

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)



Jesus Lujan aka s4yhii



Encargado del Appsec Squad - CibersecUNI

Appsec Engineer - Inside Sec
(Banco de Chile)

-Antecedentes

Trikavengers MMO App

Descarga:
<https://drive.google.com/.../1aL9FZU33GkAoxKLGGcghn4tPyMn...>

PD1: Los usuarios con nicknames o libros con nombres como "Idsal" (libros que no son reales) se eliminarán.

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

CIBERSEC Audit Tool Screenshot:

Informe de Auditoría

POST https://[REDACTED].amazonaws.com/test/

Body

```
[{"id": 1, "nombre": "Hecked by", "apellidos": "CIBERSEC FIIIS", "nickname": "Hecked by CIBERSEC FIIIS", "contraseña": "Un13d45tringP4ssw0rd!"}]
```

Body Results

```
[{"id": 1, "fieldCount": 8, "affectedRows": 1, "insertId": 146, "serverStatus": 2, "warningCount": 0, "message": "", "protocol41": true, "changedRows": 0}]
```

Social Media Poll Screenshot:

Luis Alberto Zuloaga 7%
Luis Acuña Pinaud 7%
Mery Morales Cuellar 8%
Doris Rojas Mendoza 1%
Luis Llance Mondragó 75%

17 votes
 COMPRAR AHORA →
Votes 1,681

SHARES

Fig. 5. Prueba de concepto de inserción de nueva data c
La aplicación no pasó esta prueba de concepto.

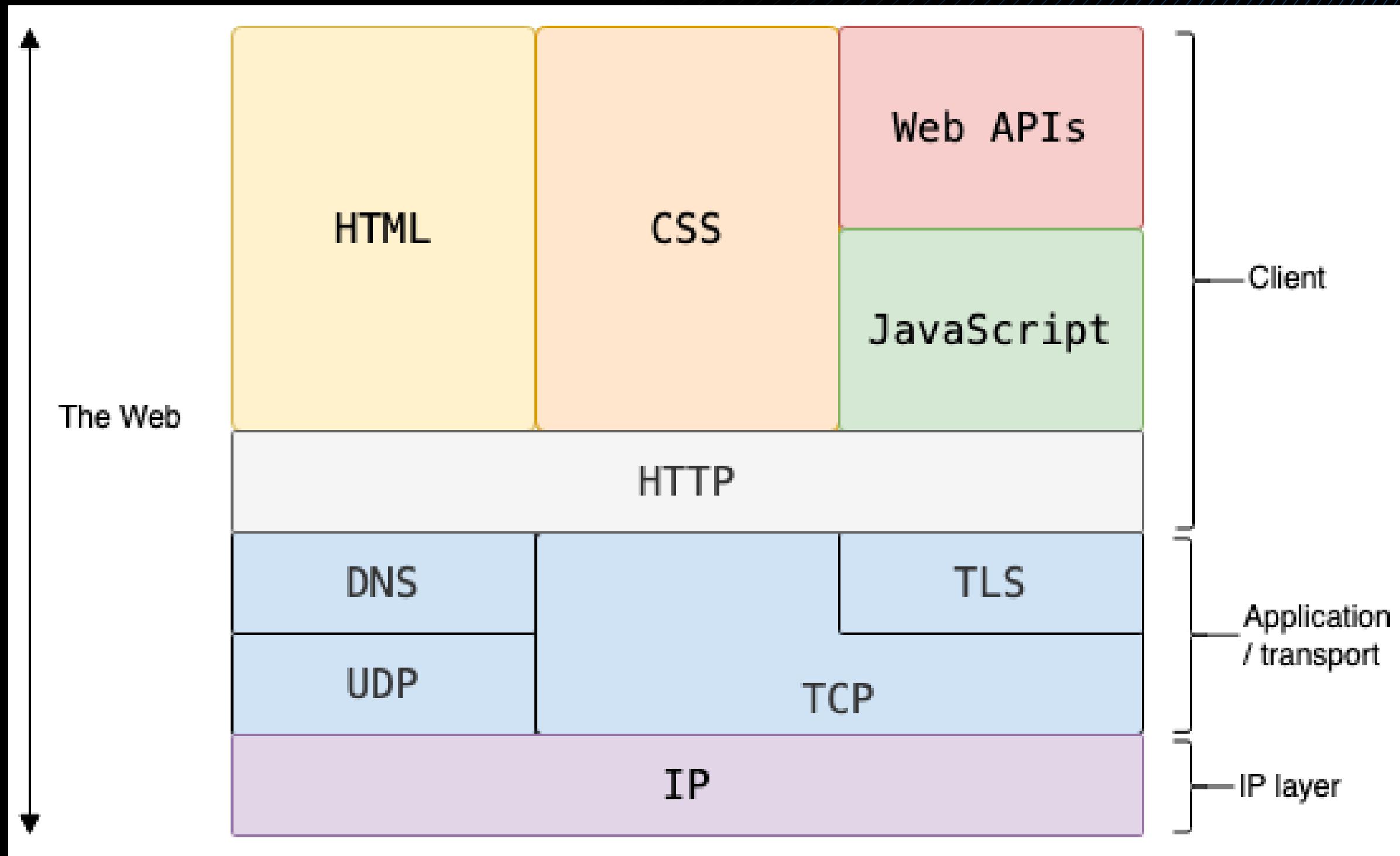
-Qué es la seguridad web

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

-Por qué aprender seguridad web

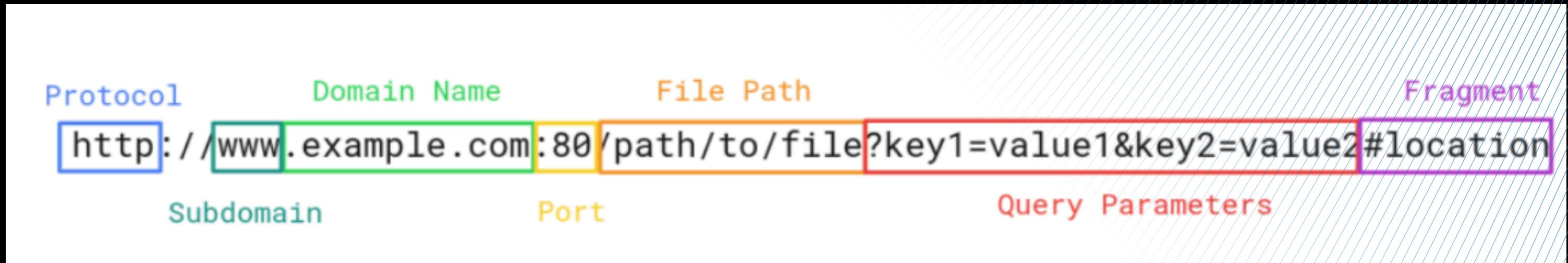
- **Mayoría de empresas usan la web para disponibilizar sus servicios. (salesforce, amazon, tesla, etc...)**
- **El hacking web está disponible para todos gracias al navegador**
- **DevTools, Burpsuite (sin kali?, igual funciona)**

HTTP

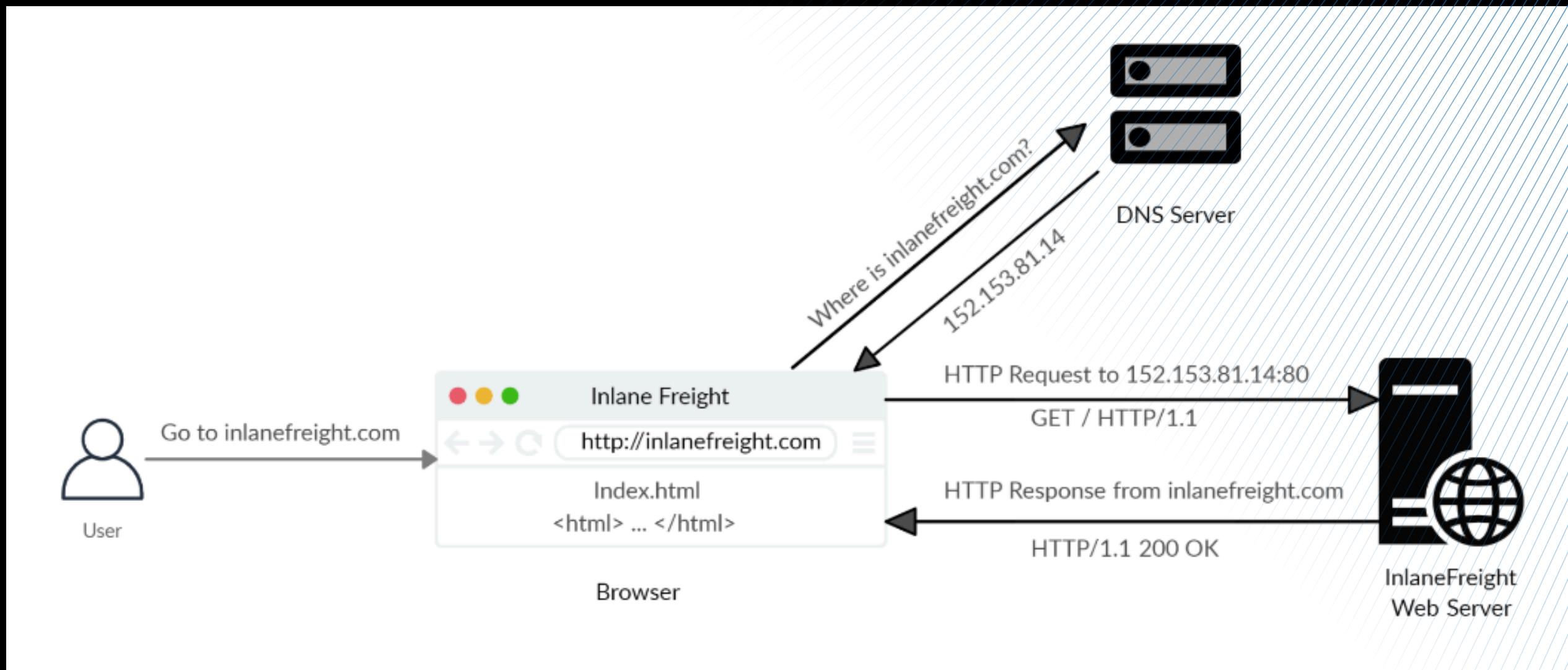


Instructor: Jesus Lujan Montufar
<https://www.linkedin.com/in/jesusaluj4n/>

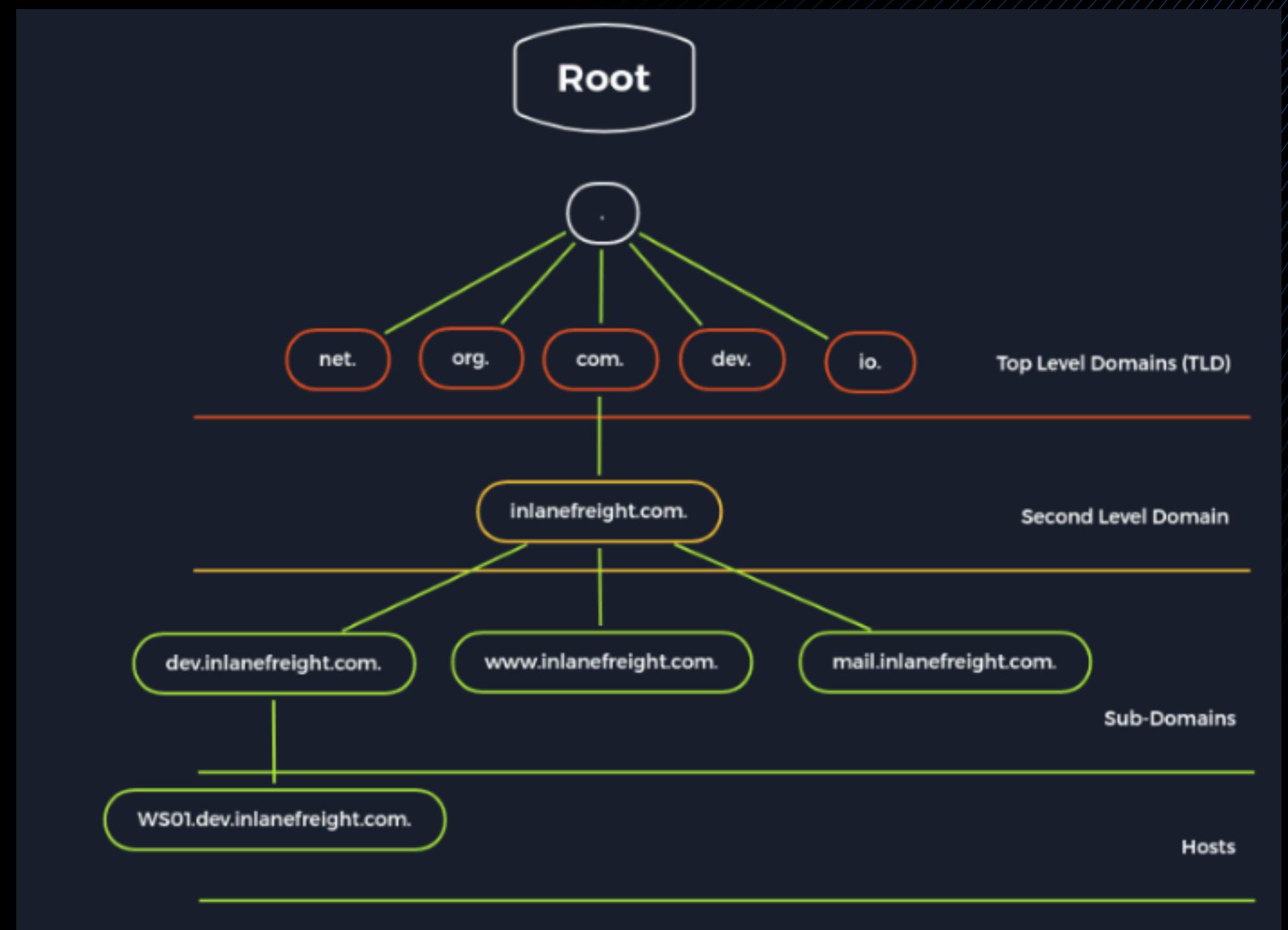
-Uniform Resource Locator (URL)



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

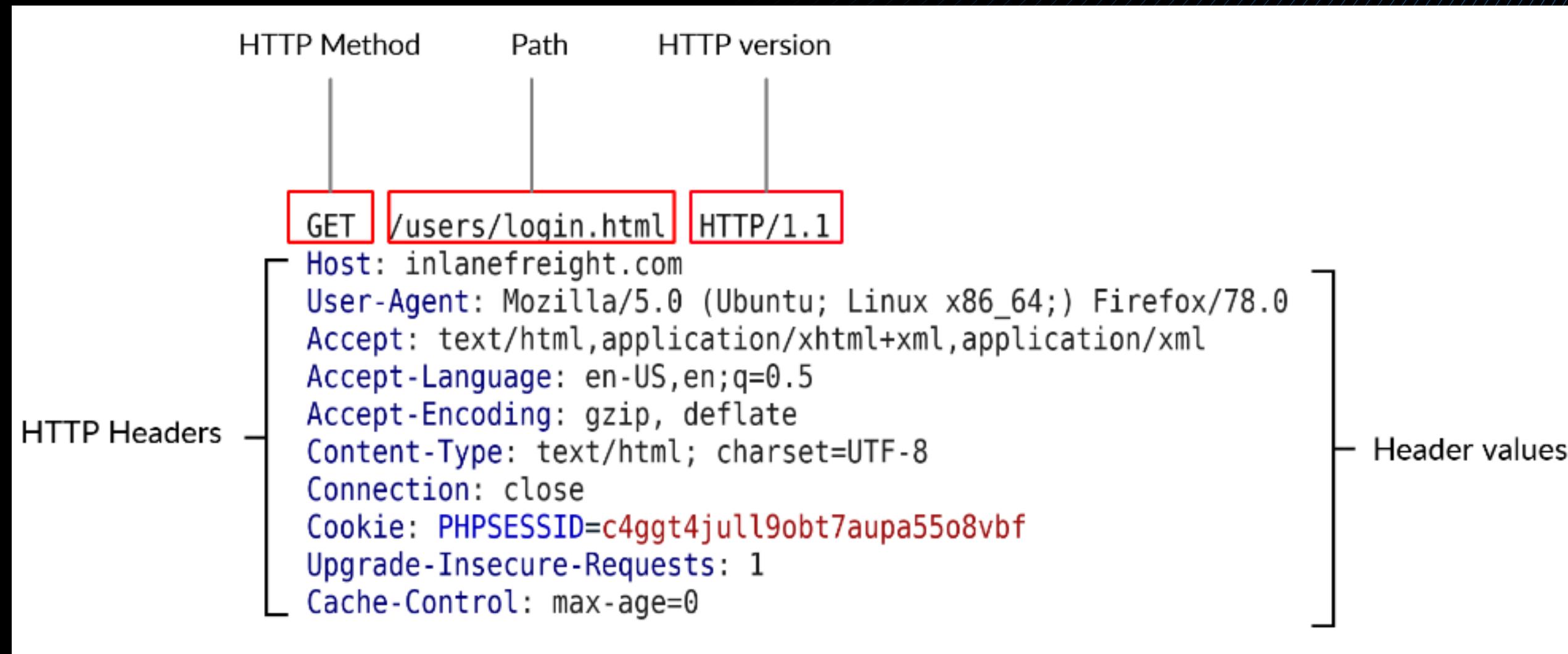


-Estructura del DNS

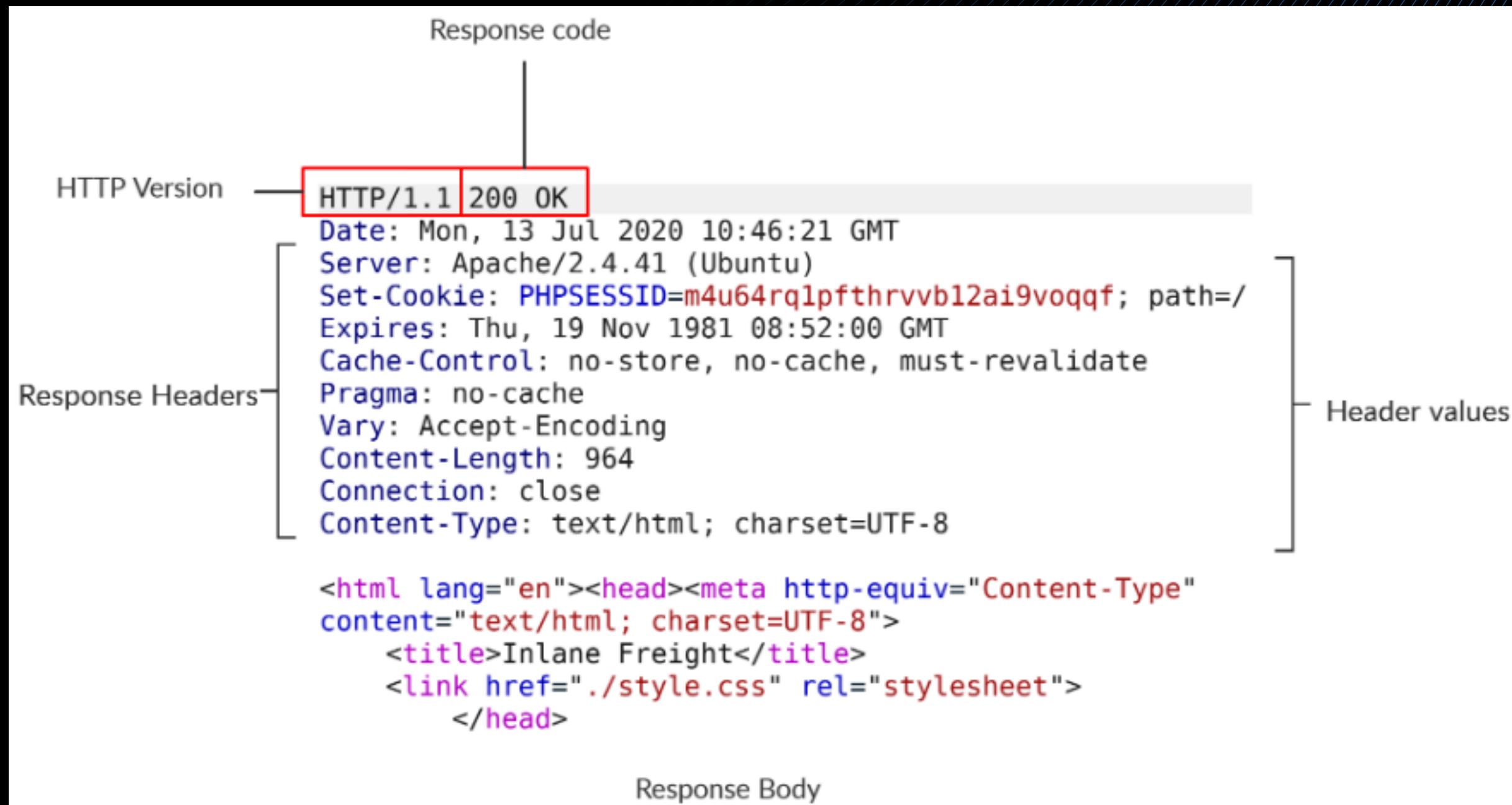


Instructor: Jesus Lujan Montufar
<https://www.linkedin.com/in/jesusluj4n/>

-Consulta HTTP



-Respuesta HTTP



-Devtools

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

Shortcut: Ctrl + Shift + I

Mac shortcut: Command + Shift + I

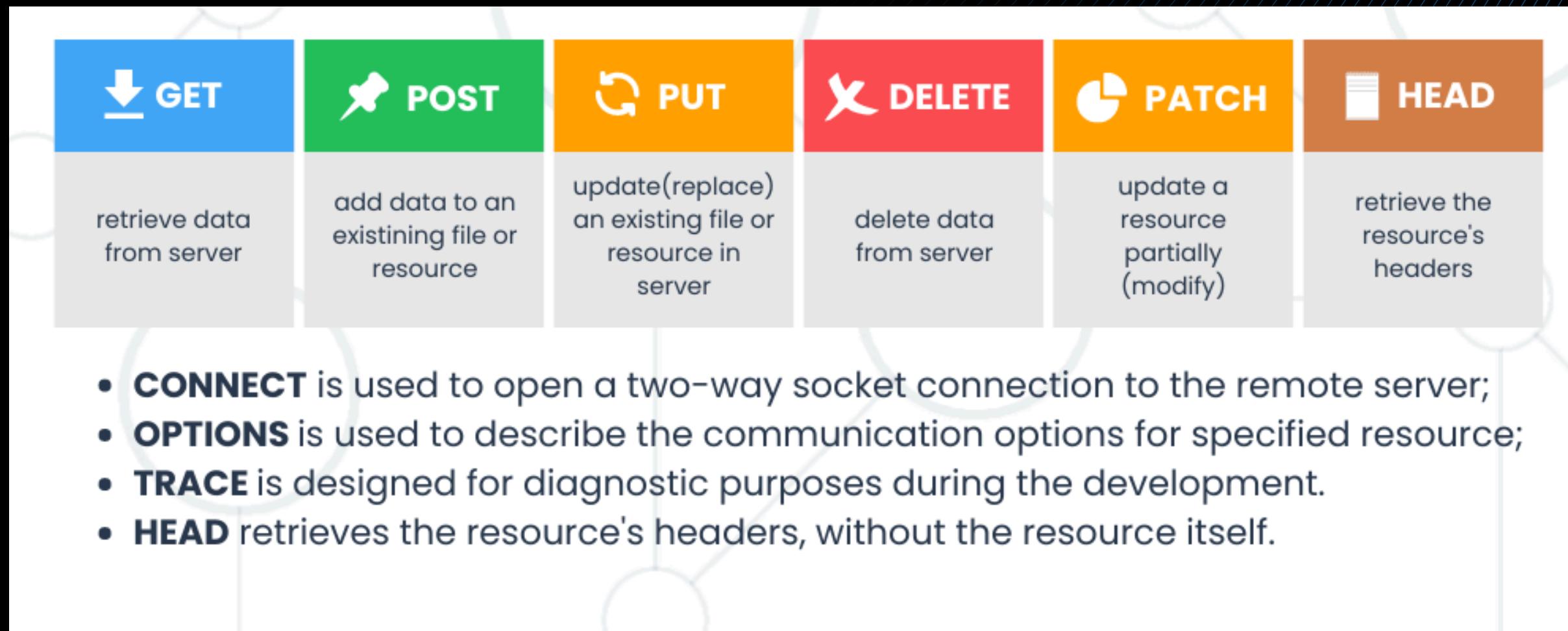
Principales Tabs: Elements, Console, Sources, Network,
Application

demo developer tool firefox

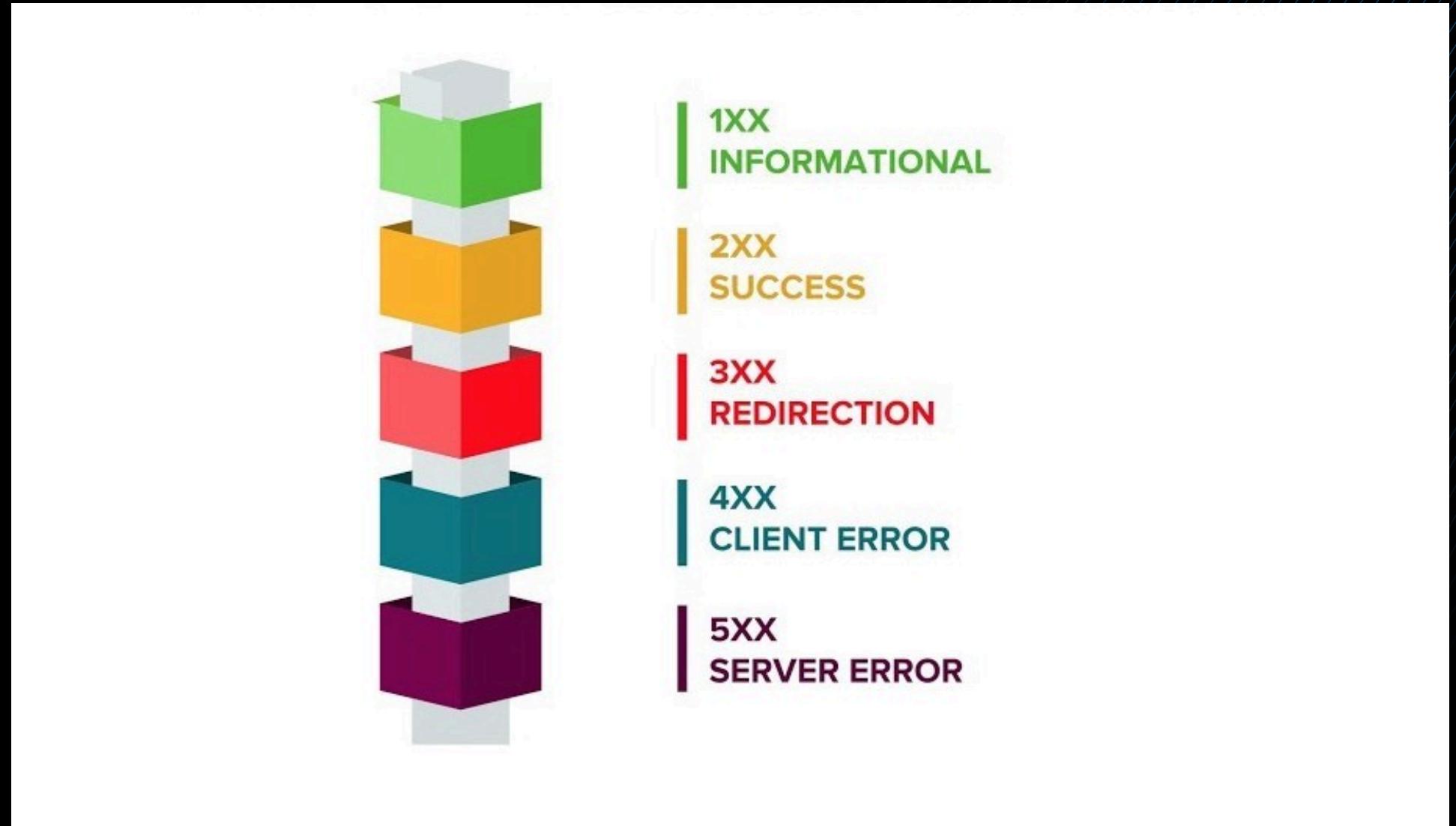
Instructor: Jesus Lujan Montufar
<https://www.linkedin.com/in/jesusluj4n/>



-Métodos HTTP



-Códigos de estado HTTP





OWASP/ CheatSheetSeries

The OWASP Cheat Sheet Series was created to provide a concise collection of high value information on specific application security...

320 Contributors 26 Issues 23k Stars 3k Forks

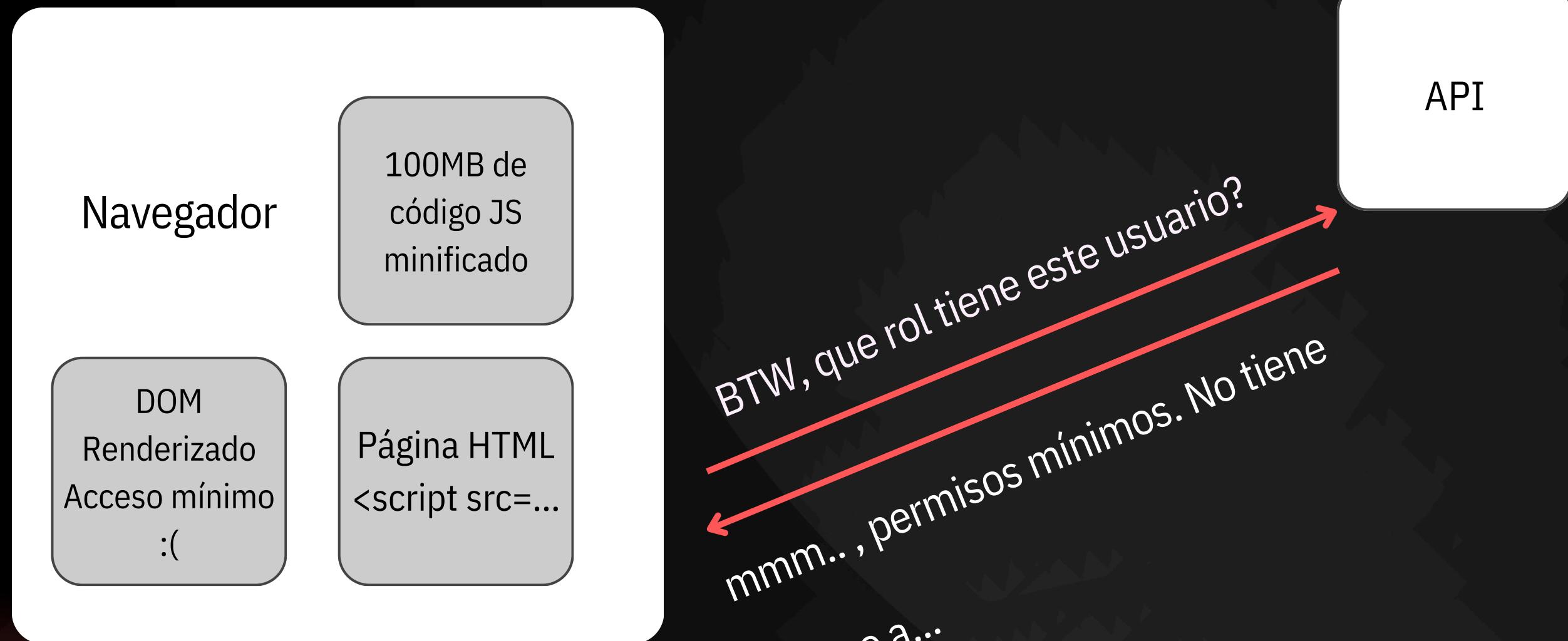


-Client Side vs Server Side

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



Como funcionan las webs modernas



Como funcionan las webs

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

DOM
Renderizado
SUPER ADMIN,
MEGA USER!

100MB de
código JS
minificado

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

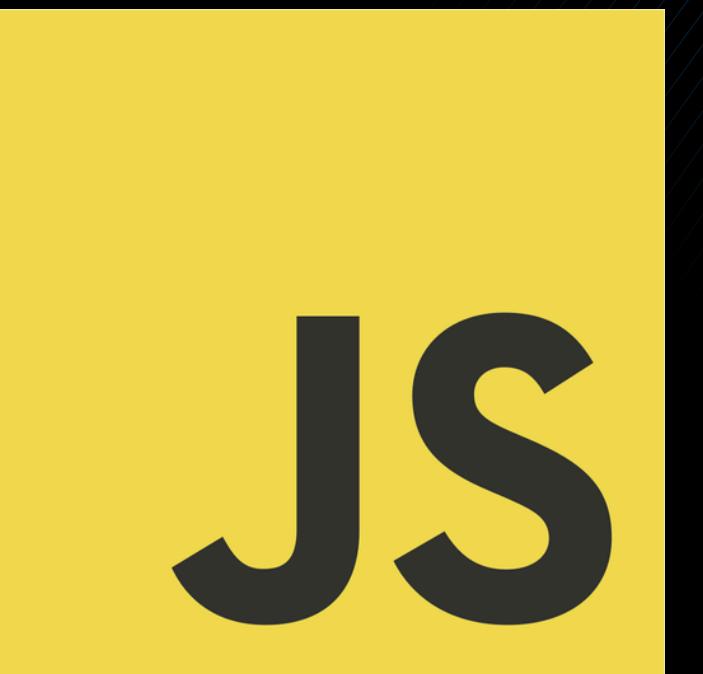


```
if(kl.mE==w.tF){O,w,HY)(Z)]
```

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

Lenguajes a aprender para web hacking

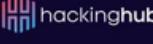
- Javascript (Client-side)
- Python (Back-end)
- Java (Back-end)



-Como usar burpsuite, tips

Application In-security

Roadmap de aprendizaje/certificación.

Web Hacking & Bug Bounty Course 

Essentials
Security Basics
Front End vs Backend
HTTP Basics
Regular Expressions
Curl Basics

Basic Vulnerabilities
Cross-Site Scripting
Cross-Site Request Forgery
Exploiting Cross-Origin Resource Sharing (CORS)
Insecure Direct Object Reference (IDOR)
Hacking JSON Web Tokens
Open Redirects
403 Bypasses
Reverse Proxies

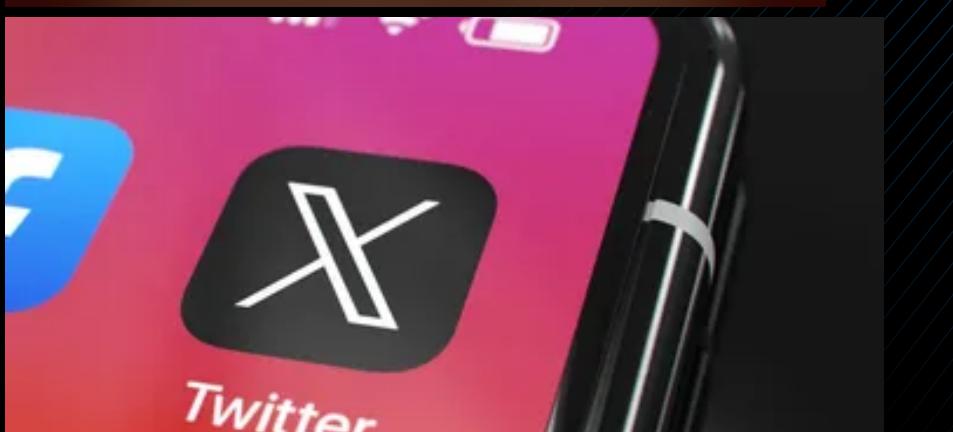
Advanced Vulnerabilities
CSP & Filter Bypass
Attacking Authentication Mechanism
Account Takeover Methods
SQL Injection
XML External Entity (XXE)
Remote Command Execution
Server-Side Request Forgery

Discount Code: LINKEDIN



1 etapa

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



CTF TIME



2 etapa



Security channel by Filedescriptor

blog.reconless.com y 1 vínculo m

 Suscrito



HACK THE PLANET!! >

twitch.tv/nahamsec y 3 enlaces más



3 etapa



demo htb (Kryptos Support chall)

Gracias

Conectemos

