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

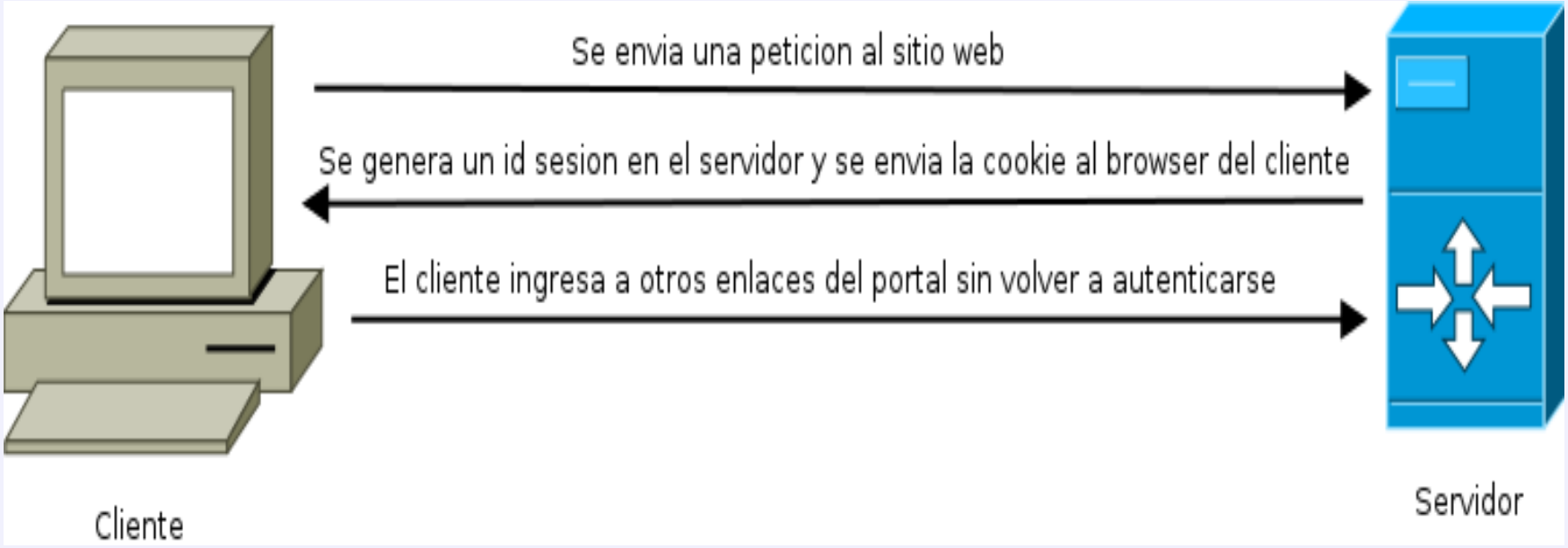
- Ingeniero de Sistemas UNEXPO
- Especialista en Seguridad de la Información
- Instructor de Ethical Hacking Vsoft Learning
- C|EH v7

Peligro en la Red

OWASP
The Open Web Application Security Project

Qué peligro implica tener información en la red?

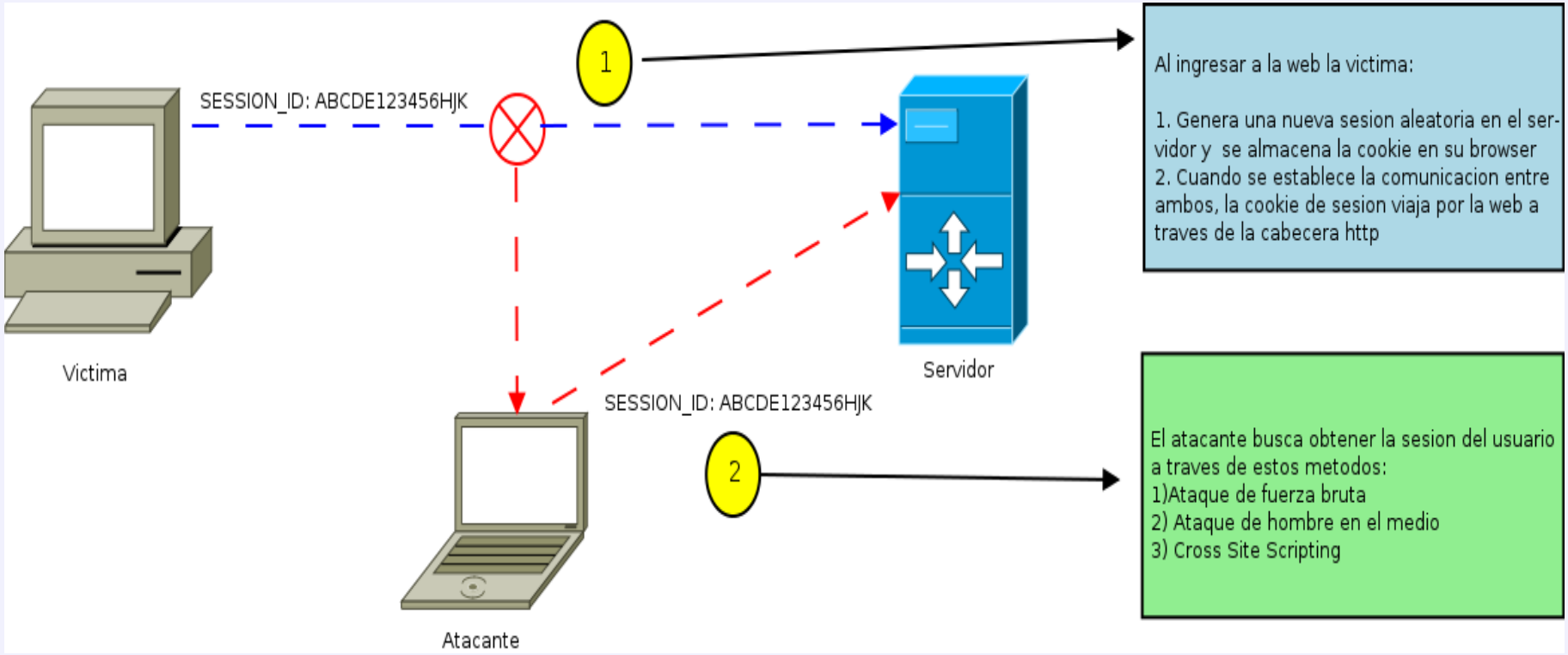
Cómo se establece una Sesión Web?



Session Hijacking

OWASP
The Open Web Application Security Project

Qué es el Session Hijacking?



Session Hijacking

OWASP
The Open Web Application Security Project

Por qué sucede esto?

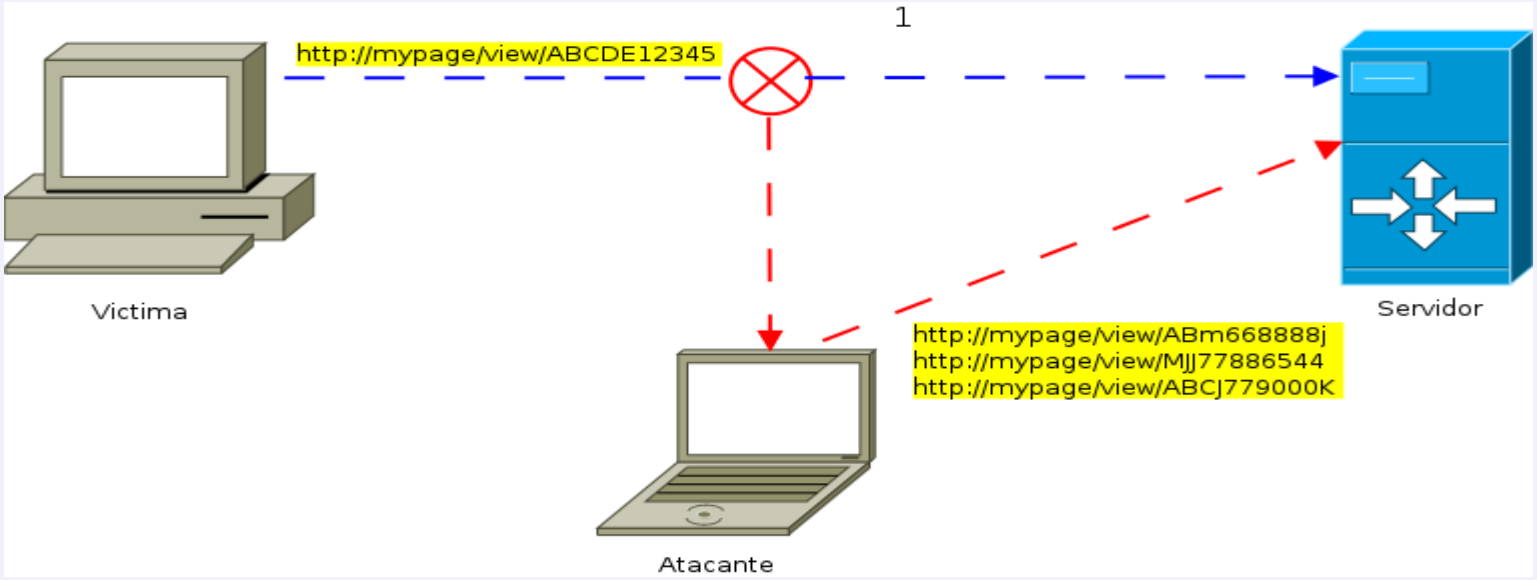
- La comunicación entre cliente y servidor se establece vía http
- Tiempo de duración de sesión demasiado grande o que nunca expira
- Algoritmo débil para generar el identificador de sesión

Tipos de Ataque

OWASP
The Open Web Application Security Project

Ataque por fuerza bruta

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

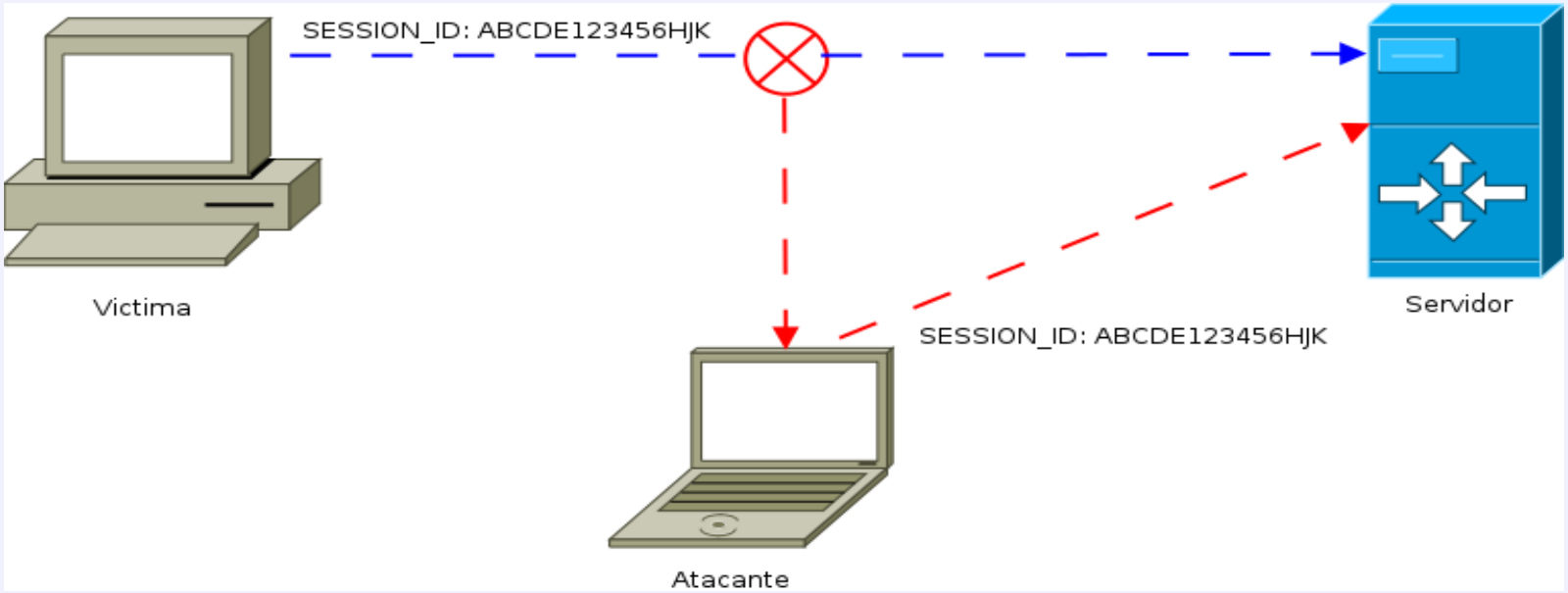


Tipos de Ataque

OWASP
The Open Web Application Security Project

Ataque de hombre en el medio

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



Tipos de Ataque

OWASP
The Open Web Application Security Project

Ataque de hombre en el medio (Laboratorio)

Se captura la sesión de usuario

Se envían los datos de las cookies capturadas vía email

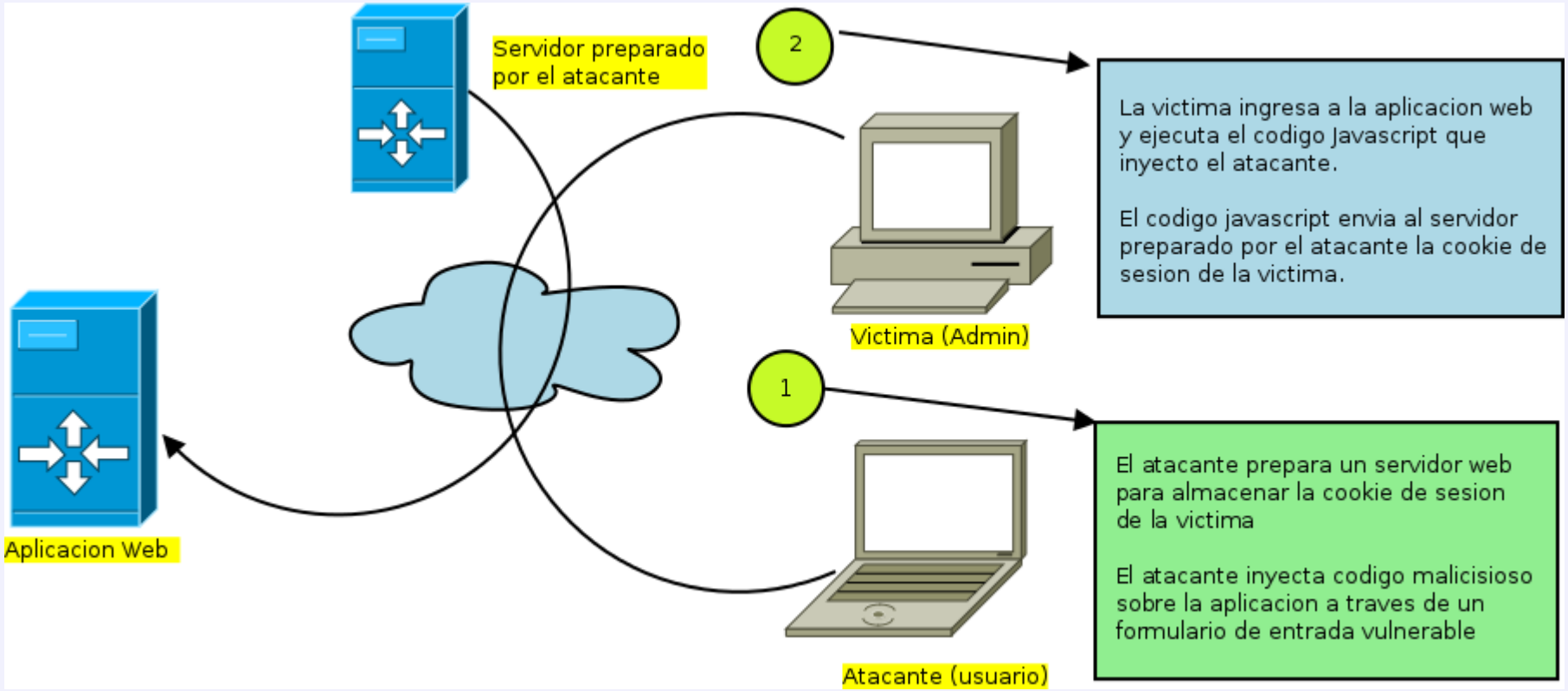
Se modifica la cookie de sesión a través de un editor de cookies (Cookies Manager)

Se ingresa a la sesión de la victima

Tipos de Ataque

OWASP
The Open Web Application Security Project

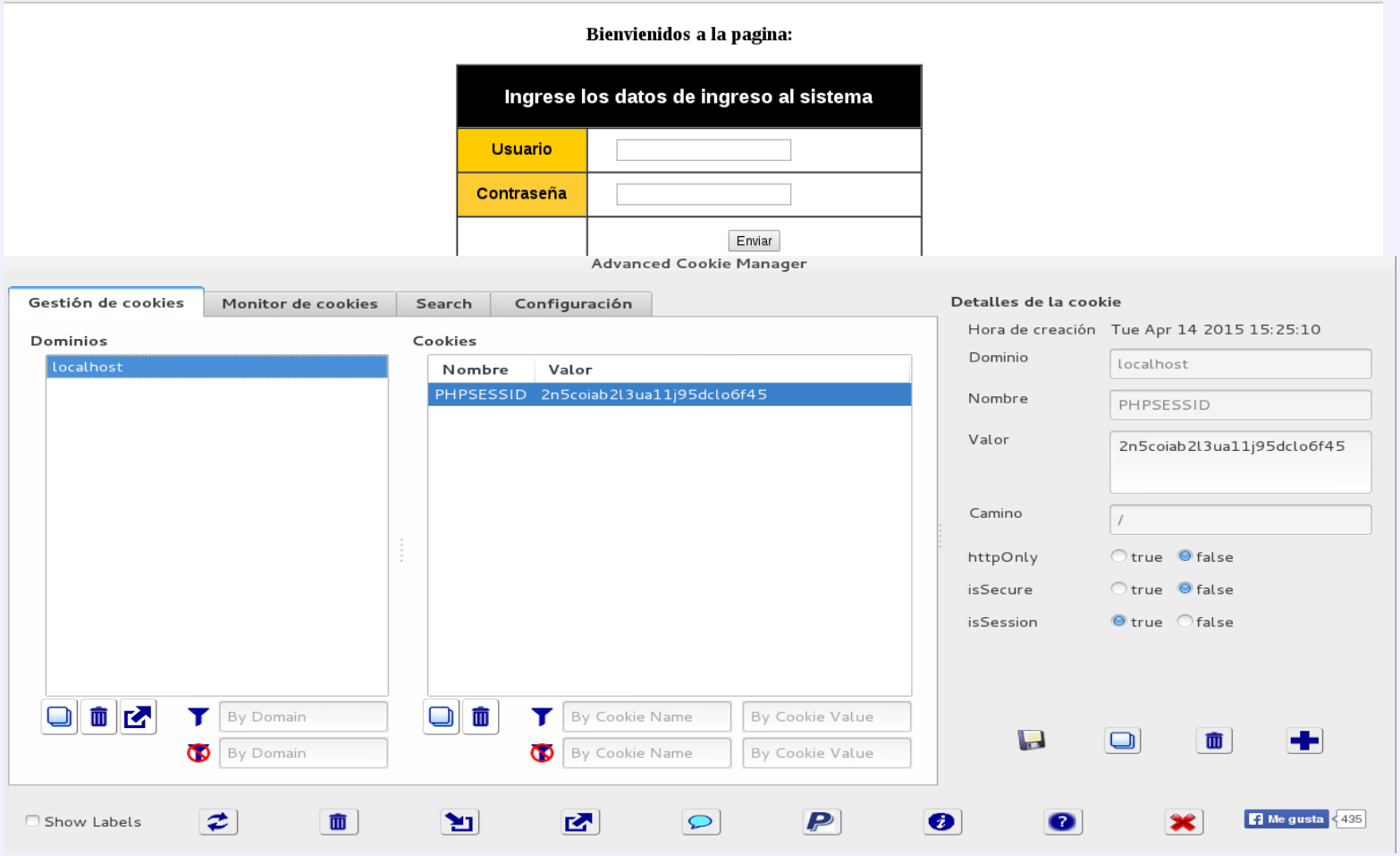
Ataque de Cross Site Scripting



Tipos de Ataque

OWASP
The Open Web Application Security Project

Ataque de Cross Site Scripting (Laboratorio)



Recomendaciones

OWASP
The Open Web Application Security Project

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