

Actividad | 1 | Pérdida de Autenticación y Gestión de Sesiones

Auditoría Informática

Ingeniería en Desarrollo de Software



TUTOR: Jessica Hernández Romero

ALUMNO: Christian Ivan Ibarra Corrales

FECHA: 17 de junio de 2025

Portada.....	1
Índice.....	2
Introducción	3
Descripción	3
Justificación	3
Descripción del sitio web	4
Ataque al sitio.....	6
Conclusion	7
Referencias	7

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.

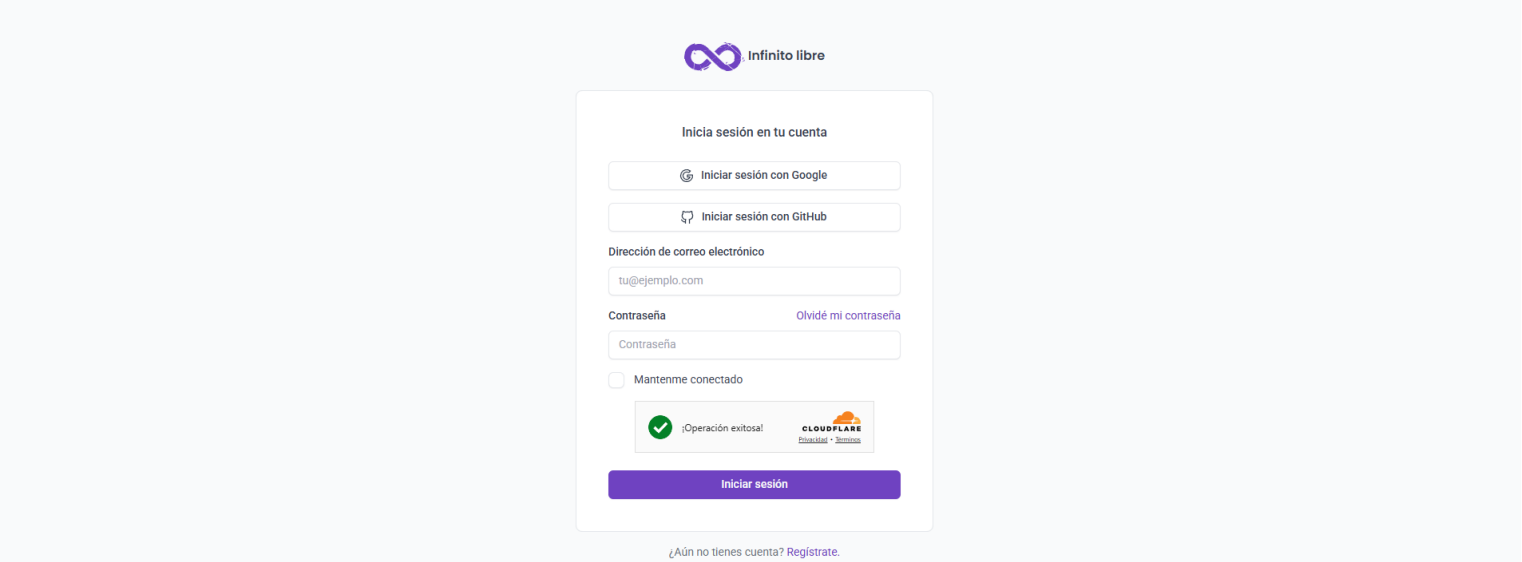
Justificación

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.

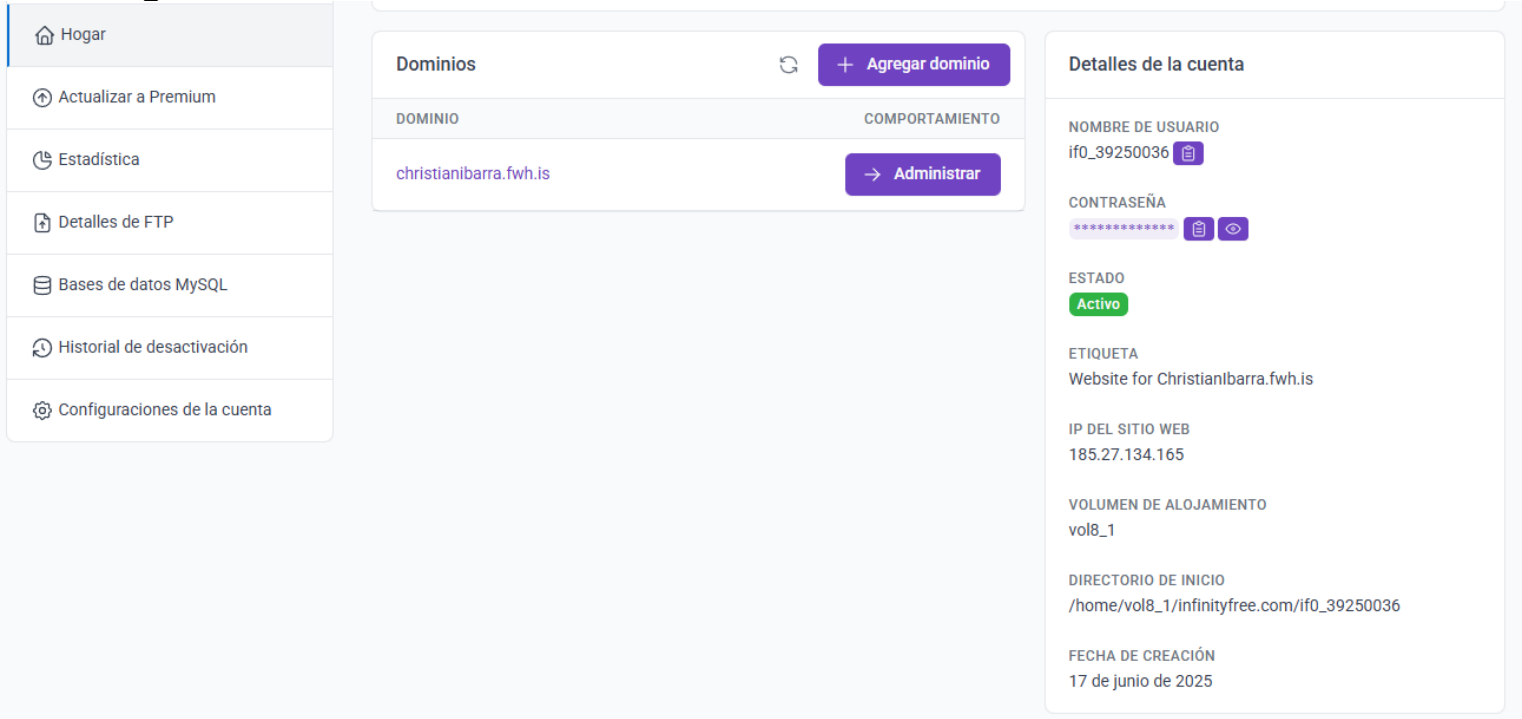
Descripción del sitio web

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**

Administrar if0_39250036

Opciones de cuenta

Hogar

Actualizar a Premium

Estadística

Detalles de FTP

Bases de datos MySQL

Historial de desactivación

Configuraciones de la cuenta

Detalles de la conexión MySQL

NOMBRE DE USUARIO DE MYSQL

if0_39250036

CONTRASEÑA DE MYSQL

NOMBRE DE LA BASE DE DATOS MYSQL

if0_39250036_XXX
(see below)

NOMBRE DE HOST DE MYSQL

sql212.infinityfree.com

PUERTO MYSQL (OPCIONAL)

3306

Lista de bases de datos MySQL

NOMBRE DE LA BASE DE DATOS	COMPORTAMIENTO
if0_39250036_universidad	<div>phpMyAdmin</div> <div>Borrar</div>

+ Crear base de datos

Cómo usar MySQL

MySQL es un sistema de bases de datos relacionales. Si desea que su sitio web tenga alguna funcionalidad interactiva, como funciones sociales o de compras, o simplemente desea gestionar el contenido fácilmente sin código, casi todos los sitios web utilizan una base de datos MySQL para almacenar los datos.

¿Tiene problemas para establecer una conexión a la base de datos? Consulte el artículo "[Errores comunes de conexión a MySQL](#)" para obtener más información.

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.

! Estas credenciales no coinciden con nuestros registros.

Iniciar sesión con Google

Iniciar sesión con GitHub

Dirección de correo electrónico

tu@ejemplo.com

Contraseña [Olvidé mi contraseña](#)

Contraseña

☐ Manténme conectado

✓ ¡Operación exitosa!

CLOUDFLARE
[Privacidad](#) • [Términos](#)

Iniciar sesión

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

Cuentas

Cuentas de alojamiento

Sus cuentas

+ Crear una cuenta

ifo_39250036
Sitio web de Christianbarra.fwh.is

Cuentas activas: 1 / 3

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

Ataque al sitio

The image shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows a sequence of packets, with the selected packet being a GET request to a Microsoft website. The packet details on the right show the structure of the HTTP request, including the method (GET), the URL, and the headers. The packet bytes on the right show the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
39...	2381.203...	2607:f8b0:4012:823::2003	2806:269:481:...	HTTP	297	HTTP/1.1 304 Not Modified
39...	2381.231...	2607:f8b0:4012:823::2003	2806:269:481:...	HTTP	297	HTTP/1.1 304 Not Modified
33...	1644.261...	2806:260:100b:9::2	2806:269:481:...	HTTP	418	HTTP/1.1 304 Not Modified
33...	1649.849...	2806:260:100b:9::2	2806:269:481:...	HTTP	418	HTTP/1.1 304 Not Modified
17...	545.4964...	2806:269:481:daf:8dd4:52fd:ad32:752a	2607:f8b0:401... HTTP	485	GET /time/1/current?cup2key=9:0-rUZJ_3C2mFswUQABysQbbdC8KUS_4MH0u3k9joiE&cup2hreq=e3b0c44298fc1c14	
33...	1644.258...	2806:269:481:daf:8dd4:52fd:ad32:752a	2806:260:100b... HTTP	361	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?6f505f1c0f7d3aa1 HTTP/1.1	
33...	1649.403...	2806:269:481:daf:8dd4:52fd:ad32:752a	2600:1406:420... HTTP	474	GET /MFewTzBNMESwSTA3BgUrDgMCGGUABBRr2bwARTxMtEy9aspRAZg5QFhagQQUgrwPZf0n89x6J13r%2F2ztwk1V88CEDWv	
33...	1649.544...	2806:269:481:daf:8dd4:52fd:ad32:752a	2607:f8b0:401... HTTP	274	GET /r/r1.cr1 HTTP/1.1	
33...	1649.680...	2806:269:481:daf:8dd4:52fd:ad32:752a	2600:1406:420... HTTP	301	GET / HTTP/1.1	
33...	1649.787...	2806:269:481:daf:8dd4:52fd:ad32:752a	2607:f8b0:401... HTTP	276	GET /r/gsr1.cr1 HTTP/1.1	
33...	1649.815...	2806:269:481:daf:8dd4:52fd:ad32:752a	2607:f8b0:401... HTTP	274	GET /r/r4.cr1 HTTP/1.1	
33...	1649.846...	2806:269:481:daf:8dd4:52fd:ad32:752a	2806:260:100b... HTTP	361	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?6bed4e0a6b96a3b0 HTTP/1.1	
39...	2381.091...	2806:269:481:daf:8dd4:52fd:ad32:752a	2a04:4e42:87:... HTTP	356	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?7c608bc417bc9d5f HTTP/1.1	
39...	2381.179...	2806:269:481:daf:8dd4:52fd:ad32:752a	2607:f8b0:401... HTTP	276	GET /r/gsr1.cr1 HTTP/1.1	
39...	2381.208...	2806:269:481:daf:8dd4:52fd:ad32:752a	2607:f8b0:401... HTTP	274	GET /r/r4.cr1 HTTP/1.1	
39...	2381.143...	2a04:4e42:87::684	2806:269:481:...	HTTP	277	HTTP/1.1 304 Not Modified

Frame 174995: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF...
 Ethernet II, Src: zte_93:4e:ba (58:d3:12:93:4e:ba), Dst: AzureWaveTec_69:8a:81 (10:68:38:69:8a:81)
 Internet Protocol Version 6, Src: 2607:f8b0:4012:822::200e, Dst: 2806:269:481:daf:8dd4:52fd:ad32:752a
 Transmission Control Protocol, Src Port: 80, Dst Port: 63288, Seq: 1134, Ack: 412, Len: 20
 Source Port: 80
 Destination Port: 63288
 [Stream index: 1023]
 [Stream Packet Number: 7]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 20]
 Sequence Number: 1134 (relative sequence number)
 Sequence Number (raw): 3854761205
 [Next Sequence Number: 1154 (relative sequence number)]
 Acknowledgment Number: 412 (relative ack number)
 Acknowledgment number (raw): 3517607821
 0101 = Header Length: 20 bytes (5)
 Flags: 0x018 (PSH, ACK)
 Window: 1051
 [Ethernet II, Src: zte_93:4e:ba (58:d3:12:93:4e:ba), Dst: AzureWaveTec_69:8a:81 (10:68:38:69:8a:81)]

Frame (94 bytes) Reassembled TCP (1153 bytes) De-chunked entity body (104 bytes) Uncompressed entity body (79 bytes)
 Paquetes: 469058 - Displayed: 26 (0.0%) Perfil: Default

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.

Conclusion

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/FKMle7UfjID47eKtTOgRqZV_51dEC0QNi8USLT_fRJHwldOouheXze5gYTSa-0gmWkm-Vb_XdGiqqxME.m_so2h_HVHPrlmno?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_iPJH0mqU8VOILHbyZQdehbqeemfUYUu.SqMmJwm-s5KUR99P



<https://www.youtube.com/watch?v=GUW1lwWivhc>



ciic2703 / Universidad-Coppel

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