📘 Glosario: Ataques de Dominio Cruzado (XSS y CSRF)

---

1. XSS (Cross-Site Scripting)

Vulnerabilidad que permite inyectar y ejecutar código JavaScript malicioso en el navegador de un usuario, explotando la confianza del navegador en el contenido del sitio web.

---

2. XSS Reflejado (Reflected XSS)

Tipo de XSS en el cual el script malicioso es enviado como parte de una solicitud y reflejado de inmediato por el servidor, ejecutándose directamente al cargar la URL o formulario.

---

3. XSS Almacenado (Stored XSS)

Vulnerabilidad en la que el script malicioso es guardado permanentemente en el servidor (por ejemplo, en una base de datos) y se ejecuta cada vez que otro usuario accede a esa información.

---

4. XSS basado en DOM (DOM-Based XSS)

Tipo de XSS que ocurre en el lado del cliente, cuando el código JavaScript del sitio manipula de forma insegura el DOM con datos proporcionados por el usuario, sin intervención del servidor.

---

5. Payload (en XSS)

Fragmento de código malicioso, generalmente JavaScript, que se inserta en una entrada vulnerable con el fin de ser ejecutado en el navegador de la víctima.

---

6. CSRF (Cross-Site Request Forgery)

Ataque que induce al navegador de un usuario autenticado a ejecutar acciones no autorizadas en una aplicación web, sin el conocimiento ni consentimiento del usuario.

---

7. Token Anti-CSRF

Valor único generado por el servidor y asociado a una sesión, que se incluye en los formularios para verificar la legitimidad de la solicitud. Ayuda a prevenir ataques CSRF.

---

8. SameSite (Cookie Attribute)

Atributo de las cookies que restringe su envío en peticiones cross-site. Configurarlo como `Strict` o `Lax` reduce el riesgo de ataques CSRF.

---

9. Content Security Policy (CSP)

Cabecera HTTP que permite definir qué fuentes de contenido son válidas en una aplicación web, limitando la ejecución de scripts externos y ayudando a mitigar XSS.

---

10. Burp Suite

Herramienta profesional para pruebas de seguridad en aplicaciones web. Permite interceptar, modificar, repetir y automatizar solicitudes HTTP, siendo útil para explotar XSS y CSRF.

---

11. OWASP ZAP (Zed Attack Proxy)

Herramienta libre de análisis de seguridad web, diseñada para escanear automáticamente aplicaciones y encontrar vulnerabilidades como XSS y CSRF.

---

12. DOM (Document Object Model)

Estructura jerárquica que representa los elementos HTML de una página. En XSS basado en DOM, el atacante manipula directamente esta estructura desde el navegador.

---

13. Referer y Origin (Cabeceras HTTP)

Cabeceras que indican el sitio de origen de una solicitud. Son utilizadas por el servidor para validar que una petición proviene de un sitio confiable, ayudando a prevenir CSRF.

---

14. Autenticación de Sesión

Proceso por el cual un usuario inicia sesión y mantiene su identidad mediante cookies o tokens. Es esencial en el contexto de CSRF, ya que el atacante explota sesiones activas.

---

15. Vector de Ataque

Ruta específica por la cual un atacante puede explotar una vulnerabilidad, como un campo de formulario, una URL o un parámetro de consulta.
