📘 Glosario: OWASP y Seguridad en Aplicaciones Web

---

1. OWASP (Open Web Application Security Project)

Organización sin fines de lucro que se enfoca en mejorar la seguridad del software, especialmente en aplicaciones web, proporcionando recursos abiertos, herramientas y metodologías.

---

2. OWASP Top 10

Lista publicada por OWASP que describe las 10 vulnerabilidades de seguridad más críticas en aplicaciones web, con el fin de sensibilizar a los desarrolladores y expertos en seguridad.

---

3. Vulnerabilidad

Debilidad en un sistema que puede ser explotada por un atacante para obtener acceso no autorizado o realizar actividades maliciosas.

---

4. Inyección SQL (SQL Injection)

Vulnerabilidad en la que un atacante introduce código malicioso en una consulta SQL, lo que puede permitirle obtener, modificar o eliminar datos en la base de datos de una aplicación web.

---

5. Cross-Site Scripting (XSS)

Vulnerabilidad que permite a los atacantes inyectar scripts maliciosos en páginas web, afectando a los usuarios finales mediante la ejecución de estos scripts en su navegador.

---

6. Cross-Site Request Forgery (CSRF)

Ataque en el que un atacante engaña a un usuario para que realice una acción no deseada en una aplicación web en la que está autenticado.

---

7. Autenticación Rota

Vulnerabilidad que ocurre cuando las aplicaciones no implementan adecuadamente las políticas de autenticación, permitiendo a los atacantes eludir la autenticación y obtener acceso no autorizado.

---

8. OWASP ZAP (Zed Attack Proxy)

Herramienta de código abierto de OWASP diseñada para realizar pruebas de seguridad automáticas y manuales en aplicaciones web, ayudando a detectar vulnerabilidades.

---

9. OWASP Juice Shop

Aplicación web intencionadamente vulnerable diseñada para proporcionar un entorno controlado donde los usuarios pueden aprender sobre seguridad y realizar pruebas de penetración.

---

10. Pruebas de Penetración (Pentesting)

Proceso de realizar ataques simulados a una aplicación para identificar y explotar vulnerabilidades antes de que lo hagan los atacantes maliciosos.

---

11. ACL (Access Control List)

Lista de control de acceso utilizada para definir reglas sobre qué usuarios o sistemas pueden acceder a determinados recursos dentro de una red o aplicación.

---

12. Seguridad en la Capa de Aplicación (Application Layer Security)

Prácticas y medidas de seguridad aplicadas a la capa de aplicación de un sistema, donde se encuentran las interfaces de usuario y las interacciones con los datos. Estas prácticas previenen vulnerabilidades que afectan la lógica de la aplicación.

---

13. HTTPS (HyperText Transfer Protocol Secure)

Versión segura del protocolo HTTP, que utiliza cifrado SSL/TLS para proteger la privacidad e integridad de los datos transmitidos entre el navegador y el servidor web.

---

14. Criptografía

Proceso de cifrar información para hacerla ilegible para usuarios no autorizados, garantizando la confidencialidad e integridad de los datos.

---

15. VPN (Virtual Private Network)

Red privada virtual que permite a los usuarios establecer una conexión segura a una red a través de Internet, cifrando el tráfico de datos para proteger la información en tránsito.

---

16. XSS Reflejado

Tipo de ataque XSS en el que el código malicioso se refleja en la respuesta del servidor, afectando solo al usuario que realiza la solicitud maliciosa.

---

17. Seguridad en el Desarrollo (Secure Development)

Enfoque que integra la seguridad a lo largo del ciclo de vida del desarrollo de software, garantizando que las vulnerabilidades sean identificadas y solucionadas antes de que el software se despliegue en producción.

---

18. OWASP SAMM (Software Assurance Maturity Model)

Modelo de madurez de seguridad que proporciona un marco para evaluar y mejorar las prácticas de desarrollo seguro en una organización, ayudando a medir y mejorar el nivel de madurez en cuanto a seguridad en el desarrollo de software.

---

19. Política de Seguridad de la Información (Information Security Policy)

Conjunto de reglas y directrices implementadas por una organización para proteger la información y los sistemas de tecnología contra amenazas y vulnerabilidades.

---

20. Seguridad por Diseño (Security by Design)

Enfoque de desarrollo en el que la seguridad se incorpora desde las primeras etapas del ciclo de vida del software, en lugar de ser añadida posteriormente.

---

21. Auditoría de Seguridad (Security Audit)

Proceso de revisión exhaustiva de los sistemas, aplicaciones y redes de una organización para identificar posibles vulnerabilidades y evaluar el cumplimiento de las políticas de seguridad.

---

22. Cifrado AES (Advanced Encryption Standard)

Estándar de cifrado simétrico utilizado en la protección de datos, ampliamente utilizado en aplicaciones de seguridad, como HTTPS y VPNs.

---

23. SSO (Single Sign-On)

Sistema de autenticación que permite a los usuarios acceder a múltiples aplicaciones con un solo conjunto de credenciales, mejorando la experiencia del usuario y la seguridad.

---

24. Desbordamiento de Búfer (Buffer Overflow)

Vulnerabilidad en la que los datos escritos en un búfer de memoria exceden su límite, lo que puede permitir a un atacante ejecutar código malicioso o sobrescribir datos críticos.

---

25. CSP (Content Security Policy)

Mecanismo de seguridad que ayuda a prevenir ataques de tipo XSS al permitir a los desarrolladores especificar qué fuentes de contenido pueden ser cargadas por la aplicación web.