Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | 1 | Pérdida de Autenticación y Gestión de Sesiones

Auditoría Informática

Ingeniería en Desarrollo de Software

academia global

TUTOR: Jessica Hernández Romero

ALUMNO: Christian Ivan Ibarra Corrales

FECHA: 17 de junio de 2025

Introducción

La pérdida de autenticación y la mala gestión de sesiones representan vulnerabilidades críticas en la seguridad web. Este tipo de fallos permite a atacantes interceptar información sensible, como credenciales de usuarios, especialmente cuando el sitio web no cuenta con cifrado SSL. Millones de usuarios ingresan diariamente sus datos personales en plataformas digitales sin conocer los riesgos que implica una mala implementación de medidas de seguridad. En entornos donde no se aplican protocolos HTTPS, herramientas como WireShark pueden capturar fácilmente la información que viaja en texto plano, dejando expuestos a los usuarios a robos de identidad, fraudes y acceso no autorizado a sus cuentas. Esta actividad permite comprobar, mediante una simulación, cómo es posible interceptar datos cuando no existe cifrado en las conexiones web. Comprender esta vulnerabilidad es esencial para prevenir ataques reales, fomentar el desarrollo de aplicaciones más seguras y generar conciencia sobre la importancia de navegar únicamente en sitios web protegidos. Esta práctica refuerza el papel de la auditoría informática en la protección de datos.

Descripción

La presente actividad busca identificar y evaluar la vulnerabilidad de pérdida de autenticación y gestión de sesiones en sitios web. El objetivo es experimentar, a través de una prueba práctica, cómo la ausencia de protocolos de seguridad como SSL puede ser aprovechada por atacantes para interceptar credenciales. Se utilizará WireShark, una herramienta de análisis de red que permite capturar paquetes de información transmitidos por la red, para detectar los datos enviados sin cifrado. El proyecto web seleccionado cuenta con funciones de registro, inicio de sesión y conexión a una base de datos, lo que permite simular un entorno real. Al subir el sitio a un servidor gratuito y acceder mediante una red no segura, se podrá observar el comportamiento de la transferencia de datos en texto plano. Esta actividad servirá como base para comprender cómo se ejecutan ataques por falta de seguridad en la autenticación, y permitirá desarrollar buenas prácticas para la programación y auditoría de sitios web seguros en entornos profesionales.

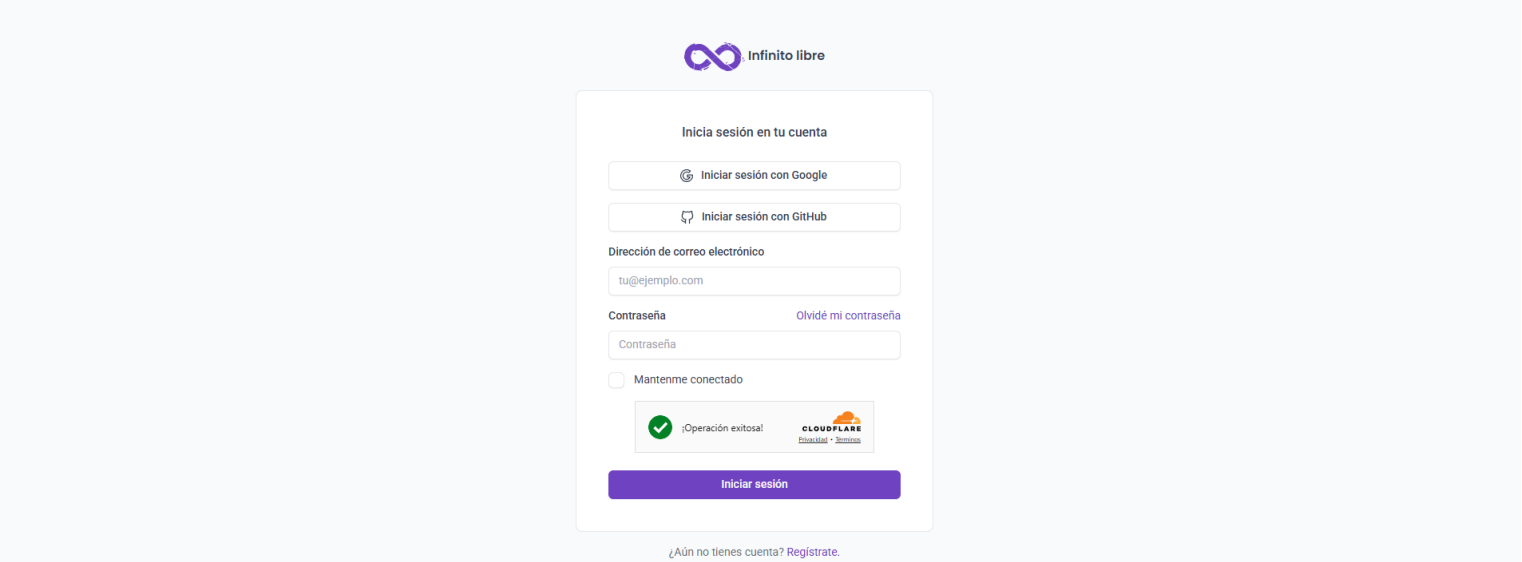
Justificación

Realizar una prueba de pérdida de autenticación y gestión de sesiones permite conocer una de las vulnerabilidades más frecuentes en el desarrollo web. Muchos desarrolladores, especialmente en proyectos académicos o pequeños, omiten la implementación de certificados SSL, exponiendo los datos personales de los usuarios. Esta actividad no solo sirve para comprobar lo que ocurre en estos escenarios, sino también para concientizar sobre la importancia de incorporar protocolos de seguridad desde el diseño del sistema. Usar WireShark como herramienta práctica permite observar de forma directa cómo viajan los datos por la red cuando no están cifrados, mostrando que es posible obtener nombres de usuario y contraseñas mediante simples capturas de paquetes. Esta prueba también destaca el valor de las auditorías informáticas, ya que pueden prevenir vulnerabilidades críticas antes de que sean explotadas. En entornos laborales o académicos, este tipo de análisis fortalece el desarrollo ético y profesional de los sistemas digitales, reforzando la cultura de la ciberseguridad.

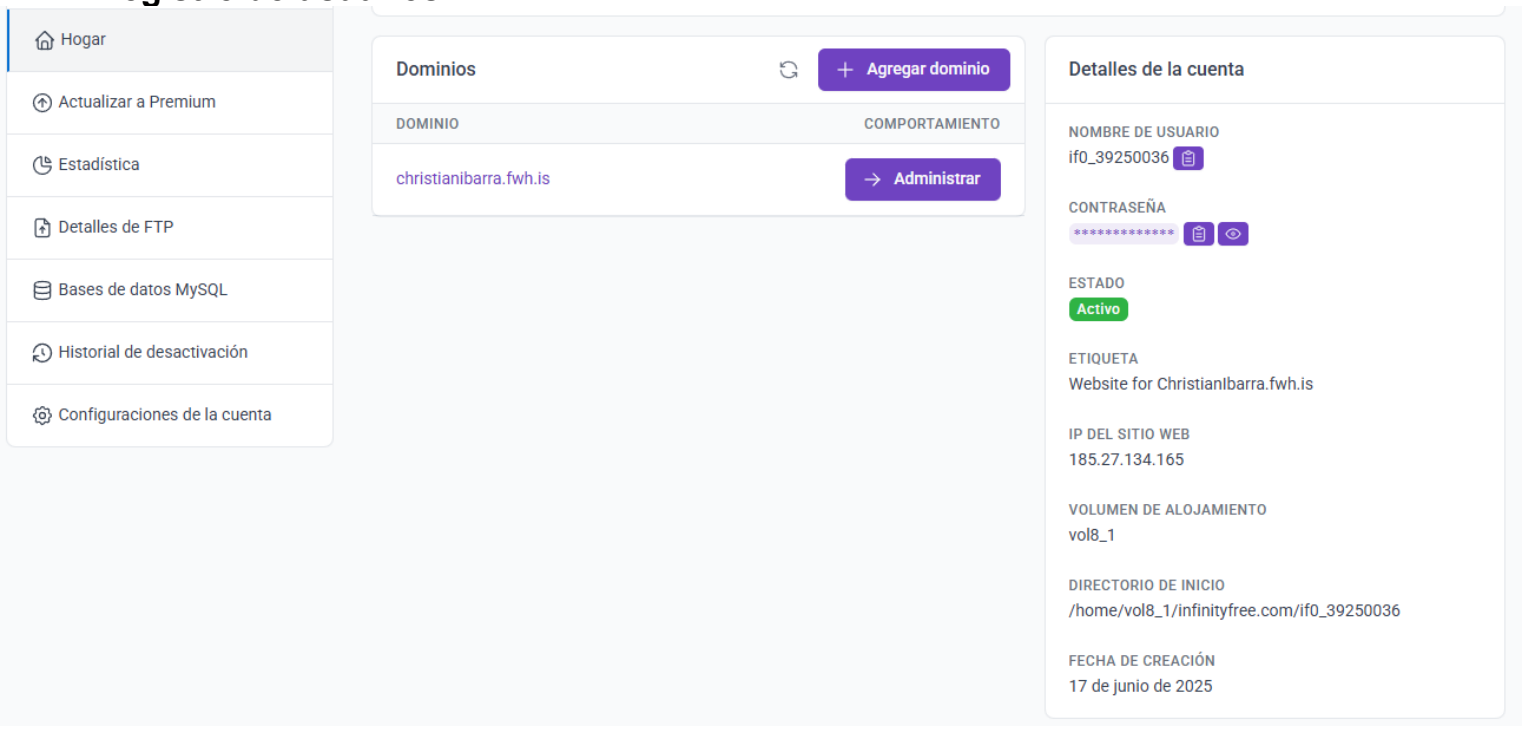
Descripción del sitio web

En mi proyecto se enfocó en la página web https://www.infinityfree.com/
Que contiene inicio de sección, registro de usuarios y conexión de base de datos.

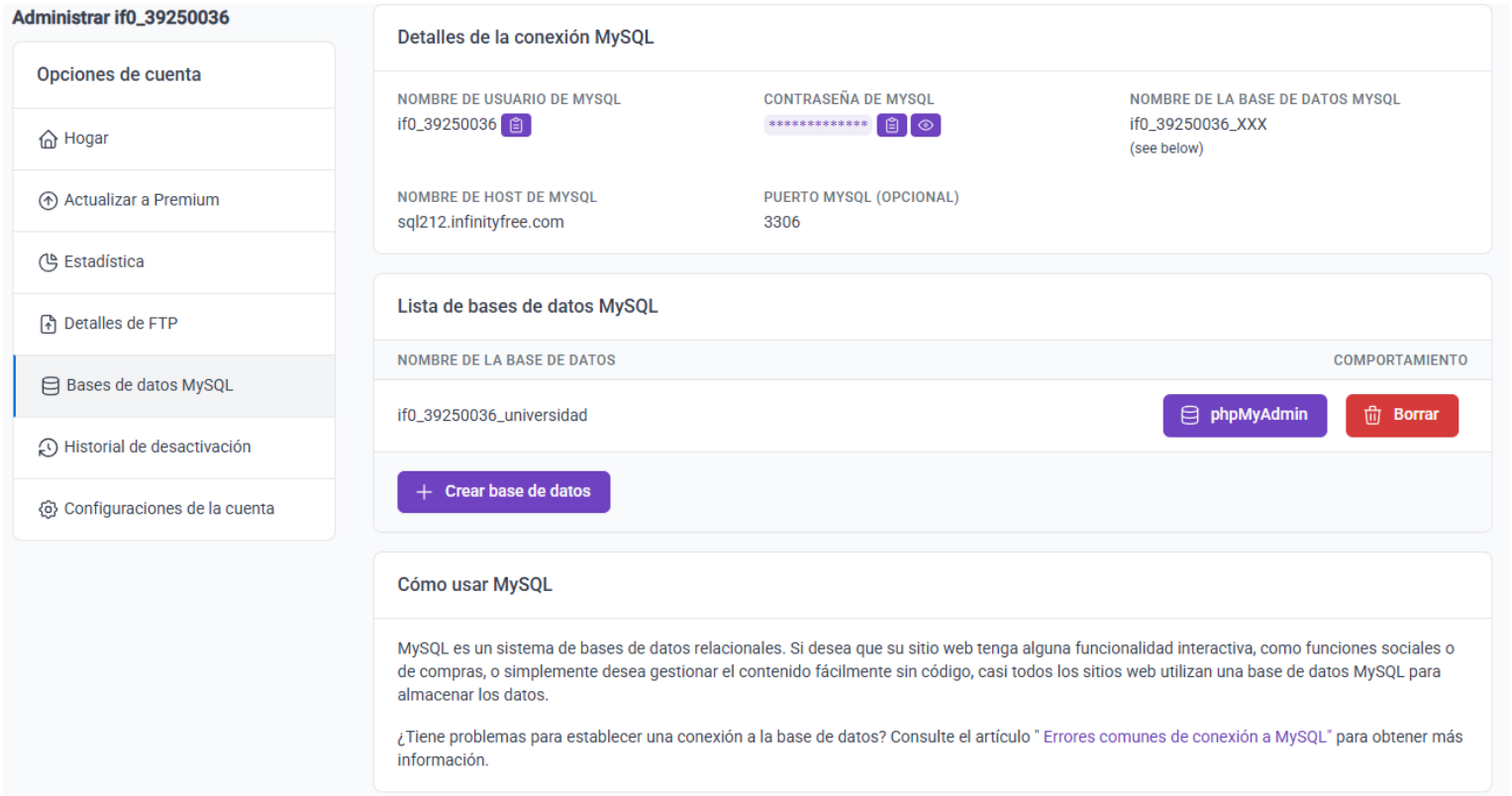
- **Inicio de sección**



- **Registro de usuarios**

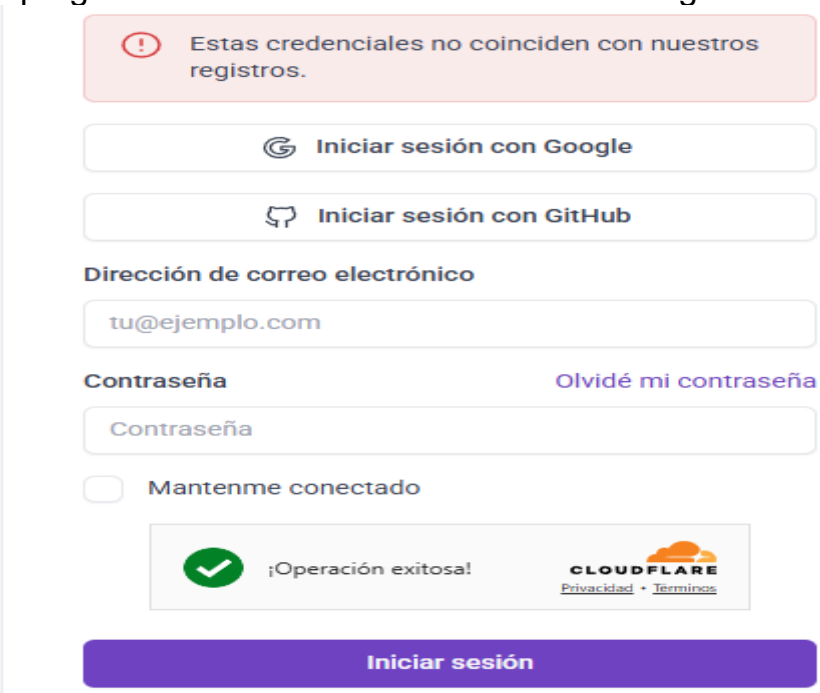


- **Conexión de base de datos**



Con las capturas tomadas fue la página web que a su vez realizamos con el Wireshark.

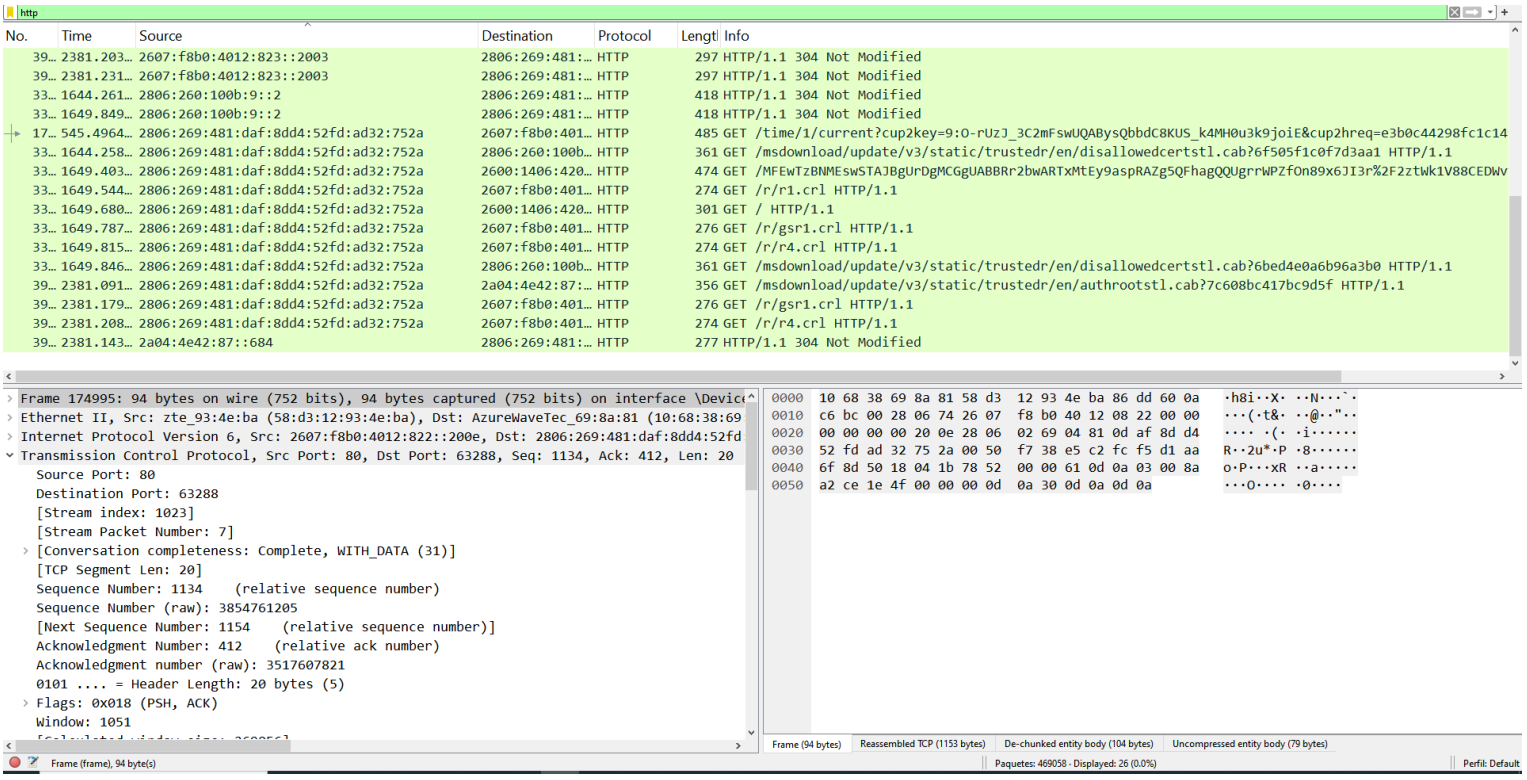
Una vez ejecutado el programa Wireshark estará tomando los registros tanto erróneos y correctos.



Aquí la sección errónea para ver los registros en la aplicación de Wireshark

Aquí en la siguiente captura mostrando la cuenta fue correctamente abierta.

Ataque al sitio



Aquí se nos brinda la información del ataque del sitio que estamos navegando en para inicio de sección, el detalle que en mi equipo al parecer tiene una protección por parte de Microsoft y no pude continuar con la muestra de mi usuario y contraseña.
Se tomo de referencias otro tutorial para sacar la información que se necesitaba en esta actividad. Sin embargo, no logre recabarla.

```
GET /r/gsr1.crl HTTP/1.1
Cache-Control: max-age = 3000
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Mon, 07 Apr 2025 13:58:00 GMT
User-Agent: Microsoft-CryptoAPI/10.0
Host: c.pki.goog

HTTP/1.1 304 Not Modified
Date: Wed, 18 Jun 2025 01:49:36 GMT
Expires: Wed, 18 Jun 2025 02:39:36 GMT
Age: 2532
Last-Modified: Mon, 07 Apr 2025 13:58:00 GMT
Cache-Control: public, max-age=3000
Vary: Accept-Encoding

GET /r/r4.crl HTTP/1.1
Cache-Control: max-age = 3000
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Thu, 03 Apr 2025 14:18:00 GMT
User-Agent: Microsoft-CryptoAPI/10.0
Host: c.pki.goog

HTTP/1.1 304 Not Modified
Date: Wed, 18 Jun 2025 01:49:30 GMT
Expires: Wed, 18 Jun 2025 02:39:30 GMT
Age: 2538
Last-Modified: Thu, 03 Apr 2025 14:18:00 GMT
Cache-Control: public, max-age=3000
Vary: Accept-Encoding
```

Esto fue lo unico que me arrojaba al darle Seguir y HTTP Stream.

Conclucion

La actividad desarrollada demuestra cómo una mala gestión de sesiones y la falta de autenticación segura en un sitio web puede generar graves riesgos para la información personal de los usuarios. Al utilizar herramientas como WireShark, es posible evidenciar de manera clara cómo viajan las credenciales en texto plano cuando el sitio no cuenta con cifrado SSL, lo que facilita ataques como la interceptación de datos (sniffing). Este ejercicio permite reforzar la importancia de integrar medidas de seguridad como el protocolo HTTPS, cifrado de contraseñas y validación adecuada de sesiones. En el ámbito profesional, esta experiencia es vital para quienes se dedican al desarrollo web, ya que proporciona conocimientos prácticos para prevenir vulnerabilidades comunes. En la vida cotidiana, también fomenta una mayor conciencia sobre los riesgos de ingresar datos personales en sitios sin candado de seguridad. En conclusión, esta práctica fortalece las competencias necesarias para construir entornos digitales más confiables y seguros, tanto desde el rol del desarrollador como del usuario final.

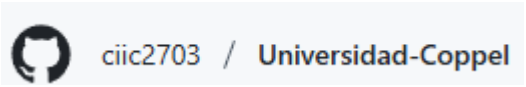
Referencias

Tutorías

https://academiaglobal-mx.zoom.us/rec/play/FKMIe7UfjID47eKtTOgRqZV_51dEC0QNi8USLT_fRJHwldOouheXze5gYTSa-0gmWkm-Vb_XdGiqqxME.m_so2h_HVHPrImno?eagerLoadZvaPages=sidemenu.billing.plan_management&accessLevel=meeting&canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-

mx.zoom.us%2Frec%2Fshare%2FZ9p2J75W9LCIYrEIRh6YkWKWw0OPfyk__iPJHOmqU8VOlLHbyZQdehbqeemfUYUu.SqMmJwm-s5KUR99P

https://www.youtube.com/watch?v=GUW1IwWivhc



https://github.com/ciic2703/Universidad-Coppel/tree/main/Auditor%C3%ADa%20Inform%C3%A1tica