z
 | Readme: http://192.168.27.5/wp-content/themes/twentytwentyfive/readme.txt
 | [!] The version is out of date, the latest version is 1.1
 | [!] Directory listing is enabled
 | Style URL: http://192.168.27.5/wp-content/themes/twentytwentyfive/style.css?ver=1.0
 | Style Name: Twenty Twenty-Five
 | Style URI: https://wordpress.org/themes/twentytwentyfive/
 | Description: Twenty Twenty-Five emphasizes simplicity and adaptability. It offers flexible design options, suppor ...
 | Author: the WordPress team
```

```
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.0 (80% confidence)
| Found By: Style (Passive Detection)
|  - http://192.168.27.5/wp-content/themes/twentytwentyfive/style.css?ver=1.0, Match: 'Version: 1.0'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] mp3-music-player-by-sonaar
| Location: http://192.168.27.5/wp-content/plugins/mp3-music-player-by-sonaar/
| Last Updated: 2025-01-29T16:08:00.000Z
| [!] The version is out of date, the latest version is 5.9.4
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 4.7 (100% confidence)
| Found By: Query Parameter (Passive Detection)
|  - http://192.168.27.5/wp-content/plugins/mp3-music-player-by-sonaar/public/css/sonaar-music-public.css?ver=4.7
|  - http://192.168.27.5/wp-content/plugins/mp3-music-player-by-sonaar/public/js/sonaar-music-public.js?ver=4.7
|  - http://192.168.27.5/wp-content/plugins/mp3-music-player-by-sonaar/public/js/iron-audioplayer/iron-audioplayer.js?ver=4.7
| Confirmed By:
|  Readme - Stable Tag (Aggressive Detection)
|   - http://192.168.27.5/wp-content/plugins/mp3-music-player-by-sonaar/README.txt
|  Readme - ChangeLog Section (Aggressive Detection)
|   - http://192.168.27.5/wp-content/plugins/mp3-music-player-by-sonaar/README.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 <=========================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sun Apr 13 12:58:17 2025
[+] Requests Done: 188
[+] Cached Requests: 5
[+] Data Sent: 45.966 KB
[+] Data Received: 22.321 MB
[+] Memory used: 275.098 MB
[+] Elapsed time: 00:00:04
```

Exploitation

An attacker would be able to look up the plugin version from the WPScan for potential exploits. They would find the one I implemented at this url: http://192.168.27.5/index.php/album_slug/musicpage/ The vulnerability is in the comment section under the uploaded playlist. This is where a user can exploit XXS by commenting in my example “<script> alert (“XSS”) </script>”.

This is what the exploit looks like: