Texto, Logotipo

Descripción generada automáticamente

**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***

***PWASP SCANNER – Sistema de Detección de Vulnerabilidades Web, Tacna,2025***

**Presentado por: •*Joel Robert Ccalli Chata***

***•Jose Luis Jarro Cachi***

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

ÍNDICE GENERAL

[**UNIVERSIDAD PRIVADA DE TACNA** 1](#_Toc202298727)

[**I. Introducción** 4](#_Toc202298728)

[**II. Justificación** 4](#_Toc202298729)

[**III. Objetivos del Proyecto** 4](#_Toc202298730)

[**IV. Alcance del Proyecto** 4](#_Toc202298731)

[**V. Cronograma del Proyecto** 5](#_Toc202298732)

[**VI. Presupuesto Referencial** 5](#_Toc202298733)

[**VII. Recursos Necesarios** 5](#_Toc202298734)

[**VIII. Metodología de Desarrollo** 5](#_Toc202298735)

[**IX. Impacto Esperado** 5](#_Toc202298736)

[**X. Conclusiones** 6](#_Toc202298737)

[**XI. Referencias Bibliográficas (Normas APA)** 6](#_Toc202298738)

**I. Introducción**

|  |  |
| --- | --- |
| Ítem | Descripción |
| Contexto | La creciente cantidad de ataques informáticos y brechas de seguridad ha puesto en evidencia la necesidad de contar con herramientas automatizadas de detección de vulnerabilidades en aplicaciones web. |
| Problemática | Muchas pequeñas y medianas empresas carecen de recursos técnicos para realizar pruebas de penetración o auditorías periódicas en sus plataformas web. Esto las deja expuestas a ataques como XSS, SQL Injection, CSRF, etc. |
| Solución Propuesta | El sistema **PWASP SCANNER** surge como una alternativa automatizada, eficiente y de fácil acceso que permite escanear aplicaciones web y detectar vulnerabilidades conocidas con base en los OWASP Top 10. |

**II. Justificación**

|  |  |
| --- | --- |
| Justificación | Detalle |
| Técnica | Facilita la implementación de pruebas de seguridad mediante un sistema automatizado, modular y escalable. |
| Económica | Reduce significativamente el costo de auditorías de seguridad al automatizar procesos clave. |
| Social | Contribuye a la protección de la información personal y financiera de los usuarios. |
| Académica | Fomenta el desarrollo de sistemas inteligentes orientados a la ciberseguridad en ambientes reales. |

**III. Objetivos del Proyecto**

**Objetivo General**

Desarrollar un sistema web denominado **PWASP SCANNER**, capaz de detectar y reportar vulnerabilidades de seguridad en aplicaciones web, en base al estándar OWASP, desde una plataforma accesible y de fácil uso.

**Objetivos Específicos**

|  |  |
| --- | --- |
| Nº | Objetivo Específico |
| 1 | Analizar las principales vulnerabilidades web basadas en OWASP Top 10. |
| 2 | Diseñar una arquitectura modular que permita escalabilidad y facilidad de mantenimiento. |
| 3 | Implementar un sistema que permita escaneo por URL, login y parámetros dinámicos. |
| 4 | Generar reportes detallados y exportables sobre los hallazgos detectados. |
| 5 | Validar el sistema en entornos de prueba simulando ataques reales controlados. |

**IV. Alcance del Proyecto**

|  |  |
| --- | --- |
| Alcance Incluido | Alcance Excluido |
| Escaneo de sitios web por URL o subdominios. | Pruebas sobre aplicaciones móviles o APIs REST. |
| Detección de vulnerabilidades OWASP (Top 10). | Corrección automática de vulnerabilidades. |
| Generación de reportes PDF o CSV. | Pruebas físicas de infraestructura de red. |
| Panel de usuario con historial de escaneos. | Integraciones con otros sistemas de seguridad. |

**V. Cronograma del Proyecto**

|  |  |  |  |
| --- | --- | --- | --- |
| Fase | Actividades Principales | Duración | Mes |
| Fase 1 | Análisis de requerimientos, investigación OWASP | 2 semanas | Julio |
| Fase 2 | Diseño del sistema y arquitectura modular | 2 semanas | Julio |
| Fase 3 | Desarrollo del sistema (Frontend + Backend) | 6 semanas | Ago - Sep |
| Fase 4 | Pruebas de funcionamiento y revisión de seguridad | 2 semanas | Septiembre |
| Fase 5 | Documentación, validación final y despliegue | 2 semanas | Octubre |

**VI. Presupuesto Referencial**

|  |  |  |  |
| --- | --- | --- | --- |
| Recurso | Costo Unitario | Cantidad | Total Estimado |
| Dominio y hosting | S/ 250 | 1 | S/ 250 |
| Herramientas de desarrollo y testing (software) | S/ 500 | 1 | S/ 500 |
| Personal técnico (desarrollador backend/frontend) | S/ 2000 | 2 | S/ 4000 |
| Diseño gráfico e interfaz UI/UX | S/ 800 | 1 | S/ 800 |
| Total estimado |  |  | **S/ 5,550** |

**VII. Recursos Necesarios**

|  |  |  |
| --- | --- | --- |
| Tipo | Recurso | Especificación |
| Humanos | Desarrollador web full stack | Con conocimientos en seguridad informática. |
| Materiales | Laptop o PC de desarrollo | Procesador i5/i7, 8 GB RAM mínimo. |
| Técnicos | Lenguajes de programación | Python, JavaScript, HTML5, CSS3 |
| Infraestructura | Hosting cloud | Soporte PHP, Node.js, o Python Flask. |

**VIII. Metodología de Desarrollo**

|  |  |
| --- | --- |
| Metodología | Descripción |
| Ágil (SCRUM) | El proyecto se ejecutará mediante iteraciones quincenales (sprints), con reuniones semanales de seguimiento. Cada entrega parcial será testeada con usuarios clave para retroalimentación inmediata. |
| Herramientas | Trello (gestión tareas), GitHub (versionamiento), Figma (prototipado), OWASP ZAP (comparación técnica). |

**IX. Impacto Esperado**

|  |  |
| --- | --- |
| Impacto | Descripción |
| Técnico | Generar una solución automatizada, segura y escalable para la detección de vulnerabilidades. |
| Académico | Contribuir al estudio de la ciberseguridad en entornos web desde una perspectiva práctica. |
| Empresarial | Proteger sitios web de pequeñas empresas contra ataques frecuentes y comunes. |

**X. Conclusiones**

|  |  |
| --- | --- |
| Nº | Conclusión |
| 1 | PWASP SCANNER representa una solución concreta frente al creciente problema de vulnerabilidades web en empresas locales. |
| 2 | La adopción de estándares internacionales como OWASP garantiza la fiabilidad del sistema. |
| 3 | Este proyecto es escalable y podrá adaptarse a nuevas amenazas con actualizaciones constantes. |

**XI. Referencias Bibliográficas (Normas APA)**

1. OWASP Foundation. (2023). *OWASP Top 10: Web Application Security Risks*. https://owasp.org/www-project-top-ten/
2. Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.
3. Grimes, R. A. (2021). *Hacking the Hacker: Learn From the Experts Who Take Down Hackers*. Wiley.
4. Kim, D., & Solomon, M. G. (2020). *Fundamentals of Information Systems Security* (4th ed.). Jones & Bartlett Learning.
5. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
6. Allen, J. H. (2022). *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley.
7. Bishop, M. (2018). *Computer Security: Art and Science* (2nd ed.). Addison-Wesley.
8. Zetter, K. (2015). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishing.
9. OWASP ZAP. (2023). *Zed Attack Proxy Project*. https://owasp.org/www-project-zap/
10. ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.