



***Instituto Superior Universitario Tecnológico del Azuay***

***Nombre:*** Steven Vallejo

***Carrera:*** Tecnología Superior en Ciberseguridad - V4A

***Tema:*** Informe de caso práctico

***Fecha del informe:*** 21/07/2025

***Periodo abril - agosto 2025***

<b>1. Selección y justificación del tema</b>	<b>3</b>
Resumen del proyecto	3
<b>2. Planteamiento del problema y objetivos</b>	<b>4</b>
Planteamiento del problema	4
Objetivo general	4
Objetivos específicos	4
<b>3. Marco teórico</b>	<b>5</b>
<b>4. Metodología, fases y herramientas utilizadas</b>	<b>6</b>
Metodología	6
Fases del proyecto	6
Herramientas utilizadas	6
<b>5. Plan de ejecución y desarrollo</b>	<b>7</b>
Desarrollo del Sitio Web "Viajes Seguros S.A."	7
Lanzamiento del Sitio Web "Viajes Seguros S.A."	9
Integración controlada de vulnerabilidades	11
Cronograma de ejecución	12
<b>6. Resultados esperados y conclusiones preliminares</b>	<b>13</b>
Resultados esperados	13
Conclusiones preliminares	13
<b>7. Redacción final</b>	<b>13</b>

## 1. Selección y justificación del tema

La seguridad de las aplicaciones web es un pilar fundamental para la protección de datos y la continuidad del negocio. Sin embargo, existe una brecha significativa entre el conocimiento teórico de las vulnerabilidades y la capacidad práctica para identificarlas, explotarlas y mitigarlas. Este proyecto aborda dicha brecha mediante la creación de un entorno de aprendizaje controlado.

La justificación de este tema se basa en tres pilares:

- **Relevancia en la industria:** La ciberseguridad es uno de los campos con mayor demanda de profesionales cualificados. Dominar las vulnerabilidades listadas por el **Open Web Application Security Project (OWASP)** es un requisito indispensable.
- **Necesidad de formación práctica:** El aprendizaje más efectivo en ciberseguridad proviene de la experiencia práctica. Un laboratorio controlado permite a los estudiantes experimentar con ataques reales sin comprometer sistemas en producción y sin incurrir en ilegalidades.
- **Impacto educativo:** La donación de este laboratorio a la institución proporcionará una herramienta pedagógica de alto valor, permitiendo a los estudiantes visualizar y comprender de forma tangible los riesgos de seguridad web.

### Resumen del proyecto

Este caso práctico consiste en el diseño, implementación y documentación de un laboratorio de ciberseguridad. El núcleo del laboratorio es una aplicación web funcional de una agencia de viajes, denominada "Viajes Seguros S.A.", desarrollada intencionadamente con cinco vulnerabilidades críticas basadas en el OWASP Top 10. El proyecto abarca desde la creación del sitio web y su alojamiento en un entorno virtualizado y seguro (Ubuntu en VirtualBox), hasta la elaboración de una guía detallada para la identificación y explotación de cada fallo de seguridad utilizando herramientas profesionales como Burp Suite y OWASP ZAP.

## 2. Planteamiento del problema y objetivos

### Planteamiento del problema

La formación tradicional en ciberseguridad a menudo se limita a conceptos teóricos, dejando a los estudiantes sin la experiencia práctica necesaria para enfrentar amenazas reales. La falta de acceso a entornos seguros y realistas donde puedan experimentar con técnicas de ataque y defensa dificulta el desarrollo de habilidades aplicadas. Este proyecto busca resolver este problema creando un recurso educativo autocontenido, seguro y replicable que simula un escenario de pentesting del mundo real.

### Objetivo general

- **Desarrollar** un laboratorio de ciberseguridad completamente funcional, implementando un entorno virtual con una aplicación web intencionadamente vulnerable, con el fin de analizar y demostrar vulnerabilidades críticas del OWASP Top 10 a través de herramientas de pruebas de penetración.

### Objetivos específicos

1. **Diseñar e implementar** una aplicación web realista ("Viajes Seguros S.A.") que integre de forma lógica y oculta cinco vulnerabilidades de seguridad clave.
2. **Configurar e instrumentar** un entorno de servidor seguro y aislado utilizando VirtualBox, Ubuntu Server y Apache, para alojar la aplicación vulnerable y permitir la realización de pruebas de penetración controladas.
3. **Analizar y demostrar** la explotación de cada una de las vulnerabilidades implementadas, documentando el proceso paso a paso desde una perspectiva de "caja gris" y simulando el uso de herramientas profesionales de pentesting.

### 3. Marco teórico

- **OWASP Top 10:** Es un documento de concienciación estándar para desarrolladores y profesionales de la seguridad de aplicaciones web. Representa un amplio consenso sobre los riesgos de seguridad más críticos. Este proyecto se basa en la lista de 2021.
- **Descripción de vulnerabilidades seleccionadas:**
  - **A01:2021 - Broken Access Control:** Fallos en la aplicación de restricciones sobre lo que los usuarios autenticados pueden hacer. Permite a los atacantes acceder a datos o funcionalidades de otros usuarios, o escalar privilegios.
  - **A02:2021 - Cryptographic Failures:** Errores relacionados con la criptografía (o la falta de ella), que pueden exponer datos sensibles. Incluye el uso de algoritmos de hash débiles (ej. MD5) o el almacenamiento de datos en texto plano.
  - **A03:2021 - Injection:** Ocurre cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. La inyección SQL es el ejemplo más conocido, permitiendo a un atacante ejecutar comandos maliciosos en la base de datos.
  - **A04:2021 - Insecure Design:** Representa una categoría de debilidades que surgen de una planificación y diseño de la lógica de negocio defectuosos, sin considerar los posibles abusos por parte de un atacante.
  - **A05:2021 - Security Misconfiguration:** Fallos en la configuración de seguridad del servidor, la aplicación o la base de datos. Incluye dejar puertos abiertos, mostrar mensajes de error detallados o no cambiar contraseñas por defecto.
- **Entornos de laboratorio (Sandboxing):** Un sandbox es un entorno de pruebas aislado que impide que el software o los procesos afecten a la aplicación o al sistema anfitrión. En este proyecto, se utiliza **VirtualBox** para crear una máquina virtual con **Ubuntu**, logrando un aislamiento completo del sistema operativo del anfitrión.

## 4. Metodología, fases y herramientas utilizadas

### Metodología

Se empleó una metodología práctica, dividida en fases secuenciales que simulan el ciclo de vida de un producto digital, pero con un enfoque en la "inseguridad por diseño" con fines educativos.

### Fases del proyecto

1. **Fase I - Investigación:** Investigación de herramientas, medir el alcance de nuestros recurso, planteamiento de objetivos y del caso, recopilación de información para desarrollo de sitio web vulnerable
2. **Fase II - Diseño y desarrollo:** Creación de la aplicación web "Viajes Seguros S.A." utilizando PHP, MySQL, HTML y CSS. En esta fase se integraron las vulnerabilidades de forma sutil y realista.
3. **Fase III - Configuración del entorno:** Instalación y configuración de la máquina virtual (VirtualBox), el sistema operativo (Ubuntu) y el stack de servidor (Apache, MySQL, PHP).
4. **Fase IV - Análisis y explotación:** Simulación de una prueba de penetración para descubrir y explotar las cinco vulnerabilidades implementadas.
5. **Fase V - Documentación:** Redacción de este informe y la guía de explotación confidencial.

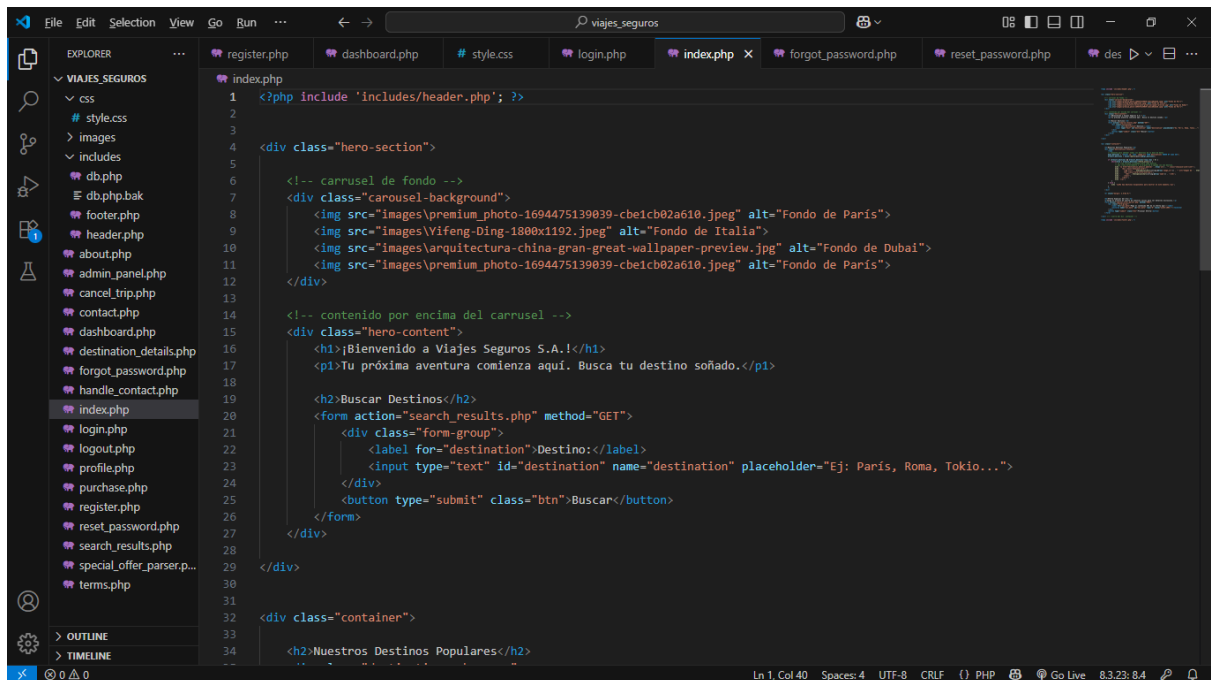
### Herramientas utilizadas

- **Visual Studio Code:** Editor de código para el desarrollo de la aplicación web.
- **Laragon (2025 v8.2.1):** Entorno de desarrollo local para pruebas rápidas.
- **VirtualBox (v7.0.12):** Software de virtualización para crear el entorno de laboratorio aislado.
- **Ubuntu (v20.04):** Sistema operativo anfitrión para el servidor web.
- **Apache (v2.4.41):** Servidor web para alojar la aplicación.
- **HeidiSQL Portable (v12.8.0.6908) / SQLite (v3.31.1):** Sistema de gestión de bases de datos.
- **Burp Suite (v2025.6.5) / OWASP ZAP (v2.15.0):** Proxies de intercepción para analizar y manipular el tráfico HTTP/S, herramientas esenciales en cualquier pentest.

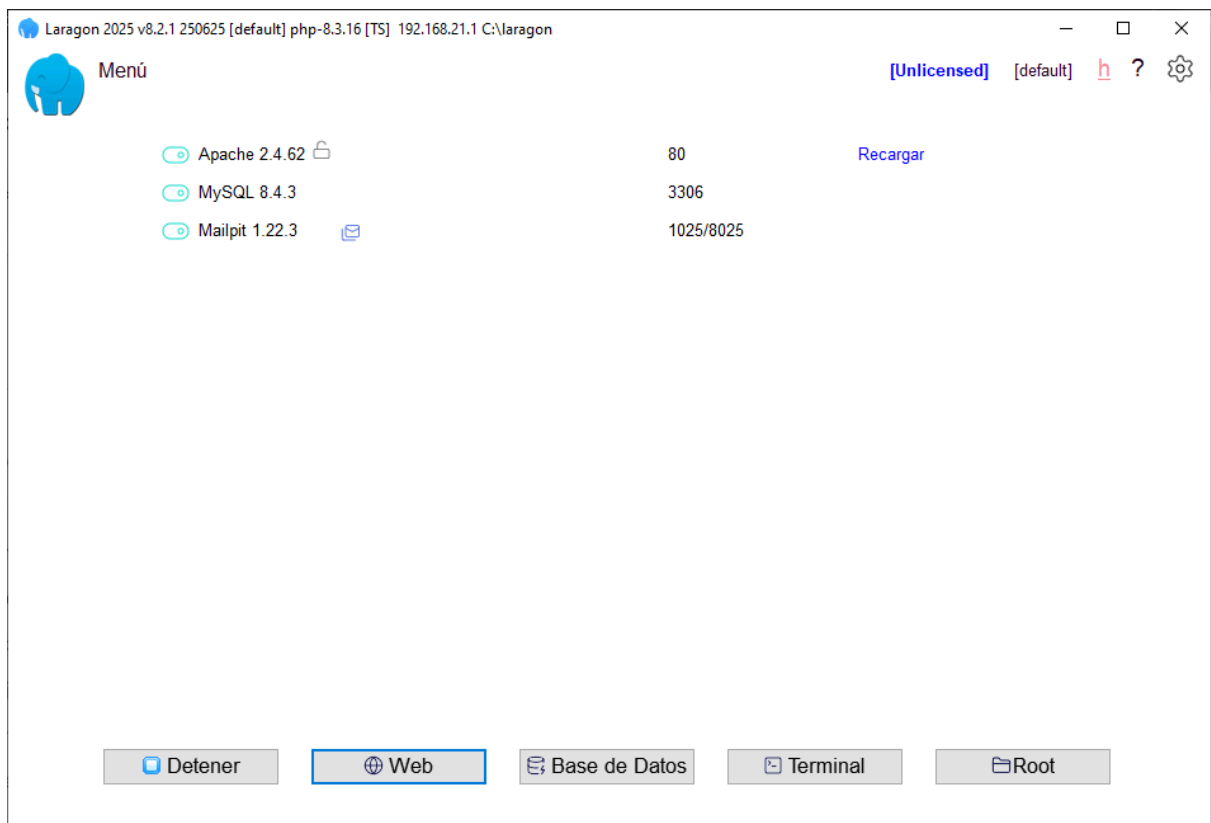
## 5. Plan de ejecución y desarrollo

### Desarrollo del Sitio Web "Viajes Seguros S.A."

Se desarrolló una aplicación web con PHP/MySQL. El sitio simula una agencia de viajes con las siguientes funcionalidades: registro de usuarios, inicio de sesión, un panel de control personalizado, un catálogo de destinos, páginas informativas y una simulación de compra y cancelación de viajes. La interfaz fue diseñada para ser moderna, ocultando eficazmente las debilidades intencionadas.



```
1 <?php include 'includes/header.php'; ?>
2
3
4 <div class="hero-section">
5
6 <!-- carrusel de fondo -->
7 <div class="carousel-background">
8 
9 
10 
11 
12 </div>
13
14 <!-- contenido por encima del carrusel -->
15 <div class="hero-content">
16 <h1>Bienvenido a Viajes Seguros S.A.¡</h1>
17 <p1>Tu próxima aventura comienza aquí. Busca tu destino soñado.</p1>
18
19 <h2>Buscar Destinos</h2>
20 <form action="search_results.php" method="GET">
21 <div class="form-group">
22 <label for="destination">Destino:</label>
23 <input type="text" id="destination" name="destination" placeholder="Ej: Paris, Roma, Tokio...">
24 </div>
25 <button type="submit" class="btn">Buscar</button>
26 </form>
27 </div>
28
29 </div>
30
31
32 <div class="container">
33
34 <h2>Nuestros Destinos Populares</h2>
35
```

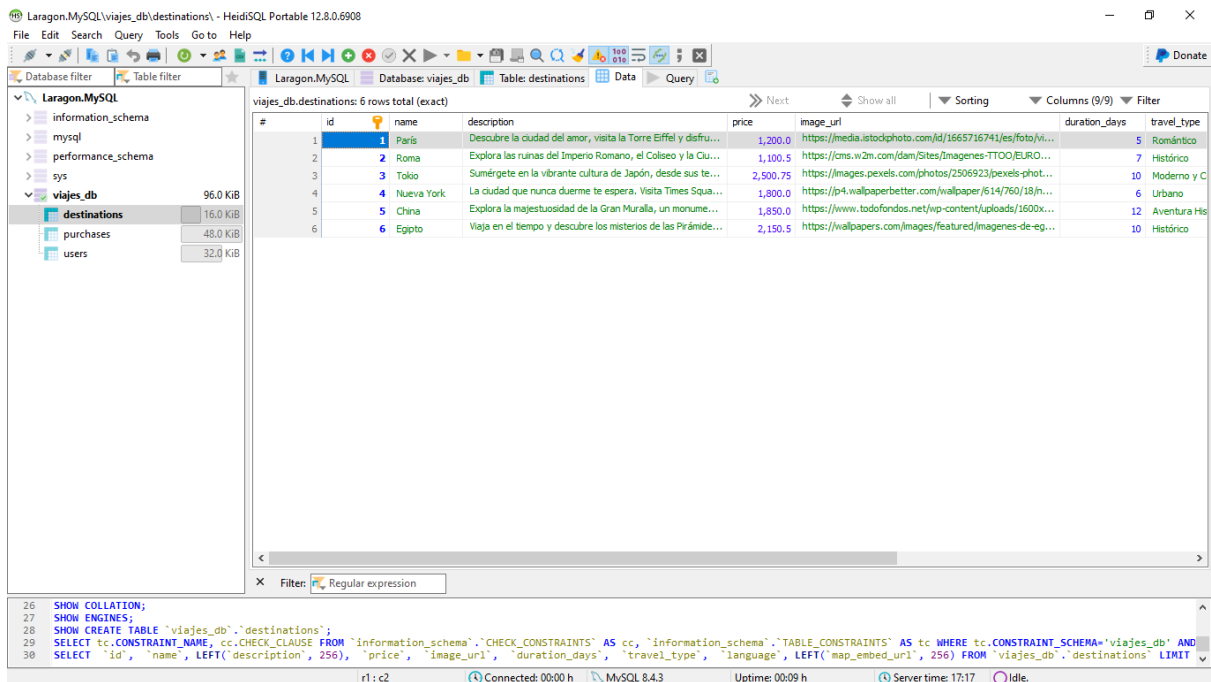
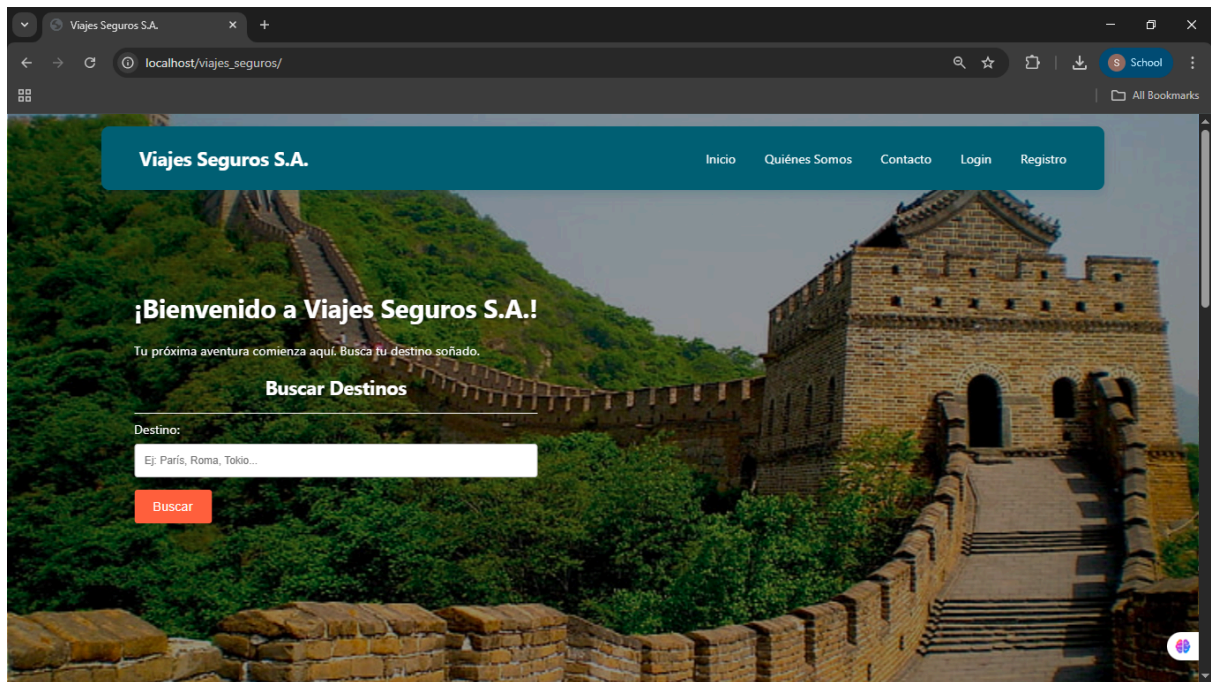


Laragon 2025 v8.2.1 250625 [default] php-8.3.16 [TS] 192.168.21.1 C:\Laragon

Menú [Unlicensed] [default] h ? ⚙

Apache 2.4.62	80	Recargar
MySQL 8.4.3	3306	
Mailpit 1.22.3	1025/8025	

Detener Web Base de Datos Terminal Root





## Lanzamiento del Sitio Web "Viajes Seguros S.A."

### ***Configuración del Entorno Virtual:***

Se instaló Virtual Box y se montó una máquina virtual con Ubuntu 20.04, ajustando los parámetros necesarios para su correcto funcionamiento.

### ***Ajustes de Red:***

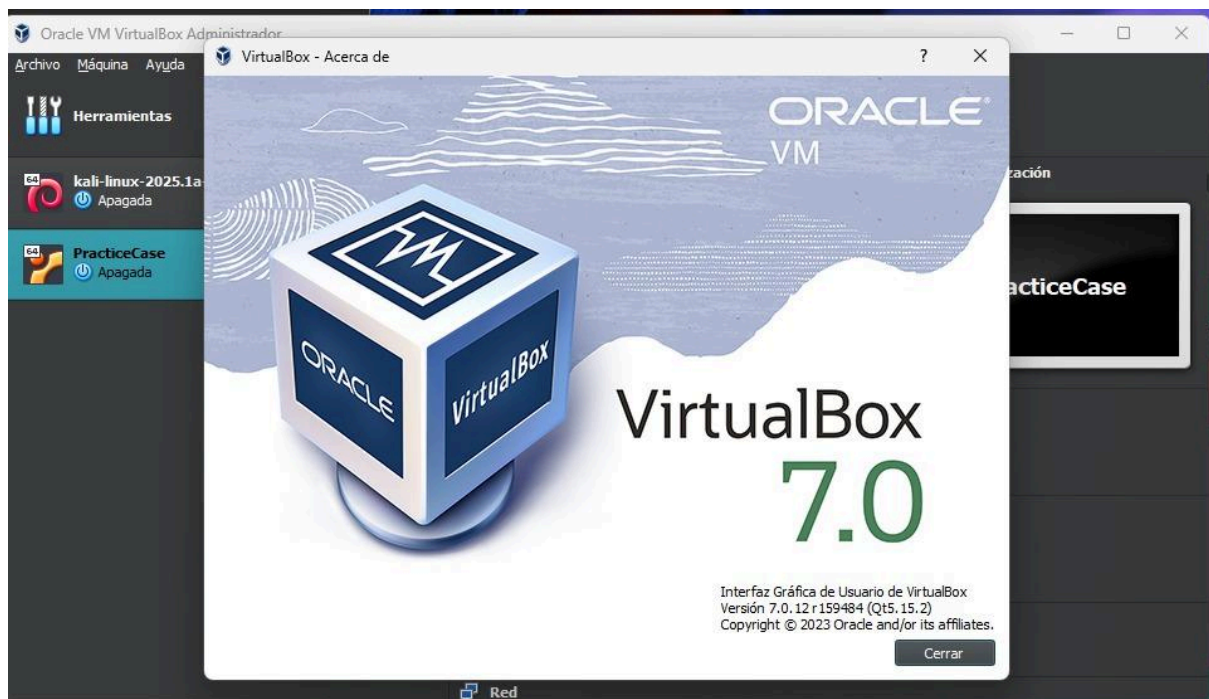
La MV se configuró en modo adaptador puente para permitir conexiones desde la red local, facilitando pruebas externas desde otros dispositivos.

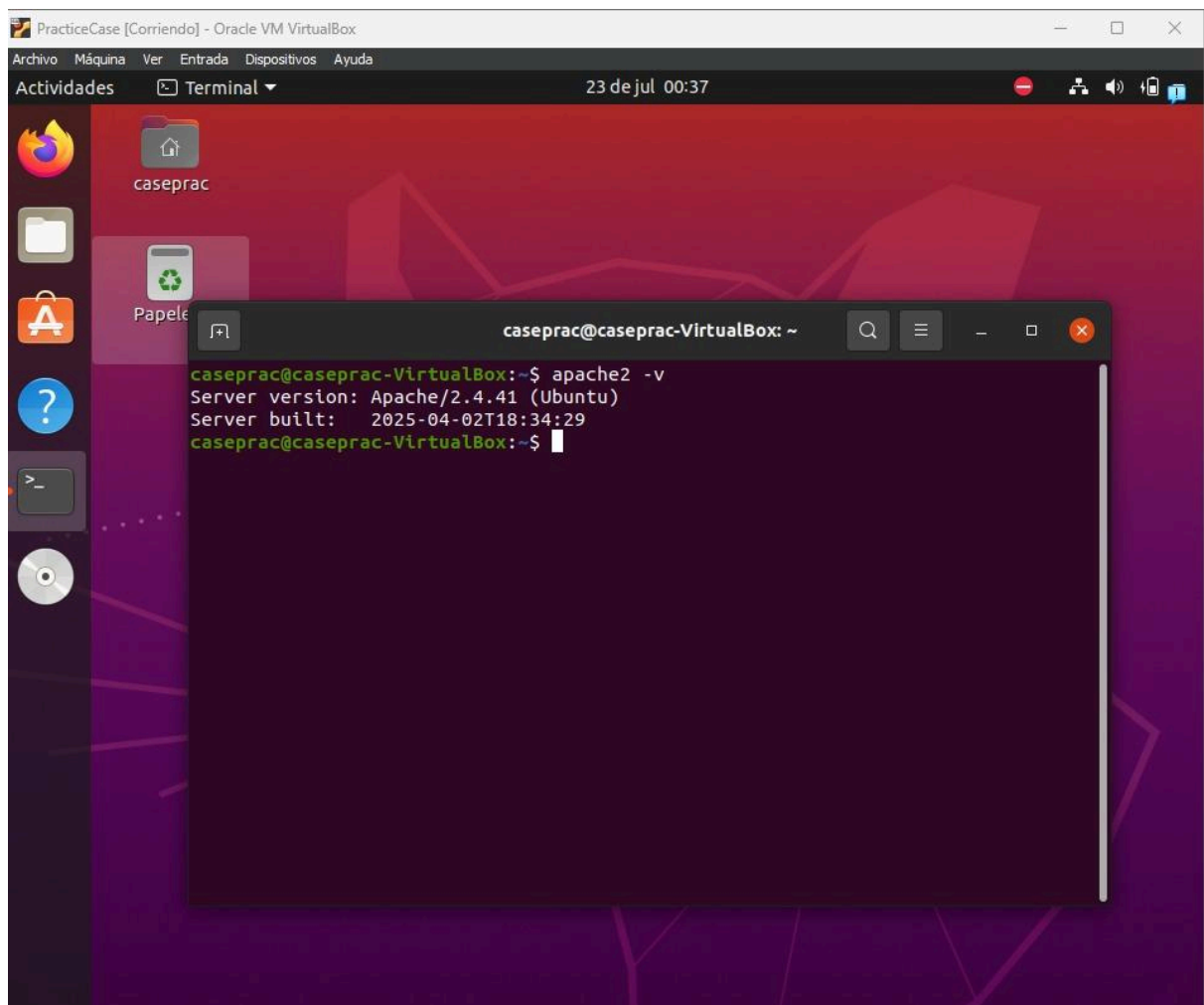
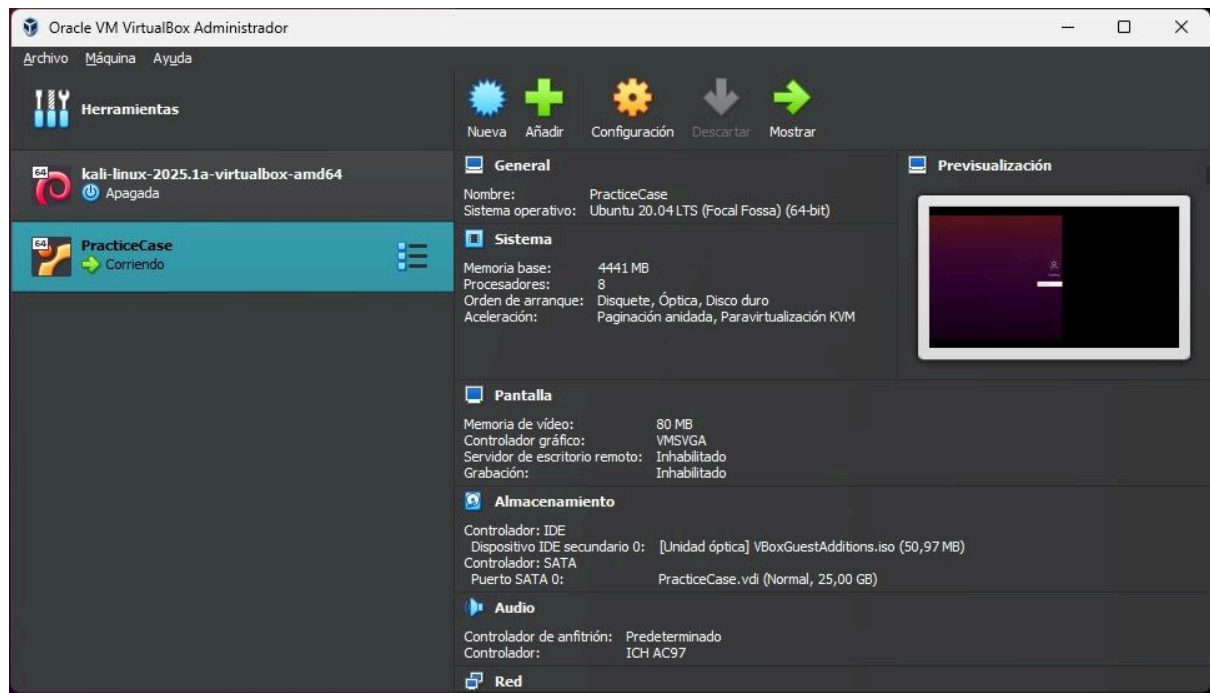
### ***Despliegue del Sitio Web:***

Se instalaron y configuraron Apache2, PHP, MySQL y SQLite en Ubuntu. Luego, se transfirieron los archivos del sitio web al directorio de Apache para su ejecución.

### ***Exportación y Distribución:***

La MV se exportó en formato .ova para su fácil distribución, asegurando que otros usuarios puedan replicar el laboratorio sin complicaciones.





## Integración controlada de vulnerabilidades

- **Broken Access Control (A01):**

- **Tipo específico:** Referencia Insegura a Objeto Directo (IDOR).
- **Resumen:** La página muestra la información del perfil basándose en el UUID proporcionado en la URL (profile.php?uuid=...). Sin embargo, el script nunca verifica si el usuario que ha iniciado sesión es el propietario de ese UUID. Esto permite que un atacante, después de obtener el UUID de otra víctima (por ejemplo, a través de la Inyección SQL), pueda ver sus datos privados simplemente cambiando el UUID en la URL.

- **Cryptographic Failures (A02):**

- **Tipo Específico:** Fuga de Token de Reseteo de Contraseña.
- **Resumen:** Aunque la aplicación genera un token de reseteo de contraseña criptográficamente seguro, comete un fallo crítico al escribir este token sensible en un archivo de log (password\_resets.log) por un supuesto "propósito de depuración". Combinado con la mala configuración del servidor que permite el listado de directorios, este archivo de log se vuelve públicamente accesible, permitiendo a un atacante robar los tokens y secuestrar las cuentas de otros usuarios.

- **Injection (A03):**

- **Tipo Específico:** Inyección SQL Ciega (Time-based y Boolean-based).
- **Resumen:** El script toma el término de búsqueda del usuario y lo inserta directamente en una consulta SQL LIKE sin ningún tipo de saneamiento o consultas preparadas. Se han implementado manejadores de errores (try-catch) para que la aplicación no muestre errores de sintaxis SQL, convirtiéndola en una inyección "ciega".

- **Insecure Design (A04):**

- **Tipo Específico:** Confianza Excesiva en los Datos del Cliente (Manipulación de Parámetros).
- **Resumen:** El proceso de compra se realiza en dos pasos. En el segundo paso, la página de confirmación envía el precio final del viaje al script de procesamiento (purchase.php) como un parámetro oculto en el formulario. El servidor, por un fallo de diseño, confía ciegamente en este precio y lo inserta en la base de datos sin volver a verificarlo. Esto permite a un atacante interceptar la petición y modificar el parámetro final\_price a cualquier valor (ej. 1.00), cometiendo fraude.

- **Security Misconfiguration (A05):**
  - **Tipo Específico:** Listado de directorios habilitado.
  - **Errores Detallados en includes/db.php:** Se configuró PHP para mostrar todos los errores (`display_errors = 1`), lo que puede filtrar información sensible como rutas de archivos en caso de un fallo. Resumen: El servidor está configurado con la opción Options +Indexes, lo que deshabilita la protección por defecto que impide a los usuarios ver el contenido de los directorios que no tienen un archivo index. Esto permite a cualquier persona navegar a directorios como `/includes/` o `/logs/` y ver una lista completa de todos los archivos que contienen, facilitando el descubrimiento de archivos sensibles como `db.php` o, en nuestro caso, el crítico `password_resets.log`.

### Cronograma de ejecución

Tarea	Seman a 1	Seman a 2	Seman a 3	Seman a 4	Seman a 5	Seman a 6
<b>Planificación y Marco Teórico</b>	X	X				
<b>Desarrollo del Sitio Web (Frontend/Backend)</b>		X	X	X		
<b>Integración de Vulnerabilidades</b>			X	X		
<b>Configuración del Entorno Virtual</b>		X				
<b>Pruebas de Explotación y Documentación</b>					X	
<b>Redacción del Informe Final</b>					X	
<b>Preparación de la Presentación/Tutoriales</b>						X

## 6. Resultados esperados y conclusiones preliminares

### Resultados esperados

Al finalizar este proyecto, se obtendrán los siguientes entregables:

1. Un **laboratorio de ciberseguridad funcional**, compuesto por una máquina virtual configurada y una aplicación web vulnerable.
2. La **aplicación web "Viajes Seguros S.A."** completamente desarrollada, sirviendo como el activo principal para las pruebas.
3. Una **guía de explotación detallada y confidencial** que documenta paso a paso el descubrimiento y ataque de cada una de las cinco vulnerabilidades.
4. Este **informe de caso práctico**, que documenta formalmente todo el proceso de diseño, implementación y análisis del proyecto, junto **videotutoriales** de cada vulnerabilidad.

### Conclusiones preliminares

El desarrollo del proyecto ha sido satisfactorio, cumpliendo con las fases del cronograma. Se concluye que los objetivos planteados son alcanzables y se están cumpliendo de la siguiente manera:

- Se ha **diseñado e implementado con éxito** la aplicación web vulnerable, cumpliendo con el **objetivo específico 1**. La integración de las cinco vulnerabilidades no interfiere con la funcionalidad aparente del sitio, aumentando su realismo.
- El **entorno de desarrollo local ha sido validado**, y los preparativos para la migración al entorno virtualizado están realizados, lo que asegura el cumplimiento del **objetivo específico 2**.
- Las pruebas iniciales de explotación confirman que todas las vulnerabilidades son accesibles y explotables como fue planeado, sentando las bases para el cumplimiento del **objetivo específico 3**.

Este proyecto demuestra ser una herramienta de gran potencial educativo. La capacidad de interactuar con vulnerabilidades reales en un entorno seguro no solo refuerza el conocimiento teórico, sino que también fomenta el pensamiento crítico y la metodología de un profesional de la ciberseguridad, cumpliendo así con el **objetivo general** de este caso práctico.

## 7. Redacción final

El presente documento ha sido redactado siguiendo un estándar formal y técnico, con el objetivo de presentar de manera clara y estructurada el alcance, la metodología y los resultados del proyecto. La terminología utilizada es consistente con los estándares de la industria de la ciberseguridad, y la estructura del informe está diseñada para guiar al lector a través del proceso completo del caso práctico.