



# Auditor Web de Seguridad

Una solución innovadora para la gestión de riesgos en aplicaciones web.

Milton Beltrán

George Albadr

# Idea General del Proyecto y Propósito

- **Plataforma de Auditoría Web Automatizada**

Permite a usuarios autenticados ejecutar auditorías de seguridad sobre sitios web autorizados, simplificando el proceso de identificación de riesgos.

- **Integración de Herramientas de Ciberseguridad Líderes**

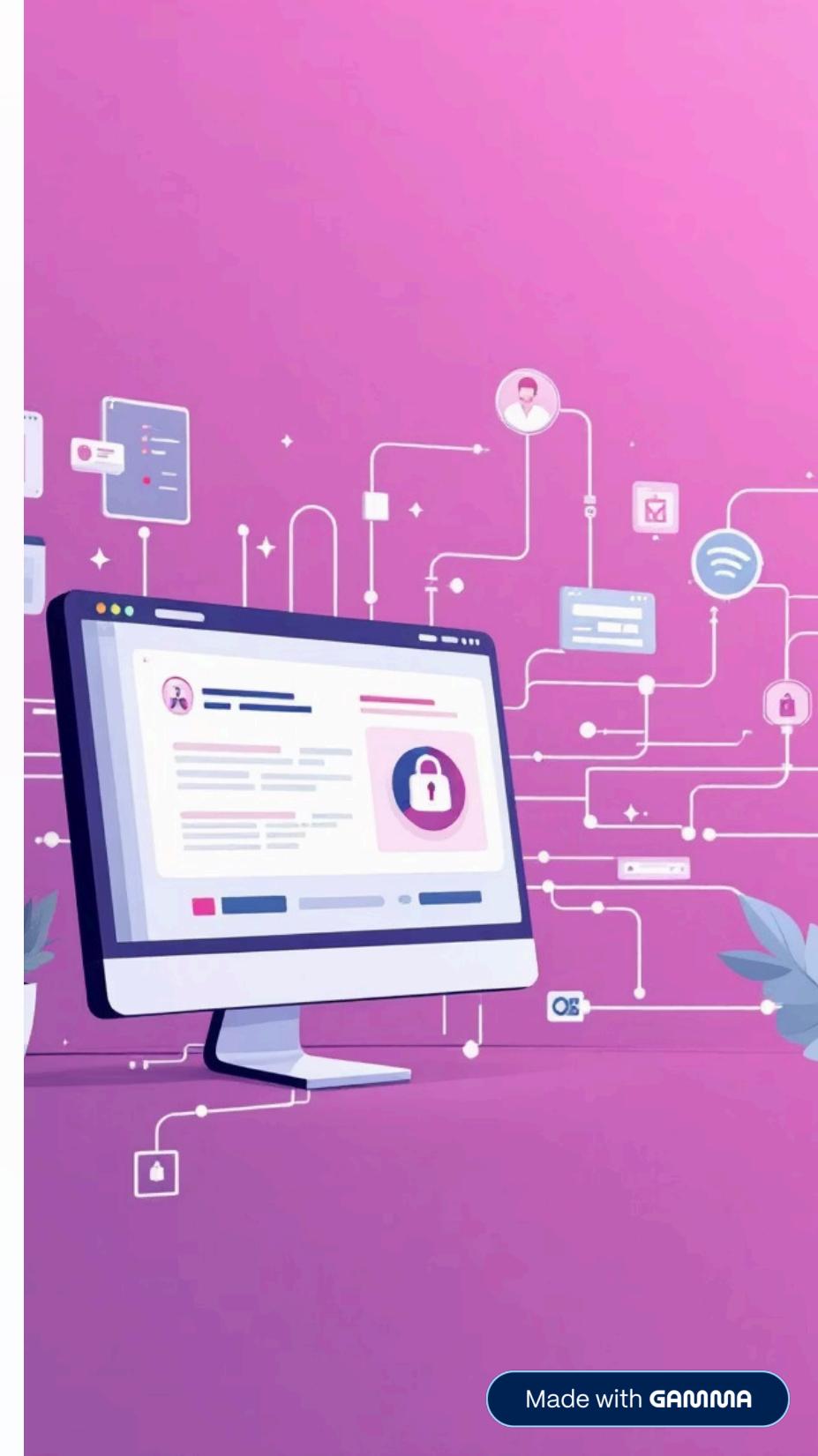
Incorpora **OWASP ZAP**, **Nuclei** y **SSLyze** en un flujo intuitivo tipo "self-service", brindando capacidades de escaneo de nivel profesional.

- **Identificación Clara de Vulnerabilidades**

Su objetivo es detectar vulnerabilidades web y presentarlas en un **dashboard interactivo** con métricas y gráficas comprensibles para perfiles técnicos y gerenciales.

- **Enfoque Ético y Académico**

La plataforma garantiza que los escaneos se realicen exclusivamente sobre recursos propios o con autorización explícita, promoviendo una práctica de seguridad responsable.



# Contexto Académico y Valor de Negocio



## Responde a una Necesidad Real del Mercado

Aborda la carencia de **visibilidad estructurada** sobre el estado de seguridad web en pymes y equipos pequeños, ofreciendo una herramienta clave.

## Un "Radar" de Riesgos para Decisiones Estratégicas

Proporciona a los decisores una visión clara de los riesgos, trascendiendo el simple listado técnico de vulnerabilidades hacia un **análisis gerencial**.



# Caso de Uso Específico Abordado

Un vistazo al flujo principal de interacción del usuario con la plataforma.

1

## Registro y Autenticación

El usuario se registra, inicia sesión y accede a su entorno seguro para gestionar auditorías.

2

## Registro de Target y Configuración de Escaneo

Se registra un sitio (target) y se configura un job de escaneo, seleccionando las herramientas deseadas.

3

## Ejecución y Normalización

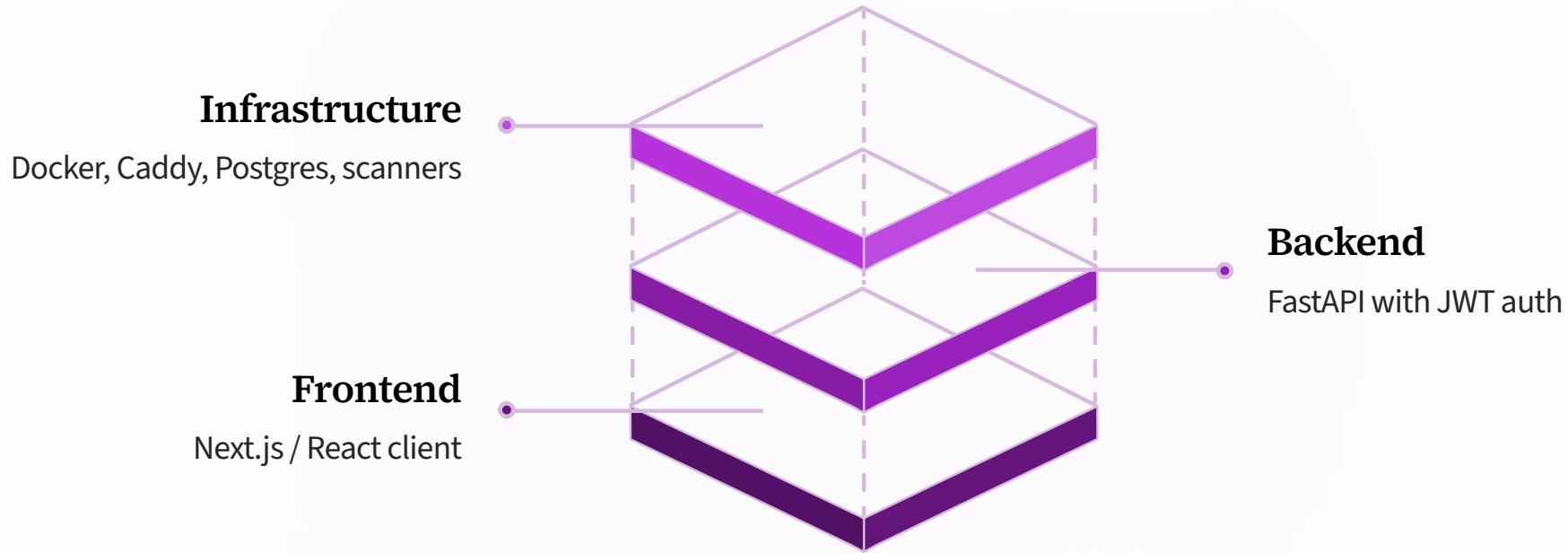
El sistema ejecuta escaneos en contenedores aislados, normaliza los hallazgos y los asocia al usuario y target.

4

## Visualización de Dashboard

El usuario consulta un dashboard personalizado con KPIs, gráficas y los targets más riesgosos para una visión integral.

# Arquitectura y Componentes Principales



La plataforma se construye sobre una robusta pila tecnológica, garantizando eficiencia y seguridad.

- **Backend en FastAPI:** Gestiona la autenticación (JWT, hash seguro de contraseñas), el modelo de datos (usuarios, targets, jobs, findings) y la orquestación de escaneos, asegurando la integridad de la información.
- **Frontend en Next.js/React:** Proporciona una interfaz de usuario moderna e intuitiva con pantallas de registro/login, creación de escaneos, listado de resultados y un **dashboard interactivo** con gráficas y KPIs, mejorando la experiencia del usuario.
- **Infraestructura Docker Compose:** Permite el despliegue orquestado del backend, frontend, base de datos y herramientas de escaneo, utilizando Caddy como reverse proxy para un acceso unificado y simplificado.
- **Modelo de Datos con Control de Acceso:** Diseñado desde el inicio para que todas las métricas estén filtradas por usuario autenticado, cuidando la privacidad y el control de acceso a la información sensible.

# Retos Técnicos Principales Superados

01

## Integración de Herramientas de Seguridad Reales

Encapsular **ZAP**, **Nuclei** y **SSLyze** en contenedores, manejar timeouts y parsear sus salidas JSON a un modelo de datos común fue un desafío clave resuelto con éxito.

02

## Esquema de Datos Unificado para Findings

Crear un esquema que permita comparar severidades y tipos de hallazgo entre herramientas tan diversas, proporcionando una visión consolidada de las vulnerabilidades.

03

## Implementación de Autenticación Robusta

Garantizar la seguridad mediante **bcrypt**, **JWT** y **dependencias de seguridad** en **FastAPI**, asegurando que cada usuario solo acceda a sus propios datos.

04

## Endpoints de Métricas Optimizados

Desarrollo de endpoints específicos como `/metrics/summary`, `/metrics/by-severity`, `/metrics/timeline` y `/metrics/top-targets` para alimentar visualizaciones en tiempo real con alta eficiencia.

05

## Coordinación Eficaz entre Roles

Sincronización entre el rol de Backend & Seguridad y el de Frontend & Infra, logrando acuerdos en contratos de API y tiempos de entrega para una implementación fluida.

# Retos de Organización y Trabajo en Equipo

La colaboración y la gestión estratégica fueron esenciales para el éxito del proyecto.



- **Definición de Roadmap por Fases:** Establecimiento de un plan claro (infraestructura, backend base, integración de herramientas, métricas, frontend, dashboard, pulido) con prioridades para el Producto Mínimo Viable (MVP), asegurando un avance estructurado.
- **Reparto de Responsabilidades y Sincronización:** Asignación estratégica de tareas y mantenimiento de una comunicación continua entre los equipos de backend (autenticación y modelos) y frontend (pantallas y UX) para una integración armónica.
- **Gestión de la Complejidad a Tiempo Parcial:** Priorización de las fases críticas (autenticación, jobs/targets, integración de herramientas y dashboard) en un proyecto de más de 5 semanas a tiempo parcial, optimizando los recursos.
- **Documentación para Mantenibilidad y Extensibilidad:** Registro detallado de decisiones técnicas y de seguridad, facilitando que futuros estudiantes o equipos puedan mantener y expandir la plataforma, garantizando su sostenibilidad a largo plazo.



# Resultados Finales del Sistema

Una plataforma completamente funcional y lista para empoderar la seguridad web.

1

## Plataforma de Gestión Personalizada

Un sistema donde los usuarios pueden **registrarse**, **autenticarse** y **gestionar sus propios targets y escaneos** de seguridad de forma autónoma.

2

## Integración Multi-Herramienta Completa

Funcionalidad con **OWASP ZAP** (vulnerabilidades web), **Nuclei** (CVEs/misconfiguraciones) y **SSLyze** (estado SSL/TLS) para un análisis de seguridad exhaustivo.

3

## Dashboard Interactivo y Detallado

Visualización de **número total de escaneos y findings**, distribución de severidades, distribución por herramienta, timeline de actividad y los **top targets** con más hallazgos.

4

## Flujo Operativo End-to-End

Desde el login hasta la generación de insights gerenciales: **login** → **nuevo escaneo** → **ejecución de herramientas** → **consolidación de hallazgos** → **visualización de métricas**.



# Conclusiones y Aprendizajes Clave

## Viabilidad de Plataformas Seguras y Usables

Demostración de que es posible construir una plataforma de auditoría web robusta y amigable usando tecnologías modernas y herramientas open-source.

## Entendimiento Práctico de Conceptos de Seguridad

Consolidación de conocimientos en autenticación, autorización, aislamiento de procesos, manejo seguro de secretos y comunicación efectiva de riesgos.

## El Dashboard como Puente Estratégico

Transformación del dashboard en una herramienta que conecta el lenguaje técnico de las vulnerabilidades con el lenguaje de negocio de los riesgos e impactos.

## Visión Clara para Futuras Mejoras

Identificación de líneas de trabajo futuras como multi-tenant avanzado, exportación de reportes en PDF, optimización de performance y nuevas integraciones de herramientas.