

# Practica – Pentesting

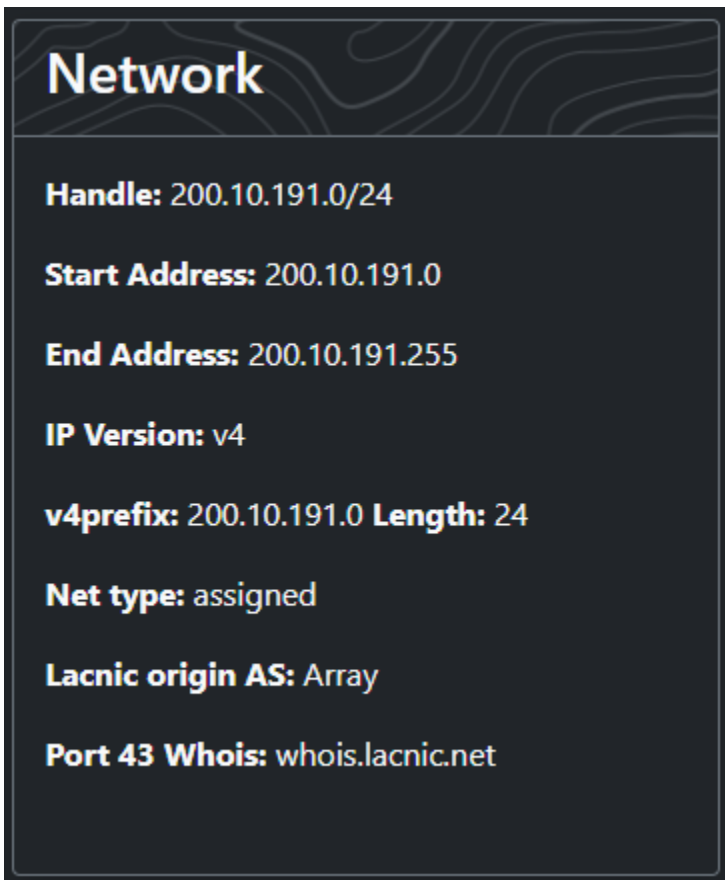
## Parte 1

1. Dado el dominio [www.frc.utn.edu.ar](http://www.frc.utn.edu.ar), se tiene por objetivo realizar fase de reconocimiento, para ello se realizarán las siguientes tareas:
  - a. Información de las IP y rangos.
  - b. Búsqueda en Google de posibles correos electrónicos de usuarios del sistema
  - c. Información de Whois
  - d. Registros TXT, MX, servidores DNS
  - e. Reconocimiento de puertos
  - f. Reconocimiento de directorios
  - g. Tecnologías utilizadas
  - h. Subdominios

Documentar cada paso en un archivo de texto (Word, Libre Docs, etc.)

Herramientas: <https://spice-eyelash-aa0.notion.site/Commands-b3477ebdfb934ae5b1d07f5b5e1eb595>

- a. Información de IPs obtenida de <https://synapsint.com/>



Información de IPs complementaria, incluyendo datos acerca de los DNS extraída de <https://www.robtext.com/dns-lookup/www.frc.utn.edu.ar>

General	
FQDN	www.frc.utn.edu.ar
Host Name	www.frc
Domain Name	utn.edu.ar
Registry	edu.ar
TLD	ar
DNS	
IP numbers	<u>190.114.208.200</u> <u>200.10.191.200</u>
Domain DNS	
Name servers	<u>ns1.riu.edu.ar</u> <u>ns1.utn.edu.ar</u> <u>ns2.utn.edu.ar</u> <u>ns3.utn.edu.ar</u> <u>ns5.utn.edu.ar</u> <u>panda.utn.edu.ar</u>
Mail servers	utn-edu-ar.mail.protection.outlook.com
IP Numbers	<u>52.151.241.218</u> <u>190.114.222.138</u>

Traceroute extraído de <https://centralops.net/co/>

## Traceroute

Tracing route to **www.frc.utn.edu.ar** [200.10.191.200]...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	1	0	0	169.254.158.58	
2	1	1	0	169.48.118.158	ae103.ppr02.dal13.networklayer.com
3	1	0	0	169.48.118.138	8a.76.30a9.ip4.static.sl-reverse.com
4	2	2	2	169.45.18.38	ae17.cbs01.dr01.dal04.networklayer.com
5	32	32	32	50.97.18.173	ad.12.6132.ip4.static.sl-reverse.com
6	32	32	32	169.45.18.127	7f.12.2da9.ip4.static.sl-reverse.com
7	*	*	*		
8	*	*	*		
9	180	180	180	200.105.108.90	
10	*	Host unreachable			

Trace aborted

b. Posibles correos electrónicos de usuarios

Google dork: *intext:\*@frc.utn.edu.ar*

ccoggiola@frc.utn.edu.ar

jsalomone@frc.utn.edu.ar

jcvazquez@frc.utn.edu.ar

mbartolomeo@frc.utn.edu.ar

garaguas@frc.utn.edu.ar

cids@sistemas.frc.utn.edu.ar

cemetro.utn@frc.utn.edu.ar

computos@frc.utn.edu.ar

c. Información de whois obtenida en <https://centralops.net/co/>

### Network Whois record

Queried **whois.lacnic.net** with "200.10.191.200"...



```
inetnum:      200.10.191.0/24
status:       assigned
aut-num:      N/A
owner:        UNIVERSIDAD TECNOLOGICA NACIONAL - FACULTAD REGIONAL CORDOBA
ownerid:      AR-UTNF-LACNIC
responsible:  Daniel Forte
address:      Maestro Marcelo Lopez esq Cruz Roja, S/N,
address:      5000 - Cordoba -
country:      AR
phone:        +54 351 5986024
owner-c:      DAF45
tech-c:       DAF45
abuse-c:      DAF45
inetrev:      200.10.191.0/24
nserver:      COLORADO2.FRC.UTN.EDU.AR
nsstat:       20221015 AA
nslastaa:     20221015
nserver:      COLORADO4.FRC.UTN.EDU.AR
nsstat:       20221015 AA
nslastaa:     20221015
nserver:      COLORADO.FRC.UTN.EDU.AR
nsstat:       20221015 AA
nslastaa:     20221015
nserver:      COLORADO3.FRC.UTN.EDU.AR
nsstat:       20221015 AA
nslastaa:     20221015
created:      20151216
changed:      20151216

nic-hdl:      DAF45
person:       Daniel Forte
e-mail:       daniel@frc.utn.edu.ar
address:      Maestro Marcelo Lopez esq Cruz Roja,
address:      5000 - Cordoba - Cb
country:      AR
phone:        +54 351 5986024
created:      20151015
changed:      20210615
```

Información complementaria de Whois de <https://whois.domaintools.com/utn.edu.ar>

## Whois Record for UTN.edu.ar

### — Domain Profile

Registrar Status	taken	
Name Servers	NS1.RIU.EDU.AR (has 16 domains) NS1.UTN.EDU.AR (has 12 domains) NS2.UTN.EDU.AR (has 12 domains) NS3.UTN.EDU.AR (has 12 domains) NS5.UTN.EDU.AR (has 12 domains) PANDA.UTN.EDU.AR (has 12 domains)	↩
Tech Contact	—	
IP Address	52.151.241.218 is hosted on a dedicated server	↩
IP Location	 - Virginia - Washington - Microsoft Corporation	
ASN	 AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)	
Hosting History	174 changes on 2 unique name servers over 9 years	↩

### d. Registros TXT, MX, servidores DNS

Información de servidores DNS extraído de <https://synapsint.com/>

## DNS records

### NS records

- panda.utn.edu.ar
- colorado.frc.utn.edu.ar
- colorado2.frc.utn.edu.ar
- colorado3.frc.utn.edu.ar
- colorado4.frc.utn.edu.ar

# Información complementaria de DNS, registros MX y registros TXT obtenida de <https://centralops.net/co/>

## DNS records

name	class	type	data	time to live
www.frc.utn.edu.ar	IN	A	200.10.191.200	600s (00:10:00)
frc.utn.edu.ar	IN	NS	colorado4.frc.utn.edu.ar	86400s (1.00:00:00)
frc.utn.edu.ar	IN	NS	colorado2.frc.utn.edu.ar	86400s (1.00:00:00)
frc.utn.edu.ar	IN	NS	colorado.frc.utn.edu.ar	86400s (1.00:00:00)
frc.utn.edu.ar	IN	NS	panda.utn.edu.ar	86400s (1.00:00:00)
frc.utn.edu.ar	IN	NS	colorado3.frc.utn.edu.ar	86400s (1.00:00:00)
frc.utn.edu.ar	IN	MX	<div> <div>preference: 5</div> <div>exchange: veladero.frc.utn.edu.ar</div> </div>	86400s (1.00:00:00)
frc.utn.edu.ar	IN	TXT	MS=43E4CA78952EFDF06BEE94C6D69F41373B3E921B	3600s (01:00:00)
frc.utn.edu.ar	IN	TXT	google-site-verification=ZcmeSG0YVLTOHIZ-pr_eq3OQtPpquhBfmsDM6TBv_-M	3600s (01:00:00)
frc.utn.edu.ar	IN	TXT	v=spf1 mx ~all	3600s (01:00:00)
frc.utn.edu.ar	IN	TXT	google-site-verification=YLy3mN_f7rpezsBU2HeC7F69PY6H3Yt67p834YO2-R8	3600s (01:00:00)
frc.utn.edu.ar	IN	A	200.10.191.200	86400s (1.00:00:00)
frc.utn.edu.ar	IN	SOA	<div> <div>server: colorado2.frc.utn.edu.ar</div> <div>email: root@colorado.frc.utn.edu.ar</div> <div>serial: 2022092501</div> <div>refresh: 7200</div> </div>	86400s (1.00:00:00)
utn.edu.ar	IN	TXT	Location: Sarmiento 440 / Ciudad Autonoma de Buenos Aires / Argentina	21600s (06:00:00)
utn.edu.ar	IN	TXT	UTN Rectorado	21600s (06:00:00)
utn.edu.ar	IN	TXT	Phone: +54-011-5371-5600	21600s (06:00:00)
utn.edu.ar	IN	TXT	v=spf1 mx include:spf.protection.outlook.com ~all	21600s (06:00:00)
utn.edu.ar	IN	NS	ns3.utn.edu.ar	21600s (06:00:00)
utn.edu.ar	IN	NS	ns1.utn.edu.ar	21600s (06:00:00)
utn.edu.ar	IN	NS	panda.utn.edu.ar	21600s (06:00:00)
utn.edu.ar	IN	NS	ns2.utn.edu.ar	21600s (06:00:00)
utn.edu.ar	IN	NS	ns1.riu.edu.ar	21600s (06:00:00)
utn.edu.ar	IN	NS	ns5.utn.edu.ar	21600s (06:00:00)
utn.edu.ar	IN	A	52.151.241.218	21600s (06:00:00)
utn.edu.ar	IN	MX	<div> <div>preference: 0</div> <div>exchange: utn-edu-ar.mail.protection.outlook.com</div> </div>	3600s (01:00:00)
200.191.10.200.in-addr.arpa	IN	PTR	lanin.frc.utn.edu.ar	86400s (1.00:00:00)
191.10.200.in-addr.arpa	IN	SOA	<div> <div>server: colorado2.frc.utn.edu.ar</div> <div>email: root@frc.utn.edu.ar</div> <div>serial: 2021111601</div> <div>refresh: 3600</div> <div>retry: 3600</div> </div>	86400s (1.00:00:00)

e. Información de puertos extraída de <https://synapsint.com/>

Ports and Services			
Services	Product	Vulns	Headers
tcp - 80 http	Apache httpd 2.4.18	CVE-2019-0220 CVE-2017-7679 CVE-2020-1934 CVE-2018-17189 CVE-2017-9798 CVE-2016-4975 CVE-2016-1546 CVE-2022-29404 CVE-2018-1312 CVE-2020-35452 CVE-2018-1333 CVE-2019-0211 CVE-2018-11763 CVE-2022-28330 CVE-2017-15710 CVE-2016-8612 CVE-2019-0217 CVE-2019-0196 CVE-2022-22721 CVE-2022-22720 CVE-2019-10092 CVE-2019-17567 CVE-2017-15715 CVE-2022-31813 CVE-2019-10098 CVE-2016-5387 CVE-2021-40438 CVE-2022-23943 CVE-2020-1927 CVE-2018-17199 CVE-2017-9788 CVE-2022-22719 CVE-2018-1301 CVE-2018-1302 CVE-2018-1303 CVE-2017-3167 CVE-2021-34798 CVE-2017-3169 CVE-2020-11985 CVE-2021-44790 CVE-2016-4979 CVE-2021-26690 CVE-2021-26691 CVE-2022-26377 CVE-2022-30556 CVE-2020-13938 CVE-2018-1283 CVE-2019-10082 CVE-2016-8740 CVE-2016-8743 CVE-2021-44224 CVE-2021-39275 CVE-2022-28615 CVE-2022-28614 CVE-2021-33193	
tcp - 443 https	Apache httpd 2.4.18	CVE-2019-0220 CVE-2017-7679 CVE-2020-1934 CVE-2018-17189 CVE-2017-9798 CVE-2016-4975 CVE-2016-1546 CVE-2022-29404 CVE-2018-1312 CVE-2020-35452 CVE-2018-1333 CVE-2019-0211 CVE-2018-11763 CVE-2022-28330 CVE-2017-15710 CVE-2016-8612 CVE-2019-0217 CVE-2019-0196 CVE-2022-22721 CVE-2022-22720 CVE-2019-10092 CVE-2019-17567 CVE-2017-15715 CVE-2022-31813 CVE-2019-10098 CVE-2016-5387 CVE-2021-40438 CVE-2022-23943 CVE-2020-1927 CVE-2018-17199 CVE-2017-9788 CVE-2022-22719 CVE-2018-1301 CVE-2018-1302 CVE-2018-1303 CVE-2017-3167 CVE-2021-34798 CVE-2017-3169 CVE-2020-11985 CVE-2021-44790 CVE-2016-4979 CVE-2021-26690 CVE-2021-26691 CVE-2022-26377 CVE-2022-30556 CVE-2020-13938 CVE-2018-1283 CVE-2019-10082 CVE-2016-8740 CVE-2016-8743 CVE-2021-44224 CVE-2021-39275 CVE-2022-28615 CVE-2022-28614 CVE-2021-33193	

Escaneo de puertos de <https://centralops.net/co/>

Service scan

**FTP - 21** Error: TimedOut

**SMTP - 25** Error: TimedOut

**HTTP - 80** HTTP/1.1 301 Moved Permanently  
Date: Sun, 16 Oct 2022 13:19:46 GMT  
Server: Apache/2.4.18 (Ubuntu)  
Location: https://www.frc.utn.edu.ar/  
Connection: close  
Content-Type: text/html; charset=iso-8859-1

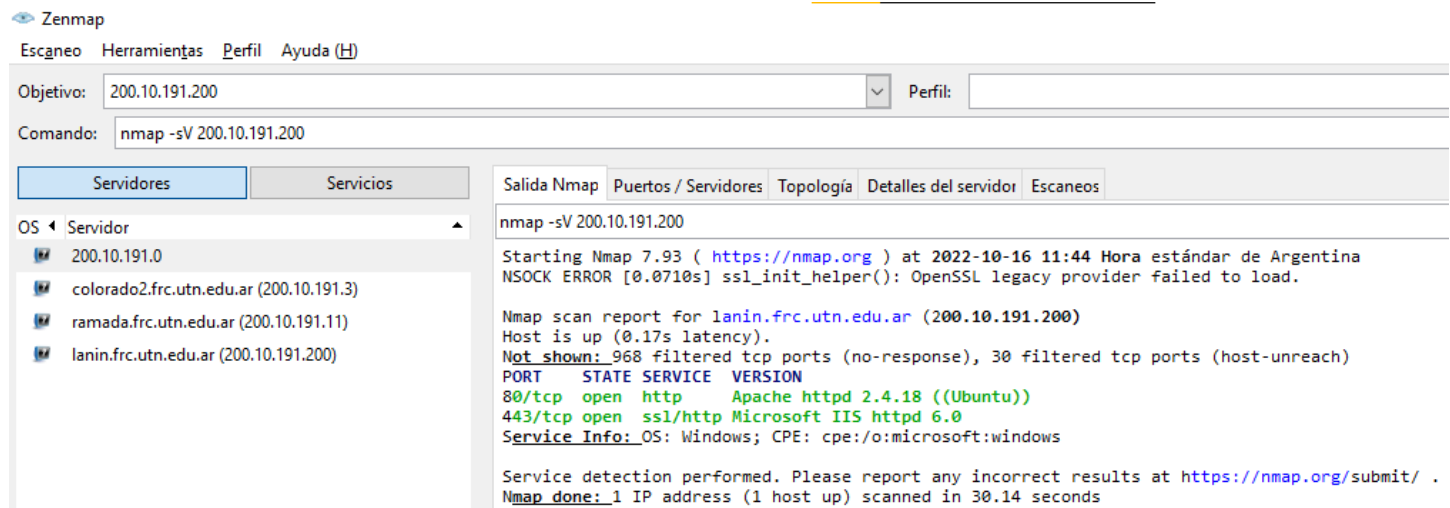
**POP3 - 110** Error: TimedOut

**IMAP - 143** Error: TimedOut

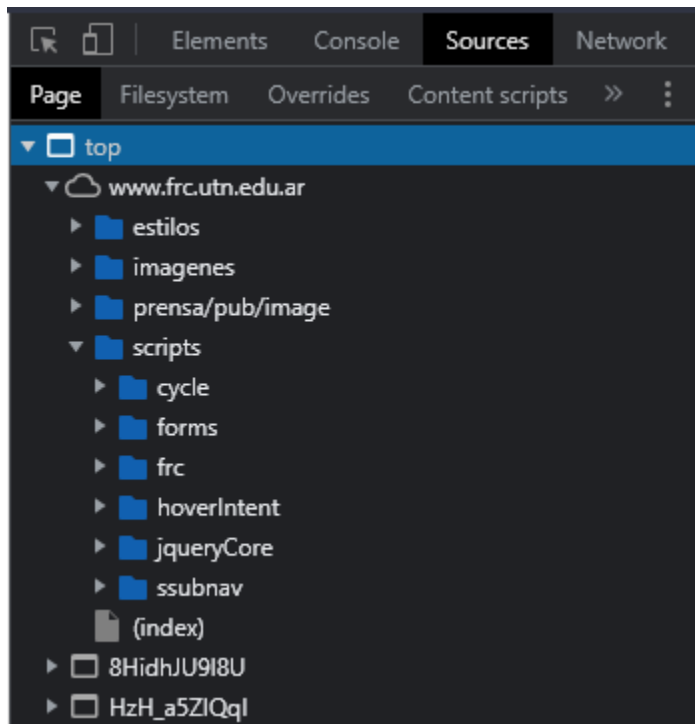
**HTTPS - 443** Certificate validation errors: None  
Signature algorithm: sha256RSA  
Public key size: 2048 bits  
Issuer: CN=R3, O=Let's Encrypt, C=US  
Subject: CN=www.frc.utn.edu.ar  
Subject Alternative Name: DNS Name=autogestion.frc.utn.edu.ar, DNS Name=eduroam.frc.utn.edu.ar, DNS Name=www.frc.utn.edu.ar  
Serial number: 03E20776CA83BBF1F5CDFA086C31C0357ECD  
Not valid before: 2022-10-06 04:15:44Z  
Not valid after: 2023-01-04 04:15:43Z  
SHA1 fingerprint: 4025A745CDC73A4675A9F0CBB3D09D5AD0A8C065

HTTP/1.1 200 OK  
Date: Sun, 16 Oct 2022 13:19:51 GMT  
Server: Microsoft-IIS/6.0  
Content-Type: text/html  
Cache-control: private  
Set-Cookie: ASPSESSIONIDCSBDQCTS=NFPLLNKBCIHCDJOCCEALKPGC; path=/  
Connection: close

## Escaneo de puertos con herramienta nmap

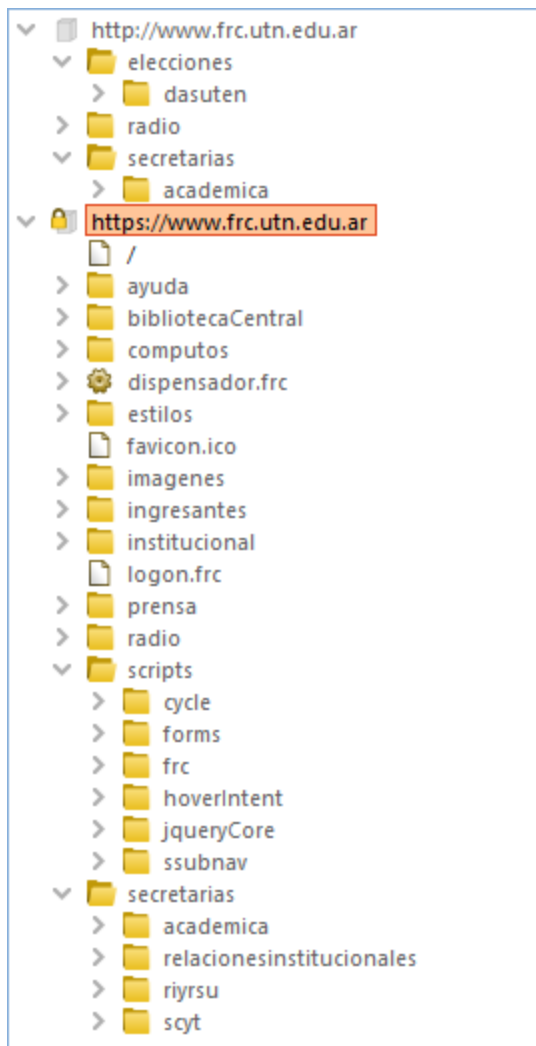


### f. Reconocimiento de directorios



Navegador





Burp suite

## g. Tecnologías utilizadas

Extraído de <https://synapsint.com/>

### Technologies

Category	Software	Version
Web Server	Apache	2.4.18
Operating System	Ubuntu	

Información complementaria obtenida en <https://w3techs.com/sites/info/utn.edu.ar>

#### Server-side Programming Language

PHP	PHP is a scripting language for creating websites.
-----	--

#### Client-side Programming Language

JavaScript	JavaScript is a lightweight, object-oriented, cross-platform scripting language, often used within web pages.
------------	---

#### JavaScript Libraries

jQuery	jQuery is a JavaScript library that simplifies HTML document traversing, event handling, animating and Ajax interaction. Originally developed by John Resig.
--------	--

Bootstrap	Bootstrap is an open source HTML, CSS, and JavaScript framework.
-----------	--

Popper	Popper is an open source JavaScript library for tooltips and popovers.
--------	--

UIkit	UIkit is a lightweight and modular front-end framework for developing web interfaces.
-------	---

#### CSS Frameworks

Bootstrap	Bootstrap is an open source HTML, CSS, and JavaScript framework.
-----------	--

Animate	Animate is a CSS library focusing on animations.
---------	--

#### Web Server

Nginx 1.14.0 80% of sites use a newer version	Nginx (pronounced as "engine X") is a lightweight open source web server developed by Igor Sysoev.
--	--

#### Operating System

Ubuntu	Ubuntu is a Linux distribution.
--------	---------------------------------

#### Web Hosting Provider

Microsoft	Microsoft is a multinational technology company headquartered in USA. hosting info partly based on data from <a href="#">ipinfo.io</a> , <a href="#">see details</a>
-----------	---

#### Data Center Provider

Microsoft	Microsoft is a multinational technology company headquartered in USA.
-----------	---

#### Email Server Provider

Microsoft	Microsoft is a multinational technology company headquartered in USA, also offering email services.
-----------	---

#### SSL Certificate Authorities

IdenTrust	IdenTrust is a SSL certificate authority.
-----------	---

<del>Let's Encrypt</del> used until recently	Let's Encrypt is a free, automated, and open certificate authority provided by the Internet Security Research Group.
---	--

#### JavaScript Content Delivery Network

unpkg	unpkg is a JavaScript content delivery network for libraries that use the npm package manager.
-------	--

h. Subdominios - Algunos subdominios con sus direcciones IP, extraído de <https://synapsint.com/>

Subdomain	IP
a4.frc.utn.edu.ar	200.10.191.202
posgrados.frc.utn.edu.ar	200.10.191.192
bbs.frc.utn.edu.ar	190.114.208.142
industrial.frc.utn.edu.ar	190.114.208.164
st.frc.utn.edu.ar	200.10.191.221
profesores.frc.utn.edu.ar	200.10.191.192
aveit.frc.utn.edu.ar	200.10.191.192
labsys.frc.utn.edu.ar	190.114.208.140
materialeducativo.frc.utn.edu.ar	138.99.7.66
asistenciatecnica.frc.utn.edu.ar	200.10.191.8
www.frc.utn.edu.ar	200.10.191.200
goldlink.frc.utn.edu.ar	200.10.191.226
sysacaddocs.frc.utn.edu.ar	200.10.191.226
educacionadistancia.frc.utn.edu.ar	200.10.191.226
webmaterialeducativo.frc.utn.edu.ar	138.99.7.66
pagos.frc.utn.edu.ar	200.10.191.215
seu.frc.utn.edu.ar	200.10.191.192
calidaddeaireciqa.frc.utn.edu.ar	200.10.191.223
rc.frc.utn.edu.ar	190.114.208.210
conaiisi.frc.utn.edu.ar	200.69.137.172
box.frc.utn.edu.ar	200.10.191.225
listas.frc.utn.edu.ar	200.10.191.11
uve.frc.utn.edu.ar	200.10.191.212
ramada.frc.utn.edu.ar	200.10.191.11
git.frc.utn.edu.ar	200.10.191.4

## Parte 2

1. Levantar el proyecto de "Pixi" y acceder a localhost.
2. Buscar / retomar las vulnerabilidades.
3. Con **una** de ellas, armar la plantilla de vulnerabilidad, definiendo:
  - Título de la vulnerabilidad
  - Categoría de vulnerabilidad
  - Score **CVSS**
  - Descripción (determinando el impacto)
  - Pasos de reproducción
  - Capturas de pantalla
  - Recomendaciones

**Título de la vulnerabilidad:** Logueo en sitio web, sin conocer la contraseña

**Categoría de vulnerabilidad:** Inyección NoSQL - NoSQLi

**Score CVSS:** 9.1 (Crítica)

Vector string CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

**Descripción (determinando el impacto):** puedo loguearme en el sitio Pixi sin necesidad de conocer la contraseña de un usuario determinado.

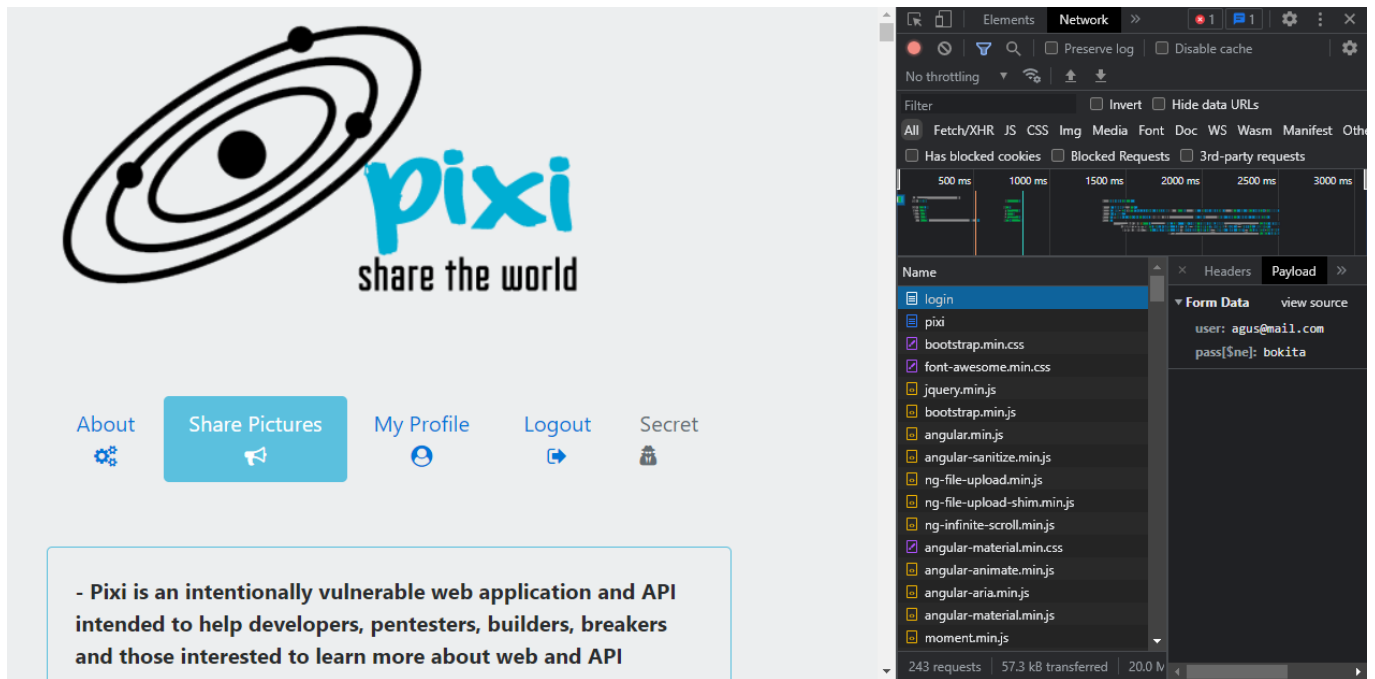
### **Pasos de reproducción:**

1. Ingreso al sitio Pixi, e inspecciono el elemento correspondiente al text box de contraseña.
2. Modifico el name del input type password para verificar si el backend procesa lo que le estoy mandando

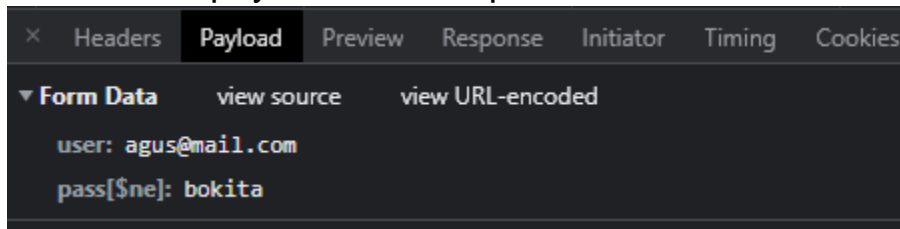
```
<input type="password" class="form-control form-control-lg" id="pass" name="pass[$ne]" placeholder="Password"> == $0
```

De esta forma veremos si el backend toma el operador \$ne para validar que la clave sea not equal al valor ingresado en el input

3. Indico un nombre de usuario existente, en este caso [agus@mail.com](mailto:agus@mail.com), y en la password ingresamos un string cualquiera, como ser "bokita". Cualquier valor serviría, inclusive dejarlo en blanco.
4. Seleccionamos Login y podremos loguearnos



Si vemos el payload de la request



## Recomendaciones:

Implementación de mejoras en el código:

- Sanitización del campo password, es decir, validar que el parámetro sea exactamente un string y no un array.
- Otra alternativa, es validando el parámetro con la función con `filter_input()`