Universidad de la Cuenca del Plata
Autorización Definitiva. Decreto Poder Ejecutivo Nacional N°091/2006

CyberLab Finder

CARRERA: Ingeniería en Sistemas de información

MATERIA: Paradigmas y Lenguajes de Programación III

COMISIÓN: “U” (única) “A”

PROFESOR: Mgter. Ing. Agustín Encina

ESTUDIANTE: Viñales Facundo

FECHA: 23-08-2025

Contenido

Introducción

El presente trabajo tiene como objetivo la presentación del proyecto **CyberLab Finder**, una propuesta orientada al ámbito del hacking ético y la ciberseguridad.

La idea surge a partir de la necesidad de contar con un sistema que unifique en un solo lugar recursos prácticos (máquinas y laboratorios) y teóricos (herramientas y documentación), con el fin de facilitar el aprendizaje de estudiantes y profesionales de la seguridad informática.

Este informe expone la descripción de la propuesta, los objetivos generales y específicos, los requisitos del sistema, así como los avances iniciales que fundamentan su desarrollo.

Desarrollo

Nombre del Proyecto

CyberLab Finder

Link Repositorio

https://github.com/icufaa/CyberLab-Find.git

Breve descripción de la idea

CyberLab Finder será una plataforma que centralice recursos para la práctica del hacking ético. La propuesta integra dos ejes principales:

1. **Buscador de máquinas de práctica:** permitirá explorar e indexar laboratorios de **HackTheBox** y **VulnHub**, ofreciendo filtros por dificultad, categoría de vulnerabilidad y sistema operativo.
2. **Catálogo de herramientas filtrables:** Repositorios, scripts y utilidades de ciberseguridad (principalmente de GitHub), organizados por categorías como enumeración, explotación, post-explotación y forense.

Un valor agregado será la vinculación con HackTricks, permitiendo que cada máquina esté asociada a documentación teórica específica de la vulnerabilidad que explota, reforzando la relación entre la práctica y la teoría.

Objetivos Generales

- Desarrollar una plataforma que centralice recursos prácticos de hacking ético.
- Brindar un sistema de búsqueda y filtrado para facilitar la selección de laboratorios y herramientas.
- Contribuir al aprendizaje práctico en ciberseguridad de manera accesible y organizada.

Objetivos específicos

- Implementar un buscador de máquinas de HackTheBox y VulnHub con filtros avanzados.
- Incorporar un módulo de filtrado de herramientas clasificadas por etapa del pentesting.
- Diseñar una interfaz sencilla y clara para el usuario.
- Sentar las bases para una futura comunidad de usuarios que pueda recomendar, valorar y comentar recursos.

- Integrar un sistema de vinculación entre máquinas y documentación técnica (Ejemplo: HackTricks).
- Incorporar una sección que indique para qué certificación puede servir cada máquina/laboratorio (ej.: OSCP, eJPT), de que modo que el estudiante sepa qué práctica le aporta valor en su formación profesional

Requisitos

Requisitos Funcionales

- Sistema de búsqueda y filtrado avanzado.
- Base de datos que almacene máquinas y herramientas.
- Interfaz web responsive y amigable.
- Posibilidad de expandirse con nuevas fuentes de datos.

Requisitos no funcionales

- Seguridad básica implementada (prevención de inyecciones, sanitización de inputs, etc.)
- Arquitectura escalable para soportar futuros usuarios.
- Código organizado y mantenible, para facilitar su crecimiento.

Avances Iniciales

- Inspiración en plataformas como HackingVault.
- Diferencia clave: integración de un filtrado de herramientas, no presente en otras plataformas similares.
- Vinculación con HackTricks para repasar conceptos de vulnerabilidades relacionadas con cada laboratorio.
- Propuesta de valor agregado: incluir un apartado en cada máquina que indique qué certificación refuerza (ejemplo:
    - Máquina con explotación de buffer overflow → útil para OSCP.
    - Máquina con foco en enumeración y ataques básicos → útil para eJPT.
    - Máquina con orientación en metodologías de auditoría → útil para CEH).
- Definición de categorías iniciales para las herramientas:
    - **Enumeración:** nmap, gobuster, enum4linux, wfuzz.
    - **Explotación:** metasploit, sqlmap.
    - **Post-Explotación:** mimikatz, linpeas.
    - **Forense:** autopsy, volatility.

Diagramas

Diagrama de casos de uso

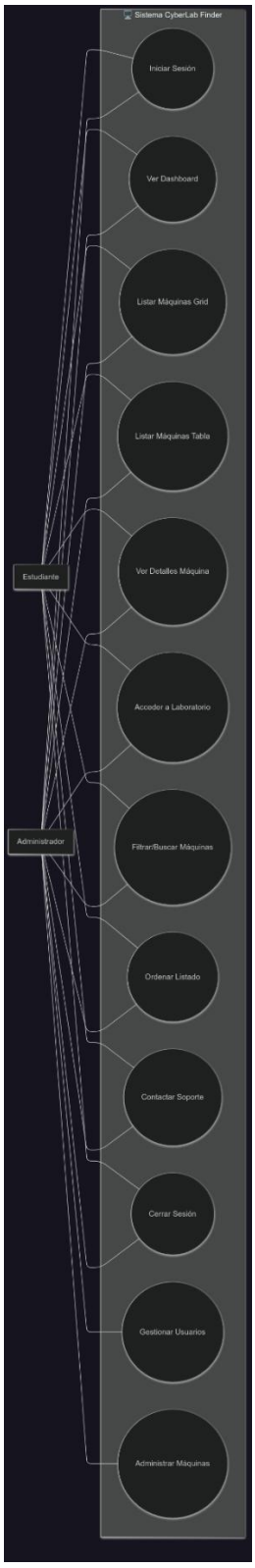


Diagrama de arquitectura de sistema (Propuesto)

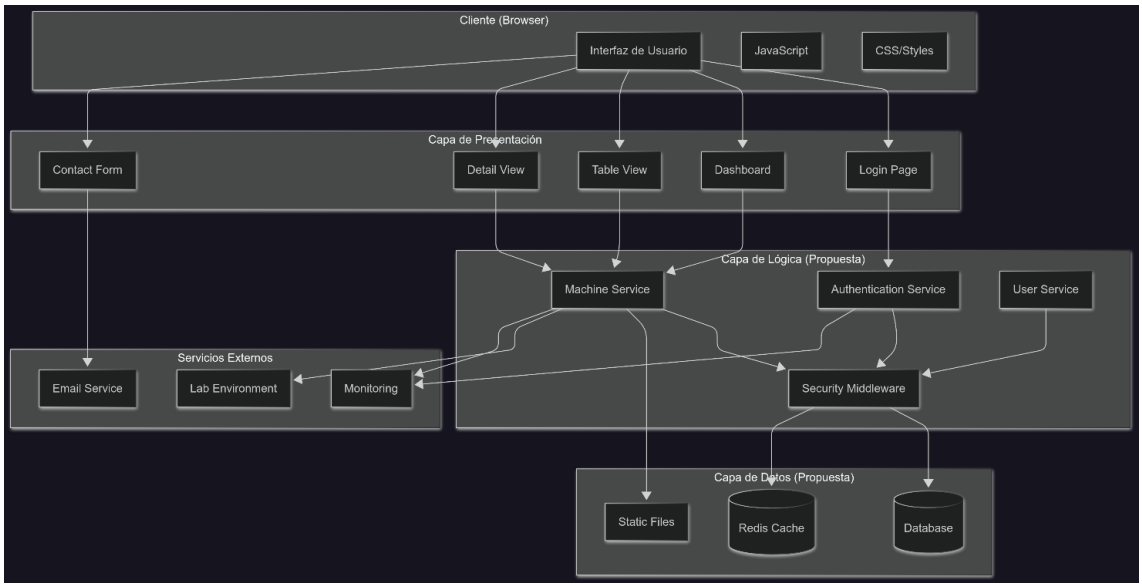
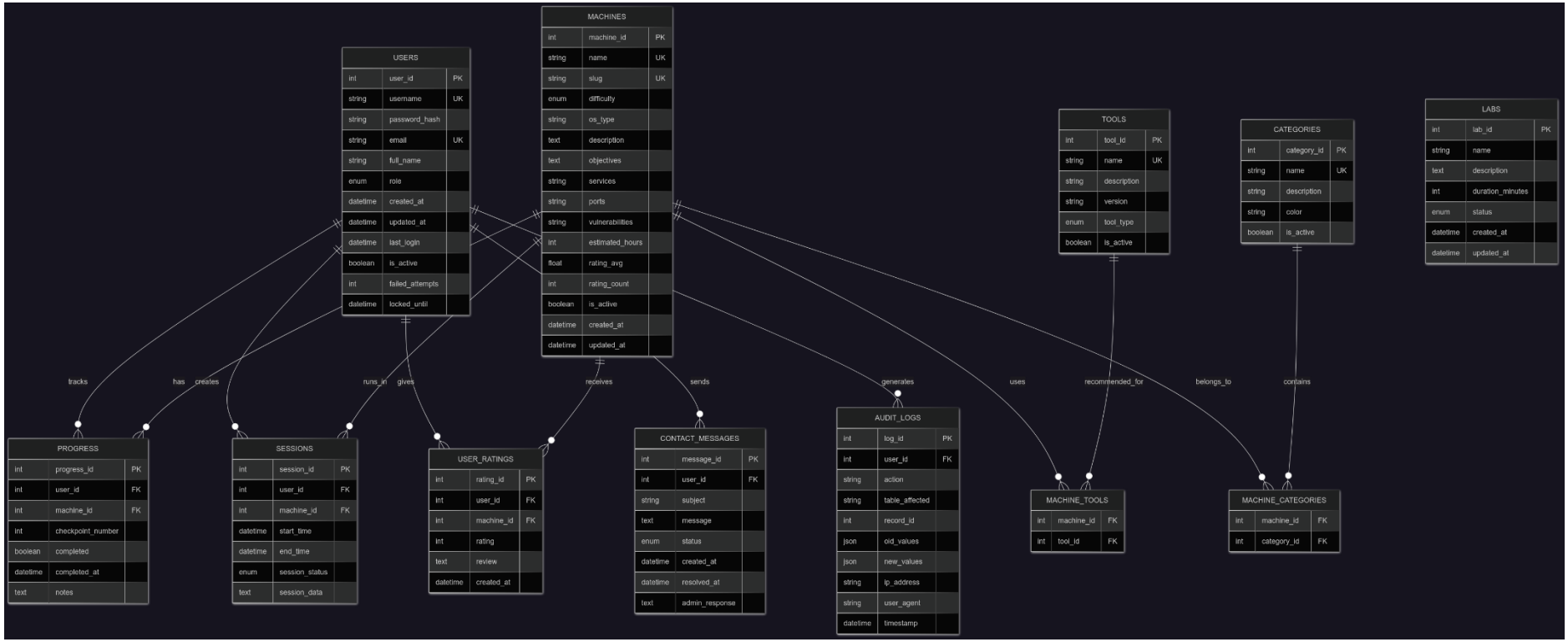


Diagrama Entidad Relación



Conclusiones

El proyecto **CyberLab Finder** busca ofrecer un espacio innovador en el ámbito de la ciberseguridad, combinando la práctica a través de laboratorios reconocidos (HackTheBox y VulnHub) con un catálogo de herramientas y recursos de apoyo.

La inclusión de documentación vinculada (HackTricks) permite potenciar el aprendizaje, dado que el estudiante puede repasar conceptos al mismo tiempo que los aplica en un laboratorio práctico.

En conclusión, este proyecto propone una plataforma integral que contribuirá al aprendizaje autónomo, organizado y eficiente en el camino hacia el hacking ético.

Bibliografía

HackTheBox. (2025). https://www.hackthebox.com

VulnHub. (2025). https://www.vulnhub.com

HackTricks. (2025). https://book.hacktricks.wiki