Práctica 2.9: Session Prediction

<Incluye en un documento Word capturas de pantalla de todo el proceso>

Objetivo del ataque: Modificar el ID de sesión para acceder a la sesión de otro usuario.

Preparación:

1) Instalar Java: https://java.com/es/download

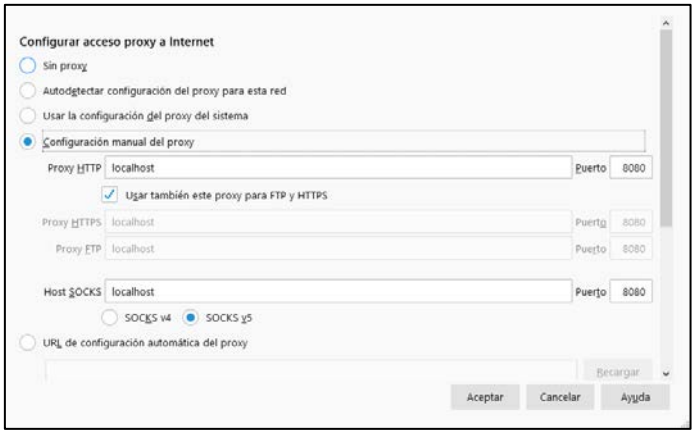
2) Instalar ZAP: https://www.zaproxy.org/download/

3) (Si no está instalado) instalar el navegador Firefox.

4) Configurar Firefox:

- En el navegador poner "about:config" y poner la propiedad "network.proxy.allow_hijacking_localhost" a "true".

- En Opciones -> Configuración de red, indicar esta configuración:



5) Despliega en el servidor los archivos sqli.php y sqliDatos.php. Comprueba en firefox que puedes acceder al login/password usando user1/pass1.

Actividades:

1) Realiza un ataque Session Prediction usando ZAP. Para ello captura el envío de la petición HTTP que realiza user1 y cambia el valor la variable de sesión a “user2”. Comprueba que el usuario conectado pasa a ser user2.

2) Modifica el programa para evitar el ataque Session Prediction. Para ello, usa la creación del ID de sesión por defecto en PHP.

3) Con respecto al ID de sesión de PHP:

- ¿Es creado en el servidor?

- ¿Es único?

- ¿Es aleatorio?

- ¿Está encriptado?

- ¿Cuál es su tiempo de expiración?