UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE INGENIERIA

Escuela Profesional de Ingeniería de Sistemas

PWASP SCANNER – Sistema de Detección de Vulnerabilidades Web

Curso: *Patrones de Software*

Docente: Ing. Patrick Jose Cuadros Quiroga

Integrantes:

Ccalli Chata, Joel Robert ***(2017057528)***

Jarro Cachi, Jose Luis ***(2020067148)***

Tacna – Perú

2025

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	JCC	JPC	JCC	26/06/2025	Versión Original

PWASP SCANNER – Sistema de Detección de Vulnerabilidades Web
FD02 - Documento de Visión

Versión *1.0*

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	JCC	JCC	JCC	19/04/2025	Versión Original

ÍNDICE GENERAL

1. Introducción

1.1 Propósito

Este documento tiene como objetivo definir y comunicar la visión integral del proyecto denominado **"PWASP SCANNER"**, un sistema automatizado de detección de vulnerabilidades web, enfocado en mejorar la seguridad de aplicaciones y plataformas en línea. Este sistema está diseñado como una herramienta tecnológica que permita a desarrolladores, auditores y administradores de sistemas identificar, analizar y reportar vulnerabilidades web de forma eficiente, ayudando a prevenir ataques cibernéticos antes de que afecten la integridad de los sistemas o los datos.

1.2 Alcance

El sistema cubrirá funcionalidades esenciales para llevar a cabo un escaneo completo y automatizado de sitios web, incluyendo: análisis de seguridad basado en la lista OWASP Top 10, detección de errores de configuración, inyecciones SQL, XSS, CSRF, fallos de autenticación, y otras vulnerabilidades comunes. También permitirá la generación de informes detallados, integración con flujos DevSecOps, recomendaciones de mitigación, y control de versiones de pruebas anteriores. El PWASP SCANNER estará disponible como una solución SaaS y como software local para entornos restringidos.

1.3 Definiciones, Siglas y Abreviaturas

- **OWASP**: Open Web Application Security Project
- **XSS**: Cross-Site Scripting
- **SQLi**: SQL Injection
- **CSRF**: Cross-Site Request Forgery
- **SaaS**: Software como Servicio
- **API**: Interfaz de Programación de Aplicaciones
- **CVE**: Common Vulnerabilities and Exposures
- **UI**: Interfaz de Usuario
- **PoC**: Proof of Concept (Prueba de Concepto)

1.4 Referencias

- Proyectos de OWASP (OWASP Top 10, ZAP Proxy, Dependency Check).
- Estándares ISO/IEC 27001 e ISO/IEC 27005 sobre gestión de riesgos.
- Guías del NIST para análisis de vulnerabilidades.
- Artículos científicos sobre escaneo de seguridad en aplicaciones web.
- Manuales de herramientas como Burp Suite, Nikto, Wapiti, y Nmap.

1.5 Visión General

PWASP SCANNER es una plataforma integral diseñada para fortalecer la ciberseguridad en entornos web, orientada a identificar vulnerabilidades de forma automatizada y con un enfoque

práctico. Permitirá a sus usuarios realizar pruebas de seguridad periódicas, con acceso a análisis avanzados, priorización de hallazgos por riesgo, y reportes en múltiples formatos. El objetivo principal del sistema es brindar una herramienta confiable, escalable y alineada con las mejores prácticas de seguridad web para prevenir brechas en sistemas informáticos.

2. Posicionamiento

2.1 Oportunidad de Negocio

En un entorno digital en constante expansión, la superficie de ataque web aumenta proporcionalmente al número de aplicaciones y servicios desplegados. Muchas pequeñas y medianas empresas no cuentan con personal experto en seguridad ni con herramientas adecuadas para realizar auditorías continuas. PWASP SCANNER representa una oportunidad estratégica en el mercado de ciberseguridad automatizada, al ofrecer una solución asequible, adaptable y de fácil uso. Puede ser adoptada por desarrolladores independientes, instituciones educativas, entidades gubernamentales y empresas del sector privado.

2.2 Definición del Problema

Los ataques web representan una de las amenazas más comunes y críticas en el panorama actual de ciberseguridad. Fallos como inyecciones de código, configuración insegura, autenticación rota y exposición de datos confidenciales, se encuentran presentes en múltiples sistemas sin ser detectados oportunamente. La falta de herramientas automatizadas y de fácil comprensión para escaneo de vulnerabilidades genera altos riesgos de explotación. PWASP SCANNER busca resolver este problema proporcionando una solución digital capaz de ejecutar pruebas automatizadas, interpretar resultados y proponer medidas correctivas.

3. Descripción de los Interesados y Usuarios

3.1 Resumen de los Interesados

- Desarrolladores web interesados en asegurar sus aplicaciones.
- Administradores de sistemas que gestionan servidores y sitios web.
- Equipos de ciberseguridad encargados de auditorías periódicas.
- Directivos y responsables de cumplimiento normativo en seguridad.

3.2 Resumen de los Usuarios

El público objetivo incluye desarrolladores técnicos con conocimientos básicos o intermedios en seguridad informática, así como equipos de TI de pequeñas organizaciones. También se contempla el uso por parte de estudiantes de ciberseguridad y consultores externos en auditorías de seguridad.

3.3 Entorno de Usuario

La plataforma estará disponible en versión web y de escritorio, con una interfaz gráfica intuitiva basada en dashboards de riesgo, alertas automáticas y módulos personalizables. Será

compatible con los principales navegadores, sistemas operativos (Windows, Linux, macOS) y estará optimizada para operar tanto en línea como en modo offline para entornos críticos.

3.4 Perfiles de los Interesados

- **Desarrolladores Web**: Profesionales que integran medidas de seguridad en el ciclo de desarrollo.
- **Auditores de Seguridad**: Especialistas encargados de realizar análisis técnicos y generar reportes.
- **Empresas/Instituciones**: Organizaciones preocupadas por el cumplimiento de normativas como GDPR o PCI-DSS.

3.5 Perfiles de los Usuarios

- Usuarios con conocimientos técnicos de redes y desarrollo web.
- Usuarios con interés en pruebas de penetración automatizadas.
- Usuarios con necesidad de generar informes ejecutivos de seguridad.

3.6 Necesidades de los Interesados y Usuarios

- **Identificar vulnerabilidades antes de que sean explotadas.**
- **Recibir orientación sobre cómo mitigar los hallazgos.**
- **Obtener reportes de cumplimiento en formatos PDF/JSON.**
- **Monitorear sitios web periódicamente con bajo esfuerzo operativo.**

4. Descripción del Producto

4.1 Perspectiva del Producto

PWASP SCANNER se desarrollará como un sistema autónomo pero integrable, que puede funcionar de forma independiente o enlazado con otras plataformas de desarrollo, CI/CD (Integración Continua / Despliegue Continuo), y sistemas de gestión de vulnerabilidades. Se planea que se ofrezca en dos formatos:

- Versión Web SaaS (Software as a Service).
- Aplicación de Escritorio para escaneo local y redes internas.

El sistema incluirá módulos de:

- Gestión de proyectos y escaneos.
- Mapeo del sitio (Spidering).
- Identificación de vulnerabilidades OWASP Top 10.
- Motor de reglas de detección.
- Reportes ejecutivos y técnicos.
- Recomendaciones de mitigación.
- Integración con APIs externas (Shodan, VirusTotal, CVE databases).

4.2 Supuestos y Dependencias

- El usuario deberá contar con conexión a internet para actualizaciones automáticas de firmas de vulnerabilidades (excepto en versión local).

- Se asume que el usuario tendrá acceso autorizado a los sitios a escanear, respetando políticas de uso.
- Dependerá de bibliotecas externas para análisis de código, pruebas de inyección y verificación de configuraciones.
- Las recomendaciones se basarán en bases de datos oficiales como CVE, NIST y OWASP.

5. Funcionalidades del Producto

Las funcionalidades más destacadas de PWASP SCANNER incluyen:

5.1 Escaneo de Vulnerabilidades

Permite realizar análisis automáticos en busca de:

- Inyección SQL (SQLi)
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Direct Object Reference
- Fallas de configuración de seguridad
- Exposición de cabeceras HTTP inseguras
- Fallos de autenticación
- Inclusión de archivos locales/remotos
- Descubrimiento de ficheros sensibles (robots.txt, .git, .env)

5.2 Generación de Reportes

- Exportación de resultados en PDF, HTML y JSON.
- Categorización de vulnerabilidades por nivel de riesgo (alto, medio, bajo).
- Historial de escaneos con comparativas.
- Visualización mediante gráficos de radar, barras y líneas de tiempo.

5.3 Interfaz Amigable

- Dashboard centralizado.
- Filtros de búsqueda por tipo de vulnerabilidad, nivel de riesgo y fecha.
- Navegación intuitiva para usuarios no expertos.
- Sección de ayuda con glosario, documentación y videos guía.

5.4 Seguridad y Privacidad

- Escaneos cifrados y almacenados localmente (modo privado).
- Control de acceso mediante autenticación de doble factor (2FA).
- Logs de actividad con auditoría interna.
- Aislamiento de escaneos por proyecto.

6. Requisitos No Funcionales

6.1 Rendimiento

- Escaneo promedio de sitios pequeños en menos de 5 minutos.
- Capacidad de análisis concurrente hasta 10 sitios simultáneos.
- Optimización de recursos para reducir uso de CPU y memoria.

6.2 Seguridad

- Uso de TLS en todas las conexiones.
- Protección ante uso indebido mediante sandboxing.
- Validación de entradas y prevención de explotación de comandos.

6.3 Mantenibilidad

- Código documentado y modular.
- Soporte para actualizaciones automáticas y parches.
- Pruebas unitarias y funcionales incluidas en cada release.

6.4 Usabilidad

- Diseño adaptativo (responsive).
- Manuales interactivos integrados.
- Navegación accesible y conforme a estándares WCAG.

7. Restricciones

- El sistema no realizará pruebas de denegación de servicio (DoS/DDoS).
- La precisión puede variar según la configuración del servidor de destino.
- El uso de la herramienta debe contar con permiso explícito del propietario del sitio escaneado.
- Algunas funcionalidades avanzadas (como fuzzing o PoC automáticos) estarán limitadas a usuarios con licencia extendida.

8. Evolución Previsible del Producto

PWASP SCANNER está diseñado para evolucionar en diferentes fases. Entre las funcionalidades previstas para versiones futuras se incluyen:

- Integración con herramientas de ticketing como Jira y GitHub Issues.
- Escaneo de aplicaciones móviles (Android/iOS).
- Escaneo de APIs REST y SOAP.
- Soporte para bases de datos no relacionales (NoSQL Injection).
- Motor de inteligencia artificial para priorizar vulnerabilidades según contexto empresarial.
- Módulo de aprendizaje asistido para personalización de reglas de escaneo.

9. Apéndices

9.1 Glosario

- **Exploit**: Código que aprovecha una vulnerabilidad para ejecutar acciones maliciosas.
- **Payload**: Información enviada con el propósito de comprobar o explotar una falla.
- **False Positive**: Resultado que indica erróneamente la presencia de una vulnerabilidad.
- **Fuzzer**: Herramienta que envía datos aleatorios para detectar fallos en la entrada.

Conclusión

PWASP SCANNER representa un avance significativo en la automatización del análisis de vulnerabilidades web, respondiendo a la necesidad urgente de soluciones accesibles, eficientes y adaptables para mitigar riesgos en entornos digitales. Su diseño contempla las necesidades tanto de usuarios expertos como de técnicos en formación, ofreciendo una interfaz amigable y funcionalidades robustas. Además, su orientación hacia los estándares internacionales y el cumplimiento normativo garantiza su utilidad como herramienta de confianza en auditorías profesionales. Con el tiempo, su evolución planeada permitirá consolidarlo como un recurso esencial dentro del ecosistema de seguridad informática, contribuyendo activamente a la protección de los activos digitales y la prevención de ataques cibernéticos.

Referencias

1. OWASP Foundation. (2023). *OWASP Top Ten Project*. https://owasp.org/www-project-top-ten/
2. ISO/IEC. (2018). *ISO/IEC 27001: Information Security Management Systems*.
3. National Institute of Standards and Technology. (2022). *Guide to Vulnerability Assessment*. NIST Special Publication 800-115.
4. Ristic, I. (2017). *Bulletproof SSL and TLS*. Feisty Duck.
5. Kim, D., & Solomon, M. G. (2021). *Fundamentals of Information Systems Security*. Jones & Bartlett Learning.
6. PortSwigger. (2024). *Burp Suite Documentation*. https://portswigger.net/burp/documentation
7. Shostack, A. (2014). *Threat Modeling: Designing for Security*. Wiley.
8. Scarfone, K., & Mell, P. (2007). *NIST Guide to Security Test and Evaluation*. NIST SP 800-53.
9. Sutton, M., Greene, A., & Amini, P. (2007). *Fuzzing: Brute Force Vulnerability Discovery*. Addison-Wesley.
10. Zeltser, L. (2022). *Modern Web Application Security Testing Tools*. SANS Institute.