🛠️ Ejercicio Práctico

📌 **Título:** Detección y explotación de vulnerabilidades XSS almacenado y CSRF en DVWA

🎯 Objetivo:

Simular un escenario en el que un atacante explota vulnerabilidades XSS almacenado y CSRF en una aplicación vulnerable (**DVWA**) para comprometer la seguridad de los usuarios. Se espera que identifiques el fallo, lo explotes de forma ética y propongas soluciones.

🧱 Escenario:

Estás realizando una auditoría ética en la plataforma **DVWA**. Se sospecha que el módulo "XSS Stored" permite guardar código JavaScript malicioso que se ejecuta en el navegador de otros usuarios. Además, se debe verificar si el sistema es vulnerable a **ataques CSRF en acciones sensibles** como el cambio de contraseña.

🔍 Actividades:

✅ Parte 1 – XSS Almacenado

1. Accede a DVWA desde `http://localhost/dvwa`.
2. Inicia sesión con:
    - Usuario: `admin`
    - Contraseña: `password`
3. Asegúrate de que el nivel de seguridad esté en **Low**.

a) Inyección XSS

1. Ve al módulo **"XSS (Stored)"**.
2. En los campos **Name** o **Message**, ingresa el siguiente payload:

```
<script>alert('XSS almacenado')</script>
```

3. Envía el formulario y revisa si el script aparece ejecutado al volver a cargar la página o acceder con otro usuario.

✅ Parte 2 – Ataque CSRF básico

1. Crea un archivo HTML local con el siguiente contenido:

```
<form action="http://localhost/dvwa/vulnerabilities/csrf/" method="POST">
  <input type="hidden" name="password_new" value="hack123">
  <input type="hidden" name="password_conf" value="hack123">
  <input type="hidden" name="Change" value="1">
  <input type="submit" value="Haz clic aquí">
</form>
```

2. Accede al módulo **"CSRF"** en DVWA.
3. Asegúrate de tener sesión activa como un usuario válido.
4. Abre tu archivo HTML desde el navegador local.
5. Haz clic en el botón o deja que el formulario se autoenvíe (agrega `onload="this.submit()"` si deseas automatizar).

📋 Entregables:

1. Captura de pantalla de la ejecución del script XSS.
2. Comprobación del cambio de contraseña usando CSRF.
3. Breve informe con:

- Payloads utilizados
- Resultados observados
- Evaluación del impacto
- Recomendaciones técnicas de mitigación

🧠 Preguntas de reflexión:

- ¿Qué diferencia hay entre un XSS reflejado y uno almacenado en cuanto a alcance y persistencia?
- ¿Por qué CSRF es especialmente peligroso en usuarios con sesión activa?
- ¿Cómo se relaciona la validación de origen y los tokens anti-CSRF con la defensa?
