



# SESSION HIJACKING: PELIGRO EN LA RED

***Randy Ortega***

***Email: ortega571@gmail.com***



**OWASP**

The Open Web Application Security Project

# Acerca de mi



**OWASP**

The Open Web Application Security Project

- Ingeniero de Sistemas UNEXPO
- Especialista en Seguridad de la Información
- Instructor de Ethical Hacking Vsoft Learning
- C|EH v7

# Peligro en la Red

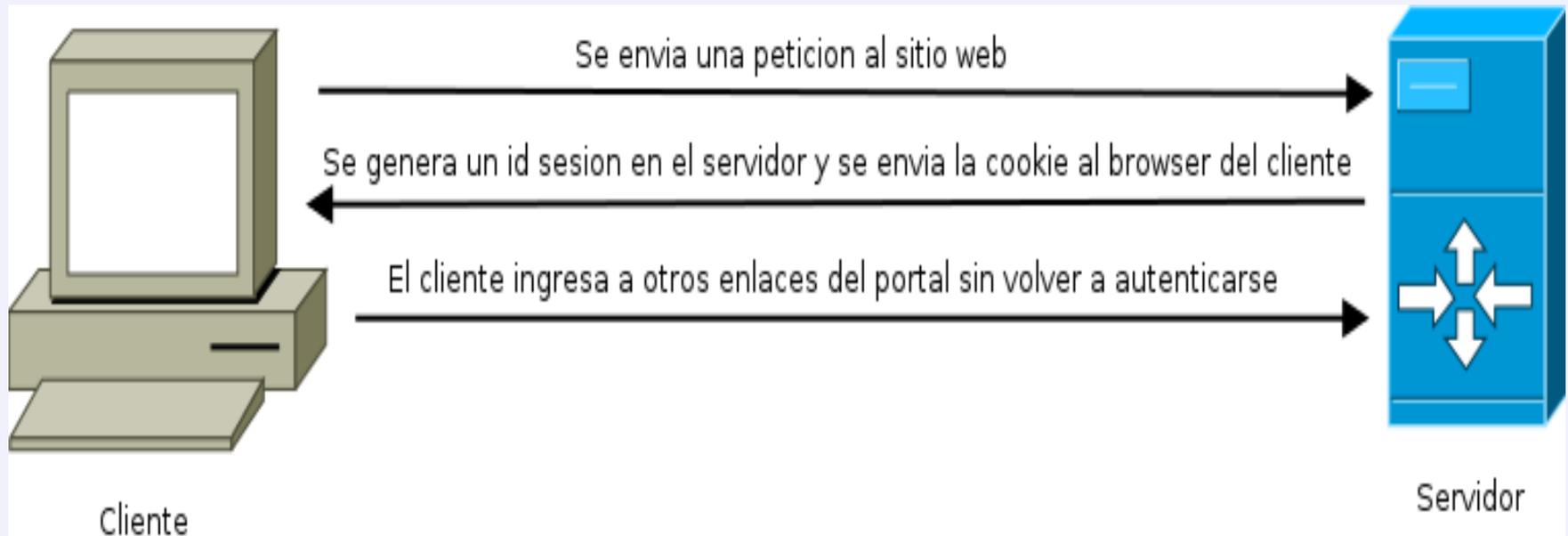


**OWASP**

The Open Web Application Security Project

**Qué peligro implica tener información en la red?**

**Cómo se establece una Sesión Web?**



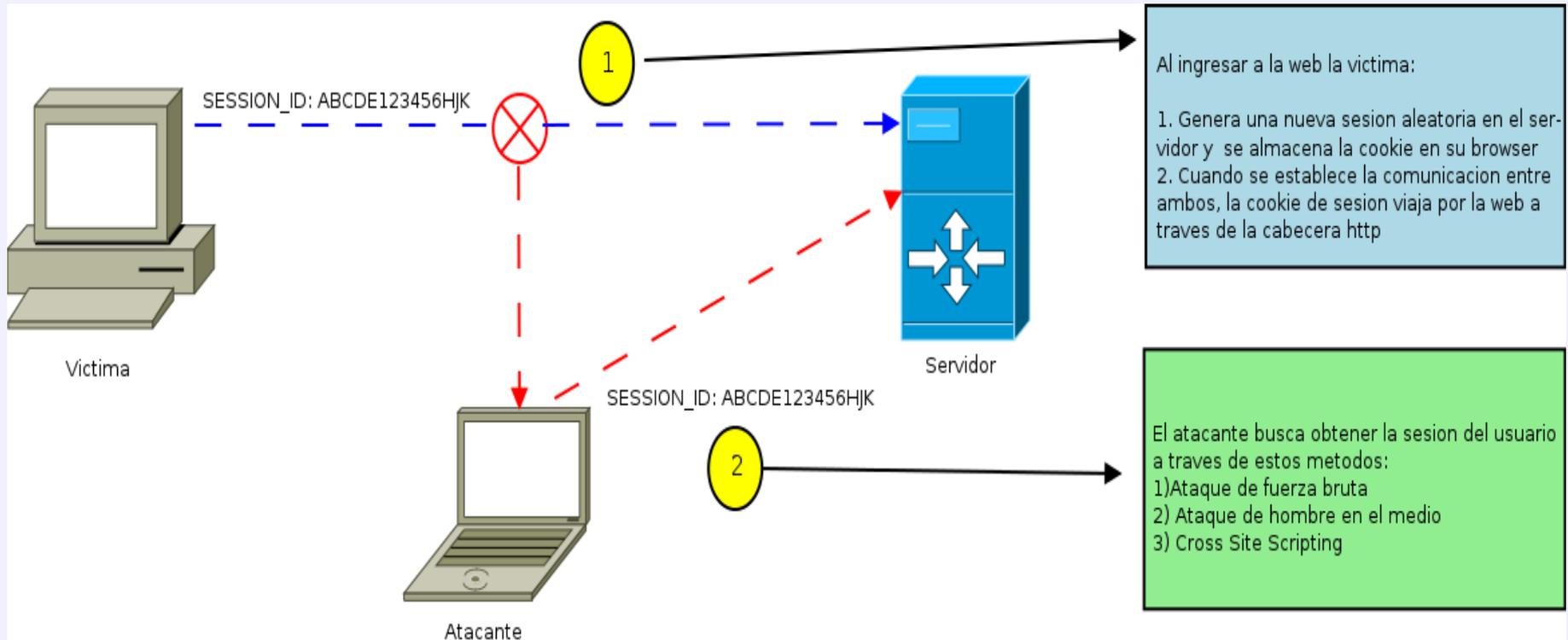
# Session Hijacking



**OWASP**

The Open Web Application Security Project

## ¿Qué es el Session Hijacking?





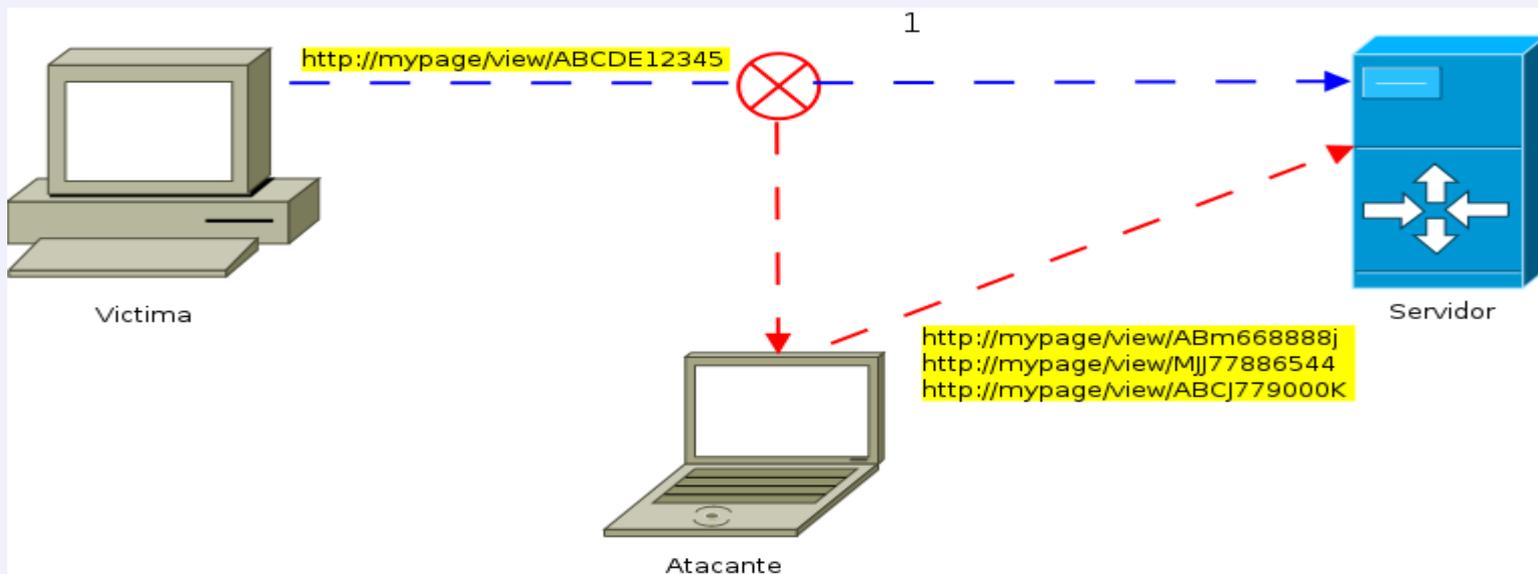
## Por qué sucede esto?

- La comunicación entre cliente y servidor se establece vía http
- Tiempo de duración de sesión demasiado grande o que nunca expira
- Algoritmo débil para generar el identificador de sesión



## Ataque por fuerza bruta

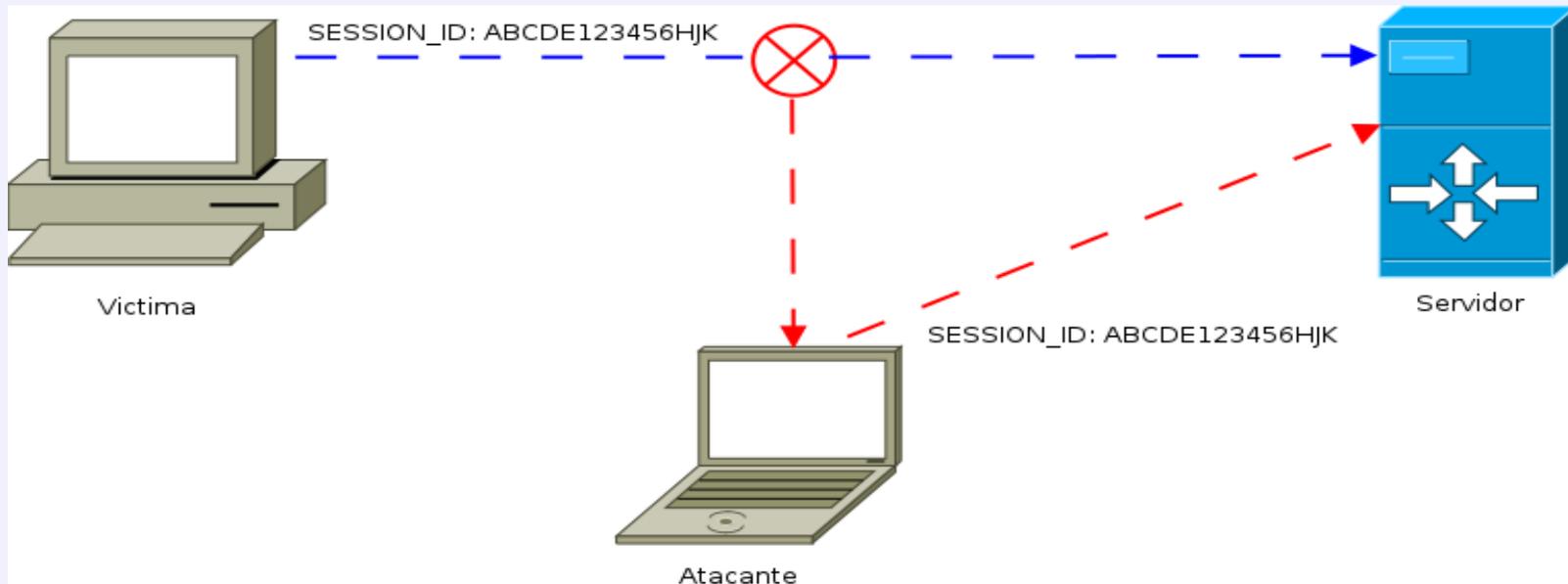
El atacante intentará adivinar el identificador de sesión de la víctima hasta conseguir el id correcto.





## Ataque de hombre en el medio

El atacante esnifea la red o lanza un ataque arp spoofing con el fin de quedar como la puerta de enlace entre la victima y el servidor web





## Ataque de hombre en el medio (Laboratorio)



Se captura la sesión de usuario

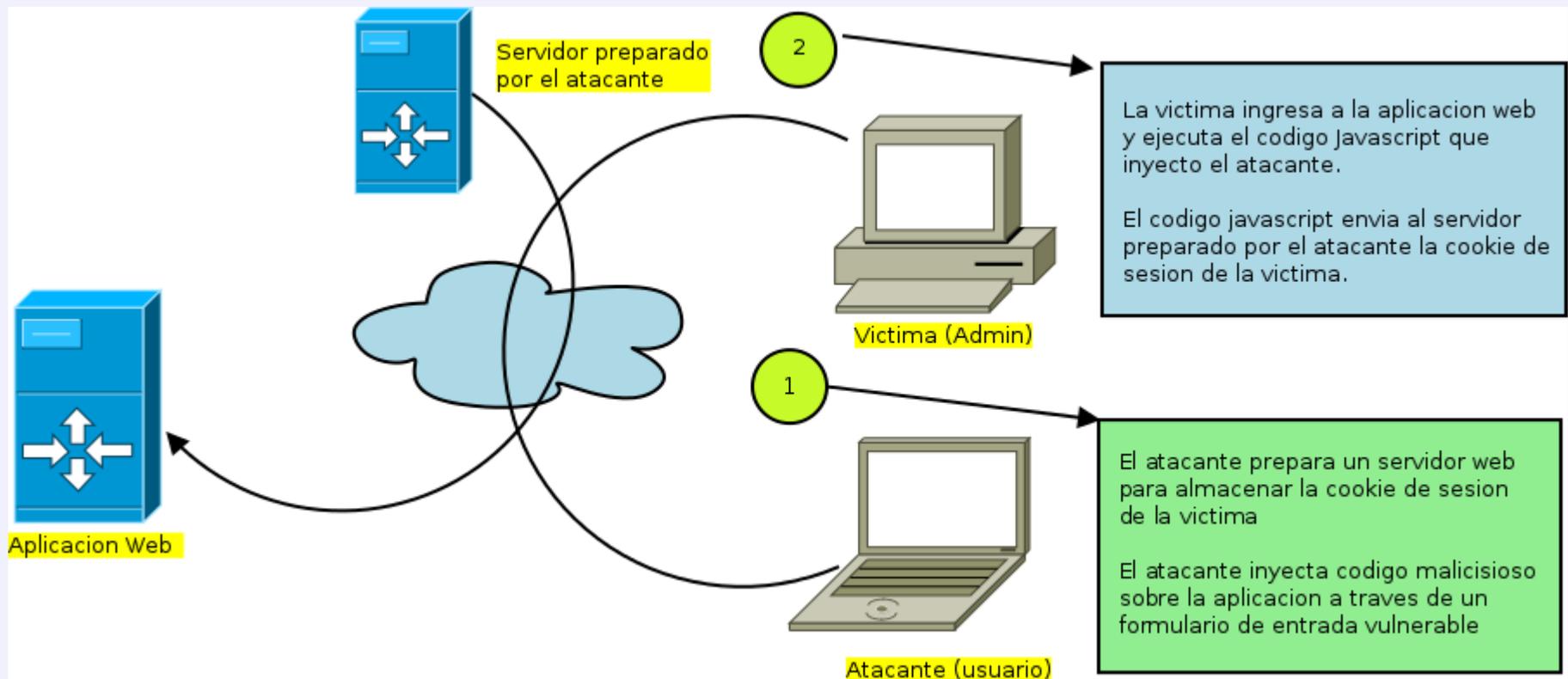
Se envían los datos de las cookies capturadas vía email

Se modifica la cookie de sesión a través de un editor de cookies (Cookies Manager)

Se ingresa a la sesión de la víctima



## Ataque de Cross Site Scripting



# Tipos de Ataque



## Ataque de Cross Site Scripting (Laboratorio)

Bienvienidos a la pagina:

**Ingrese los datos de ingreso al sistema**

Usuario	<input type="text"/>
Contraseña	<input type="text"/>
<input type="button" value="Enviar"/>	

Advanced Cookie Manager

**Gestión de cookies** | Monitor de cookies | Search | Configuración

**Dominios**

- localhost

**Cookies**

Nombre	Valor
PHPSESSID	2n5coiab2l3ua11j95dcl06f45

**Detalles de la cookie**

Hora de creación: Tue Apr 14 2015 15:25:10

Dominio: localhost

Nombre: PHPSESSID

Valor: 2n5coiab2l3ua11j95dcl06f45

Camino: /

httpOnly:  true  false

isSecure:  true  false

isSession:  true  false

Footer: Show Labels, navigation icons, Facebook Me gusta 435



## Como se evita el session hijacking

- La comunicación entre el cliente y el sitio web debe hacerse a través de un canal encriptado (HTTPS)
- Colocar un tiempo moderado de duración de la sesión del usuario.
- Evitar vulnerabilidades de aplicaciones web: XSS



**OWASP**

The Open Web Application Security Project

Gracias por su atención