H4ppy H4cking

Hacking Web 101

-Agenda

HTPP Basics
Proceso de carga de una web
Devtools
Documentación básica: OWASP, CVE, CWE
Client Side vs Server Side
Lenguajes para hacking web
Burpsuite 101
Roadmap de aprendizaje/certificación
Demo portswigger (xss, bac)

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

Jesus Lujan aka s4yhii

Encargado del Appsec Squad - CibersecUNI

Appsec Engineer - Banco de Chile

🎁🎉🎉🎁 Trikavengers MMO App🎁🎉🎉🎁

Descarga:

https://drive.google.com/.../1aL9FZU33GkAxxKLGGCghn4tPYMn...

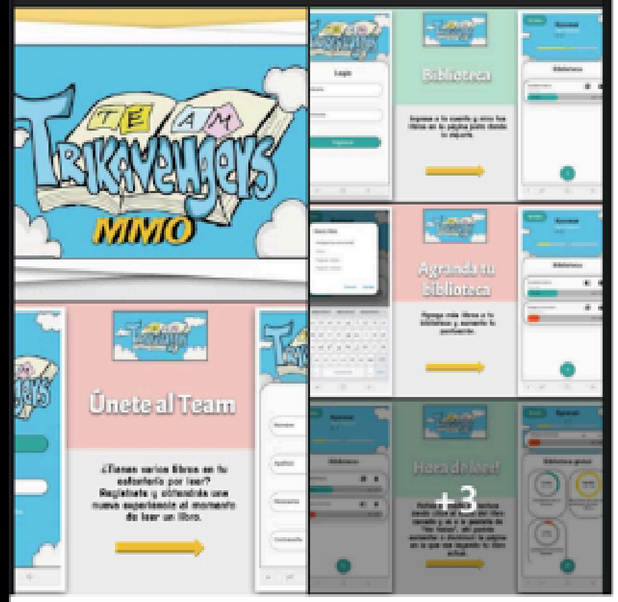
PD: Los usuarios con nicknames o libros con nombres como "fdsafd" (libros que no son reales) se eliminaran.

PD2: Usen contraseñas nuevas para esta app, no usen ninguna personal por si me hackean la base de datos xd.

PD3: La app estará disponible en PlayStore en unas semanas xd, pero no se preocupen porque sus datos no se perderán.

PD4: Si alguien ve algun error o vulnerabilidad me la hace saber por favor, para poder mejorar esos detalles

PD5: Agradecimientos [redacted]



CIBERSECFIS

Informe de Auditoria

POST [redacted]

Params Authorization Headers (9) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL Text

```
{
  "nombres": "Hacked by",
  "apellidos": "CiberSec FIIS",
  "nickname": "Hacked by CiberSec FIIS",
  "contrasenia": "Un33d4Str0ngP4ssw0rd!"
}
```

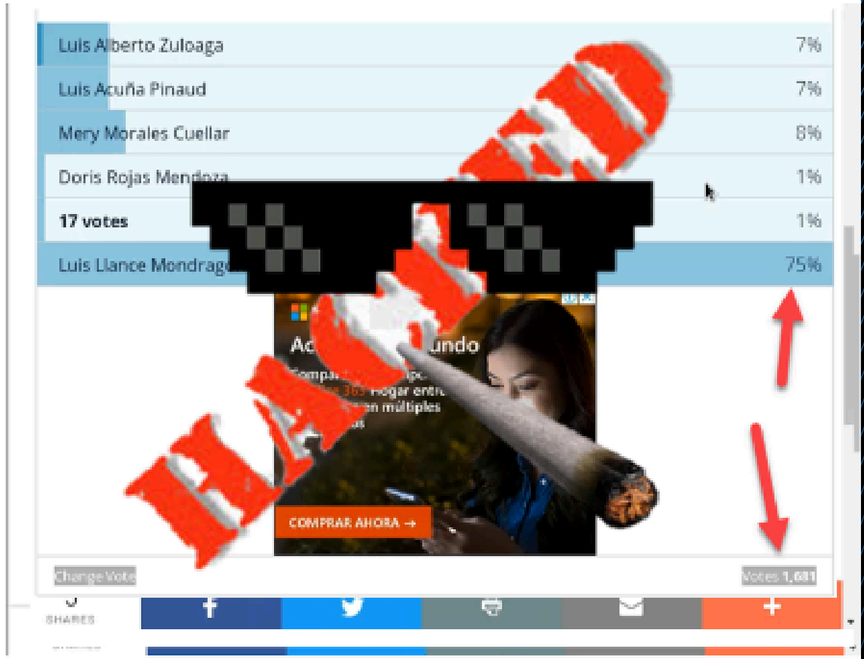
Body Cookies Headers (7) Test Results

Pretty Raw Preview Visualize JSON

```
{
    "fieldCount": 0,
    "affectedRows": 1,
    "insertId": 146,
    "serverStatus": 2,
    "warningCount": 0,
    "message": "",
    "protocol41": true,
    "changedRows": 0
}
```

Fig. 5. Prueba de concepto de inserción de nueva data c

La aplicación no pasó esta prueba de concepto.



Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

-Qué es la seguridad web

- **Proteger nuestras aplicaciones ante acciones malintencionadas o acciones no previstas.**
- **Prevenir que el usuario sea atacado mientras usa alguna aplicación web**

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

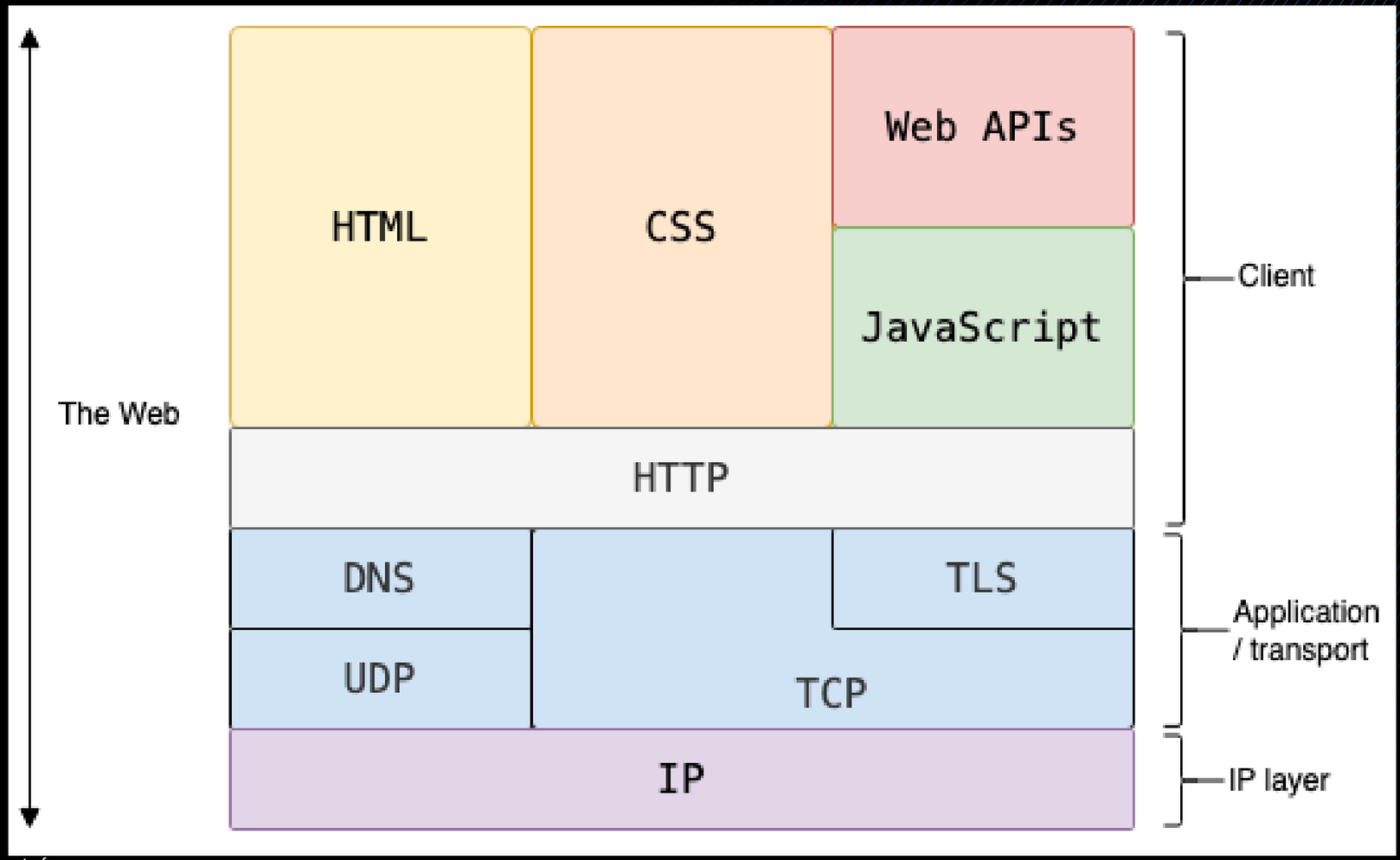
<CIBERSEC>
UNI

-Por qué aprender seguridad web

- Mayoría de empresas usan la web para disponibilizar sus servicios. (salesforce, amazon, tesla, etc...)
- El hacking web está disponible para todos gracias al navegador
- DevTools, Burpsuite (sin kali?, igual funciona)

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

HTTP



Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

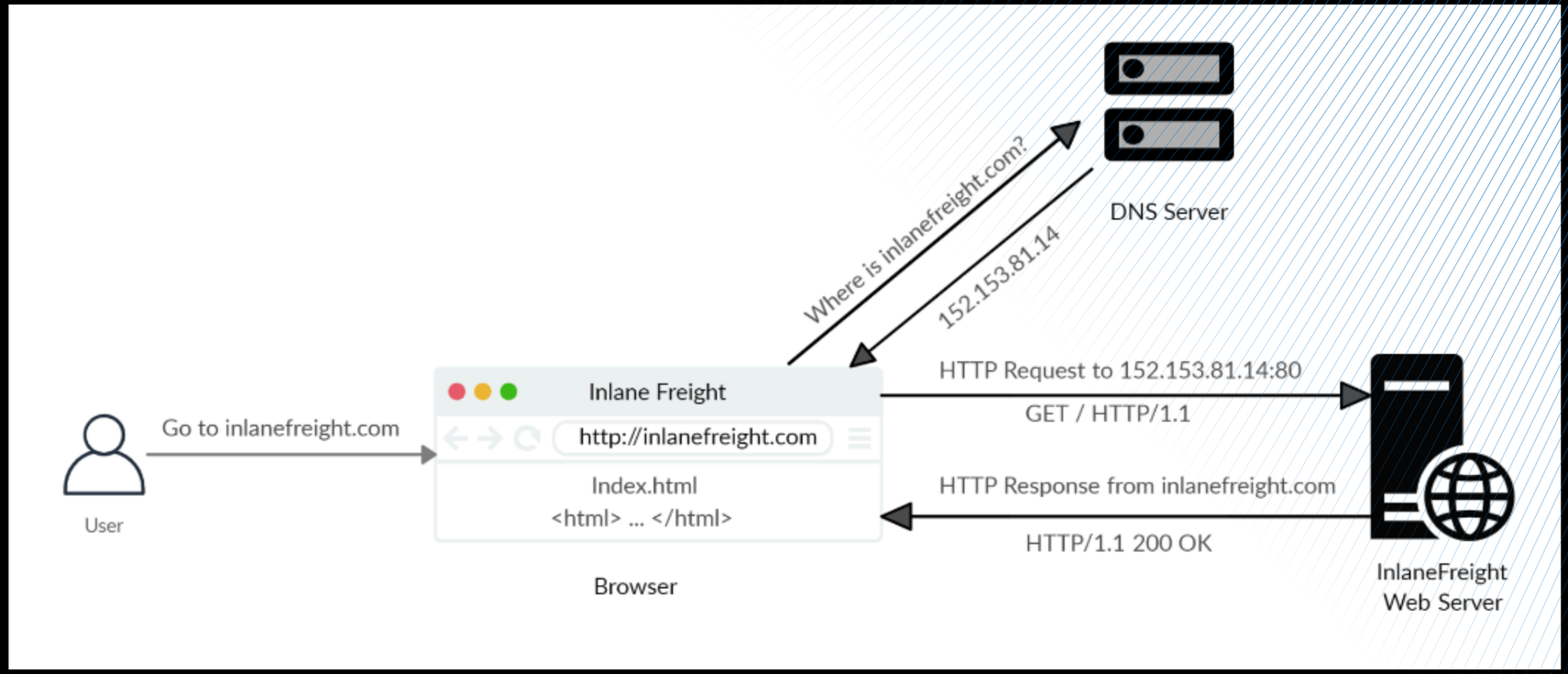
<CIBERSEC>
UNI

-Uniform Resource Locator (URL)

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

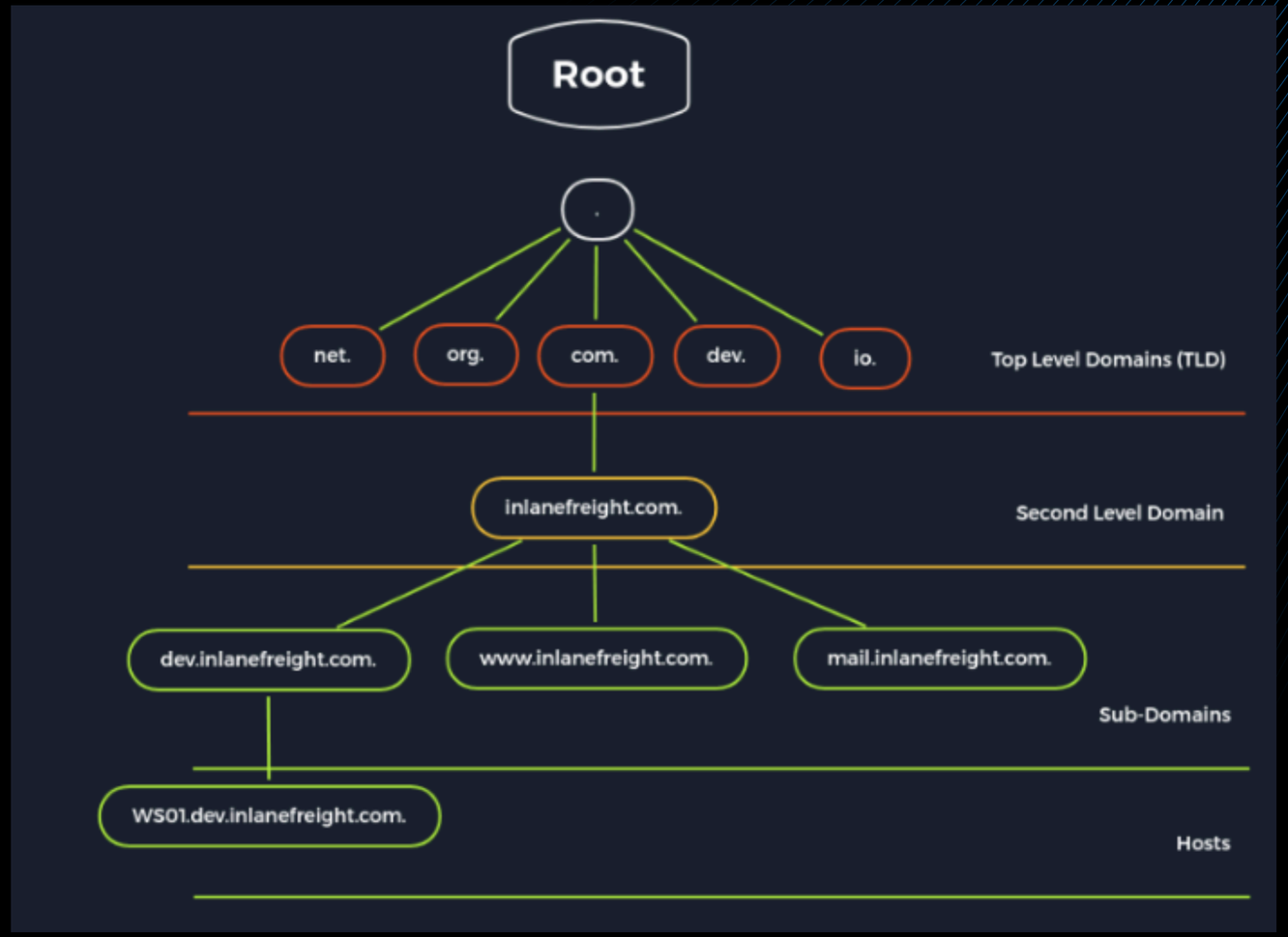
-¿Cual es el proceso de carga de una web?



Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

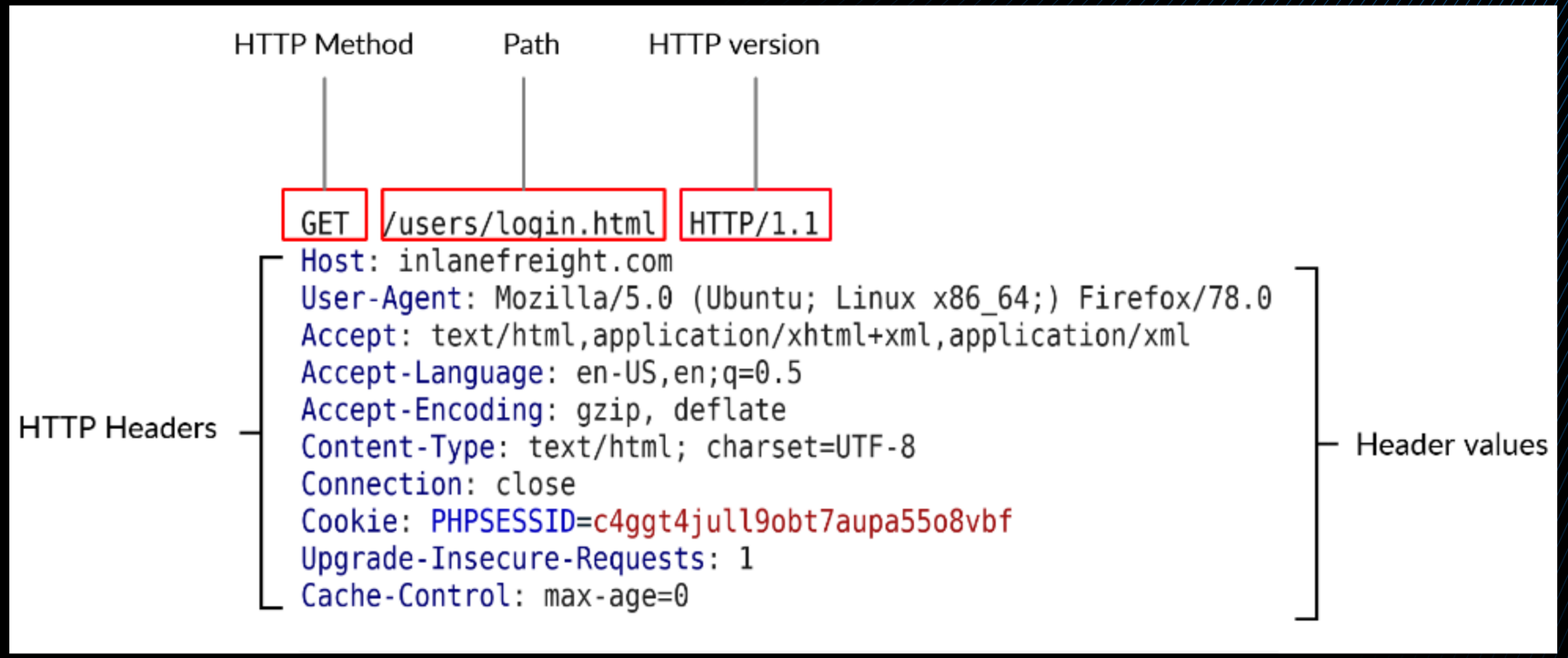
-Estructura del DNS



Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

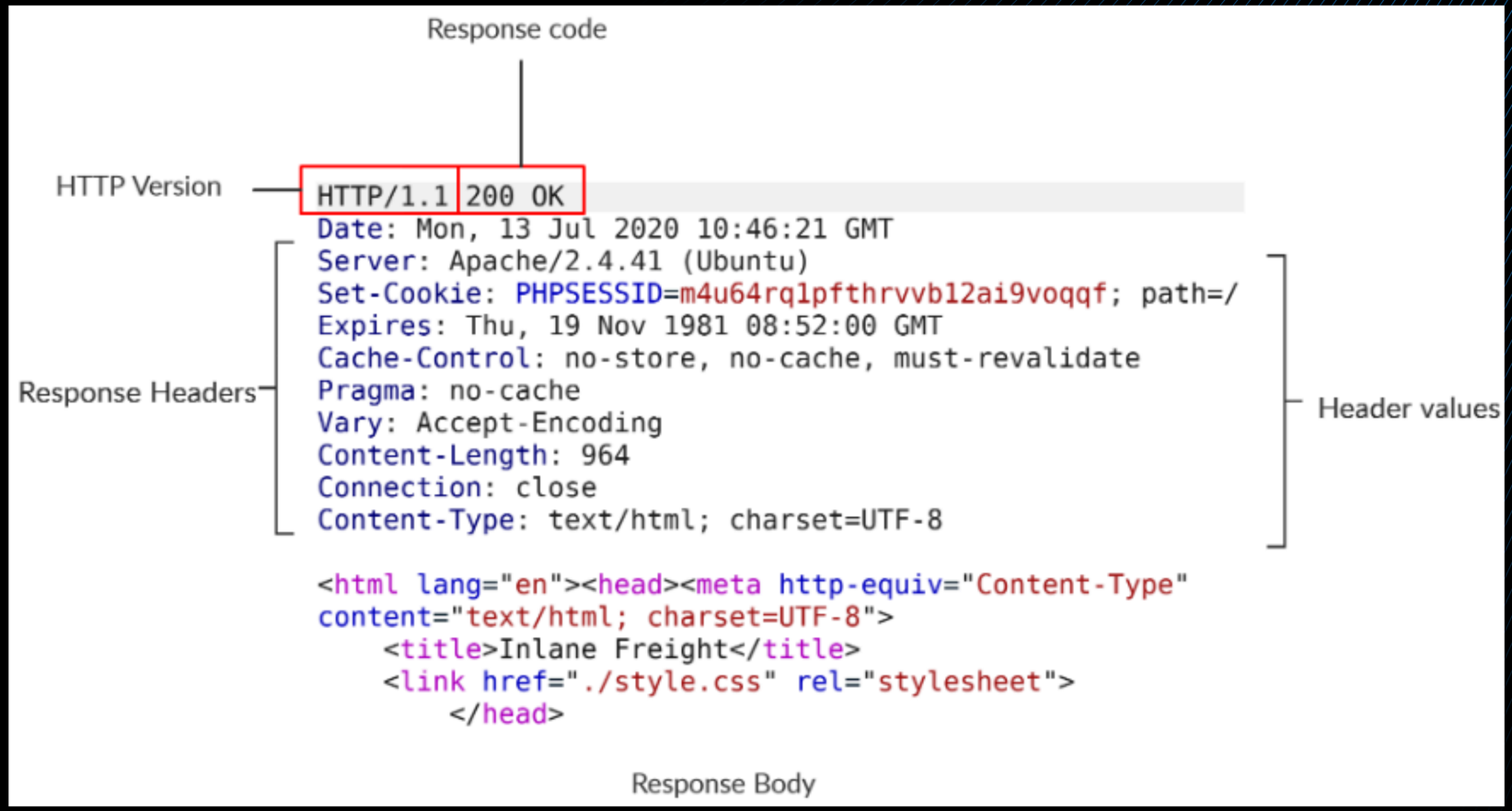
-Consulta HTTP



Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

-Respuesta HTTP



Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

-Devtools

Devtools será nuestro principal instrumento para analizar páginas web y encontrar vulnerabilidades.

Shortcut: Ctrl + Shift + I
Mac shortcut: Command + Shift + I
Principales Tabs: Elements, Console, Sources, Network, Application

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

demo developer tool firefox

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

-Métodos HTTP

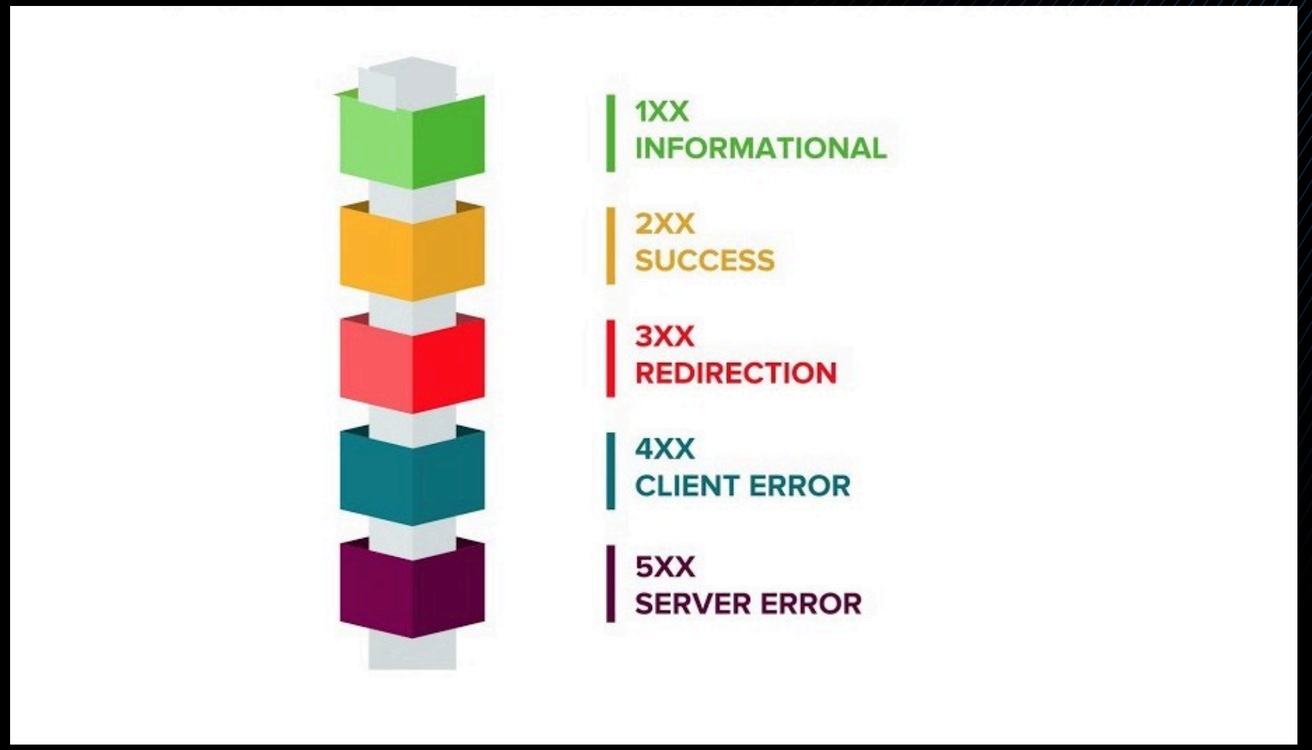
GET	POST	PUT	DELETE	PATCH	HEAD
retrieve data from server	add data to an existining file or resource	update(replace) an existing file or resource in server	delete data from server	update a resource partially (modify)	retrieve the resource's headers

- **CONNECT** is used to open a two-way socket connection to the remote server;
- **OPTIONS** is used to describe the communication options for specified resource;
- **TRACE** is designed for diagnostic purposes during the development.
- **HEAD** retrieves the resource's headers, without the resource itself.

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

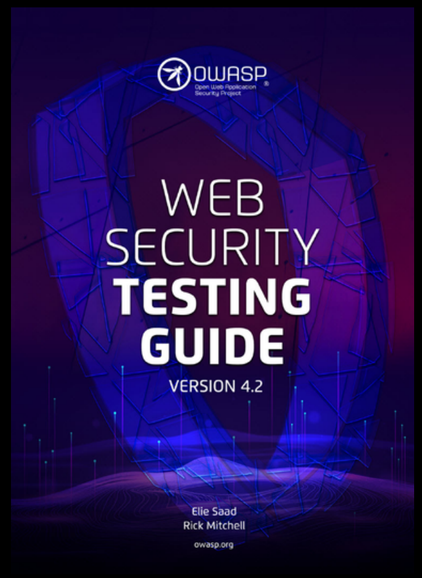
<CIBERSEC>
UNI

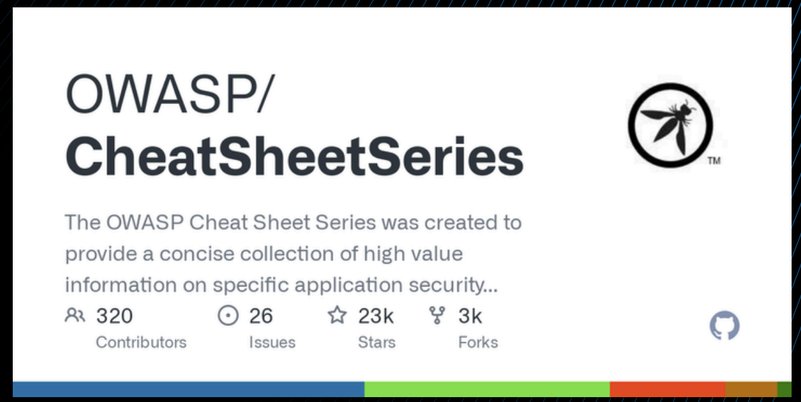
-Códigos de estado HTTP



Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI





Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

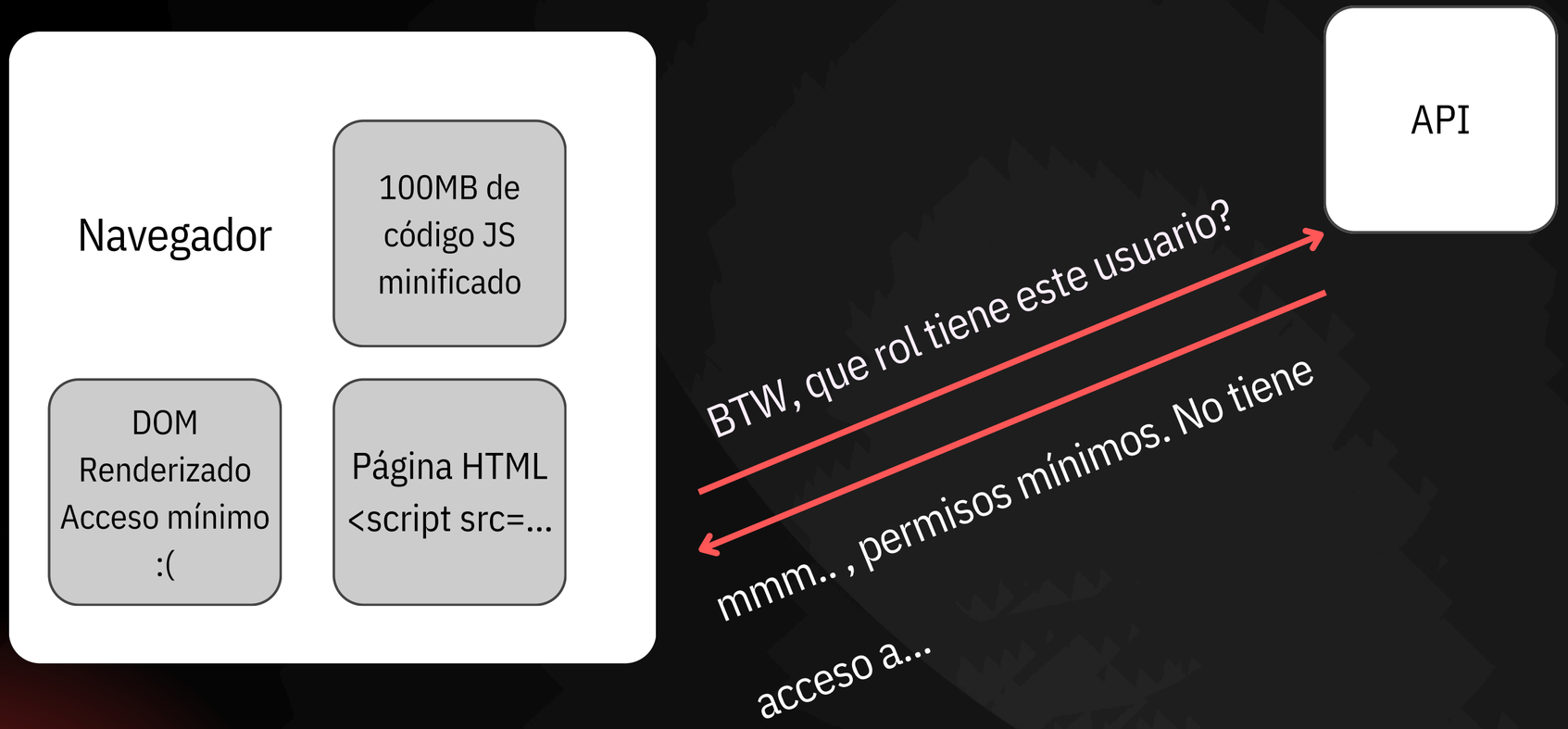
<CIBERSEC>
UNI

-Client Side vs Server Side

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

Como funcionan las webs modernas



Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

Como funcionan las webs

Navegador
- “Lo que tu digas, mr API!”

100MB de código JS minificado

DOM Renderizado SUPER ADMIN, MEGA USER!

Página HTML <script src=...

BTW, que rol tiene este usuario?

TODOS LOS ACCESOS, SUPER ADMIN, TODAS LAS FUNCIONES, MEGA USER!

Obviamente no soy Burpsuite.
Api legítima

if(kl.mE===w.tF){0,w,HY)(Z)]

if(user.role===”MEGA_ADMIN”){Enseña las funciones ocultas del UI}

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

Lenguajes a aprender para web hacking

- Javascript (Client-side)
- Python (Back-end)
- Java (Back-end)

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

-Como usar burpsuite, tips

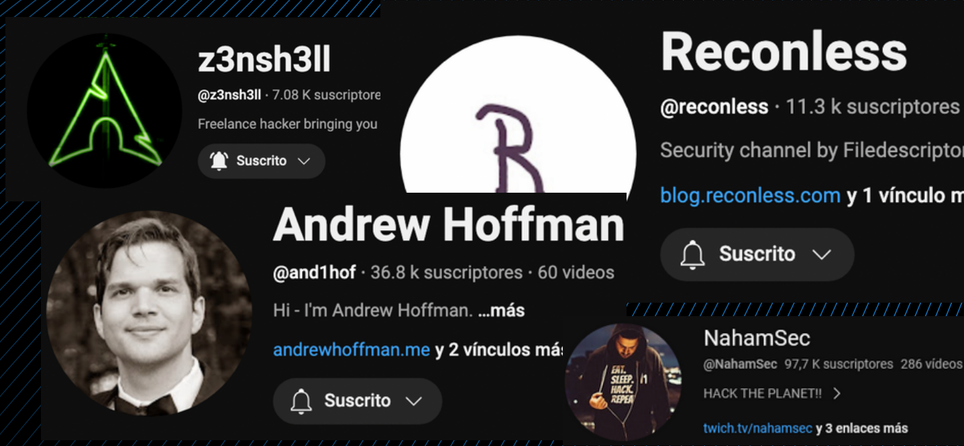
Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

Application In-security

Roadmap de aprendizaje/certificación.

1 etapa

2 etapa



3 etapa

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

<CIBERSEC>
UNI

demo htb (Kryptos Support chall)

Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

Gracias

CIBERSEC
UNI

Conectemos