# HACK & PATCH 2

## Taller Ataque y técnicas de defensa de aplicaciones web

# Tus ponentes favoritos

ERNI

Barcelona

## David Soto

Cybersecurity Principal

ERNI

Alicante

## Samuel Hernández

FullStack Expert

# ¿Qué vas a ver hoy?

- Cómo se explotan vulnerabilidades reales del OWASP Top 10.
- Qué errores de desarrollo las hacen posibles.
- Cómo corregirlas de forma práctica en tu código.
- Modo ataque

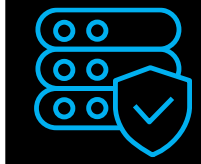
# Sobre el TOP 10 OWASP

Seguridad web

10 vulnerabilidades más críticas

Referencia estándar en la industria

Actualizado periódicamente

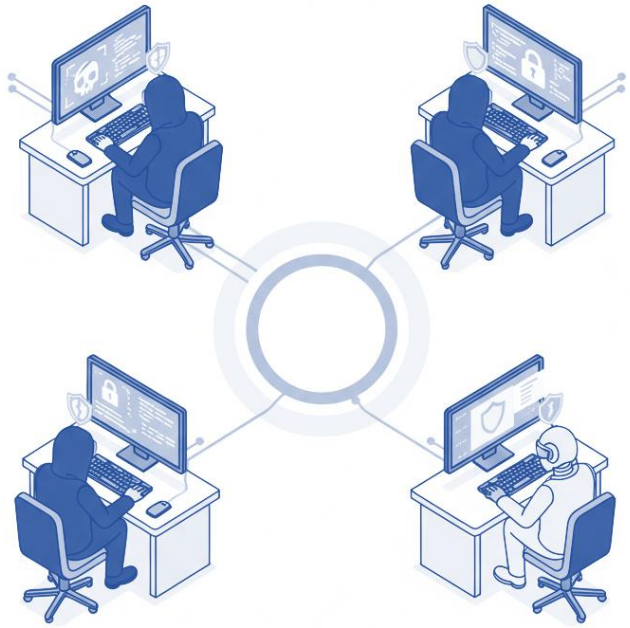


Ayudar a construir software seguro

# Etapa 1: Reconocimiento

## Objetivo

Presentación y exploración de la aplicación.



# Por donde empezar...

- Sistema de Control de acceso.
- Sistema de Logging.
- Palancas y carrito.
- Panel de administración.
- Perfil del usuario.
- Lo que no se ve.

# Atacando un sitio web...

## 0. Preparación mental (antes del paso 1)

Objetivo del atacante: que queremos conseguir

Siempre minimizamos ruido

Empezamos observando, no atacando

# Atacando un sitio web...

1. Reconocimiento Manual

   Entender qué es la aplicación.

   Qué se analiza:

   ¿Qué tipo de aplicación es?
   ¿Tiene login?
   ¿Tiene roles?
   ¿Qué inputs acepta?
   ¿Hay formularios?
   ¿Carga datos dinámicamente?
   ¿API visible?
   ¿Tecnologías aparentes?

# Atacando un sitio web...

## 2. Mapeo de superficie

Descubrir qué no está visible en la navegación normal.

### Incluye:

Enumeración de rutas
Descubrimiento de endpoints
Parámetros ocultos
Archivos expuestos

# Atacando un sitio web...

## 3. Exploración de rutas encontradas

Entender qué hace cada endpoint.

### Se analiza:

¿Requiere autenticación?
¿Devuelve datos sensibles?
¿Acepta parámetros?
¿Confía en datos del cliente?

# Atacando un sitio web...

## 4. Manipulación de Inputs

### Aquí entran las inyecciones

**4A – Inyección de código interpretado**
SQL
NoSQL
LDAP
OS Command

**4B – Inyección en cliente**
XSS
Manipulación DOM

**4C – Manipulación de lógica**
Cambiar parámetros
Alterar IDs
Forzar estados
Repetir requests

# Atacando un sitio web...

## 5. Escalada de privilegios

### Una vez dentro:

- ¿Soy usuario?
- ¿Puedo ser admin?
- ¿Puedo acceder a datos de otros?

### Técnicas:

- IDOR
- Broken Access Control
- Falta de validación de rol

# Atacando un sitio web...

## Configurar mal no es un bug. Es una bomba de tiempo

- Security Misconfiguration

# Atacando un sitio web...

## Tu backend no debería ser el navegador de tu atacante

- Server-Side Request Forgery

# Atacando un sitio web...

## Nunca deserialices lo que no controlas

- Insecure Deserialization

# La seguridad no es opcional

- ¡No uses ganchitos por favor!
- Los Cheetos se comen, no protegen.


# ¡MUCHAS GRACIAS!

# **ESKERRIK ASKO!**