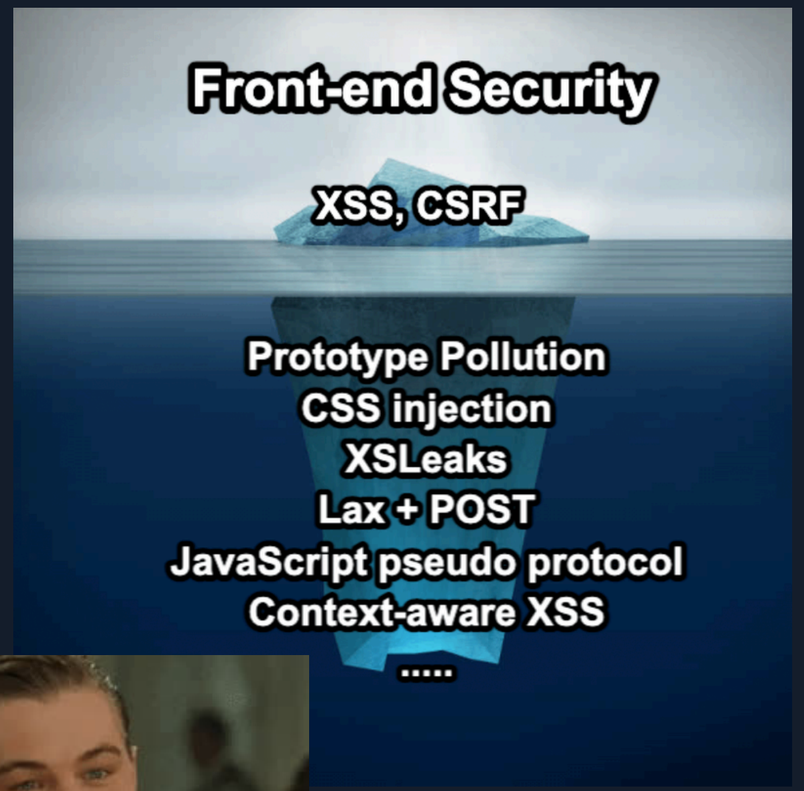
Breaking the Frontend - Client Side Hacking 101

Jesus Lujan (Aka. s4yhii)



Hack The Box Meetup:
Lima, PE.

HACKTHEBOX

<CIBERSEC>
UNI

Contenido

Introducción al Hacking Client-Side

1. Qué es client-side?
2. Web Architecture + Browser Security Model
3. Casos reales
    - (Tampering javascript, Local Storage attack, Cookie attacks, XSS, Postmessage, Source Mapping...)

Devtools for hacking

Devtools 101: **Elements, Console, Sources, Network, Application**

Reverseando Javascript en el navegador

1. Source Mapping: Revelando código original
2. Lazy Loading (Carga diferida) de Javascript
3. Desofuscación de archivos JS

Vulnerabilidades Client-Side

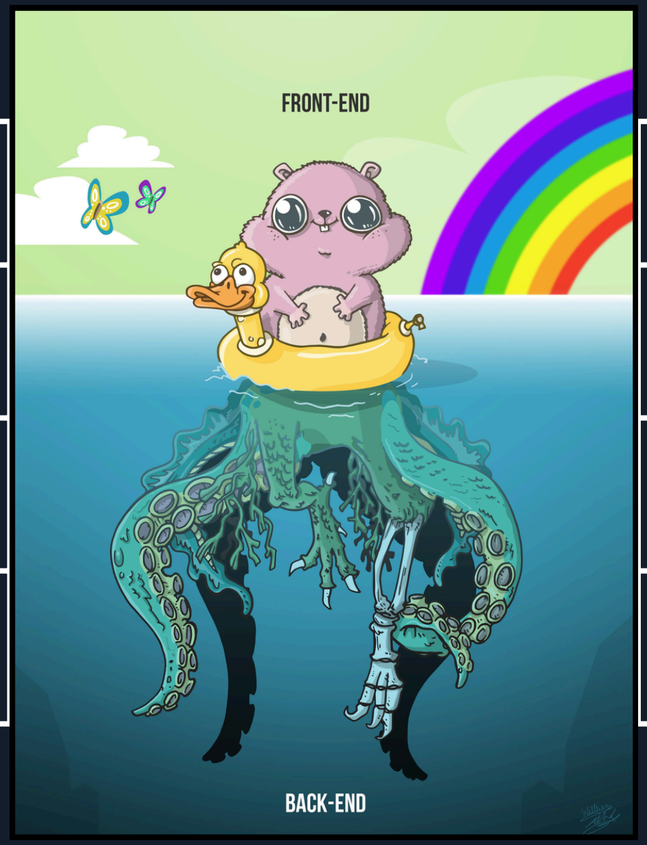
1. Habilitando funciones restringidas
2. Sobreecribir funciones y redefinir eventos
3. Usando Breakpoints para debuggear JS
4. Proximamente... (CSPT, CSTI)

CTF Time (2 Vip+ winners)

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

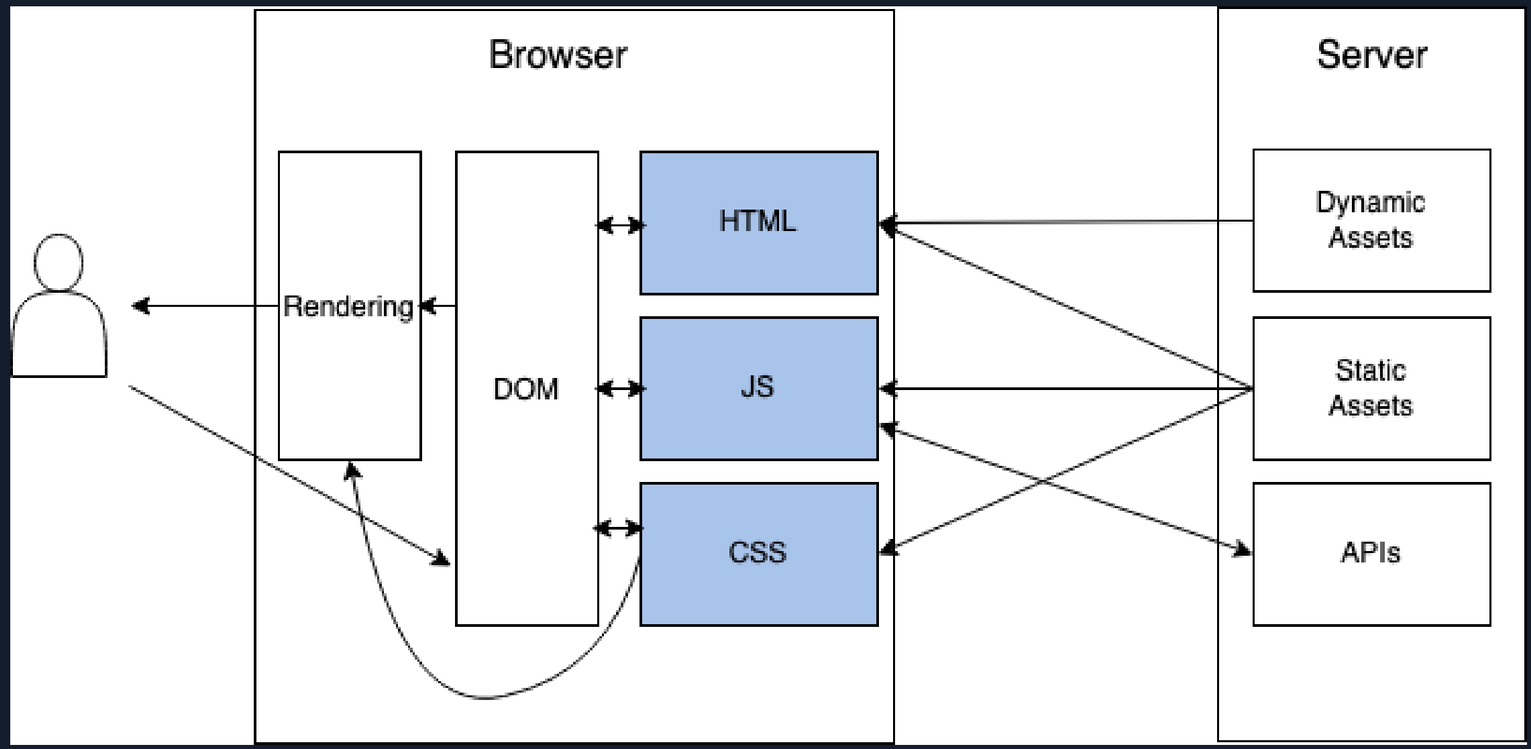
Qué es client side?

Client-Side	Server-Side
Se ejecuta en el navegador (HTML, CSS, JS)	Se ejecuta en el servidor (PHP, Python, Node)
Modificable por los usuarios (DevTools)	No es visible por los usuarios (Lógica de la app)
Ejemplos: Botones como click, Validaciones en formularios	Ejemplo: Consultas a la bd, autenticación?



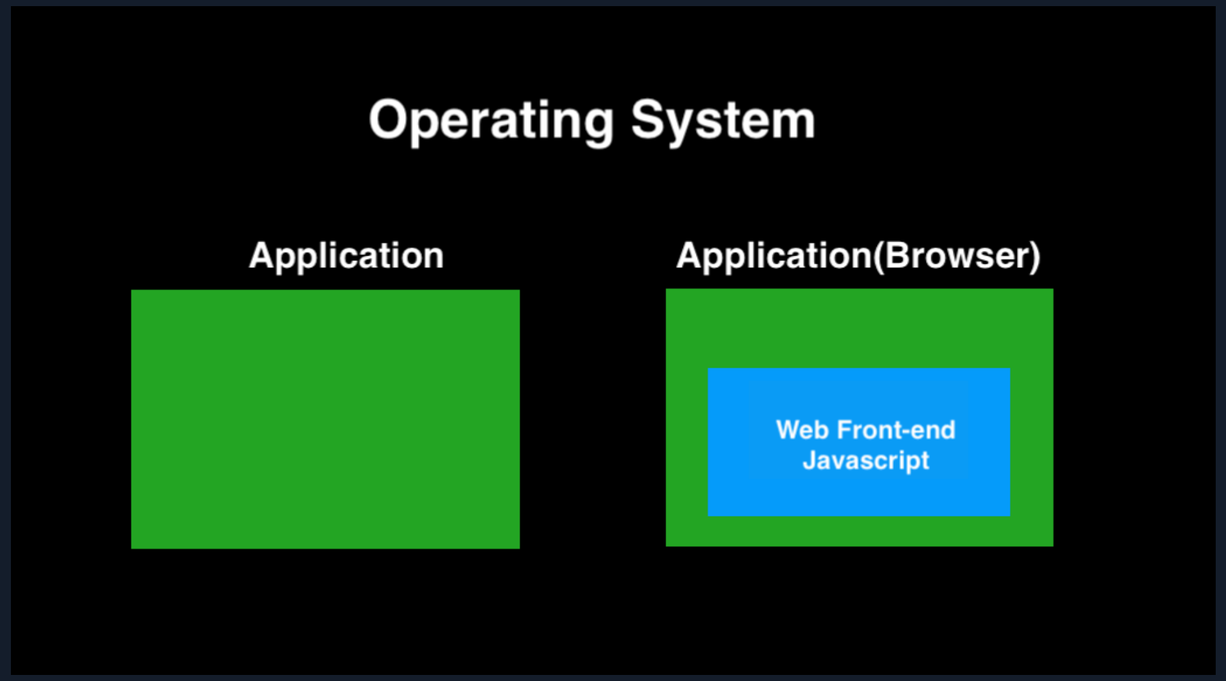
Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

Web Architecture



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

Browser Security Model



Limitaciones del navegador

- Archivos locales
- APIs del sistema
- Contenidos de otras páginas web

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

Importante??

HACKTHEBOX

<CIBERSEC> UNI

Client-side RCE via symlink following in Google Web Designer for macOS/Linux: CVE-2025-1079

Using YouTube to steal your files

Hacking Starbucks and Accessing Nearly 100 Million Customer Records

Sat Jun 20 2020

Links de referencia al final

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

Devtools for hacking 101

HACKTHEBOX

<CIBERSEC> UNI

- Panel Elements:

Modificar el DOM (editar formularios, botones, campos ocultos)

- Panel Console:

Ejecutar JavaScript en tiempo real, sobreescribir variables, usar debugger

- Panel Network:

Interceptar llamadas a APIs, modificar peticiones fetch

- Panel Application:

Manipular cookies, localStorage, sessionStorage, IndexedDB

- Panel Sources:

Depurar la ejecución de JavaScript, establecer puntos de interrupción (breakpoints)

Lab URL : http://localhost:3000

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

CTF TIME
(10 min)

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

Ingresa a:
http://spooky.bugcrowd.zw.ink/klown.cfm

Y enviame Screenshoot por Disc del Secret password

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

Reverseando JS

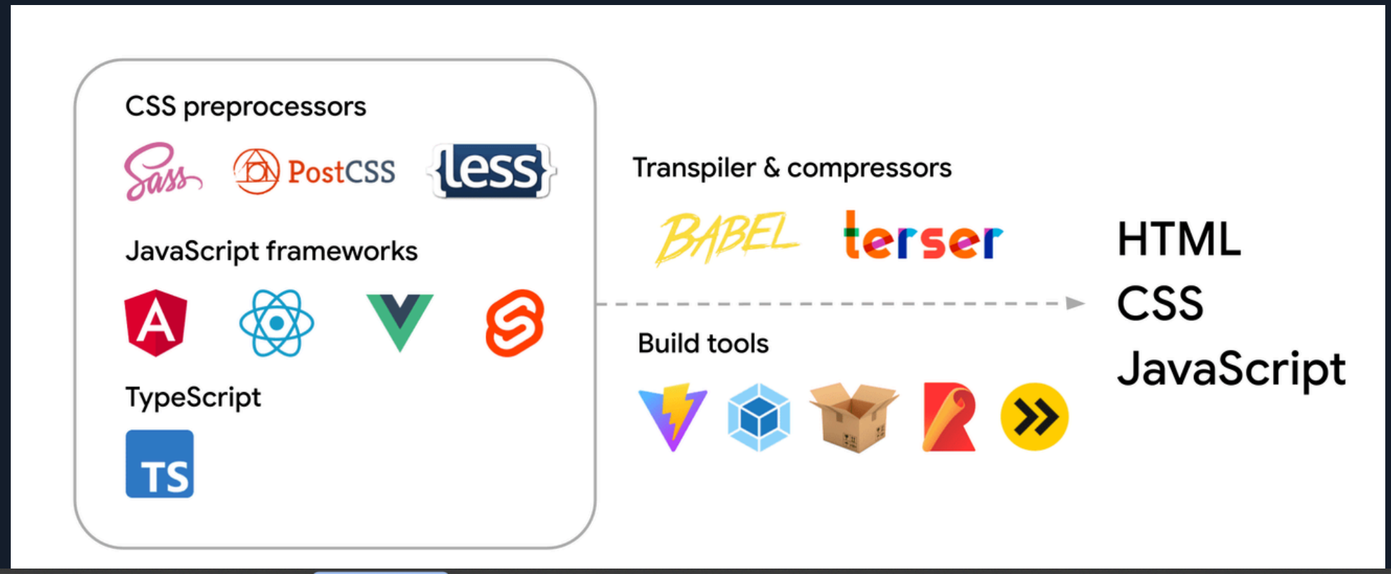
Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

Source Mapping, que es?

HACKTHEBOX

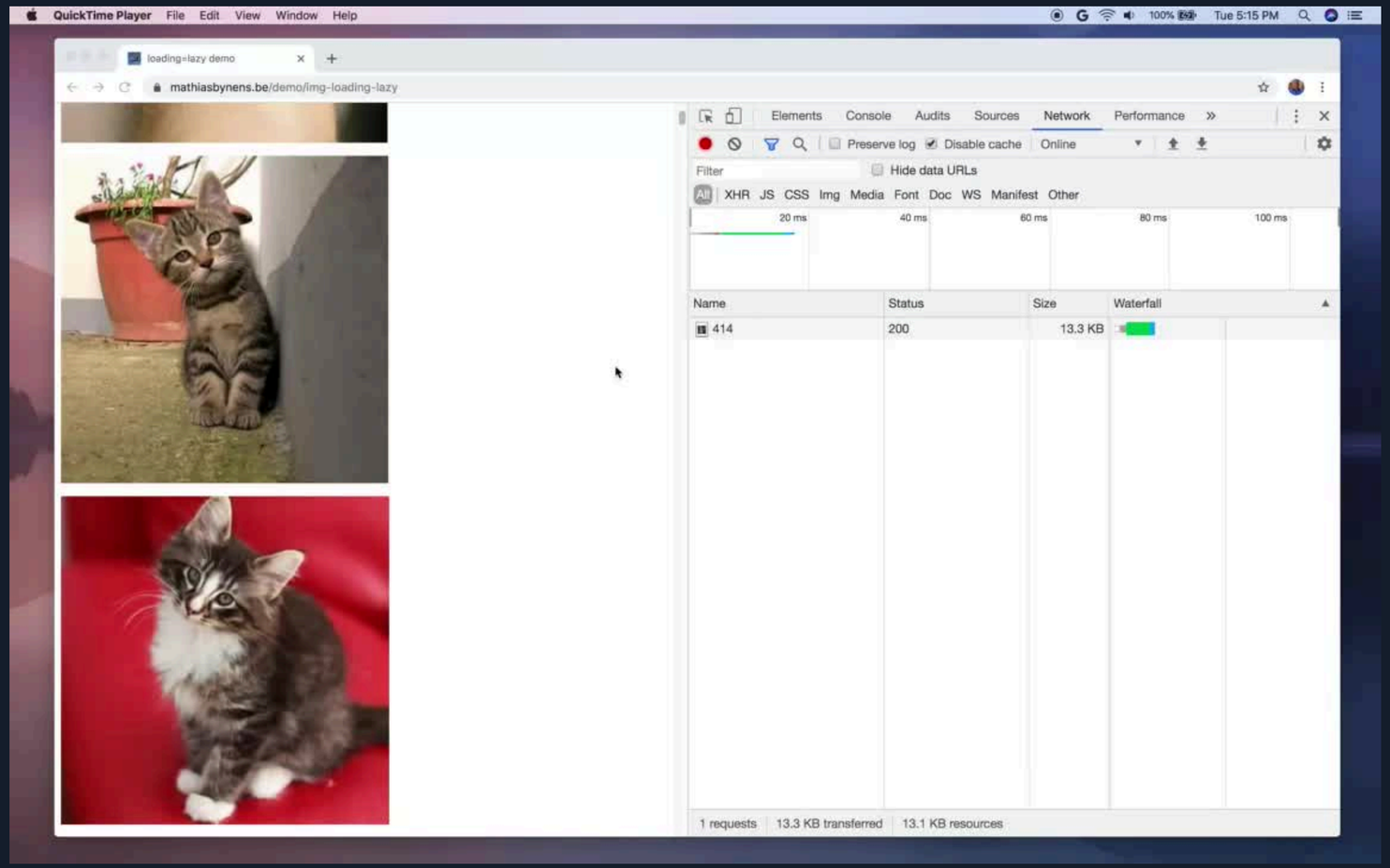
<CIBERSEC> UNI

Herramienta que permite debugear código más facil.



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

Lazy Loading o Carga diferida

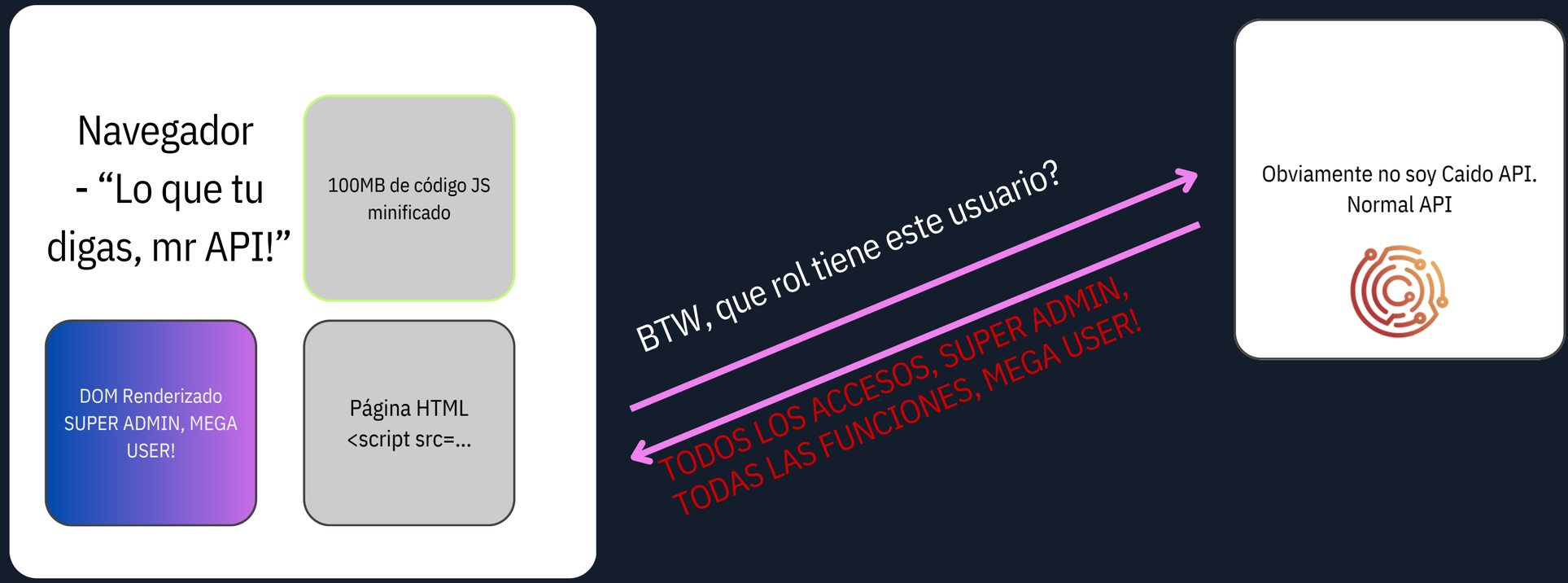


Instructor: Jesus Lujan Montufar
https://www.linkedin.com/in/jesusluj4n/

Vulnerabilidades Client Side 101

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

Lógica Client Side

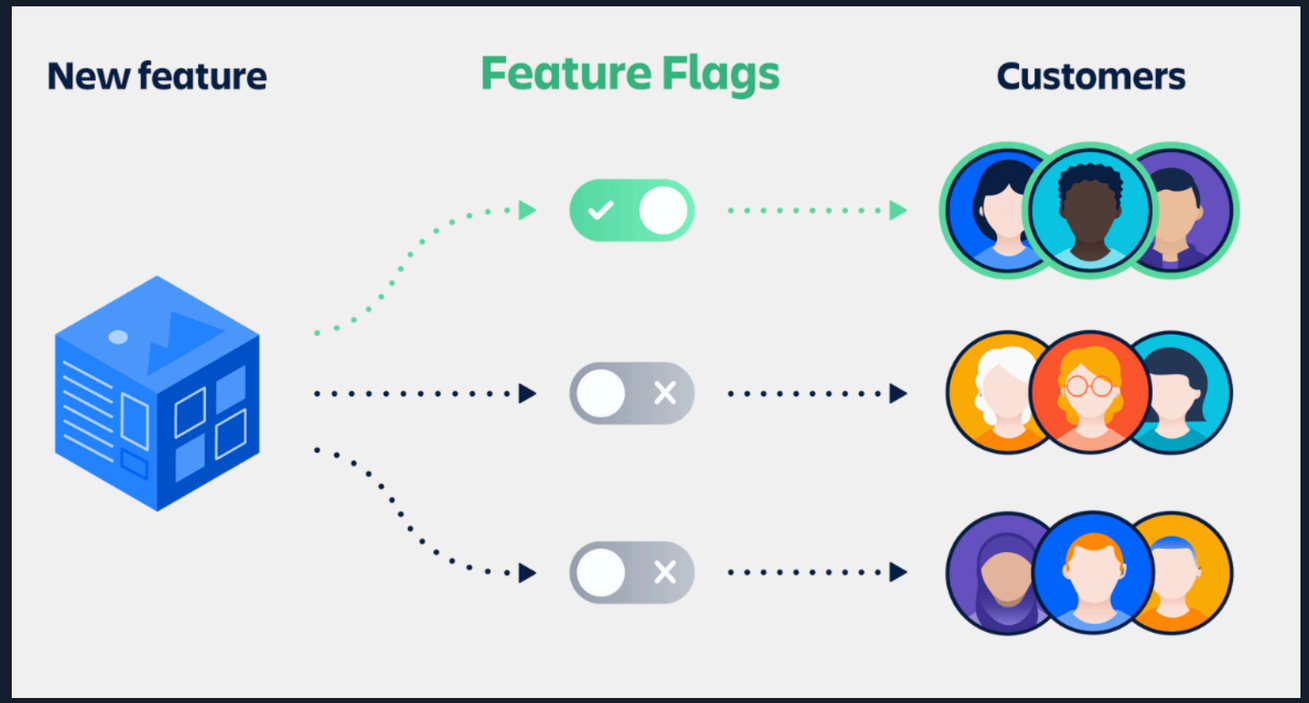


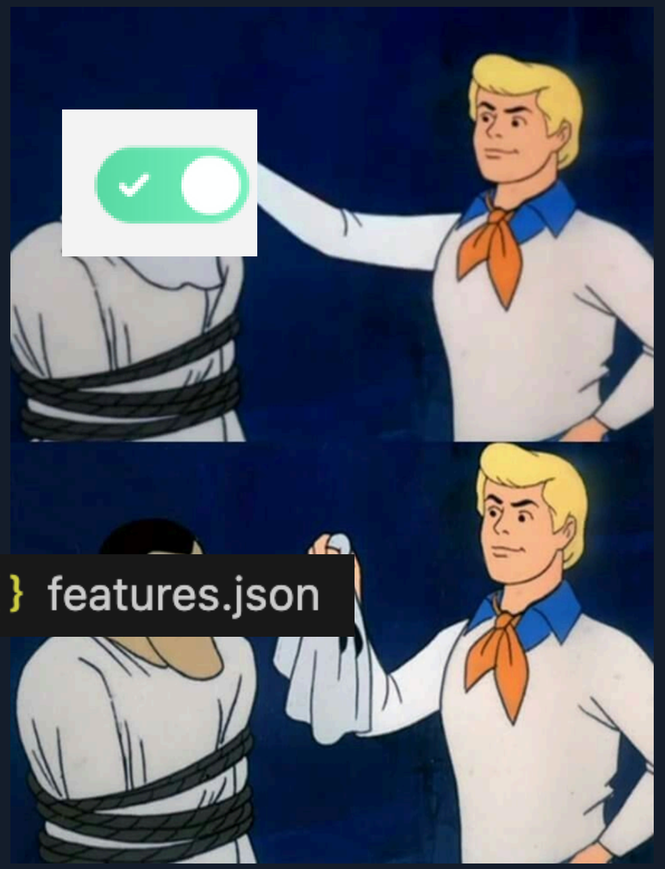
if(kl.mE===w.tF){0,w,HY)(Z)]

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

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

Habilitando Feature Flags

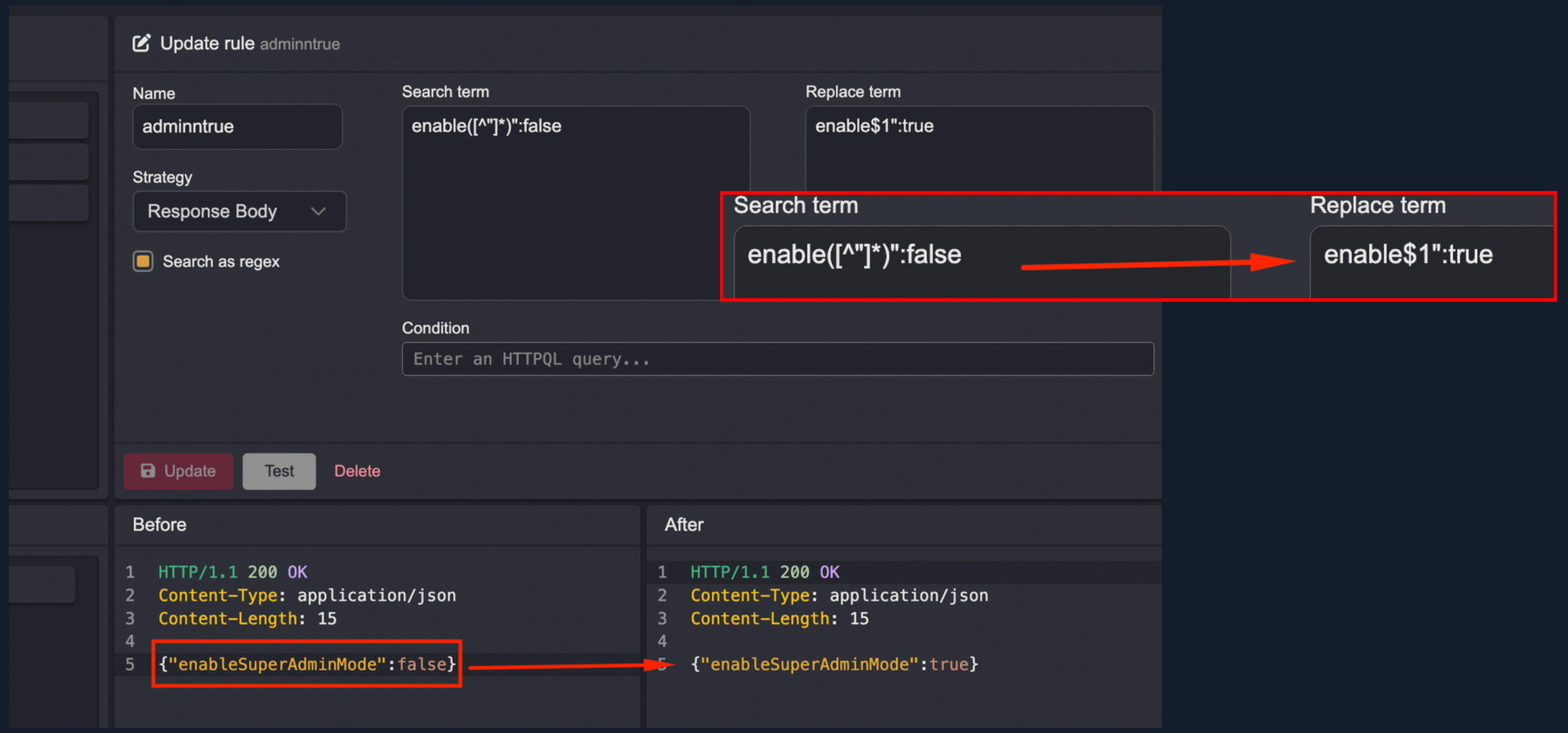




{} features.json {"enableNewHelpDeskBot":~~false~~"true"}

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

Bienvenido Match & Replace



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

Sobreescribiendo funciones

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

Usando breakpoints

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

CTF TIME
(10 min)

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

HACKTHEBOX

<CIBERSEC>
UNI

Accede a http://localhost:80 y obtén la flag.

Premio: HTB voucher vip+

Hint: Existe + de una solución

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

Recursos 403

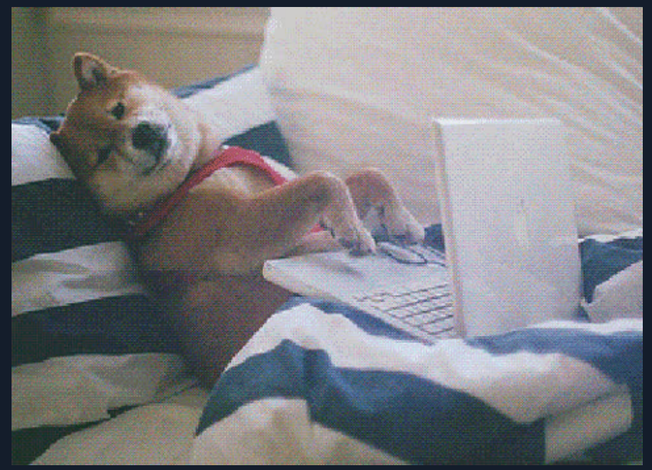
Must!: https://aszx87410.github.io/beyond-xss/en/

Links blogs interesantes

- https://balintmagyar.com/articles/google-web-designer-symlink-client-side-rce-cve-2025-1079
- https://lyra.horse/blog/2024/09/using-youtube-to-steal-your-files/
- https://samcurry.net/hacking-starbucks
- https://web.dev/articles/browser-level-image-lazy-loading

Links Laboratorios para prácticar

- https://verified.capitalone.com/
- http://spooky.bugcrowd.zw.ink/klown.cfm



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

Proximamente

- CSPT (Client Side Path Traversal ../../si, pero en el cliente)
- Prototype Pollution
- DOM Clobbering
- DOM Logger ++
- Json Injection

O quieren ver lado del servidor

- SQLi
- OS Command Injection
- IDORs, etc ...

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

Conectemos.

HACKTHEBOX

<CIBERSEC>
UNI

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

Graciass

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