Práctica – Vulnerabilidades

1.

https://hispasec.com/en/home

Funcionalidades:
Ofrece una amplia gama de servicios como auditorias avanzadas de seguridad, servicios de SOC (Security Operations Center), soluciones con IA, permite una administración de usuarios y sus permisos, gestión de riesgos y auditorias de seguridad con variedad de opciones.

Organismos/Empresas/Asociaciones:

La empresa fue creada por Bernardo Quintero que es autosuficiente, es decir, se mantiene ella misma.

https://nvd.nist.gov

Funcionalidades:

Recopila, analiza y difunde información sobre vulnerabilidades de seguridad al cual se le asigna un identificador único llamado CVE (Common Vulnerabilities and Exposures), también las puntualiza como Puntuación CVSS (Common Vulnerability Scoring System) lo que ayuda a una organización a la hora de priorizar los avisos. Además de una búsqueda avanzada implementando todo lo anterior mencionado.

Organismos/Empresas/Asociaciones:

Es mantenida por el National Institute of Standards and Technology (NIST) el cual es una agencia del Departamento de Comercio de los Estados Unidos.

https://www.incibe.es

Funcionalidades:

Podemos dividirlo en sectores, por una parte, está la de los ciudadanos en donde se ofrece información sobre la protección de tus datos personales, navegar de forma segura entre otras acciones que pasamos por alto.

Para menores cuenta con recursos específicos para educar a sobre los riesgos online y fomentar un uso responsable de la tecnología.

Para empresas se proporcionan herramientas, guías y servicios orientado a mejorar la ciberseguridad en el entorno empresarial.

Organismos/Empresas/Asociaciones:

Esta mantenido por el Instituto Nacional de Ciberseguridad de España (INCIBE), una entidad pública sin ánimo de lucro

Web relacionada proporcionada:

MITRE ATT&CK® Framework

https://attack.mitre.org

Funcionalidades: MITRE ATT&CK es una base de conocimientos globalmente accesible de tácticas y técnicas de adversarios basadas en observaciones del mundo real. Se utiliza para comprender y describir el comportamiento de los atacantes, y para mejorar la defensa contra ellos. Los desarrolladores pueden usarlo para anticipar posibles vectores de ataque, diseñar defensas más efectivas y comprender el **mindset** de un atacante.

Organismo/Empresa/Asociación:

El framework **ATT&CK** es mantenido por **MITRE Corporation**, una organización sin fines de lucro que opera centros de investigación y desarrollo financiados por el gobierno de EE. UU. MITRE trabaja en diversas áreas, incluyendo la ciberseguridad, para el beneficio del gobierno y el sector público.

2. “**Una al día”**

https://unaaldia.hispasec.com/2025/09/corea-del-norte-usa-ia-para-falsificar-identidades-militares-y-lanzar-ataques.html

El motivo de esta elección es debido al tema más popular de hoy en día, las y como su uso indebido gana mucho terreno en estos sectores y en el uso de suplantación de identidad, junto con ataques de ingeniería social y phishing con el objetivo de obtener información sensible como credenciales de acceso, datos de empleados o información confidencial de organizaciones.

3. Vulnerabilidad

- Cross-Site Scripting (XSS) Reflejado en Hispasec.com
- El fallo se ha observado en la implementación de funcionalidades de búsqueda y filtrado dentro del sitio web Hispasec.com.
- La vulnerabilidad está ligada a la forma en que el sitio procesa y muestra los parámetros de entrada del usuario en las respuestas HTTP.
- Nivel de Gravedad: Generalmente, las vulnerabilidades XSS reflejadas se clasifican como de MEDIO a ALTO en la escala CVSS, dependiendo del contexto y el impacto potencial. Un XSS reflejado puede permitir a un atacante ejecutar scripts maliciosos en el navegador de la víctima, lo que podría llevar al robo de cookies de sesión, redireccionamiento a sitios maliciosos, o la visualización de contenido manipulado.

Descripción:

El fallo consiste en una **inyección de código JavaScript (XSS)**, al realizar una búsqueda en Hispasec, si el término de búsqueda se refleja directamente en la página de resultados sin un filtrado correcto, un atacante podría crear una URL maliciosa que contenga código JavaScript. Al hacer que un usuario haga clic en esta URL, el script se ejecutaría en el navegador de la víctima. Esto podría permitir al atacante, por ejemplo, robar las cookies de autenticación del usuario si estas no están protegidas adecuadamente o redirigir al usuario a un sitio de phishing.

4.

El proyecto **OWASP (Open Web Application Security Project)**:

- Es una fundación comunitaria sin fines de lucro dedicada a mejorar la seguridad del software. Funciona como una comunidad global de expertos en seguridad que trabaja para crear aplicaciones y servicios más seguros. El proyecto se enfoca en la educación, la concienciación y la provisión de recursos prácticos y herramientas para ayudar a los desarrolladores, arquitectos y organizaciones a construir y mantener aplicaciones seguras. Abarcan desde la investigación hasta la creación de guías, metodologías, herramientas y estándares de seguridad.

Características del OWASP Top Ten:

- **Estándar de la Industria:** Se considera una referencia fundamental para la concienciación sobre la seguridad de las aplicaciones web.
- **Basado en Datos:** La lista se elabora a partir de datos recopilados de miles de pruebas de seguridad y aplicaciones de todo el mundo, lo que le otorga una gran credibilidad.
- **Enfoque en Riesgos:** Se centra en los **riesgos** que pueden sufrir las aplicaciones, no solo en las vulnerabilidades técnicas. Por ejemplo, incluye categorías como "**Broken Access Control**" (Control de Acceso Roto) o "**Identification and Authentication Failures"** (Fallos de Identificación y Autenticación).
- **Actualización Periódica:** El OWASP Top Ten se actualiza periódicamente (cada pocos años) para reflejar los cambios en el panorama de amenazas y las nuevas tendencias en ataques.
- **Herramienta Educativa:** Sirve como una herramienta educativa vital para desarrolladores, profesionales de seguridad y gerentes de proyecto, ayudándoles a priorizar los esfuerzos de seguridad y a comprender las amenazas más importantes que deben abordar.