

Home exam

IN5290 – Ethical Hacking

Candidate: 15757



1. Information gathering (140/140p)

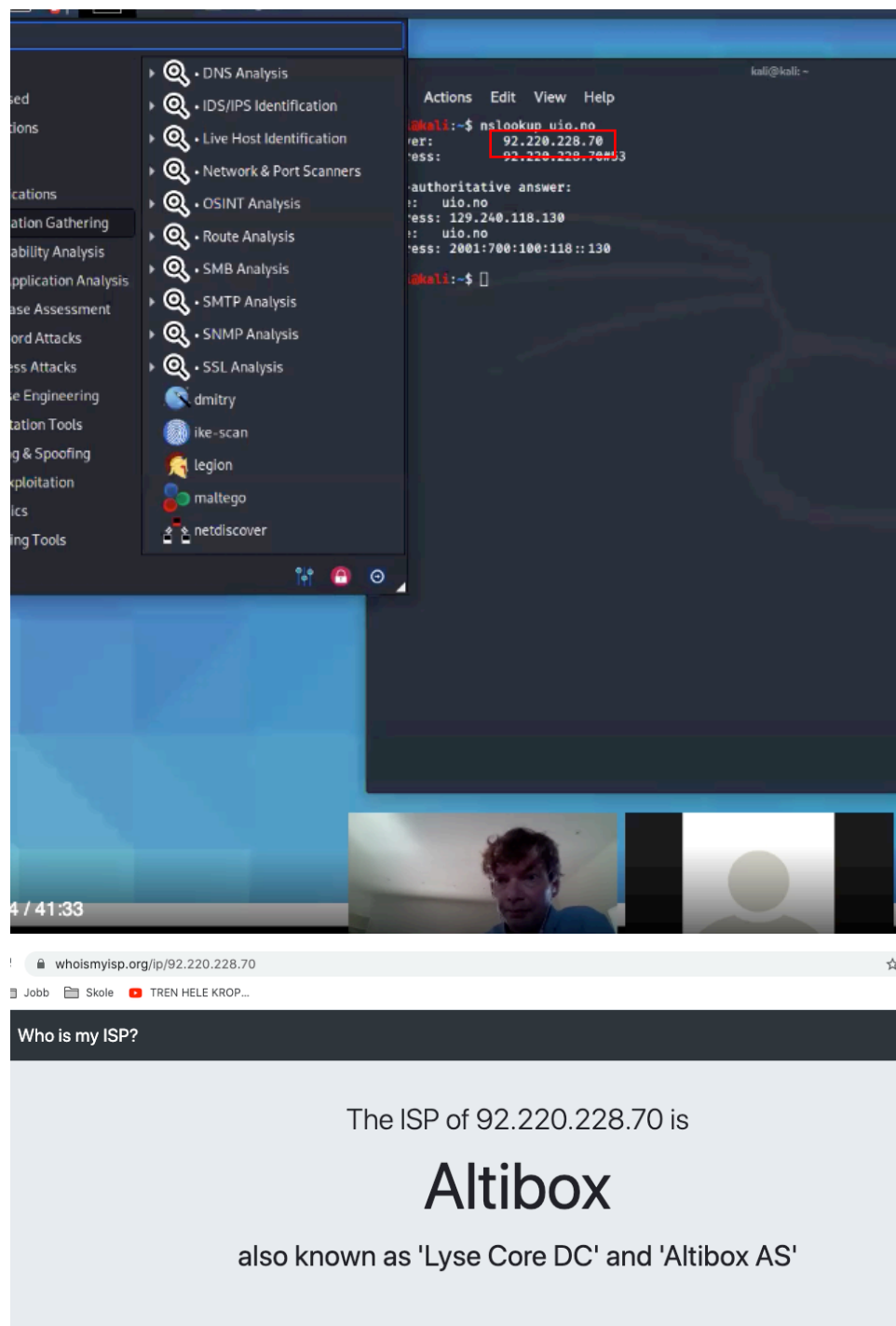
Who is my internet provider? (20)

Laszlo made a **nslookup** that showed his IP-address in lecture 2, which was:

92.220.228.70. I was able to do this task in two different ways, either go to

<https://www.whoismyip.org/> and search for the internet provider using his IP-address

or use my terminal and do a nslookup on his IP-address, **nslookup 92.220.228.70**. Both ways gave me the same internet provider and flag “**Altibox**”.



The image is a composite of three screenshots. The top-left screenshot shows a Kali Linux terminal window with a menu on the left and a terminal window on the right. The terminal window shows the command `nslookup uio.no` being executed, with the IP address `92.220.228.70` highlighted in red. The top-right screenshot shows a web browser window with the address bar displaying `whoismyip.org/ip/92.220.228.70`. The main content of the browser shows the text "Who is my ISP?" followed by "The ISP of 92.220.228.70 is" and "Altibox" in large font, with "also known as 'Lyse Core DC' and 'Altibox AS'" below it. The bottom screenshot shows a video call interface with a person's face in the center and a placeholder for another participant on the right.

```

cm-84:~ pilasilda$ nslookup 92.220.228.70
Server:      84.208.20.110
Address:     84.208.20.110#53

Non-authoritative answer:
70.228.220.92.in-addr.arpa      name = dns-site-b.altibox.no.

Authoritative answers can be found from:

cm-84:~ pilasilda$ █

```

What is the sum of their mobile numbers? - (40)

Lecture page in IN5290 Ethical Hacking gives us first name and surname of 2 teacher assistants and the PhD student. I assumed that all of them are IFI-students therefore I visited <https://www.mn.uio.no/ifi/> and searched for Humza Ahmad. I got one hit with his first name and surname. Thereafter I went to <https://www.gulesider.no/> and searched for Humza Ahmad. I got several hits here, but only one hit with the same name combination that I found on the UiO-page. I Therefore assumed that this would be his phone number. I followed the same steps for finding Tamas's phone number. It was a bit more difficult to find the phone number of André. But I used the same method as over, went to the UiO-page and searched for André. I got several hits here, but only two of them matched the preferences (being an IFI-student and having André in his full name). I so on went to google searched for Lidre, Philip André Augestad which where one of the hits on the UiO page. The search gave me a hit, and it was his LinkedIn page. His profile on LinkedIn gave me information about him being a teaching assistant at UiO for Ethical Hacking and it also gave me his phone number. At the end the lecturer's phone number, first I searched for his name on UiO-page but couldn't find the phone number there. Searched for his name on google and found his phone number at <https://www.oslomet.no/om/ansatt/laszloer/>. At the end I summed up all the phone numbers: $40724331 + 45263138 + 911\ 48\ 827 + 465\ 27\ 815 = 223664111$


UiO : Institutt for informatikk
 Det matematisk-naturvitenskapelige fakultet

[Forsiden IFI](#)
[Forskning](#)
[Studier](#)
[Livet rundt studiene](#)
[Tjenester og verktøy](#)
[Om instituttet](#)
[Personer](#)

Søk etter personer

Navn	Telefon	E-post	Emneord
 Ahmad, Humza Undyp u/gdkj.ped.utd		humzaa @ifi.uio.no	

[Alt innhold](#)
[Personer](#)
[Enheter](#)
[Bibliotek](#)
[Teknisk/administrativt ansatte](#)
[Alle personer](#)
[Studenter](#)

[Firma \(0\)](#)
[Personer \(15\)](#)

[I nærheten](#)

humza ahmad ga 15 personer

Humza Ahmad
 Olav M. Troviks vei 46
 0864 Oslo
 465 27 ...

Abdulrahman Ahmad Hamza
 Jernbanegata 33C
 8250 Rognan
 909 49 ...

Ahmad Mohammad Hamza
 Skogveien 35
 8250 Rognan
 462 17 ...

Amal Ahmad Hamza
 Åsenveien 54A
 1400 Ski
 455 72 ...


UiO : Institutt for informatikk
 Det matematisk-naturvitenskapelige fakultet

[Forsiden IFI](#)
[Forskning](#)
[Studier](#)
[Livet rundt studiene](#)
[Tjenester og verktøy](#)
[Om instituttet](#)
[Personer](#)

Søk etter personer

Navn	Telefon	E-post	Emneord
 Bisztray, Tamas Stipendiat		tamasbi @ifi.uio.no	

[Alt innhold](#)
[Personer](#)
[Enheter](#)
[Bibliotek](#)
[Vitenskapelig ansatte](#)
[Studenter](#)
[Alle personer](#)

[Firma \(0\)](#)
[Personer \(1\)](#)

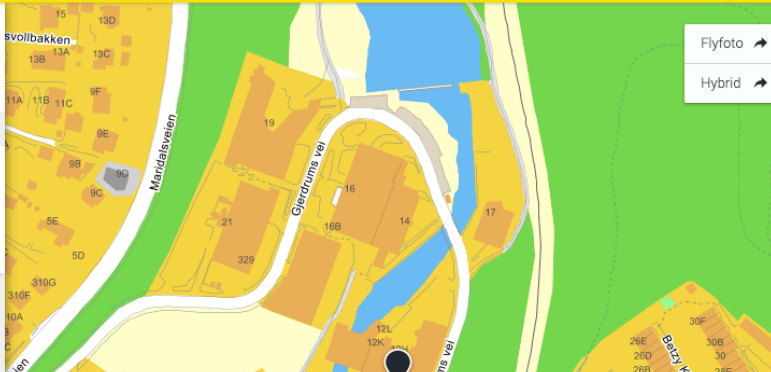
[I nærheten](#)

tamas bisztray ga 1 personer

Tamas György Bisztray
 Gjerdrums vei 12G
 0484 Oslo
 911 48 ...






Ditt søk på **tamas bisztray** ga 1 personer og du har nådd slutten av listen.

Veibeskrivelse



[Flyfoto](#)
[Hybrid](#)

GULE SIDER

André		Søk	
Navn	Telefon	E-post	Emneord
 Birkedal, Tor-André Student		torandrb @ifi.uio.no	
 Hermannrud, Joachim André Strandvåg Student		jaherman @student.mat-nat.uio.no	
 Heskja, Håkon André Undvp ulgdkj.ped.utd		haakoashe @ifi.uio.no	
 Kristensen, Kais André Student		kaisak @math.uio.no	
 Lidre, Philip André Augestad Undvp ulgdkj.ped.utd		paldre @ifi.uio.no	



Lidre, Philip André Augestad

Alle Bilder Nyheter Google Maps Shopping Mer Innstillinger Verktøy

Omtrent 1 410 resultater (0,33 sekunder)

no.linkedin.com › andrelidre

Philip André Augestad Lidre - Service Desk Technician - Telia ...

Philip André Augestad Lidre. Master of Science - MS at University of Oslo (UiO). Telia Norge University of Oslo (UiO). Oslo, Oslo, Norway 179 forbindelser.

Du har besøkt denne siden 2 ganger. Siste besøk: 02.09.20

Om

Programmer with a strong passion to learn about anything that is related to computers. I have a BSc in programming and networks, and are currently working on my masters degree in information security. For inquiries, contact me at 45263138.

Erfaring



Teaching Assistant

University of Oslo (UiO) · Deltid

aug. 2020 - nå · 2 md

Oslo, Norway

Group teacher in IN5290 - Ethical Hacking



laszlo erdodi

Alle Bilder Nyheter Google Maps Videoer Mer Innstillinger Verkt

Omtrent 11 700 resultater (0,40 sekunder)

Tips: Bare søk etter norske resultater. Du kan spesifisere søkespråket ditt i Innstillinger

www.mn.uio.no › ifi › personer › vit › laszloe

Laszlo Erdodi - Institutt for informatikk

13. mai 2019 - Erdodi, Laszlo & Jesang, Audun (2017). Exploit prevention, quo vadis?. Lecture Notes in Computer Science (LNCS). ISSN 0302-9743.

Du har besøkt denne siden 4 ganger. Siste besøk: 01.09.20

www.mn.uio.no › ifi › aca › laszloe

Laszlo Erdodi - Department of Informatics - UiO

8. mai 2017 - L Erdodi, A Jesang. Exploit Prevention, Quo Vadis?. Proceedings of the 13th International Workshop on Security and Trust Management (STM ...

Du har besøkt denne siden 2 ganger. Siste besøk: 01.09.20

www.oslomet.no › ansatt › laszloe

Laszlo Erdodi - OsloMet

Laszlo Erdodi. Stillingstittel. Førsteamanuensis. Besøksadresse. Pilestredet 35, 0166 Oslo; Kontonummer ...

Du har besøkt denne siden mange ganger. Siste besøk: 04.09.20



Laszlo Erdodi

Stillingstittel
Førsteamanuensis

Besøksadresse
Pilestredet 35, 0166 Oslo
Kontonummer: PS338

Telefon
Mobil: +47 407 24 331
Kontor: +47 67 23 70 57

E-post
Laszlo.Erdodi@oslomet.no

Find the password of the mysql server on 64.227.10.191. - (40)

At first, I copied the IP-address given in the task, then I ran it in my browser, and it forwarded me to an index of page. I then I went to the ProyectoValentiApi/ folder. Went through the src/ folder, I couldn't find any interesting things there, I therefore went to the config/ folder. The config/ folder has a file named config-db.ini, I opened that file. In that file we can find the password, **15628123**.

← → ↻ Not Secure | 64.227.10.191 **Index of /ProyectoValentiApi**

Apps Jobb Skole Klær cadooz eCard

Name	Last modified	Size	Description
Parent Directory	-	-	-
composer.json	2020-01-16 21:20	1.1K	-
composer.lock	2020-01-16 21:20	83K	-
docker-compose.yml	2020-01-16 21:20	343	-
files/	2020-10-30 15:49	-	-
phpunit.xml	2020-01-16 21:20	189	-
public/	2020-01-16 21:20	-	-
src/	2020-01-16 21:20	-	-
vendor/	2020-01-16 21:20	-	-

Apache/2.4.29 (Ubuntu) Server at 64.227.10.191 Port 80

Index of /ProyectoValentiApi/srcIndex of /ProyectoValentiApi/src/config

Name	Last modified	Size	Description
Parent Directory	-	-	-
config/	2020-01-24 20:39	-	-
controller/	2020-01-16 21:20	-	-
logs/	2020-01-16 21:20	-	-
model/	2020-01-16 21:20	-	-
routes/	2020-01-23 15:04	-	-
utils/	2020-01-23 17:05	-	-

Name	Last modified	Size	Description
Parent Directory	-	-	-
config-db.ini	2020-01-16 21:20	100	-
db.php	2020-01-16 21:20	4.1K	-
settings.php	2020-01-16 21:20	576	-
valenti.sql	2020-01-16 21:20	9.9K	-

Apache/2.4.29 (Ubuntu) Server at 64.227.10.191 Port 80

Apps Jobb Skole

```

driver = mysql
host = 64.227.10.191
port = 3306
user = backend
name = Valenti
password = "15628123"

```

Find the mysql password of vistaweb.co.uk. (40)

Searched site: “vistaweb.co.uk” intitle: “index of” in my browser. The first hit forwarded me to **index of page**, here the **application.ini** file contains the password and the flag for this task “**Surrey1975**”.

site:"vistaweb.co.uk" intitle:"index of"

AI

Images

Videos

News

Books

More

Settings Tools

About 894 results (0.41 seconds)

www.vistaweb.co.uk > application > configs

Index of /irmtest/application/configs

Index of /irmtest/application/configs. Icon Name Last modified Size Description. [PARENTDIR]

Parent Directory - [] application.ini 2017-01-02 03:30 3.4K.

www.vistaweb.co.uk > vendor > zendframework

Index of /zend2TestProject1/vendor/zendframework

Index of /zend2TestProject1/vendor/zendframework. Icon Name Last modified Size Description. [PARENTDIR]

Parent Directory - [DIR] zendframework/ ...

www.vistaweb.co.uk > irmtest > docs

Index of /irmtest/docs

Index of /irmtest/docs. Icon Name Last modified Size Description. [PARENTDIR]

Parent Directory -

Index of /irmtest/application/configs

Name	Last modified	Size	Description
Parent Directory	-	-	-
application.ini	2017-01-02 03:30	3.4K	

```

#####

;resources.multidb.maindb.adapter          = PDO_MYSQL
;resources.multidb.maindb.host              = localhost
;resources.multidb.maindb.username          = irmtestuser
;resources.multidb.maindb.password          = 123qwe
;resources.multidb.maindb.dbname            = test
;resources.multidb.maindb.default           = true

resources.multidb.maindb.adapter            = PDO_MYSQL
resources.multidb.maindb.host                = "mysql51-135.perso"
resources.multidb.maindb.username            = "shirefreauvista"
resources.multidb.maindb.password            = "Surrey1975"
resources.multidb.maindb.dbname              = "shirefreauvista"
resources.multidb.maindb.default              = true

;resources.multidb.maindb.driver_options.1002 = "SET NAMES 'utf8', CHARACTER SET 'utf8', time_zone = 'UTC'"

;resources.multidb.maindb.driver_options.1002 = "SET NAMES 'utf8', CHARACTER SET 'utf8', time_zone = 'UTC'"
#####

```

2. Technical information gathering (140/140p)

Find the British domain with the same mail server as flytoget.no! (30)

Searched for flytoget.no at <http://mxlookup.online-domain-tools.com/>, the result gave me a list of mail servers. Went to <https://viewdns.info/> and in the reverse mxlookup field I searched for mail.initility.com. The search gave me a long list of websites, I searched for websites with co.uk endings, it was only one hit which was which was **thepurewaterco.co.uk** which is the flag for this task.

SuperTool Beta7

MX Lookup

mx:flytoget.no

Find Problems

Solve Email Delivery Problems

mx

Pref	Hostname	IP Address	TTL		
10	mail.initility.com	137.221.26.4 Initility AS (AS49586)	5 min	Blacklist Check	SMTP Test
10	mail2.initility.com	137.221.30.4 Initility AS (AS49586)	5 min	Blacklist Check	SMTP Test

The screenshot shows the viewdns.info website with several tools available. The 'Reverse MX Lookup' tool is highlighted with a red box, showing a list of domains including 'thepurewaterco.co.uk'.

Tools available:

- Reverse IP Lookup**: Find all sites hosted on a given server.
- Reverse Whois Lookup**: Find domain names owned by an individual or company.
- IP History**: Show historical IP addresses for a domain.
- DNS Report**: Provides a complete report on your DNS settings.
- Reverse MX Lookup [NEW]**: Find all sites that use a given mail server.
- Reverse NS Lookup**: Find all sites that use a given nameserver.
- IP Location Finder**: Find the geographic location of an IP Address.
- Chinese Firewall Test**: Checks whether a site is accessible from China.
- DNS Propagation Checker**: Check whether recent DNS changes have propagated.

The 'Reverse MX Lookup' tool is currently active, showing a list of domains including 'thepurewaterco.co.uk'.

To which city do you have to travel to physically access the wikileaks.com files (if you cannot access them from Oslo)?(30)

Went to <https://whois.domaintools.com/>, searched for wikileaks.com in the search field.

The search gave me this information, I tried to enter **Victoria** as a flag and it was the correct answer.

Whois Record for WikiLeaks.com

Domain Profile

IP Address	185.165.168.41 - 2 other sites hosted on this server	➔
IP Location	🇧🇷 - Braila - Victoria - Flokinet Ltd	
ASN	🇧🇷 AS200651 FLOKINET, SC (registered May 15, 2015)	
Domain Status	Registered And Active Website	
IP History	28 changes on 28 unique IP addresses over 13 years	➔
Registrar History	2 registrars with 2 drops	➔
Hosting History	6 changes on 6 unique name servers over 13 years	➔

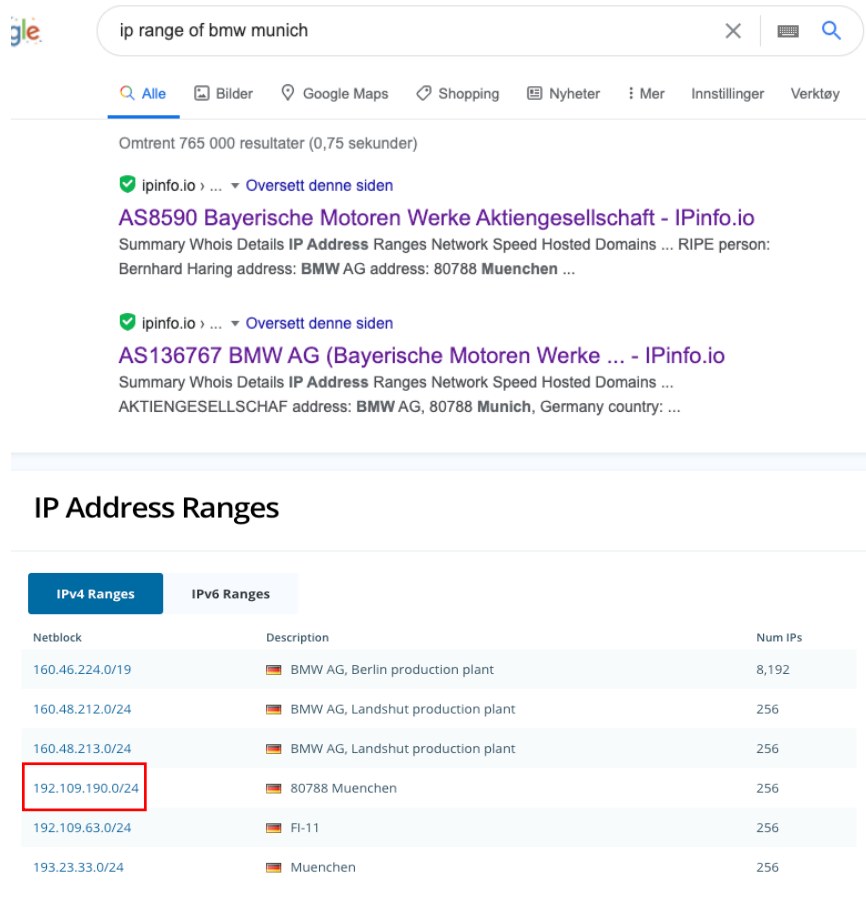
Website

Website Title	🏆 WikiLeaks	➔
Server Type	nginx	
Response Code	200	

Find the /24 network range of BMW in Munich! Write the result in CIDR format!

(40)

Searched for IP range of bmw Munich clicked on link nr one which. Forwarded me to this page. The answer is the IP range nr four in the list: **192.109.190.0/24**.



The screenshot shows a Google search for "ip range of bmw munich". The search results include two entries from IPinfo.io. The first entry is for AS8590 Bayerische Motoren Werke Aktiengesellschaft - IPinfo.io, and the second is for AS136767 BMW AG (Bayerische Motoren Werke ... - IPinfo.io. Below the search results, there is a table titled "IP Address Ranges" with two tabs: "IPv4 Ranges" and "IPv6 Ranges". The table lists several IP ranges with their descriptions and the number of IP addresses. The range 192.109.190.0/24 is highlighted with a red box.

Netblock	Description	Num IPs
160.46.224.0/19	BMW AG, Berlin production plant	8,192
160.48.212.0/24	BMW AG, Landshut production plant	256
160.48.213.0/24	BMW AG, Landshut production plant	256
192.109.190.0/24	80788 Muenchen	256
192.109.63.0/24	FI-11	256
193.23.33.0/24	Muenchen	256

Find the network range of DNB (Den Norske Bank) and submit it in CIDR format!

(The description and the name of the network range refers to DNB) (40)

Searched for IP range of DNB in google, clicked on this page <https://ipinfo.io/AS201627>.

On this website further down, I was able to find the information Further down in the about the cidr format of the network. The answer is first IP range [185.68.168.0/22](https://ipinfo.io/AS201627).

ip range of dnb

Omrent 426 000 resultater (0,42 sekunder)

db-ip.com · all · Oversett denne siden

[193.71.225.dnb.no - DNB BANK ASA - Search IP addresses](#)

193.71.225.0 - 193.71.225.255 is an IP address range owned by DNB BANK ASA and located in Norway - select an address below for more geolocation details.

Du har besøkt denne siden 2 ganger. Siste besøk: 26.09.20

Folk spør også om dette

- What is the range of an IP address?
- What is IP pool range?
- How do I find a company's IP range?
- How many IP addresses can 6 bits make?

Tilbakemelding

ipinfo.io · ... · Oversett denne siden

[AS201627 DNB BANK ASA - IPinfo.io](#)

AS201627 DNB BANK ASA Network Information, IP Address Ranges and Whois Details.

Du har besøkt denne siden 2 ganger. Siste besøk: 26.09.20

AS201627-dnb.no

DNB BANK ASA

Summary

Whois Details

IP Address Ranges

Network Speed

Hosted Domains

Peers

Upstreams

Downstreams

Related Networks

Details

AS201627 DNB BANK ASA

DOMAIN	dnb.no	COUNTRY	Norway
ALLOCATED	2014-09-01T07:13:37Z	REGISTRY	ripe
IP ADDRESSES	3,072	TYPE	business

Network Speed

17.88 Mbps

Hosted Domains

There are 42 domain names hosted across 13 IP addresses on this ASN.

IP Address Ranges

IPv4 Ranges			IPv6 Ranges		
Netblock	Description		Num IPs		
185.68.168.0/22	DNB BANK ASA		1,024		
193.71.224.0/21	Den Norske Bank, Oslo-Bergen		2,048		

3. Network mapping (130/130p)

There's one dns name in the UiO network range that contains the word "phone".
Find it and submit the full domain name! (30)

At first, I searched for top subdomain finders in google. I found a list of programs where: <https://securitytrails.com/> was listed. Then I searched for uio.no in the search field, the search gave me thousands of subdomains. I wrote "phone" in the filter field, and the search gave me one option: **persephone.uio.no** which is the answer.

uio.no subdomain records
APEX_DOMAIN RECORDS **uio.no**

Filter by keyword ... Filter Clear Filter

1 - 100 of 18,477 results

#	Domain	Rank	Hosting Provider	Mail Provider
1	uio.no	51,507	UNINETT, The Norwegian University & Research Network	UNINETT, The Norwegian University & Research Network
2	folk.uio.no	52,604	UNINETT, The Norwegian University & Research Network	-
3	heim.fifi.uio.no	78,620	UNINETT, The Norwegian University & Research Network	-
4	sv.uio.no	78,859	UNINETT, The Norwegian University & Research Network	-
5	hf.uio.no	81,589	UNINETT, The Norwegian University & Research Network	-
6	dokpro.uio.no	83,451	UNINETT, The Norwegian University & Research Network	-
7	duo.uio.no	106,845	UNINETT, The Norwegian University & Research Network	-

SecurityTrails **uio.no**

DOMAIN

- DNS Records
- Historical Data
- Subdomains 18,476**
- Upgrade now!

uio.no subdomain records
APEX_DOMAIN RECORDS **uio.no**

phone Filter Clear Filter

1 - 1 of 1 results

#	Domain	Rank	Hosting Provider	Mail Provider
1	persephone.uio.no	-	UNINETT, The Norwegian University & Research Network	-

Find the website on sidious.hackingarena.com in the port range 2000-3000 (30)

Running `nmap -p2000-3000 sidious.hackingarena.com` in terminal gave me port number 2945. I then went to my browser and wrote the website and the port number, as following: **sidious.hackingarena.com:2945**. Entering this URL gave me the flag:

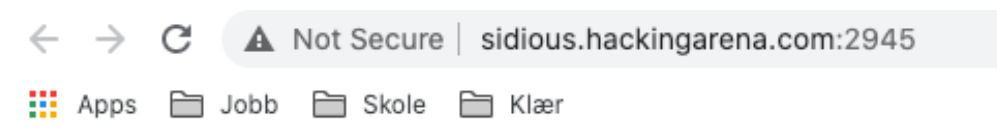
UiO-Hacking-Arena{I'm a hidden website}.

```

ruaweimediapadt310:~ pilasilda$ sudo nmap -p2000-3000 sidious.hackingarena.com
Password:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-01 18:28 CEST
Nmap scan report for sidious.hackingarena.com (158.37.63.67)
Host is up (0.011s latency).
Not shown: 900 filtered ports, 100 closed ports
PORT      STATE SERVICE
2945/tcp  open  h248-binary

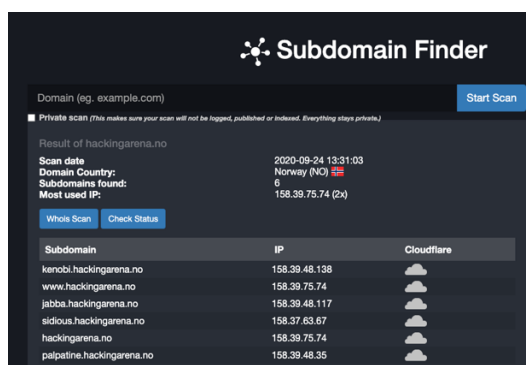
Nmap done: 1 IP address (1 host up) scanned in 3.85 seconds
ruaweimediapadt310:~ pilasilda$

```



How many ports are open in the range between 1800 and 1900 in all hackingarena.com servers?(30)

At first, I had to find all subdomains on the hackingarena.com servers. Using viewdns reverse IP lookup tool I found out that both hackingarena.no and hackingarena.com were sharing the same IP-address, I assumed that for every .no page it would also exist an .com-page. On <https://subdomainfinder.c99.nl/> I searched for hackingarena.no the search gave me a list of subdomains for hackingarena.no which is listed below, in addition by doing a pen test tool check I found **backup.hackingarena.no**.



www.hackingarena.com
www.backup.hackingarena.com
www.palpatine.hackingarena.com
www.jabba.hackingarena.com
www.sidious.hackingarena.com
www.kenobi.hackingarena.com

Then I used the following command **nmap -sT -p1800-1900 hackingarena.com -open |grep open | wc -l** to list all open ports between 1800-1900. By scanning all the ports between 1800-1900, using the same command for all subdomains I found number of open ports. I then summed up all the numbers and got **50** which is the flag and answer for this task.

```

Nmap done: 1 IP address (1 host up) scanned in 3.75 seconds
[cm-84:~ pilasilda$ nmap -sT -p1800-1900 hackingarena.com -open |grep open | wc -l
0
[cm-84:~ pilasilda$ nmap -sT -p1800-1900 kenobi.hackingarena.com -open |grep open | wc -l
8
[cm-84:~ pilasilda$ nmap -sT -p1800-1900 jabba.hackingarena.com -open |grep open | wc -l
20
[cm-84:~ pilasilda$ nmap -sT -p1800-1900 palpatine.hackingarena.com -open |grep open | wc -l
22
[cm-84:~ pilasilda$ nmap -sT -p1800-1900 backup.hackingarena.com -open |grep open | wc -l
0
[cm-84:~ pilasilda$ nmap -sT -p1800-1900 sidious.hackingarena.com -open |grep open | wc -l
0
[cm-84:~ pilasilda$

```

A service is running on the sidious.hackingarena.com server in the port range 3000-3500. Find an exploit in the exploit-db that can take advantage of the vulnerability of the service. The solution is the exploit id. (40)

At first, I run **nmap -p3000-3500 sidious.hackingarena.com** to find the port that the service is running on, and it was running on port 3099. I then went to my browser searching for this page: <http://sidious.hackingarena.com:3099/>, it gave me a blank page. I

then inspected the webpage, looked through the network part at first, I found nothing but if I update the page it started to log. If I under network clicked on sidious.hackingarena.com and looked at server I saw that the server name was lighttpd 1.4.15. This probably had something to do with exploit-db, so I went to <https://www.exploit-db.com/> and searched for lighttpd 1.4.15 and found the EDB-ID 30322, which is the flag for this task.

```
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-10 12:47 CET
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 12:47 (0:00:00 remaining)
Nmap scan report for sidious.hackingarena.com (158.37.63.67)
Host is up (0.014s latency).
Not shown: 400 filtered ports, 100 closed ports
PORT      STATE SERVICE
3099/tcp  open  chmd

Nmap done: 1 IP address (1 host up) scanned in 2.57 seconds
cm-84:~ pilasilda$
```

The screenshot shows a web browser with the Network tab open, displaying a list of network requests. The first request is to sidious.hackingarena.com with status 304 and type document. The second request is a blob with status 200 and type script. Below the browser, the Exploit Database search results are shown for the query 'Lighttpd 1.4.15'. The results table shows one entry: 'Lighttpd 1.4.15 - Multiple Code Execution / Denial of Service / Information Disclosure Vulnerabilities' by Abhisek Datta, dated 2007-04-16. The entry is marked as verified and has a download icon.

Name	Status	Type	Initiator	Size	Time	Server	Waterfall
sidious.hackingarena.com	304	document	Other	135 B	53...	Lighttpd 1.4.15	
blob:http://sidious.hackingarena.com:3...	200	script	include_preload...	0 B	27...		

Date	D	A	V	Title	Type	Platform	Author
2007-04-16				Lighttpd 1.4.15 - Multiple Code Execution / Denial of Service / Information Disclosure Vulnerabilities	Remote	Windows	Abhisek Datta

Showing 1 to 1 of 1 entries (filtered from 43,259 total entries)

EXPLOIT DATABASE

Lighttpd 1.4.15 - Multiple Code Execution / Denial of Service / Information Disclosure Vulnerabilities

EDB-ID: 30322	CVE: 2007-3947	Author: ABHISEK DATTA	Type: REMOTE	Platform: WINDOWS	Date: 2007-04-16
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App:	

Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

4. Get in touch with services (220/220p)

Find the service and the flag on sidious.hackingarena.com in the port range between 7500 and 8000 - (70)

At first I used `nmap Sidious.hackingarena.com -p7500-8000` to find the open ports between 7500-8000, here I found to services port 7774 and 7777. Then I tried to log into `telnet sidious.hackingarena.com -p7774`, by trying this I realized I need a password to go further. I therefore went to my browser and searched for **emergency agency for nuclear alert password**, all of the websites I checked pointed to **Warningpoint2** as a password. I then tried to use Warningpoint2 as a password and it was correct. Logging inn with password Warningpoint2 gave me the right flag: **UiO-Hacking Arena{Hawa11_gr455_5k1rt}**.

emergency agency for nuclear alerts password

About 7,370,000 results (0.64 seconds)

As Business Insider points out, a few press photos from the HEMA headquarters reveal that the **agency** has been keeping some of its **passwords** scrawled out on Post-it notes, pasted to various computer monitors. Some savvy Twitter users were even able to zoom in on one photo enough to make out the word: "warningpoint2." Jan 17, 2018

www.vice.com › Home › The VICE Guide to Right Now
The Agency That Messed Up Hawaii's Nuclear Alert Keeps ...

www.businessinsider.com › Tech Insider › Politics
Hawaii emergency agency password in photo sparks security ...
Jan 16, 2018 — On Saturday, people in Hawaii were awakened by a terrifying false alert about an inbound missile. Hawaii's Emergency Management Agency has ...

www.dailymail.co.uk › news › article-5279525 › Photo...
Photo of Hawaii emergency agency shows password on Post-it
Jan 17, 2018 — The Hawaii office responsible for putting out the false missile alert that ... An Associated Press photo of the Hawaii's Emergency Management Agency ... Fearing a nuclear attack, terrified residents and tourists ran for their lives, ...

```

cm-84:desktop pilasilda$ nmap sidious.hackingarena.com -p7500-8000
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-25 16:00 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.12 seconds
cm-84:desktop pilasilda$ sudo nmap sidious.hackingarena.com -p7500-8000
Password:
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-25 16:00 CET
Nmap scan report for sidious.hackingarena.com (158.37.63.67)
Host is up (0.026s latency).
Not shown: 299 closed ports, 200 filtered ports
PORT      STATE SERVICE
7774/tcp  open  unknown
7777/tcp  open  cbt

cm-84:desktop pilasilda$ sudo telnet sidious.hackingarena.com 7774
Password:
Trying 158.37.63.67...
Connected to sidious.hackingarena.com.
Escape character is '^]'.
Aloha!
Welcome to the Emergency Agency for Nuclear Alerts!
Password:Warningpoint2
UiO-Hacking-Arena{Hawa11_gr455_5k1rt}
Bye
Connection closed by foreign host.
cm-84:desktop pilasilda$ █

```

Hi guys, I need your help. I've got an email to pay 0.5 bitcoin. If not, they release all my private files stored on my secure server here: <http://sidious.hackingarena.com:848> My username is casanova. Ok, ok, I'm using the same password everywhere for like 5 years now and probably the password is not so strong. But I've never had any incident before (except for this embarrassing Ashley Madison case, but fortunately nobody could identify me). Could you please help me out? - (70)

Searched for Ashley Maddison password list on google, found this

<https://theatlask.com/charts/NyL3uhCp>. Copied the password into a txt file. In terminal run **hydra -l Casanova -P passlist.txt -s 848 sidious.hackingarena.com ssh**. This gave me the password **kazuga**. Then run **ssh casanova@sidious.hackingarena.com -p848**, enter password **kazuga**. Enter **ls** to get list of files in directory. Then I used **cat flag.txt** to open the file which gave me the flag **UiO-Hacking-Arena{Ult1mate_ka0s_Casanova}**.

```
Pilasildas-MacBook-Air:desktop pilasilda$ hydra -l casanova -P passlist.txt -s 848 sidious.hackingarena.com ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for il
re laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-10-10 21:44:50
[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 (1:1/p:100), ~7 tries per task
[DATA] attacking ssh://sidious.hackingarena.com:848/
[848][ssh] host: sidious.hackingarena.com login: casanova password: kazuga
1 of 1 target successfully completed, 1 valid password found
[Pilasildas-MacBook-Air:desktop pilasilda$ ssh casanova@sidious.hackingarena.com -p848
casanova@sidious.hackingarena.com's password:
Permission denied, please try again.
casanova@sidious.hackingarena.com's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 4.19.0-10-cloud-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: Sat Oct 10 19:22:54 2020 from 46.9.82.144

```
[casanova@ea2a8a0da188:~]$ la
.bash_logout .bashrc .cache .profile flag.txt
[casanova@ea2a8a0da188:~]$ cat flag.txt
UiO-Hacking-Arena{Ultimate_ka0s_Casanova}
```

Find the service on sidious.hackingarena.com in the port range 5000-5500. Find and submit the flag! – (80)

Run **sudo nmap sidious.hackingarena.com -p5000-5500** and got the port number, which was 5110. Logging into **ftp sidious.hackingarena.com 5110**. Logging into the service using anonymous as user and guest as password. After entering ftp running **ls** to see the directory. Reading the access.log file by running **fget access.log**. The file shows that there are two users **MarkZuckerberg** and **Billgates**, but the passwords are not shown. I therefore searched for Mark Zuckerberg password on google and found out that **dadada** where a password he used before. I then logged into ftp again using markZuckerberg as a user and dadada as password. Running **ls** gave me the **flag.txt** file, then run **fget flag.txt** which read the file and gave me the flag.

```
[cm-84:~ pilasilda$ sudo nmap sidious.hackingarena.com -p5000-5500
[Password:
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-14 23:41 CET
Nmap scan report for sidious.hackingarena.com (158.37.63.67)
Host is up (0.018s latency).
Not shown: 500 closed ports
PORT      STATE SERVICE
5110/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
cm-84:~ pilasilda$
```



```

cm-84:~ pilasilda$ ftp sidious.hackingarena.com 5110
Connected to sidious.hackingarena.com.
220 (vsFTPd 3.0.3)
Name (sidious.hackingarena.com:pilasilda): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||10085|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 153 Sep 26 17:21 access.log
drwxr-xr-x 2 0 0 4096 Sep 26 17:23 pub
226 Directory send OK.
ftp> fget access.log
local: 16:34:12 40.112.72.205 USER BillGates 331 remote: 16:34:12 40.112.72.205 USER BillGates 331
229 Entering Extended Passive Mode (|||10088|)
550 Failed to open file.
local: 16:34:12 40.112.72.205 PASS - 530 remote: 16:34:12 40.112.72.205 PASS - 530
229 Entering Extended Passive Mode (|||10084|)
550 Failed to open file.
local: 18:55:45 31.13.72.36 USER MarkZuckerberg 331 remote: 18:55:45 31.13.72.36 USER MarkZuckerberg
331
229 Entering Extended Passive Mode (|||10089|)
550 Failed to open file.
local: 18:55:45 31.13.72.36 PASS - 530 remote: 18:55:45 31.13.72.36 PASS - 530
229 Entering Extended Passive Mode (|||10082|)
550 Failed to open file.
ftp>

```

le MarkZuckerberg password

[All](#)
[Images](#)
[News](#)
[Videos](#)
[Maps](#)
[More](#)
[Settings](#)
[Tools](#)

About 5,310,000 results (0.70 seconds)

Did you mean: **Mark Zuckerberg** password

Mark Zuckerberg suffered a major breach of privacy on June 5 when hackers gained access to his personal social media accounts. Many people criticized the Facebook CEO's simple **password** — "**dadada**" — as well as the fact he reused the same **password** across multiple services. Jun 13, 2016

[www.cmswire.com > information-management > why-yo...](#)

Why You Shouldn't Make Fun of Mark Zuckerberg's Password

[About Featured Snippets](#)
[Feedback](#)

```

[cm-84:~ pilasilda$ ftp sidious.hackingarena.com 5110
Connected to sidious.hackingarena.com.
220 (vsFTPd 3.0.3)
Name (sidious.hackingarena.com:pilasilda): MarkZuckerberg
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
[ftp> ls
229 Entering Extended Passive Mode (|||10084|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 42 Sep 26 17:29 flag.txt
226 Directory send OK.
[ftp> fget flag.txt
local: UiO-Hacking-Arena{Stop_listening_us_Mark} remote: UiO-Hacking-Arena{Stop_listening_us_Mark}
229 Entering Extended Passive Mode (|||10080|)
550 Failed to open file.
ftp>

```

5. Web (230/700p)

Find the flag here: <http://palpatine.hackingarena.com:812> – States (60)

I thought this task had to do something with URL-tampering, I first searched for all states in USA, on https://simple.wikipedia.org/wiki/List_of_U.S._states I found a list. I then went to the sidious website and clicked on one of the links and saw that the URL had state=Alabama, for example. So, I thought maybe I could try to tamper this part of the URL. By using burp repeater, I tried to change the part state=Alabama with name of some other states, I went through almost all the states in this list when I tried **states=Oklahoma** the repeater gave me the flag and answer for this task.

```

1 GET /states.php?state=Arizona HTTP/1.1
2 Host: palpatine.hackingarena.com:812
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
  ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer: http://palpatine.hackingarena.com:812/
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
9 Cookie: _ga=GA1.1.342678687.1603185573; _ga_NSPGR3TV35=
  GS1.1.1603185574.1.1.1603187118.0
10 Connection: close
11
12

```

Pretty Raw \n Actions ▾

```

1 GET /states.php?state=Oklahoma HTTP/1.1
2 Host: palpatine.hackingarena.com:812
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
  ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
9 Cookie: _ga=GA1.1.342678687.1603185573; _ga_NSPGR3TV35=
  GS1.1.1603185574.1.1.1603187118.0
10 Connection: close
11
12

```

```

HTTP/1.1 200 OK
Date: Mon, 16 Nov 2020 14:04:35 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 71
Connection: close
Content-Type: text/html; charset=UTF-8

<h1>
  UiO-Hacking-Arena{Where the Wind Comes Sweeping Down the Plain}<br>

```

Find the flag here: <http://sidious.hackingarena.com:801> – High ground(70)







This task is all about URL-tampering. At first, I opened the website: **sidious.hackingarena.com:801**, then I inspected the source code.

```
(a.attachEvent("onLoad",g),b.attachEvent("onreadystatechange",function(){
e["complete"]==b.readyState&&c.readyStateCallback()))},f=c.source[0],f.concatemoji?
e(f.concatemoji):f.wpemoji&&f.twemoji&&(e(f.twemoji),e(f.wpemoji)))}
(window,document>window._wpemojiSettings);

</script>
<style type="text/css">_</style>
<link rel="stylesheet" id="twentyseventeen-fonts-css" href="https://
fonts.googleapis.com/css?
family=Libre+Franklin%3A300%2C300i%2C400%2C400i%2C600%2C600i%2C800%2C800i&subset=latin
2&latin-ext" type="text/css" media="all">
<link rel="stylesheet" id="twentyseventeen-style-css" href="http://
sidious.hackingarena.no:801/wp-content/themes/twentyseventeen/style.css?ver=4.8.14"
type="text/css" media="all"> == $0
<!--[if lt IE 9]>
<link rel="stylesheet" id="twentyseventeen-ie8-css"
href="http://sidious.hackingarena.no:801/wp-
content/themes/twentyseventeen/assets/css/ie8.css?ver=1.0" type="text/css" media="all"
/>
<!--[endif]>-->
<!--[if lt IE 9]>
<script type="text/javascript" src="http://sidious.hackingarena.no:801/wp-
content/themes/twentyseventeen/assets/js/html5.js?ver=3.7.3"></script>
<!--[endif]>-->
```

In the source code I saw that some of the code was commented out the comments included a website related to sidious:801 page. I copied this link: <http://sidious.hackingarena.no:801/wp-content/themes/twentyseventeen/style.css?ver=4.8.14> then I tried to remove some part of the link. At the end, I was left with this <http://sidious.hackingarena.no:801/wp-content/>. This link forwarded me to the **index of page**, here I found the **flag.txt** file, where I also found the answer to this task

Index of /wp-content

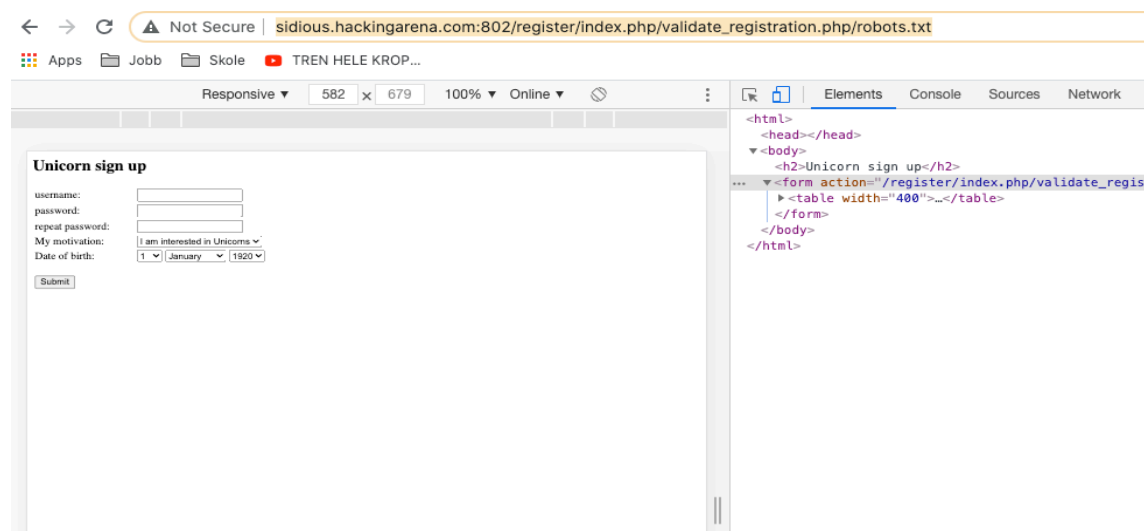
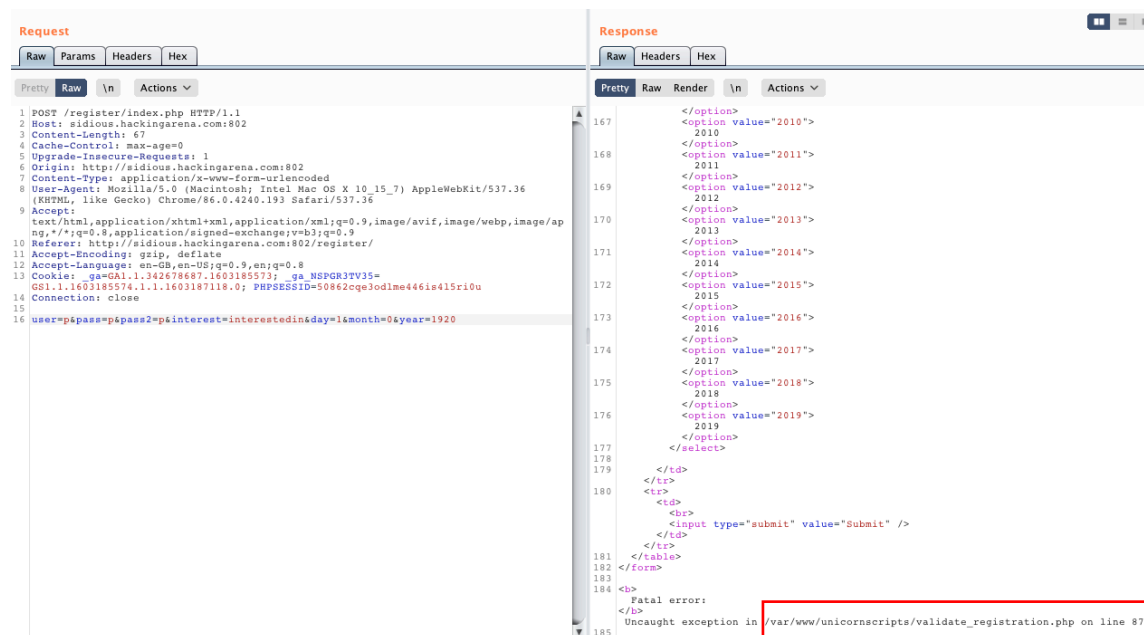
Name	Last modified	Size	Description
 Parent Directory		-	
 flag.txt	2020-10-03 21:45	44	
 plugins/	2020-10-25 23:21	-	
 themes/	2017-06-20 09:16	-	
 upgrade/	2020-10-03 21:37	-	
 uploads/	2020-10-03 21:32	-	

```
UiO-Hacking-Arena{D4fault W0rdpr4ss Dang4r}
```

Find the flag on the following site: <http://sidious.hackingarena.com:802> – Unicorn
(100)

Went to the sign-up page, <http://sidious.hackingarena.com:802/register/> and signed up with a random user and password. I tried to register with different values and noticed that it didn't fail in any of my attempts. After pondering over how I could solve this I thought that I could try using 0 as a value for **month** or **year** to see if it could cause an error on the page, by changing month=0 it failed. The error message gave me `/var/www/unicornscripts/validate_registration.php` this line. By using URL-tampering, I tried many combinations to try to find the answer. At the end <http://sidious.hackingarena.com:802/unicornscripts/> this URL gave me the index of page

and there I could also find the flag.txt file which gave me the flag for this task: UiO-Hacking-Arena{Capture_the_Unicorn_it's_fun!}.



Index of /unicorns/scripts

Name	Last modified	Size	Description
Parent Directory	-		
flag.txt	2020-10-04 12:55	49	
validate_registration.php	2020-10-04 12:54	2.0K	

Apache/2.4.41 (Ubuntu) Server at sidious.hackingarena.com Port 802

```
UiO-Hacking-Arena{Capture_the_Unicorn_it's_fun!}
```

Resources: all lectures from 1 – 7 was frequently used

1. Erdodi L. (2020). *Lecture Plan*.

<https://www.uio.no/studier/emner/matnat/ifi/IN5290/h20/lecture-plan.html>