pspspsps-ctf / writeups

Code · Issues · Pull requests · Actions · Projects · Security · Insights

Files

main

Go to file

- 2024/0xL4ugh CTF 2024
  - Forensics/Wordpress
    - 1
    - 2
      - 2_1.png
      - 2_2.png
      - 2_3.png
      - 2_4.png
      - 2_5.png
      - 2_6.png
      - 2_7.png

writeups / 2024 / 0xL4ugh CTF 2024 / Forensics / Wordpress / 2 /

Add file

chonkyNyan Add writeups for 0xL4ugh CTF 2024 · c708982 · last week · History

Name	Last commit message	Last commit date
..		
2_1.png	Add writeups for 0xL4ugh CTF 2024	last week
2_2.png	Add writeups for 0xL4ugh CTF 2024	last week
2_3.png	Add writeups for 0xL4ugh CTF 2024	last week
2_4.png	Add writeups for 0xL4ugh CTF 2024	last week
2_5.png	Add writeups for 0xL4ugh CTF 2024	last week
2_6.png	Add writeups for 0xL4ugh CTF 2024	last week
2_7.png	Add writeups for 0xL4ugh CTF 2024	last week
2_7.png	Add writeups for 0xL4ugh CTF 2024	last week
2_8.png	Add writeups for 0xL4ugh CTF 2024	last week
2_9.png	Add writeups for 0xL4ugh CTF 2024	last week
readme.md	Add writeups for 0xL4ugh CTF 2024	last week

readme.md

WordPress - 2

[Medium]

Same file from WordPress - 1

Q1. During enumeration, the attacker tried to identify users on the site. List all the users that the attacker enumerated. Seperate them with `:`. Sort them by alphabetical order.

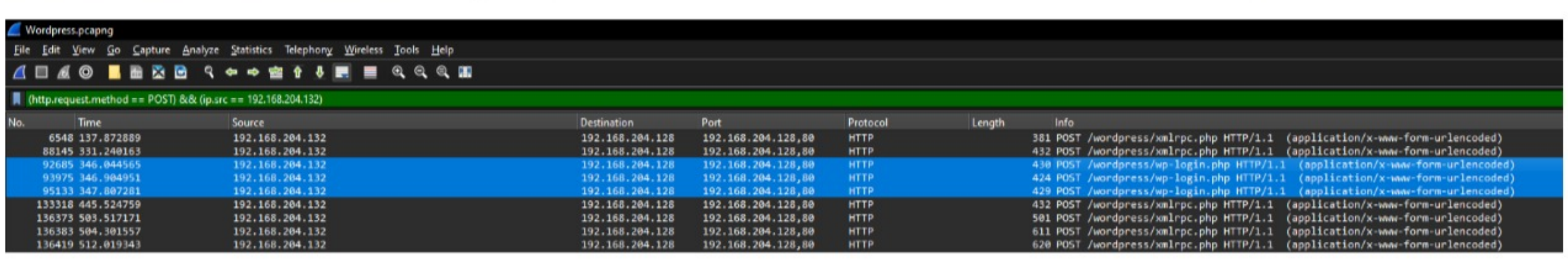
Q2. After enumeration, a brute force attack was launched against all users. The attacker successfully gained access to one of the accounts. What are the username and password for that account, and what is the name of the page used for the brute force attack?

Flag Format `0xL4ugh{A1_A2}`

Example: `0xL4ugh{username1:username2_username:password_pageName.ext}`

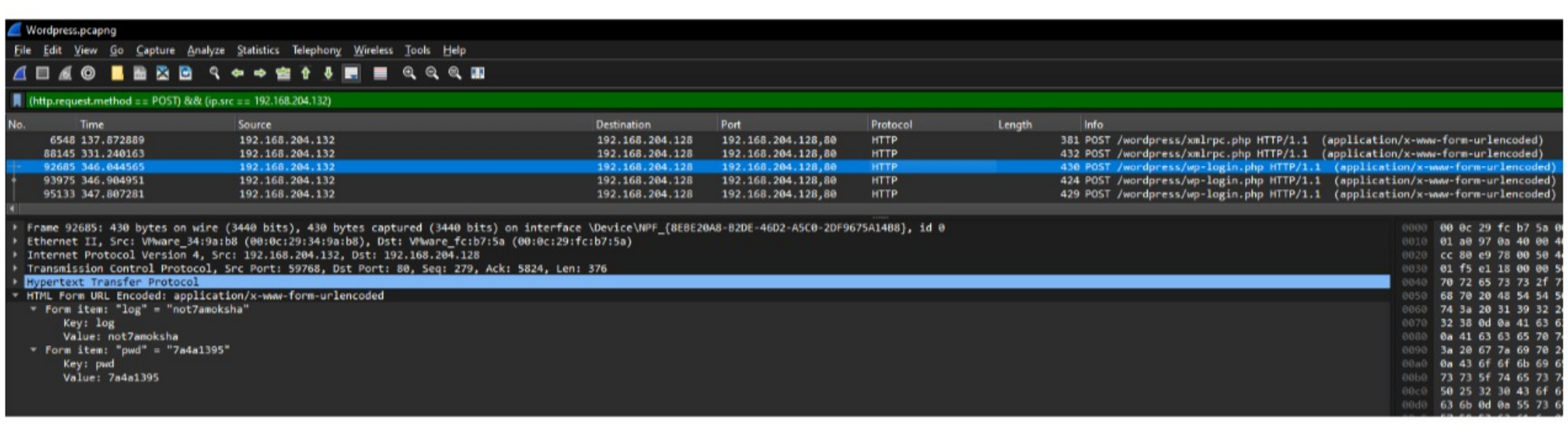
Solution:

I decided to check if the attacker tried to login via `(http.request.method == POST) && (ip.src == 192.168.204.132)`

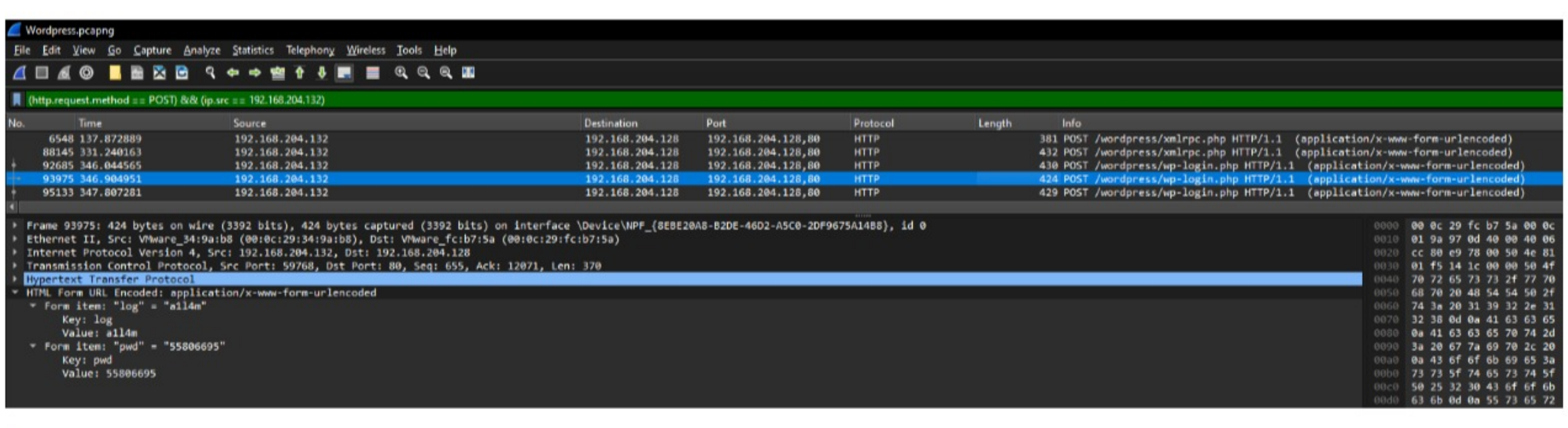

Wordpress.pcapng

```
(http.request.method == POST) && (ip.src == 192.168.204.132)
No.     Time        Source           Destination      Port                Protocol  Length  Info
  6548 137.872889   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      381 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
 88145 331.240163   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      432 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
 92685 346.044565   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      430 POST /wordpress/wp-login.php HTTP/1.1  (application/x-www-form-urlencoded)
 93975 346.904951   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      424 POST /wordpress/wp-login.php HTTP/1.1  (application/x-www-form-urlencoded)
 95133 347.807281   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      429 POST /wordpress/wp-login.php HTTP/1.1  (application/x-www-form-urlencoded)
133318 445.524759   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      432 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136373 503.517171   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      501 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136383 504.301557   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      611 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136419 512.019343   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      620 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
```

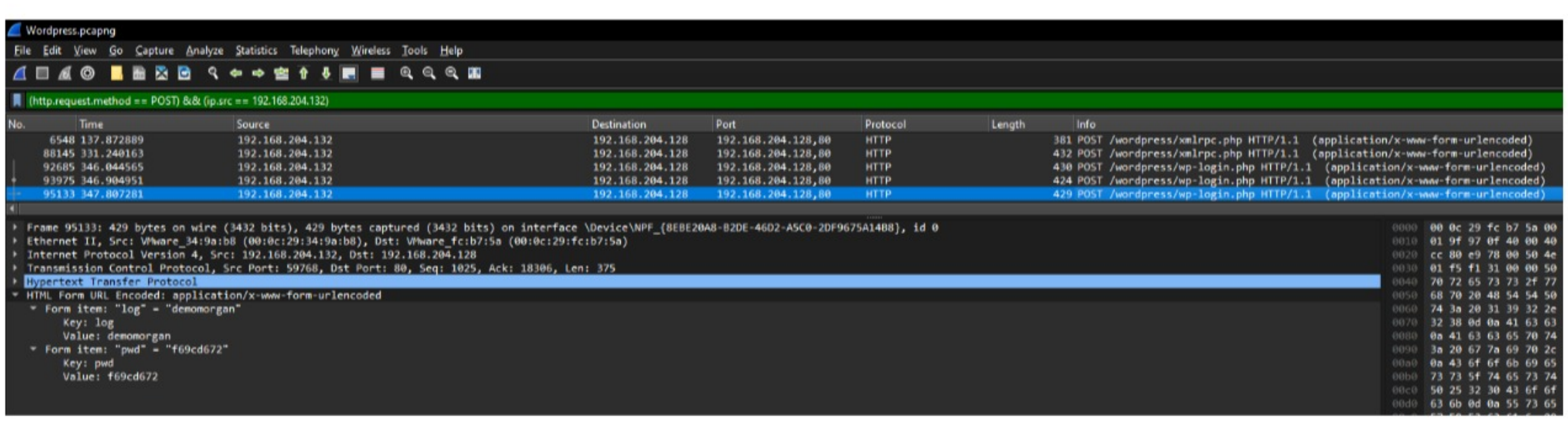
We have three attempts!


Wordpress.pcapng

```
(http.request.method == POST) && (ip.src == 192.168.204.132)
Frame 92685: 430 bytes on wire (3440 bits), 430 bytes captured (3440 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: 59768, Dst Port: 80, Seq: 279, Ack: 5824, Len: 376
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "log" = "not7amoksha"
    Key: log
    Value: not7amoksha
  Form item: "pwd" = "7a4a1395"
    Key: pwd
    Value: 7a4a1395
```


Wordpress.pcapng

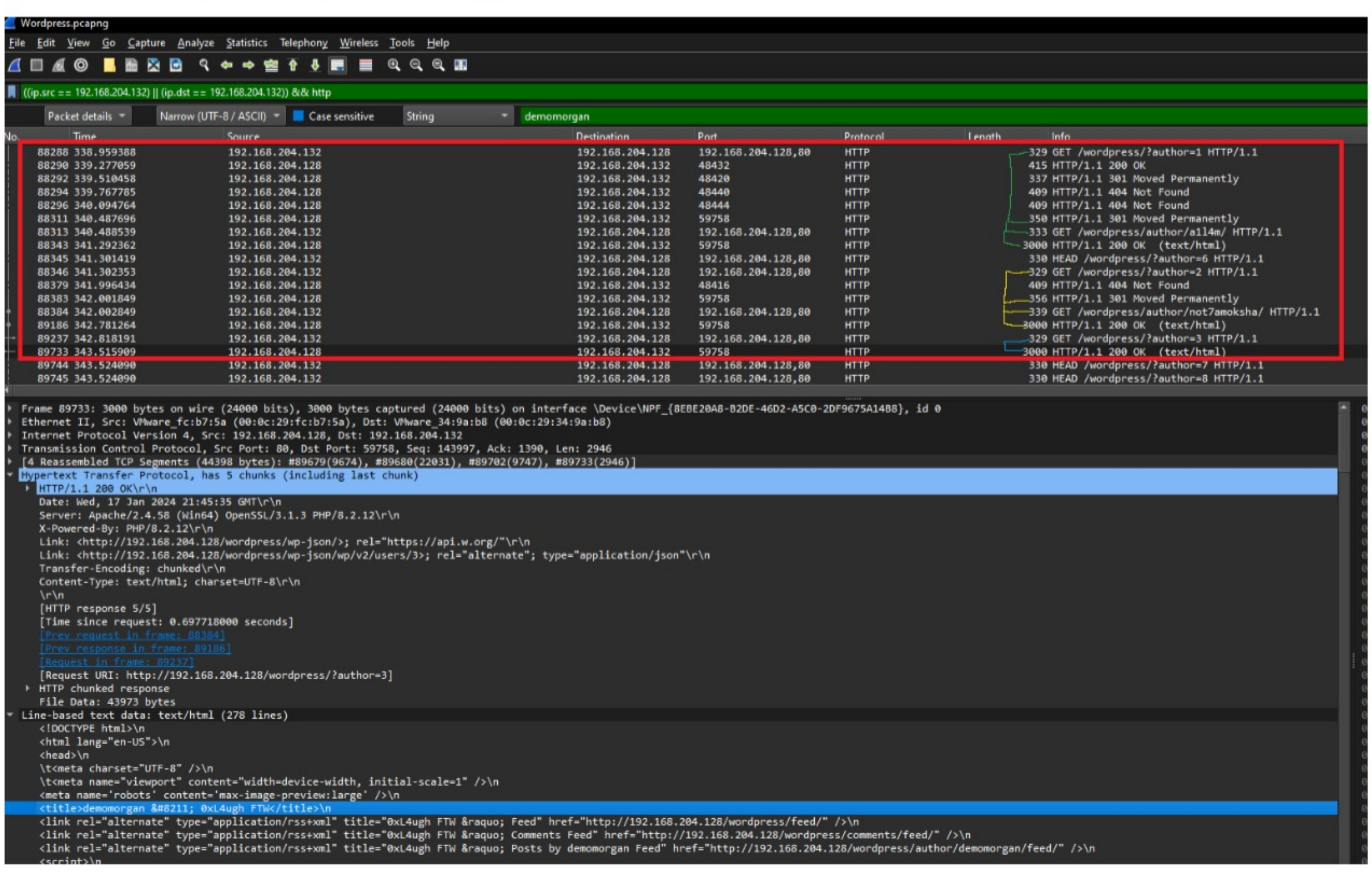
```
Frame 93975: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits) on interface \Device\NPF_{8EBE20A8-B2DE-46D2-A5C0-2DF9675A14B8}, id 0
Ethernet II, Src: VMware_34:9a:b8 (00:0c:29:34:9a:b8), Dst: VMware_fc:b7:5a (00:0c:29:fc:b7:5a)
Internet Protocol Version 4, Src: 192.168.204.132, Dst: 192.168.204.128
Transmission Control Protocol, Src Port: 59768, Dst Port: 80, Seq: 655, Ack: 12071, Len: 370
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "log" = "a114m"
    Key: log
    Value: a114m
  Form item: "pwd" = "55806695"
    Key: pwd
    Value: 55806695
```


Wordpress.pcapng

```
Frame 95133: 429 bytes on wire (3432 bits), 429 bytes captured (3432 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: 59768, Dst Port: 80, Seq: 1025, Ack: 18306, Len: 375
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "log" = "demomorgan"
    Key: log
    Value: demomorgan
  Form item: "pwd" = "f69cd672"
    Key: pwd
    Value: f69cd672
```

Double-checked via `((ip.src == 192.168.204.132) || (ip.dst == 192.168.204.132)) && http` as well...

We can see that it was able to query those three authors.


Wordpress.pcapng

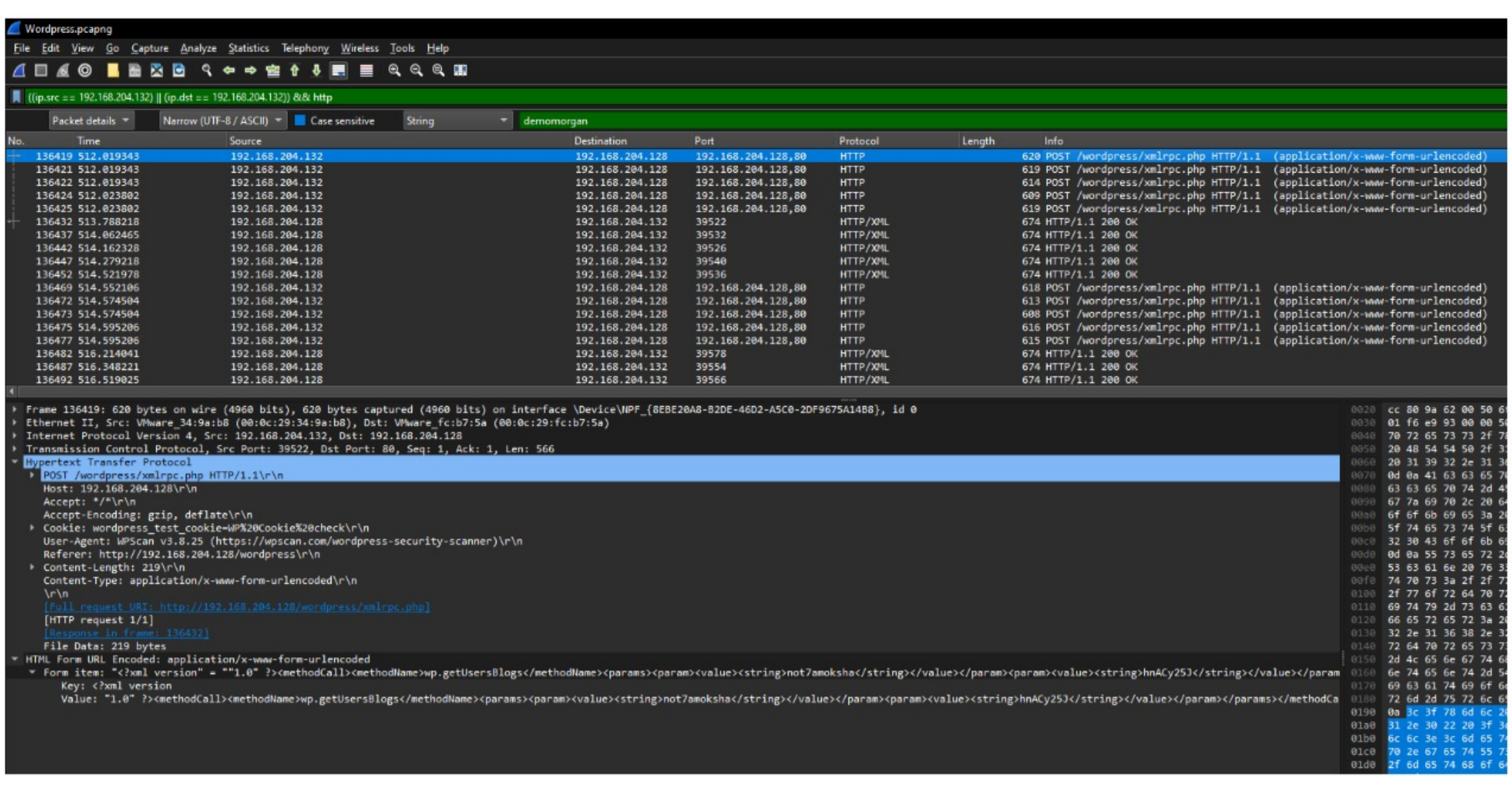
```
((ip.src == 192.168.204.132) || (ip.dst == 192.168.204.132)) && http
Packet details   Narrow (UTF-8 / ASCII)   Case sensitive   String   demomorgan
No.     Time        Source           Destination      Port                Protocol  Length  Info
 88288 338.959388   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      329 GET /wordpress/?author=1 HTTP/1.1
 88290 339.277059   192.168.204.128  192.168.204.132  48432               HTTP      415 HTTP/1.1 200 OK
 88292 339.510458   192.168.204.128  192.168.204.132  48420               HTTP      337 HTTP/1.1 301 Moved Permanently
 88294 339.767785   192.168.204.128  192.168.204.132  48440               HTTP      409 HTTP/1.1 404 Not Found
 88296 340.094764   192.168.204.128  192.168.204.132  48444               HTTP      409 HTTP/1.1 404 Not Found
 88311 340.487696   192.168.204.128  192.168.204.132  59758               HTTP      350 HTTP/1.1 301 Moved Permanently
 88313 340.488539   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      333 GET /wordpress/author/a114m/ HTTP/1.1
 88343 341.292362   192.168.204.128  192.168.204.132  59758               HTTP      3000 HTTP/1.1 200 OK  (text/html)
 88345 341.301419   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      330 HEAD /wordpress/?author=6 HTTP/1.1
 88346 341.302353   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      329 GET /wordpress/?author=2 HTTP/1.1
 88379 341.996434   192.168.204.128  192.168.204.132  48416               HTTP      409 HTTP/1.1 404 Not Found
 88383 342.001849   192.168.204.128  192.168.204.132  59758               HTTP      356 HTTP/1.1 301 Moved Permanently
 88384 342.002849   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      339 GET /wordpress/author/not7amoksha/ HTTP/1.1
 89186 342.781264   192.168.204.128  192.168.204.132  59758               HTTP      3000 HTTP/1.1 200 OK  (text/html)
 89237 342.818191   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      329 GET /wordpress/?author=3 HTTP/1.1
 89733 343.515909   192.168.204.128  192.168.204.132  59758               HTTP      3000 HTTP/1.1 200 OK  (text/html)
 89744 343.524090   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      330 HEAD /wordpress/?author=7 HTTP/1.1
 89745 343.524090   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      330 HEAD /wordpress/?author=8 HTTP/1.1

Frame 89733: 3000 bytes on wire (24000 bits), 3000 bytes captured (24000 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_34:9a:b8 (00:0c:29:34:9a:b8)
Internet Protocol Version 4, Src: 192.168.204.128, Dst: 192.168.204.132
Transmission Control Protocol, Src Port: 80, Dst Port: 59758, Seq: 143997, Ack: 1390, Len: 2946
[4 Reassembled TCP Segments (44398 bytes): #89679(9674), #89680(22031), #89702(9747), #89733(2946)]
Hypertext Transfer Protocol, has 5 chunks (including last chunk)
  HTTP/1.1 200 OK\r\n
  Date: Wed, 17 Jan 2024 21:45:35 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
  Link: <http://192.168.204.128/wordpress/wp-json/>; rel="https://api.w.org/"\r\n
  Link: <http://192.168.204.128/wordpress/wp-json/wp/v2/users/3>; rel="alternate"; type="application/json"\r\n
  Transfer-Encoding: chunked\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 5/5]
  [Time since request: 0.697718000 seconds]
  [Prev request in frame: 88384]
  [Prev response in frame: 89186]
  [Request in frame: 89237]
  [Request URI: http://192.168.204.128/wordpress/?author=3]
  HTTP chunked response
  File Data: 43973 bytes
Line-based text data: text/html (278 lines)
  <!DOCTYPE html>\n
  <html lang="en-US">\n
  <head>\n
  \t<meta charset="UTF-8" />\n
  \t<meta name="viewport" content="width=device-width, initial-scale=1" />\n
  <meta name='robots' content='max-image-preview:large' />\n
  <title>demomorgan &#8211; 0xL4ugh FTW</title>\n
  <link rel="alternate" type="application/rss+xml" title="0xL4ugh FTW &raquo; Feed" href="http://192.168.204.128/wordpress/feed/" />\n
  <link rel="alternate" type="application/rss+xml" title="0xL4ugh FTW &raquo; Comments Feed" href="http://192.168.204.128/wordpress/comments/feed/" />\n
  <link rel="alternate" type="application/rss+xml" title="0xL4ugh FTW &raquo; Posts by demomorgan Feed" href="http://192.168.204.128/wordpress/author/demomorgan/feed/" />\n
```

So it's `a114m:demomorgan:not7amoksha`

For Q2, I decided to continue with `((ip.src == 192.168.204.132) || (ip.dst == 192.168.204.132)) && http`

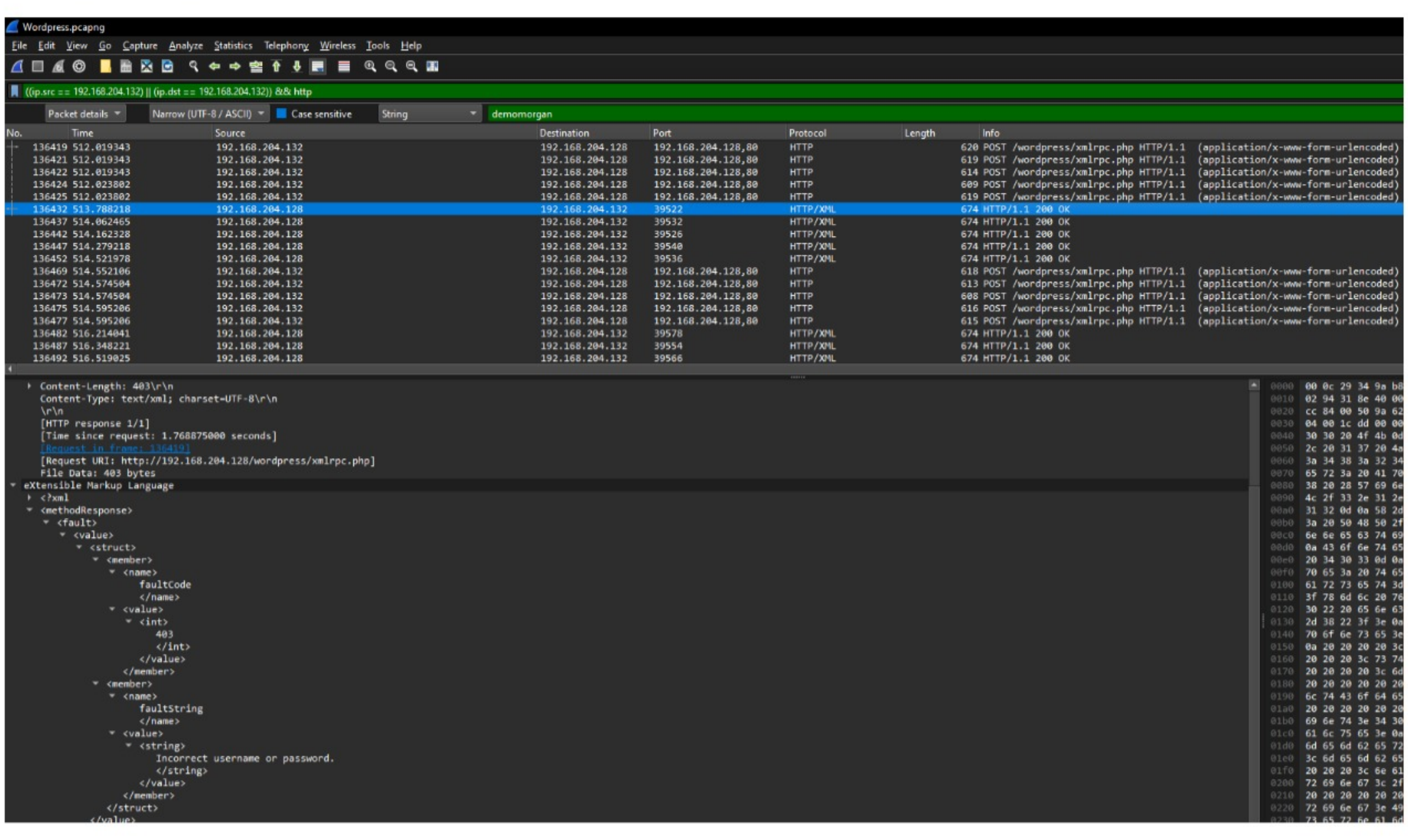
I noticed several POST requests to `/wordpress/xmlrpc.php`

Example, packet 136419, invokes `wp.getUsersBlogs` with two parameters, the username (in this case, it's `not7amoksha`), and another text which seems to be the password.


Wordpress.pcapng

```
((ip.src == 192.168.204.132) || (ip.dst == 192.168.204.132)) && http
Packet details   Narrow (UTF-8 / ASCII)   Case sensitive   String   demomorgan
No.     Time        Source           Destination      Port                Protocol  Length  Info
136419 512.019343   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      620 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136421 512.019343   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      619 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136422 512.019343   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      614 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136424 512.023802   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      609 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136425 512.023802   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      619 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136432 513.788218   192.168.204.128  192.168.204.132  39522               HTTP/XML  674 HTTP/1.1 200 OK
136437 514.062465   192.168.204.128  192.168.204.132  39532               HTTP/XML  674 HTTP/1.1 200 OK
136442 514.162328   192.168.204.128  192.168.204.132  39526               HTTP/XML  674 HTTP/1.1 200 OK
136447 514.279218   192.168.204.128  192.168.204.132  39540               HTTP/XML  674 HTTP/1.1 200 OK
136452 514.521978   192.168.204.128  192.168.204.132  39536               HTTP/XML  674 HTTP/1.1 200 OK
136469 514.552106   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      618 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136472 514.574504   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      613 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136473 514.574504   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      608 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136475 514.595206   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      616 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136477 514.595206   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      615 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136482 516.214041   192.168.204.128  192.168.204.132  39578               HTTP/XML  674 HTTP/1.1 200 OK
136487 516.348221   192.168.204.128  192.168.204.132  39554               HTTP/XML  674 HTTP/1.1 200 OK
136492 516.519025   192.168.204.128  192.168.204.132  39566               HTTP/XML  674 HTTP/1.1 200 OK

Frame 136419: 620 bytes on wire (4960 bits), 620 bytes captured (4960 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: 39522, Dst Port: 80, Seq: 1, Ack: 1, Len: 566
Hypertext Transfer Protocol
  POST /wordpress/xmlrpc.php HTTP/1.1\r\n
  Host: 192.168.204.128\r\n
  Accept: */*\r\n
  Accept-Encoding: gzip, deflate\r\n
  Cookie: wordpress_test_cookie=WP%20Cookie%20check\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
  Content-Length: 219\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
  \r\n
  [Full request URI: http://192.168.204.128/wordpress/xmlrpc.php]
  [HTTP request 1/1]
  [Response in frame: 136432]
  File Data: 219 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "<?xml version" = ""1.0" ?><methodCall><methodName>wp.getUsersBlogs</methodName><params><param><value><string>not7amoksha</string></value></param><param><value><string>hnACy25J</string></value></param
    Key: <?xml version
    Value: "1.0" ?><methodCall><methodName>wp.getUsersBlogs</methodName><params><param><value><string>not7amoksha</string></value></param><param><value><string>hnACy25J</string></value></param></params></methodCa
```

Looking at the response...

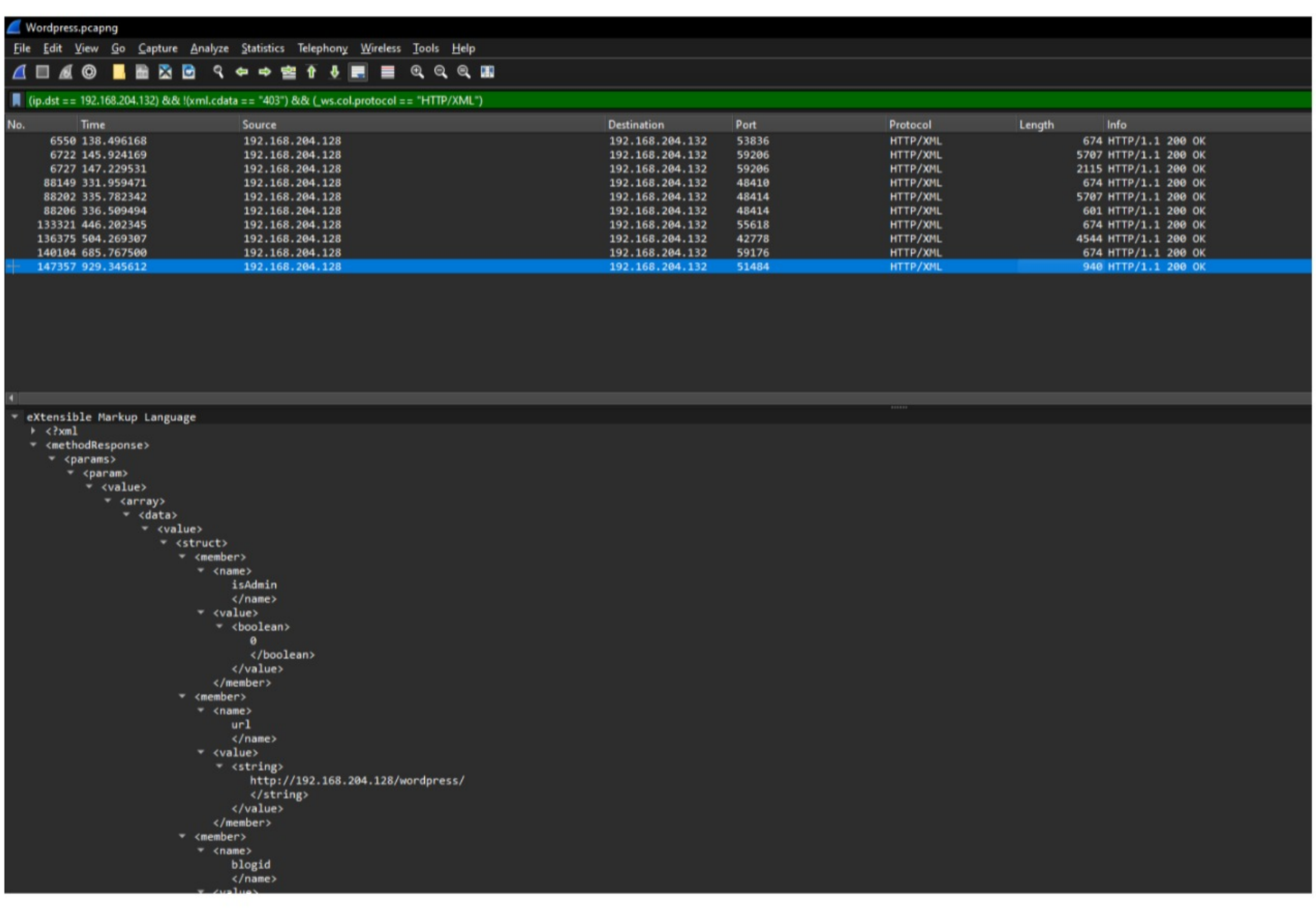

Wordpress.pcapng

```
((ip.src == 192.168.204.132) || (ip.dst == 192.168.204.132)) && http
Packet details   Narrow (UTF-8 / ASCII)   Case sensitive   String   demomorgan
No.     Time        Source           Destination      Port                Protocol  Length  Info
136419 512.019343   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      620 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136421 512.019343   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      619 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136422 512.019343   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      614 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136424 512.023802   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      609 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136425 512.023802   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      619 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136432 513.788218   192.168.204.128  192.168.204.132  39522               HTTP/XML  674 HTTP/1.1 200 OK
136437 514.062465   192.168.204.128  192.168.204.132  39532               HTTP/XML  674 HTTP/1.1 200 OK
136442 514.162328   192.168.204.128  192.168.204.132  39526               HTTP/XML  674 HTTP/1.1 200 OK
136447 514.279218   192.168.204.128  192.168.204.132  39540               HTTP/XML  674 HTTP/1.1 200 OK
136452 514.521978   192.168.204.128  192.168.204.132  39536               HTTP/XML  674 HTTP/1.1 200 OK
136469 514.552106   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      618 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136472 514.574504   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      613 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136473 514.574504   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      608 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136475 514.595206   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      616 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136477 514.595206   192.168.204.132  192.168.204.128  192.168.204.128,80  HTTP      615 POST /wordpress/xmlrpc.php HTTP/1.1  (application/x-www-form-urlencoded)
136482 516.214041   192.168.204.128  192.168.204.132  39578               HTTP/XML  674 HTTP/1.1 200 OK
136487 516.348221   192.168.204.128  192.168.204.132  39554               HTTP/XML  674 HTTP/1.1 200 OK
136492 516.519025   192.168.204.128  192.168.204.132  39566               HTTP/XML  674 HTTP/1.1 200 OK

  Content-Length: 403\r\n
  Content-Type: text/xml; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 1.768875000 seconds]
  [Request in frame: 136419]
  [Request URI: http://192.168.204.128/wordpress/xmlrpc.php]
  File Data: 403 bytes
eXtensible Markup Language
  <?xml
  <methodResponse>
    <fault>
      <value>
        <struct>
          <member>
            <name>
              faultCode
              </name>
            <value>
              <int>
                403
                </int>
              </value>
            </member>
          <member>
            <name>
              faultString
              </name>
            <value>
              <string>
                Incorrect username or password.
                </string>
              </value>
            </member>
          </struct>
        </value>
```

The second parameter is indeed a password! Searching via the documentation also confirms it. https://developer.wordpress.org/reference/classes/wp_xmlrpc_server/wp_getusersblogs/

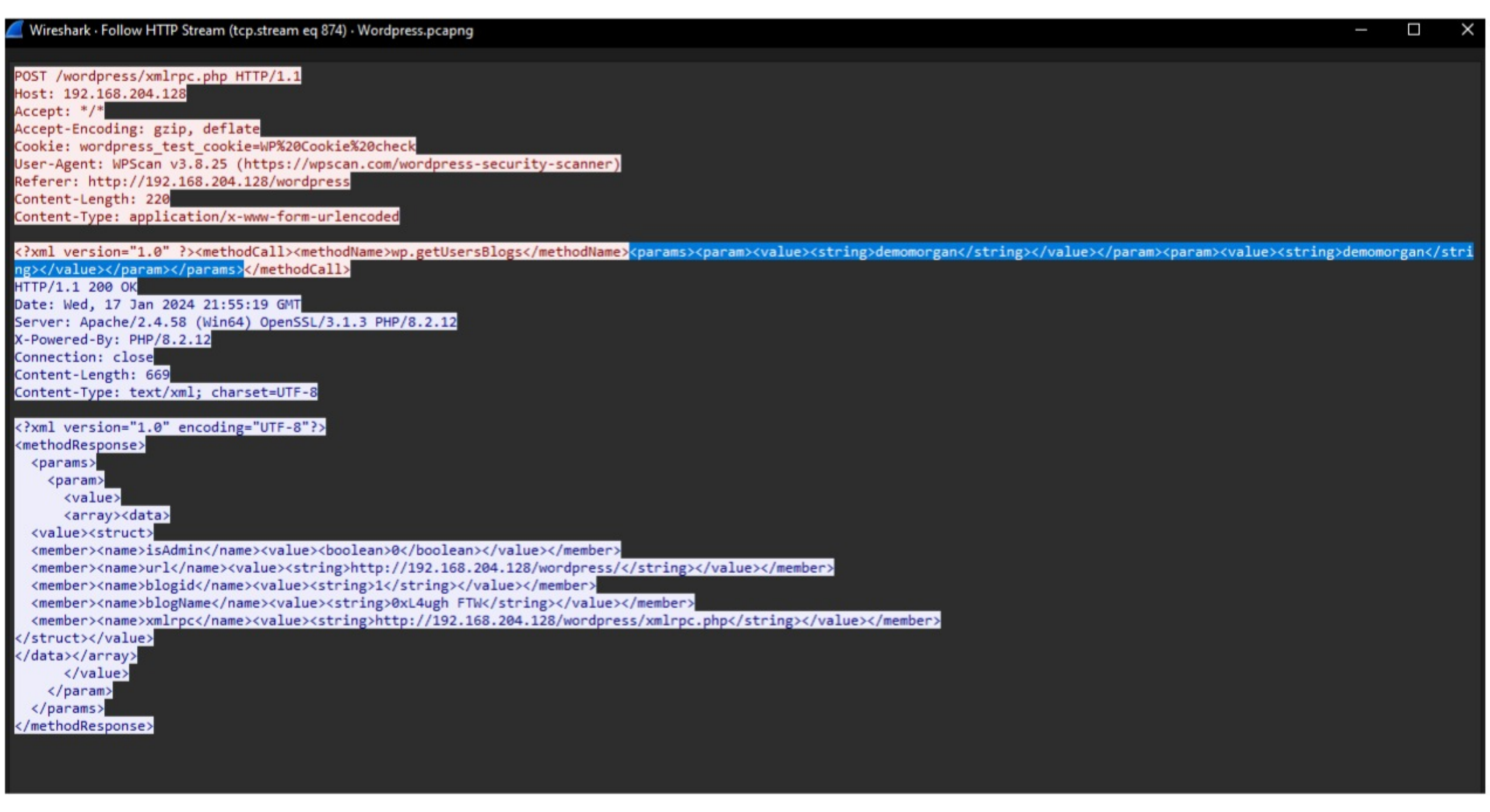
Now let's look for a successful request that doesn't return a 403.

Let's use `(ip.dst == 192.168.204.132) && !(xml.cdata == "403") && (_ws.col.protocol == "HTTP/XML")`


Wordpress.pcapng

```
(ip.dst == 192.168.204.132) && !(xml.cdata == "403") && (_ws.col.protocol == "HTTP/XML")
No.     Time        Source           Destination      Port   Protocol  Length  Info
  6550 138.496168   192.168.204.128  192.168.204.132  53836  HTTP/XML   674 HTTP/1.1 200 OK
  6722 145.924169   192.168.204.128  192.168.204.132  59206  HTTP/XML  5707 HTTP/1.1 200 OK
  6727 147.229531   192.168.204.128  192.168.204.132  59206  HTTP/XML  2115 HTTP/1.1 200 OK
 88149 331.959471   192.168.204.128  192.168.204.132  48410  HTTP/XML   674 HTTP/1.1 200 OK
 88202 335.782342   192.168.204.128  192.168.204.132  48414  HTTP/XML  5707 HTTP/1.1 200 OK
 88206 336.509494   192.168.204.128  192.168.204.132  48414  HTTP/XML   601 HTTP/1.1 200 OK
133321 446.202345   192.168.204.128  192.168.204.132  55618  HTTP/XML   674 HTTP/1.1 200 OK
136375 504.269307   192.168.204.128  192.168.204.132  42778  HTTP/XML  4544 HTTP/1.1 200 OK
140104 685.767500   192.168.204.128  192.168.204.132  59176  HTTP/XML   674 HTTP/1.1 200 OK
147357 929.345612   192.168.204.128  192.168.204.132  51484  HTTP/XML   940 HTTP/1.1 200 OK

eXtensible Markup Language
  <?xml
  <methodResponse>
    <params>
      <param>
        <value>
          <array>
            <data>
              <value>
                <struct>
                  <member>
                    <name>
                      isAdmin
                      </name>
                    <value>
                      <boolean>
                        0
                        </boolean>
                      </value>
                    </member>
                  <member>
                    <name>
                      url
                      </name>
                    <value>
                      <string>
                        http://192.168.204.128/wordpress/
                        </string>
                      </value>
                    </member>
                  <member>
                    <name>
                      blogid
                      </name>
```

There's a hit! Let's check the HTTP stream...


Wireshark · Follow HTTP Stream (tcp.stream eq 874) · Wordpress.pcapng

```
POST /wordpress/xmlrpc.php HTTP/1.1
Host: 192.168.204.128
Accept: */*
Accept-Encoding: gzip, deflate
Cookie: wordpress_test_cookie=WP%20Cookie%20check
User-Agent: WPScan v3.8.25 (https://wpscan.com/wordpress-security-scanner)
Referer: http://192.168.204.128/wordpress
Content-Length: 220
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" ?><methodCall><methodName>wp.getUsersBlogs</methodName><params><param><value><string>demomorgan</string></value></param><param><value><string>demomorgan</string></value></param></params></methodCall>
HTTP/1.1 200 OK
Date: Wed, 17 Jan 2024 21:55:19 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Connection: close
Content-Length: 669
Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <params>
    <param>
      <value>
      <array><data>
  <value><struct>
  <member><name>isAdmin</name><value><boolean>0</boolean></value></member>
  <member><name>url</name><value><string>http://192.168.204.128/wordpress/</string></value></member>
  <member><name>blogid</name><value><string>1</string></value></member>
  <member><name>blogName</name><value><string>0xL4ugh FTW</string></value></member>
  <member><name>xmlrpc</name><value><string>http://192.168.204.128/wordpress/xmlrpc.php</string></value></member>
</struct></value>
</data></array>
      </value>
    </param>
  </params>
</methodResponse>
```

So it's `demomorgan:demomorgan`

For the page that was used to bruteforce, it's `xmlrpc.php`

Now we have the flag! :D

Flag: `0xL4ugh{a114m:demomorgan:not7amoksha_demomorgan:demomorgan_xmlrpc.php}`