



Ejercicio Práctico

 **Título:** Explorando solicitudes HTTP con Burp Suite (o ZAP)

Objetivo:

Aprender a interceptar, visualizar y analizar una solicitud HTTP utilizando **Burp Suite** o **OWASP ZAP**, para identificar posibles puntos de entrada en una aplicación web sencilla.

Escenario:

Estás evaluando un sitio web de práctica local (como <http://testphp.vulnweb.com> o <http://localhost:8080>) que contiene formularios y enlaces básicos.

Tu tarea consiste en **capturar y analizar una solicitud HTTP** desde el navegador a través del proxy de Burp o ZAP, y describir los elementos clave de esa solicitud.

Actividades:

Paso 1 – Configuración inicial

1. Abre **Burp Suite** o **OWASP ZAP**.
 2. Configura tu navegador para usar el **proxy local** (127.0.0.1:8080).
 3. Verifica que la herramienta esté interceptando tráfico correctamente.
-

Paso 2 – Interceptar una solicitud

1. Navega al sitio de prueba.

2. Realiza una acción sencilla:
 - Completar y enviar un formulario, o
 - Hacer clic en un enlace.
 3. Deja la **interceptación activada** y observa la solicitud que se genera.
-

Paso 3 – Analizar la solicitud capturada

Registra los siguientes elementos de la solicitud interceptada:

- Método HTTP utilizado (**GET**, **POST**, etc.)
 - URL solicitada
 - Cabeceras HTTP relevantes (**Host**, **User-Agent**, **Cookie**)
 - Parámetros enviados (en URL o en cuerpo del mensaje)
-

Entregables:

1. Captura de pantalla de la solicitud interceptada.
 2. Descripción de los componentes de la solicitud: método, URL, headers, parámetros.
 3. Análisis simple: ¿Qué parte de la solicitud crees que podría ser vulnerable si no se valida correctamente?
-

Preguntas de reflexión:

- ¿Qué tipo de información se está enviando desde el navegador al servidor?
 - ¿Dónde podrías probar un ataque de inyección en esa solicitud?
 - ¿Qué información debería estar protegida o cifrada en un entorno real?
-

Solución Modelo – Ejercicio Práctico

Exploración de solicitudes HTTP con Burp Suite

Paso 1 – Configuración inicial

- Herramienta utilizada: **Burp Suite Community Edition**
 - Navegador: **Firefox** (con proxy configurado en **127.0.0.1:8080**)
 - Sitio de pruebas: **<http://testphp.vulnweb.com>**
 - Verificado que Burp capturara tráfico desde **Proxy > Intercept > Intercept is on**
-

Paso 2 – Solicitud interceptada

Se realizó clic en el enlace “Search” del sitio web y se envió una búsqueda con la palabra clave **laptop**.

Solicitud HTTP capturada:

GET /artsearch.php?artname=laptop&submit=Search HTTP/1.1

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:118.0) Gecko/20100101
Firefox/118.0

Accept: text/html,application/xhtml+xml

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Upgrade-Insecure-Requests: 1

Análisis de la solicitud:

Elemento	Descripción
Método	GET: se están enviando los parámetros en la URL.
URL	/artsearch.php?artname=laptop&submit=Search: solicitud con parámetros.
Host	testphp.vulnweb.com: dominio objetivo.
Parámetros	artname=laptop y submit=Search: enviados desde un formulario.
User-Agent	Indica que el navegador utilizado es Firefox.

Reflexión técnica

- El parámetro `artname` podría ser **vulnerable a inyecciones**, ya que su valor se refleja en una búsqueda.
 - Como es una solicitud `GET`, los parámetros están expuestos en la URL (posibles vectores para XSS o SQLi).
 - No se observan **cabeceras de autenticación** ni cookies, lo que sugiere un sistema sin login activo.
-




Posibles pruebas en solicitudes futuras

- Inyección SQL:
Probar `artname=' OR '1'='1`

- XSS básico:
Probar `artname=<script>alert('XSS')</script>`

Ambas pruebas pueden realizarse fácilmente desde el **Repeater** de Burp Suite.

Entregables simulados

-  **Captura de pantalla:** solicitud interceptada desde la pestaña Proxy.
 -  **Análisis por campo:** desglosado en tabla.
 -  **Reflexión:** propuesta de vectores de prueba para fases futuras.
-

Conclusión

Este ejercicio demuestra cómo una solicitud simple puede ofrecer información crítica sobre el comportamiento de la aplicación. Comprender la estructura de cada solicitud es el primer paso para realizar auditorías éticas de forma profesional y efectiva. La inspección manual es tan importante como el escaneo automático.
