**Propuesta de Proyecto: Aplicación Centralizada para Análisis de Vulnerabilidades Web y Cloud**

**Objetivo**

Desarrollar un prototipo funcional que centralice el análisis de vulnerabilidades en páginas web y entornos cloud, integrando información sobre mitigación de riesgos y un sistema innovador de “toquen de antesala” para el análisis preventivo de archivos antes de su almacenamiento.

**Alcance Realista y Modular (320 horas totales)**

**Funcionalidades Esenciales a Desarrollar**

1. **Módulo de Análisis de Vulnerabilidades Web y Cloud**
   * Integrar una herramienta gratuita y open source como OpenVAS para escanear vulnerabilidades en aplicaciones web y recursos cloud, aprovechando su capacidad de pruebas autenticadas y no autenticadas, así como su compatibilidad multiplataforma[2](https://www.revistacloudcomputing.com/2024/02/4-herramientas-gratuitas-para-el-analisis-de-vulnerabilidades/)[5](https://www.guru99.com/es/vulnerability-scanning-tools.html).
   * Mostrar los resultados de los escaneos y recomendaciones básicas de mitigación.
2. **Módulo “Toquen de Antesala” (Versión Básica)**
   * Implementar un sistema que reciba archivos antes de almacenarlos, identifique su tipo y realice un análisis básico (por ejemplo, escaneo antivirus o verificación de integridad).
   * Encaminamiento a “toquen” responsables según el tipo de archivo/sistema.
   * Garantizar que solo los archivos inocuos se almacenen.
3. **Interfaz Web Sencilla**
   * Dashboard para lanzar análisis, subir archivos y consultar resultados.
   * Visualización clara de vulnerabilidades detectadas y pasos de mitigación.
4. **Documentación y Manual de Usuario**
   * Guía de instalación, uso y posibles ampliaciones futuras.

**Innovación y Valor Añadido**

* **Arquitectura modular basada en “toquen”**: Cada “toquen” se genera en la instalación y colabora con otros para analizar y mitigar vulnerabilidades, permitiendo una protección dinámica y adaptable.
* **Prevención proactiva**: El “toquen de antesala” añade una capa de seguridad previa al almacenamiento, diferenciándose de la mayoría de soluciones que actúan solo tras el almacenamiento.
* **Centralización**: Consolida el análisis de vulnerabilidades web y cloud en un solo panel, facilitando la gestión y priorización de riesgos[6](https://www.paloaltonetworks.es/cortex/cloud/vulnerability-management).
* **Mitigación guiada**: Presenta recomendaciones claras y contextualizadas para cada vulnerabilidad detectada, ayudando a equipos con menos experiencia a actuar rápidamente[4](https://geekflare.com/es/cybersecurity/best-website-security-scanner/)[5](https://www.guru99.com/es/vulnerability-scanning-tools.html).

**Distribución del Trabajo**

| **Persona** | **Módulo Principal** | **Horas estimadas** |
| --- | --- | --- |
| 1 | Integración de OpenVAS y análisis web | 60 |
| 2 | Desarrollo del “toquen de antesala” | 60 |
| 3 | Interfaz web y visualización | 60 |
| 4 | Integración, pruebas y documentación | 60 |
| Todos | Revisión, testing y ajustes finales | 80 (20 c/u) |

**Posicionamiento y Ventaja Competitiva**

* **Frente a herramientas como Nessus, Qualys o Intruder**, que ofrecen análisis avanzados pero requieren licencias o no integran análisis preventivo de archivos, vuestra solución destaca por:
  + Ser open source y modular.
  + Incluir un sistema de análisis previo al almacenamiento (“toquen de antesala”).
  + Centralizar la gestión de vulnerabilidades web y cloud en una interfaz sencilla y didáctica, ideal para equipos pequeños o en formación[4](https://geekflare.com/es/cybersecurity/best-website-security-scanner/)[5](https://www.guru99.com/es/vulnerability-scanning-tools.html)[2](https://www.revistacloudcomputing.com/2024/02/4-herramientas-gratuitas-para-el-analisis-de-vulnerabilidades/).
* **Mercado objetivo**: Pymes, equipos de TI en formación y organizaciones educativas que buscan una solución asequible, extensible y fácil de usar.

**Conclusión**

Con este enfoque modular y realista, el equipo puede entregar un prototipo funcional y diferenciador en el plazo disponible, demostrando innovación y capacidad de integración de herramientas líderes del sector, y sentando las bases para futuras ampliaciones.

1. <https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview>
2. <https://www.revistacloudcomputing.com/2024/02/4-herramientas-gratuitas-para-el-analisis-de-vulnerabilidades/>
3. <https://www.wiz.io/es-es/academy/oss-vulnerability-management-tools>
4. <https://geekflare.com/es/cybersecurity/best-website-security-scanner/>
5. <https://www.guru99.com/es/vulnerability-scanning-tools.html>
6. <https://www.paloaltonetworks.es/cortex/cloud/vulnerability-management>
7. <https://www.manageengine.com/latam/vulnerability-management/analisis-de-vulnerabilidades.html>
8. <https://codster.io/blog/seguridad-en-aplicaciones/aplication-vulnerability/herramientas-del-analisis-de-vulnerabilidades/>