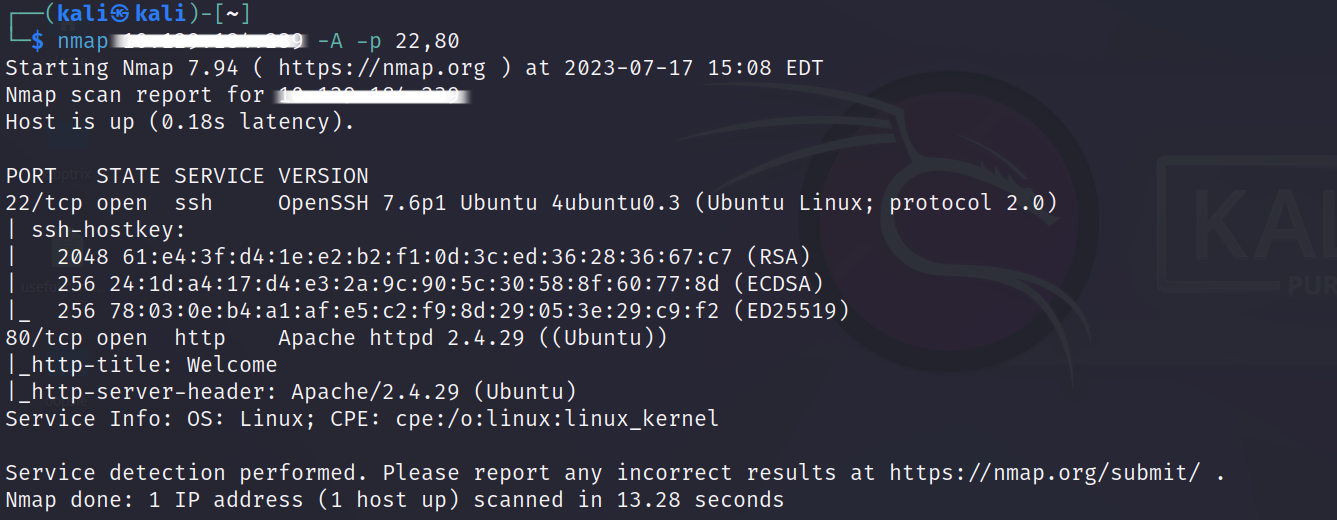
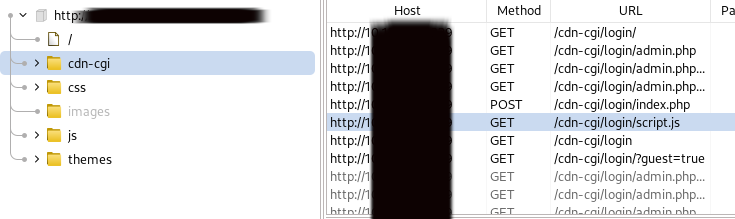
Oopsie ctf writeup

First of all I started with nmap scan.

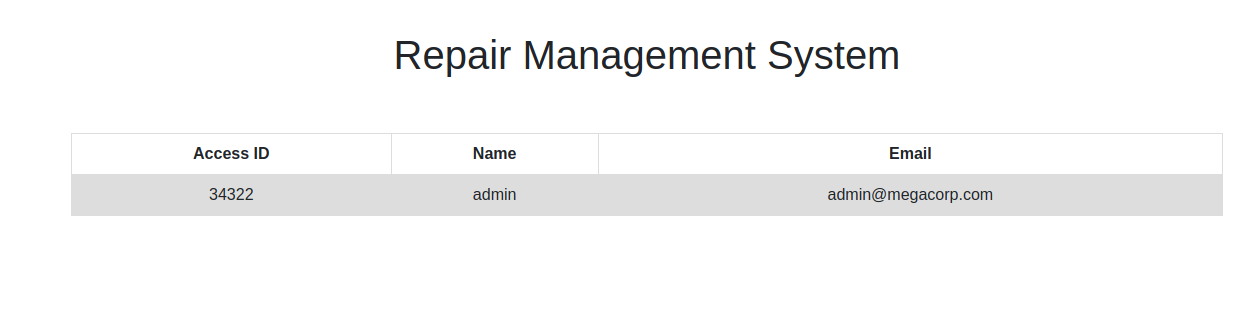


I noticed that http server is old and it might be a vulnerability inside of it. Then I started to spider website by using burpsuite.

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.

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

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



Then I modified user and role parameter.

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

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

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

After that I triggered the exploit by listening my port. metin, ekran görüntüsü içeren bir resim

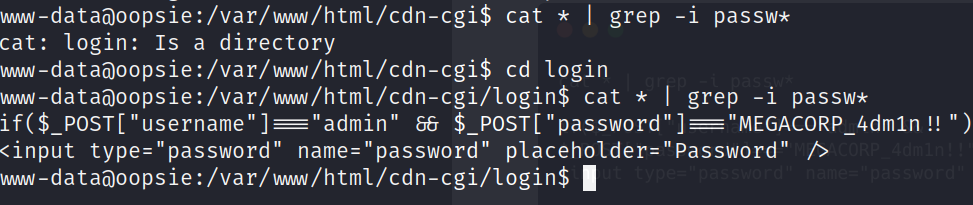
Açıklama otomatik olarak oluşturuldu

metin, yazılım, multimedya yazılımı, web sayfası içeren bir resim

Açıklama otomatik olarak oluşturuldu

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



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.

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

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

metin, ekran görüntüsü, yazı tipi, tasarım içeren bir resim

Açıklama otomatik olarak oluşturuldu

After checking robert’s privilages I noticed a group named 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.

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

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

