Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias de la Computación

TESIS

# IDENTIFICACIÓN DE RIESGOS EN LA WEB: EVALUACIÓN DE VULNERABILIDADES PARA LA PROTECCIÓN DE DATOS

que para obtener el grado de:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

presenta:

Emmanuel Marquez Cortez


Asesores

M.C. Ana Claudia Zenteno Vázquez

Dr. Gustavo Trinidad Rubín Linares

Noviembre 2024

# Agradecimientos

Quiero expresar mi agradecimiento a mis padres por haberme brindado la oportunidad de estudiar con la tranquilidad de saber que cuento con su respaldo y a mi pareja que ha supuesto un apoyo siempre que lo he necesitado.

# Resumen

Este proyecto de tesis analiza las vulnerabilidades en las páginas web, se usan tres aplicaciones para auditoría: 1) Rencon-ng que es una herramienta de prueba de penetración que se usa para recopilar información sobre los objetivos, 2) Social-Engineer toolkit que es una herramienta de prueba de penetración que se usa para hacer ataques de ingeniería social, y 3) Zap Proxy que es una herramienta de prueba de seguridad que se usa para evaluar la seguridad de las aplicaciones web. Se realiza un testeo de cómo funcionan y cómo identifican ataques hacia una página web y como la otra realiza una prueba análisis de seguridad a la página web para saber si es segura o si existe alguna vulnerabilidad en ella. Brindando un reporte completo de vulnerabilidades expuestas.

La seguridad web es muy importante ya que las organizaciones o empresas tiene sus páginas web en internet y son muy vulnerables a ataques y amenazas ya que ponen en riesgo su información. Por lo que la organización o empresa debe de considerar por medio de su metodología el implementar la seguridad en sus aplicaciones o páginas web, ya que son susceptibles a perder información sensible como datos de sus clientes, indisponibilidad de sus sistemas, si esto sucede se puede ver afecta la empresa u organización en su reputación, productividad y finanza por la pérdida de negocios o multas de entes reguladores .

Lo más importante dentro de las páginas web es proteger la información y los datos que se almacenan en ella y esto se puede hacer mediante la seguridad de la información que tiene como objetivo mantener el conocimiento, datos y significados libres de eventos indeseables como el robo, espionaje amenazas u otros peligros y también nos permite anticipar acciones y evitar eventos no deseados que puedan vulnerar las páginas o aplicaciones de la organización o empresa por lo que es recomendable tener una buena seguridad web.

# Contenido

# Capítulo 1

# Introducción a la Seguridad Web y Protección de Datos

En la actualidad, casi todo puede gestionarse a través de sitios o aplicaciones web, móviles o de escritorio, lo que ha dado lugar a un incremento en las actividades de ciberdelincuencia. Los atacantes se enfocan en identificar vulnerabilidades en estos sistemas y, una vez que las encuentran, no dudan en explotarlas para atacar, infectar o dañar el sistema. Esto puede incluir el robo de información, la interrupción parcial de los servicios o tener el control total del sistema, con la intención de exigir un rescate para liberarlo. Para que una empresa prevenga este tipo de vulnerabilidades, existen diversas metodologías de ciberseguridad que permiten analizar, detectar, solucionar y mitigar las debilidades presentes en sus sistemas o aplicaciones.

## 1.1 Conceptos Básicos de Ciberseguridad

**Ciberseguridad:** ser refiere a la protección de equipos de cómputo, redes, aplicaciones, sistemas y datos de todas las amenazas digitales que existen.(Amazon Web Services, s/f)

**Amenaza Informática:** una amenaza informática es un evento que se puede presentar en cualquier momento y represente un daño material o inmaterial a los archivos informáticos y sistemas de información como lo puede ser una base de datos. (Coronel Suárez & Quirumbay Yagual, 2022)

**Vulnerabilidad:** es cualquier debilidad de un activo que pueda afectar el buen funcionamiento del sistema informático, también se les conoce como “agujeros de seguridad”, esto representa un fallo a la hora de la implementación o configuración del sistema. (Coronel Suárez & Quirumbay Yagual, 2022)

**Ataque Informático:** es la acción de aprovechar una vulnerabilidad dentro de un sistema con la finalidad de provocar un fallo, robo de información o tomar control total del sistema y pedir dinero o algún otro bien a favor del atacante.(Coronel Suárez & Quirumbay Yagual, 2022)

**Hacker:** Persona con habilidades y conocimientos sobre tecnologías de la información y comunicación, que puede manejar cualquier software, hardware, lenguaje de programación y protocolos de red.(Coronel Suárez & Quirumbay Yagual, 2022)

**Malware:** es código diseñado para infectar, dañar o acceder a los sistemas informáticos, existen diferentes tipos de malware y estos afectan de forma distinta, pero todas las variantes comparten un mismo objetivo que es poner en peligro la seguridad y privacidad del sistema informático (Belcic, 2023).

**Deserialización:** consiste en tomar una representación de datos (como un archivo, una cadena de texto o un flujo de bytes) y convertirla nuevamente en un objeto que puede ser utilizado por un programa.

## 1.2 Metodologías en ciberseguridad

Existen diferentes metodologías que las empresas pueden utilizar para mejorar la protección de sus sistemas y datos, las siguientes metodologías son las más comunes y las más usadas por empresas:

**ISO 27001**: Esta es una norma internacional que nos da un modelo para realizar la creación, implementación, supervisión, operación, revisión, mejora y mantenimiento de lo que es el Sistema de Gestión de Seguridad de la información (SGSI).

De acuerdo con el apartado 0.3 Compatibilidad de otros sistemas de gestión, este ISO sigue pautas que están marcadas en las normas ISO 9001:2000 e ISO 14001:2004 esto nos asegura que la implementación está bien integrada y es consistente. Además de que está diseñada para que una organización pueda adaptar su SGSI a los requisitos de los sistemas de gestión.(Mesquida et al., 2010)

También la norma ISO/IEC 27001 cubre el siguiente requisito en su apartado 4.3.1.g: “Los procedimientos documentados que necesita la organización para asegurar una correcta planificación, operación y control de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles”. (Mesquida et al., 2010)

Con esto podemos observar que la metodología ISO 27001 es una de las más importantes ya que nos ayuda con la parte de técnica de todos los requisitos que necesitamos en cuanto a seguridad. (Mesquida et al., 2010)

**NIST Cybersecurity Framework**: fue desarrollado por el Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos, nos proporciona un marco para que las organizaciones tengan una estructura para gestionar y mejorar la ciberseguridad basada en mejores prácticas.

NIST nos dice que las amenazas de seguridad cibernética explotan la mayor complejidad y conectividad de los sistemas de infraestructura crítica y esto pone en riesgo la seguridad de la nación, su economía, salud y seguridad pública. El riesgo de la seguridad cibernética puede afectar el final de una empresa, afectando los ingresos y aumentando costos, también afecta la capacidad de innovar, aumentar o mantener sus clientes. (The NIST Cybersecurity Framework (CSF) 2.0, 2024)

El marco que nos ofrece esta metodología es un enfoqué para la reducción del riesgo vinculado a amenazas cibernéticas que puedan comprometer lo que es la seguridad de la información y se compone de tres niveles:

- Núcleo del marco: es el conjunto de actividades de seguridad cibernética, resultados deseados y referencias, este nos presenta los estándares, directrices y prácticas de la industria que permite la comunicación de todas las actividades y resultados en toda la organización, consta de cinco Funciones simultáneas y continuas: Identificar, Proteger, Detectar, Responder y Recuperar.
- Los Niveles de Implementación del Marco: es el contexto que la organización tiene o considera para el riesgo de la seguridad cibernética y los procesos establecidos para gestionar estos riesgos. Estos niveles se encargan de describir el grado en que las prácticas de gestión de riesgos de seguridad cibernética de la organización también caracterizan las prácticas de una organización desde Parcial (Nivel 1) hasta Adaptable (Nivel 4).
- Perfil del Marco: Son los resultados que se basan en las necesidades de la empresa que la organización selecciono de las categorías y subcategorías

del marco. Generalmente el perfil se usa para identificar las oportunidades de mejora de seguridad cibernética y compara un Perfil “actual” con un Perfil “objetivo”, también realizar autoevaluaciones y comunicaciones dentro de la organización. (The NIST Cybersecurity Framework (CSF) 2.0, 2024)

**COBIT (Control Objectives for Information and Related Technologies):** COBIT es una solución integral para la gobernanza efectiva de la información y la tecnología, centrándose en la innovación y la transformación empresarial. Ofrece más recursos para la implementación, orientación práctica y oportunidades de capacitación. La implementación es más flexible, lo que permite un mejor retorno de la inversión. COBIT 2019 está diseñado para trabajar con otros, brindando orientación para integrar estándares, directivas, regulaciones y mejores prácticas de la industria. También proporciona una colección de artículos de noticias de la industria, consejos prácticos e intercambio de conocimientos de expertos en seguridad, riesgos, gobernanza, privacidad y auditoría. La plataforma también proporciona una plataforma para que las empresas compartan sus conocimientos y experiencias, promoviendo la colaboración y la innovación. COBIT 2019 es una herramienta valiosa para las empresas que buscan mejorar sus estrategias de gobernanza. COBIT nos ofrece las siguientes características que nos definen porque es que la mayoría de las empresas la usan y estas son:

- **Gobernanza efectiva**: con la gobernanza eficaz de la información y tecnología es de suma importancia ya que es importante para tener éxito empresarial, COBIT es un impulsor de la innovación y transformación de la empresa.
- **Recursos de implementación**: nos ofrece más recursos de implementación, orientación practica e ideas y oportunidad integrales de capacitación. Ahora se puede ajustar el tamaño de la solución de gobierno con la implementación que nos ofrece COBIT y para poder obtener un máximo retorno de la inversión de su solución COBIT nos da la implementación para lograr lo anterior.

- **Fácil Integración**: esta es una de las razones por la que COBIT funciona bien con los demás, ya que gracias a su diseño se le proporciona una orientación para ayudarle a integrar estándares, directrices, regulaciones y mejores prácticas de la industria y estos serás exclusivos de su empresa en solución de gobierno usando COBIT.
- **Estudios de caso:** el estudio de casos de COBIT es muy importante ya que nos ayuda a demostrar los beneficios, las aplicaciones comunes y los usos de COBIT.

**MITRE ATT&CK**: Este marco nos proporciona a detalle cada una de las tácticas y técnicas de los atacantes en tres diferentes áreas que son empresa, móvil y ICS (Sistema de Control Industrial), además nos da una matriz de las diferentes áreas para las siguientes plataformas (MITRE ATT&CK®, s/f):

- Windows
- macOS
- Linux
- PRE
- Azure AD
- Office 365
- Google Workspace
- SaaS
- IaaS
- Red
- Contenedores

Dentro de las matrices existen 14 áreas con su respectivo número de técnicas que son:

- Reconocimiento (10 técnicas)
- Desarrollo de recursos (8 técnicas)
- Acceso inicial (10 técnicas)
- Ejecución (14 técnicas)
- Persistencia (20 técnicas)

- Escalada de privilegios (14 técnicas)
- Evasión de defensas (43 técnicas)
- Acceso a credenciales (17 técnicas)
- Descubrimiento (32 técnicas)
- Movimiento lateral (9 técnicas)
- Recopilación (17 técnicas)
- Comando y control (18 técnicas)
- Exfiltración (9 técnicas)
- Impacto (14 técnicas)

Nos ofrece defensas y dentro de estas tiene una fuente de datos que contiene diversos temas de información que pueden recopilar los sensores / registros. Incluyen componentes de datos para identificar propiedades/valores específicos con el objetivo de detectar una técnica de ATT&CK determinada y contiene 41 datos en su fuente.(MITRE ATT&CK®, s/f)

También dentro de las defensas tiene un apartado de mitigaciones estas representan conceptos de seguridad y clases de tecnologías para evitar que una técnica se ejecute con éxito y existen tres tipos de mitigaciones que son:

- Mitigación empresarial: contiene 43 conceptos
- Mitigaciones móviles: contiene 13 conceptos
- Mitigación ICS: contiene 52 conceptos

**Penetration Testing Execution Standard (PTES):** Esta metodología proporciona un enfoque estandarizado para llevar a cabo pruebas de penetración de manera efectiva, identificando vulnerabilidades en los sistemas y redes de una organización. (Free Software Foundation, 2014)

Es una metodología que ofrece un enfoque estandarizado para llevar a cabo pruebas de penetración y esta consta de siete secciones principales, que va desde la comunicación inicial hasta el razonamiento detrás de las pruebas de penetración.(Free Software Foundation, 2014)

Sus pruebas consisten en recopilación de inteligencia y modelar las amenazas y estas pruebas pasan por los evaluadores que son los encargados de dar una mejor comprensión por medio de la investigación de vulnerabilidades, explotación y post-explotación y después de que estos evaluadores dan su veredicto final se realiza en la presentación de informes que es donde se captura todo el proceso para que el cliente pueda entender, comprender los resultados. (Free Software Foundation, 2014)

Las siguientes son las siete principales secciones definidas como estándar son:

- Interacciones previas al compromiso
- Recoger información
- Modelado de amenazas
- Análisis de vulnerabilidad
- Explotación
- Post-explotación
- Informes

**OSSTMM (Open Source Security Testing Methodology Manual):** Este es un estándar de pruebas de seguridad que describe las técnicas y enfoques para evaluar y mejorar la seguridad de la información. (Herzog Pete, 2010)

Rrata sobre la Seguridad Operativa (OpSec) y se trata de medir que tan bien funciona la seguridad, aunque todo esto puede parecer sencillo y obvio, debemos hacer esta distinción ya que la mayoría de los objetivos de cumplimiento solo requieren hacer coincidir los procesos y las configuraciones con un conjunto de mejores prácticas. OpSec nos dice que para que una amenaza sea efectiva esta debe de interactuar directa o indirectamente con el activo. (Herzog Pete, 2010)

Pero si queremos tener una verdadera seguridad de los activos debemos tener distintos tipos de controles, pero sin excedernos en cuanto a controles ya que si nos excedemos en estos podría resultar contraproducente porque si tenemos mas no significa que tendremos mayor seguridad, es por eso que se recomienda usar distintos tipos de controles operativos en lugar de solo agregar más controles y

también es importante categorizarlos por lo que hacen en operaciones y de así es como podemos estar seguros del nivel de protección que tenemos. (Herzog Pete, 2010)

Se puede utilizar OpSec en un entorno operativo reduciéndolo a sus elementos. Este manual contiene todo lo necesario para realizar pruebas de seguridad, además de que contiene sus limitaciones y todas las especificaciones necesarias para poder realizar pruebas y tener más claro las debilidades de una aplicación web o página web. (Herzog Pete, 2010)

Para asegurar aplicaciones web contra amenazas cibernéticas, existen varias metodologías y enfoques que se pueden seguir. A continuación, se presentan las metodologías más comunes (a octubre de 2024) de ciberseguridad para aplicaciones web:

**OWASP Top 10:** La Open Web Application Security Project (OWASP) publica una lista de las 10 vulnerabilidades de seguridad más críticas que afectan a las aplicaciones web.

Esta lista nos da la descripción de cada una de las 10 vulnerabilidades, cuando entramos a una vulnerabilidad que sea de nuestro interés nos da en porcentaje los factores, un resumen de esta vulnerabilidad y las *Common Weakness Enumerations* donde nos da las más importantes de la vulnerabilidad en específico, después nos muestra una descripción detallada y después nos dice como podemos prevenir estas vulnerabilidades. Además de que nos da ejemplos de escenarios de ataque es decir nos da una idea de que maneras pueden atacar con esa vulnerabilidad y podremos ver de una forma más rápida la vulnerabilidad dentro de nuestra página web.

**Secure SDLC (Secure Software Development Lifecycle):** Este enfoque integra la seguridad en todas las etapas del ciclo de vida de desarrollo de software, desde el diseño hasta la implementación y el mantenimiento.

**Pruebas de Penetración**: Realizar pruebas de penetración en aplicaciones web para identificar y corregir vulnerabilidades antes de que puedan ser explotadas por atacantes.

**Seguridad por Diseño (Security by Design):** Incorporar consideraciones de seguridad desde la fase inicial de diseño de la aplicación web para minimizar las vulnerabilidades.

**Firewalls de Aplicaciones Web (WAF):** Utilizar firewalls específicamente diseñados para proteger aplicaciones web contra ataques comunes, como inyecciones SQL y XSS (Cross-Site Scripting).

**Gestión de Identidad y Acceso (IAM):** Implementar medidas de autenticación y autorización sólidas para controlar quién tiene acceso a la aplicación y a qué recursos.

**Monitorización y Registro (Logging):** Establecer sistemas de monitoreo para detectar y responder a ataques o comportamientos sospechosos.

## 1.3 Vulnerabilidades en los últimos 5 años

En OWASP se encarga de recopilar los ataques cada cuatro años, como se van moviendo durante esos años y las nuevas amenazas que van surgiendo y como se van moviendo estas durante el ranking.

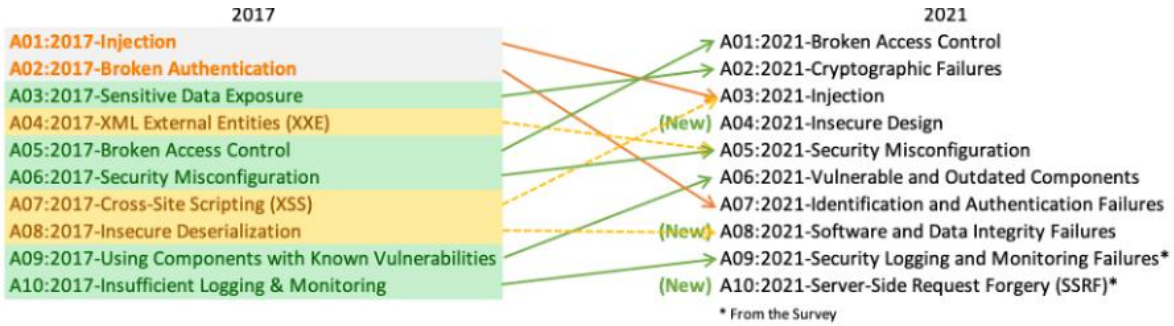


*Ilustración 1.- Top 10: Lista 2021*

Como podemos observar en el 2017 las amenazas se van moviendo durante los años esto es porque al realizar pruebas de ciberseguridad usando las metodologías

que antes se mencionaron provoca que las empresas vayan mejorando su seguridad dentro de sus aplicaciones o sitios web.
A continuación, se explicarán cada una de estas amenazas y como es que se fueron moviendo durante los últimos cuatro años.

- **01 Broken Access Control**: en el año de 2017 ocupaba el quinto lugar de la lista, pero en 2021 escalo al primer lugar ya que se probaron en 94% de las aplicaciones para detectar algún tipo de Broken Access Control y tienen una tasa de incidencia promedio del 3,81% y en cuanto a datos contribuidos es donde está la mayor cantidad de ocurrencias con más de 318K. El control de acceso es la política que restringe al usuario a actuar fuera de los permisos previstos. Sus vulnerabilidades más comunes son:
    - La violación del principio de privilegio mínimo o denegación por defecto que cuando se le otorgan las capacidades
    - Roles o usuarios particulares dentro del sitio web y está disponible para cualquiera
    - Eludir comprobaciones de control de acceso modificando la URL, el estado interno de la aplicación o sitio HTML o usando una herramienta de ataque que pueda modificar una solicitud API.
    - Permitir ver o editar la cuenta de otra persona esto pasa proporcionando su ID.
    - Acceder a la API y no tenga todos los controles de acceso para PUT, POST y DELETE.
    - Elevación de privilegios significa ingresar como usuario sin iniciar sesión o como administrador cuando inicia sesión como usuario normal.
    - La manipulación de metadatos consiste en cómo alterar un token de control de acceso JSON Web Token (JWT), una cookie o un campo oculto y de estar forma poder elevar privilegios.
    - Configurar de manera incorrecta o dar acceso a la API desde orígenes no autorizados o confiables.

- Forzar la navegación a paginas auténticas como un usuario no autenticado o paginas privilegiadas como usuario estándar.

- **02 Cryptographic Failures**: en 2017 se encontraba en la tercera posición y se conocía como Sensitive Data Exposure y en 2021 se posicionó en el segundo lugar Es un síntoma más que una causa raíz y se centra en las fallas relacionadas con la criptografía o en su ausencia y esto produce la exposición de datos confidenciales. Sus debilidades comunes notables son:
  - Uso de contraseña codificada
  - Algoritmo criptográfico roto o riesgo
  - Entropía insuficiente

  En este se deben de determinar las necesidades de protección de datos en el tránsito y reposo como contraseñas, números de tarjetas de crédito, registros médicos, información personal, secretos comerciales que requieren una protección adicional ya que están sujetos a leyes de privacidad como el Reglamento General de Protección de Datos (DGPR) o regulaciones, protección de datos financieros.

- **03 Injection:** en el año 2017 se encontraba en primer lugar, pero en el año 2021 se deslizo hasta la tercera posición en donde el 94% de las aplicaciones fueron probadas para un tipo de inyección y tuvieron una tasa de incidencia máxima del 19%, un promedio de incidencia del 3% y 274.000 ocurrencias. Esto nos da las siguientes CWE que son:
  - CWE-79: Secuencia de comandos en sitios cruzados (XSS).
  - CWE-89: Inyección SQL.
  - CWE-73: Control Externo de Nombre de archivos o ruta.

  Todas las aplicaciones están vulnerables ante un ataque de inyección, pero ante estos tipos son más:

  - Los datos que da el usuario no se validan, filtran ni se sanitizan por parte de la aplicación
  - Invocación de consultas dinaminas o que no se parametrizan, sin codificación de parámetros de forma acorde al texto.

- Se usan datos dañinos dentro de los parámetros de búsqueda en consultas Object-Relational Mapping (ORM), sirve para extraer registros adicionales sensibles.
- Se utilizan datos dañinos directamente o concatenan, de forma que el SQL o comando resultante contiene datos y estructuras con una consulta dinámicas, comandos o procedimientos almacenados.

Las inyecciones más comunes son SQL, NoSQL, comandos de sistemas operativo, Object-Relational Mapping (ORM), LDAP, expresiones de lenguaje u Object Navigation Library (OGNL). La mejor forma de detectar si una aplicación es vulnerable a inyecciones es revisar el código fuente(Felipe Bueno Carranza, 2022).

- **04 Insecure Design:** esta es una nueva categoría que apareció durante el año 2021 y se centra en los riesgos de diseño y fallas arquitectónicas y de este modo poder exhortar a los desarrolladores a utilizar el modelado de amenazas, patrones de diseño seguros y arquitecturas de referencia. Las CWE que son más notables son:
    - CWE-209: Generación de mensajes de error que contiene información confidencial.
    - CWE-256: Almacenamiento desprotegido de credenciales.
    - CWE-501: Violación de las fronteras de confianza.
    - CWE-522: Credenciales protegidas insuficientemente.

  Esta es una categoría que representa diferentes debilidades que se expresan como “Diseño de control faltante o ineficaz”, hay una diferencia entre diseño e implementación inseguros, la razón de esta diferencia es que se difiere en la causa raíz y remediaciones, ya que un diseño seguro puede tener defectos de implementación y eso nos conduce a vulnerabilidades que un hacker puede explotar. Un diseño inseguro no contiene los controles de seguridad necesarios porque nunca se crearon para defenderse de ataques específicos por lo que no se puede arreglar con una implementación perfecta. Un factor que influye en este tipo de diseños inseguros son la falta de perfiles de riesgo

empresarial inherentes al software os sistema y la falta de determinación del nivel de diseño de seguridad requerido.

- Gestión de requerimientos y recursos: se recopilan y analizan los requisitos de la aplicación basados en el negocio a desarrollar para validar la integridad, disponibilidad y autenticidad de los datos y la lógica del proceso. Además de considerar la funcionalidad y la seguridad a implementar.

- Diseño seguro: se evalúan las amenazas y garantiza que el código este diseñado y probado de una forma sólida. Para poder determinar el flujo correcto y estados de falla se usan las historias de usuario, en este apartado se debe de ser preciso y asegurarnos de que las suposiciones y condiciones para el flujo esperado y de falla sean precisos y deseables. Estos resultados se deben de reflejar en las historias de usuario(OWASP, 2023a).

- Ciclo de Desarrollo Seguro (S-SDLC): dentro del software seguro debemos tener un ciclo de desarrollo seguro, es decir, una forma de patrón de diseño seguro, metodología paved road, bibliotecas de componentes seguros, herramientas y modelado de amenazas. Se puede considerar el Modelo de Madurez para el Aseguramiento del Software (SAMM) que nos ayuda a la estructuración de los refuerzos de desarrollo de software seguro.

- **05 Security Misconfiguration:** en el año de 2017 se encontraba en la sexta posición y en el año 2021 subió un solo lugar, es decir, se encuentra en el quinto lugar del top. Se probaron 90 % de las aplicaciones esto con la finalidad de poder detectar algún tipo de configuración incorrecta y se obtuvo una tasa de incidencia del 4.5% y más de 208.000 de ocurrencias.

Una aplicación puede ser vulnerable si le hace falta el *hardening* de seguridad adecuado en cualquier *stack* tecnológico o los permisos configurados incorrectamente en los servicios en la nube. Debe considerarse también:

- funciones innecesarias habilitadas o instaladas
- se tienen habilitadas las cuentas predeterminadas
- no están habilitas las funciones de seguridad
- no se configuraron valores seguros en las configuraciones de seguridad en los servidores de aplicaciones(OWASP, 2023a)

Esto significa que si no se tiene una configuración de seguridad de aplicaciones coordinado y repetible los sistemas corren un riego mayor de poder ser vulnerados.

- **06 Vulnerable and outdated components**: en el año de 2017 se encontraba en el noveno lugar y en el 2021 ascendió al sexto lugar, es muy complicado probar y evaluar el riesgo de los componentes vulnerables y esta es la única categoría que no tiene enumeraciones de debilidades comunes (CWE). ¿Como saber si es vulnerable?, se puede saber si no se conoce las versiones de todos los componentes que se usan, incluyendo los componentes que se usan directamente, así como dependencias anidadas, el software vulnerable, carece de soporte o no está actualizado, incluyendo el sistema operativo, servidor web/ de aplicaciones, sistema de administración de bases de datos (DBMS), aplicaciones, API y los componentes, entornos de ejecución y bibliotecas, no analizar en búsquedas de vulnerabilidades de forma regular y no estar suscrito a boletines de seguridad relacionados con los componentes que se usan, si no se repara o actualiza la plataforma subyacente, *frameworks* y dependencias de forma oportuna y que se basa en el riesgo y esto puede ocurrir en entornos en los que la aplicación de parches de seguridad es una tarea mensual o trimestral bajo el control de cambios y esto ocasiona que la organización este expuesta por días o meses y por ultimo si

es que los desarrolladores no realizan testeos de compatibilidad de las bibliotecas actualizadas o parcheadas.

- **07 Identification and Autentication:** en el año de 2017 se encontraba en la segunda posición y en el año 2021 descendió hasta la séptima posición y antes se denominaba Broken Autentication (Pérdida de Autenticación) y las CWE que se relacionan con estas fallas son las fallas de identificación y estas son:
    - CWE-297: Validación incorrecta de Certificado con discrepancia de host.
    - CWE-287: Autenticación incorrecta
    - CWE-384: Fijación de sesiones

  Para protegerse de ataques relacionados con la autenticación se valida la identidad, autenticación y gestión de sesiones de usuario. Para saber si una aplicación o sitio web es débil ante las autenticaciones podemos tomar en cuenta esto:

    - Se permiten ataques automatizados como reutilización de credenciales conocidas esto quiere decir que el atacante posee una lista de pares de usuario y contraseña válidos.
    - Se permiten ataques de fuerza bruta u otros ataques automáticos.
    - Se permite utilizar contraseñas por defecto, débiles o conocidas como “admin/admin”
    - Se tienen procesos débiles o no efectivos para las funcionalidades de olvido de contraseña o recuperación de credenciales y no se pueden implementar de forma segura.
    - Almacenar las contraseñas en texto claro, cifradas o usando funciones hash débiles.
    - No se tiene autenticación multi-factor o la implementada no es eficaz.
    - Se expone el identificador de sesión en la URL
    - Se reutilizar el identificador sesión luego de iniciar sesión

- No se invalida correctamente los identificadores de sesión, es decir, las sesiones de usuario o los tokens de autenticación no se valida de forma correcta durante el cierre de sesión o después de un periodo de inactividad.

- **08 Software and Data Integrity Failures:** en el 2021 se agregó esta nueva categoría y esta se centra en hacer suposiciones relacionadas con las actualizaciones de software, datos críticos y pipelines de CI/CD sin verificación de integridad. Esta categoría surgió ya que es uno de los mayores impactos y nos los dice los sistemas de vulnerabilidades que son Common Vulnerability and Exposures (CVE) y Common VUlnerability Scoring System (CVSS). En esta categoría también se destacan algunas CWE que son:
  - CWE-829: Inclusión de funcionalidades provenientes de fuera de la zona de confianza.
  - CWE-494: Ausencia de verificación de integridad en el código descargado.
  - CWE-502: Deserialización de datos no confiables.

  Se sabe que los fallos de integridad de software y datos están relacionados con código y que la infraestructura no está protegida contra alteraciones y esto lo podemos ver si es que la aplicación tiene una dependencia de *pluglins*, bibliotecas o módulos de fuentes, repositorios o redes de entrega de contenidos que no son confiables. Si un pipeline CI/CD es inseguro puede causar accesos no autorizados, inclusión de código malicioso o corre peligro el compromiso del sistema en general. Actualmente es muy común que se implementen funcionalidades de actualización en las aplicaciones por lo que se descargan nuevas versiones de esta sin realizar verificaciones integridad que se realizaron previamente al instalar la aplicación y esto puede causar que los atacantes puedan potencialmente cargar lo que son sus actualizaciones para ser distribuidas y ejecutadas en las instalaciones. Un ejemplo podría ser cuando los objetos o datos no son codificados o

serializados en las estructuras y esto desencadena que el atacante pueda ver y modificar y de esta forma se produce la deserialización insegura.

Lo podemos prevenir usando firmas digitales o mecanismos similares para poder verificar si el software o datos provienen de la fuente esperada y estos no fueron alterados, debemos de asegurar que las bibliotecas y dependencias como *npm* o *maven* se usan desde sus repositorios oficiales, nos debemos asegurar de usar una herramienta de análisis de componentes de terceros esto con el fin de revisar la ausencia de vulnerabilidades conocidas, se debe tener un proceso de revisión de cambios de código y configuración esto nos puede ayudar a minimizar las posibilidades de que el código o configuraciones maliciosas se introduzcan en la pipeline, no se deben enviar datos no cifrados o firmar sin verificar los clientes pode medio de una verificación de integridad o firma electrónica esto es con el fin de detectar modificaciones o reutilización de datos anteriormente serializados.

- **09 Security Logging and Monitoring Failures:** en el 2017 se encontraba en la posición 10 y en el año 2021 subió una posición es decir se encuentra en la posición 9, esta categoría trata el monitoreo y registro de seguridad que proviene de la encuesta de la comunidad. Esta categoría suele ser desafiante para testear, ya que implica entrevistas o preguntas si es que los ataques fueron detectados en las pruebas de penetración. Se puede usar esta categoria para auditabilidad, visibilidad, alerta de incidentes y análisis forense y también cuenta con CWE que son:
    - CWE-117: Neutralización de salida incorrecta para registros
    - CWE-223: Omisión de información relevante para la seguridad
    - CWE-532: Inserción de información sensible en archivo de registro.

  El principal propósito de esta categoría detectar, escalar y responder ante las vulnerabilidades activas. Sin el monitorio y registro, éstas no podrían ser detectadas por lo que provocaría registros, detecciones, monitoreos y respuestas insuficientes.

  Algunos ejemplos son:

- Eventos auditables como lo son inicios de sesión, fallas en este mismo y transacciones con un alto valor que no se registraron.
- Advertencias y errores donde no se generan registros o se generan, pero son pocos claro o inadecuados.
- Registros en aplicaciones y API no monitoreadas para poder detectar las actividades sospechosas.
- Los registros que se almacenan únicamente son locales.
- No se implementan de forma correcta o no son efectivos los umbrales de alerta y los procesos de escalamiento.
- El uso de pruebas de penetración y escaneo usando las herramientas de prueba dinámica de seguridad en aplicaciones no generan algún tipo de alerta.
- Se pude ser vulnerable si se fuga la información haciendo registros y eventos de estas alertas al usuario o atacante.

- **10 Server-Side Request Forgery (SSRF):** esta categoría se agregó en el 2021 debido a que los datos muestran una tasa de incidencia relativamente baja con una cobertura de pruebas por encima del promedio y las calificaciones están por encima del promedio para la capacidad de explotación e impacto por lo que es probable que su entrada sea única o tenga un pequeño grupo de enumeraciones de debilidades comunes (CWE)(OWASP, 2023). Una falla de SSRF sucede cuando la aplicación web obtiene un recurso remoto sin validar lo que es la URL que es proporcionada por el usuario, esto permite que el atacante intervenga en la aplicación para que este envié una solicitud falsa a un destino desconocido. La posibilidad de que suceda SSFR es mayor cada vez debido a la disponibilidad de los servicios en la nube y su complejidad en arquitecturas.

No solo en OWASP se pueden encontrar las vulnerabilidades que existen y van surgiendo en los últimos años, también *Kaspersky* que es un antivirus que ofrece un extenso catálogo de soluciones de ciberseguridad para casa, empresas

pequeñas y grandes, además de que nos ofrece soluciones de seguridad para los distintos dispositivos que existen que son:

- Android: Ofrece Antivirus y servicio de VPN
- Mac: Ofrece Antivirus a los ordenadores y servicio de VPN
- Seguridad móvil
- Windows: Ofrece servicio de VPN
- iPhone: Ofrece servicio de VPN
- Enrutadores: Ofrece servicio de VPN

Kaspersky además de ofrecer sus servicios, ofrece información valiosa para empresas y personas, ya que nos ofrece un análisis de las mayores amenazas con las que se inicia en este caso, el año en curso que y nos dice que al inicio de año se registraron diferentes tipos de ataques que son:

- Deepfakes: los ciberdelincuentes se están ayudando de las Inteligencias Artificiales creando videos y audios que son convincentes, logrando engañar a las víctimas. Por lo que aumenta la usurpación de identidad. (Kaspersky, 2024)
- Phishing avanzado: las campañas son cada vez más sofisticadas mediante el uso del correo electrónico, mensajes de texto o llamadas telefónicas su único objetivo es obtener información personal, contraseñas, datos de tarjetas y esto es un riesgo mayor en la seguridad digital de hoy en día.(Kaspersky, 2024)
- Ataques de ingeniería Social: en este caso debido al incremento en usuarios dentro de las redes sociales los estafadores encontraron una forma de poder realizar ataques y lo hacen creando perfiles falsos, se hacen pasar por un conocido o usan información personal que el usuario tiene publicada en sus redes para poder estafar o engañar a las personas y obtener sus datos personales por esto se nos recomiendo no confiar en las promociones patrocinadas o cualquier enlace en redes sociales (Kaspersky, 2024).

# Capítulo 2

# Análisis de Riesgos en la Web

Como se mencionó en el capítulo anterior con el aumento del uso de Internet y el aumento de la migración de datos, creación y uso de sitos web, aplicaciones web y móviles, y aplicaciones de escritorio los delincuentes encontrar nuevas formas de realizar robos de información que pueden ser fatales para una empresa o persona ya que estos llegan a robar información personal, contraseñas, secuestros de sistemas informáticos, daños a sistemas y esto con el fin de obtener dinero ya sea de una empresa o engañando a familiares o conocidos de alguna persona a la que se le robo su identidad y es por esto que es necesario hablar de los ataques que han ido surgiendo en estos últimos años ya que con esto nos da la pauta para poder encontrar estadísticas de cómo es que han ido evolucionando las amenazas y vulnerabilidades dentro de los sistemas.

## 2.1 Tipos de Ataques

### 2.1.1 Ataques por Inyección

Los ataques *Structured Query Language Injection* (SQLI), son una técnica que modifica consultas de base de datos por medio de la inyección de código para explotar una vulnerabilidad con datos validados. Es una de las técnicas más usadas y por la cual se obtiene acceso a las tablas de una base de datos, incluyendo la información del usuario y la contraseña. Los sitios más atacados son empresas de comercio en línea con grandes bases de datos. (Hdco., 2014)

### 2.1.2 DDoS

El ataque denominado Denegación de Servicio Distribuida (por sus siglas DDoS) funciona congelando la respuestas de un sitio web. Se inunda de solicitudes externas lo que provoca que un usuario real no pueda interactuar. Estos ataques se dirigen a puertos específicos o rangos de direcciones IP, pero también se pueden dirigir a cualquier dispositivo o servicio que esté conectado (ISACA. (n.d.). ISACA., 2024).

Existen 3 variedades de DDoS:

1. Ataques de volumen, consiste en realizar acciones para inundar y desbordar el ancho de banda de un sitio.
2. Ataques de protocolo, se utilizan los protocolos de los paquetes enviados dirigidos a servicios o recursos de la red específicos.
3. Ataques a aplicaciones, se explota la capa de aplicación por medio de que exploten el servidor web. (ISACA. (n.d.). ISACA., 2024).

### 2.1.3 Fuerza Bruta

Es cuando se intenta romper o colapsar un inicio de sesión con combinaciones de nombre de usuario y contraseña en una página web. Se usan diccionarios para encontrar contraseñas débiles para ser descifradas y obtener un acceso de forma fácil. En estos casos el atacante cuenta con tiempo suficiente por lo que lo recomendable que se tenga contraseñas seguras y fuertes, así tu cuenta no sería vulnerable a este tipo de ataques. (Hdco., 2014)

### 2.1.4 Cross Site Scripting

En este tipo de ataque se inyecta scripts maliciosos en un sitio web inofensivo ya que estos sitios web parecen de confianza y el navegador del usuario final tiende a ejecutar la secuencia de comandos por lo que les da la concesión a los piratas informáticos para que tengan acceso a los tokens o a la información que contienen las cookies que son usadas por el ese sitio. Comúnmente se utiliza para obtener acceso de un usuario de la cuenta.(Laura & Saucedo, s/f)

Como identificar vulnerabilidades

- Black-box: es una técnica que consiste en probar aplicaciones desde el punto de vista del atacante. (Laura & Saucedo, s/f)
- White-box: En el lado del servidor, se tiene acceso a la información relevante de la organización. (Laura & Saucedo, s/f)
- Análisis estático de código (auditoria de código fuente): consiste en la revisión del código sin ejecutar algún programa para determinar huecos en la seguridad. (Laura & Saucedo, s/f)

- Análisis dinámico de código: se utiliza una aplicación en el *front-end* para identificar las vulnerabilidades de seguridad potenciales y debilidades que existan en la aplicación. (Laura & Saucedo, s/f)
- Pruebas de penetración: Consiste en la simulación de un ataque. (Laura & Saucedo, s/f)
- Pruebas pasivas: se captura el tráfico de para detectar fallas y faltas a la seguridad mediante el análisis de los paquetes capturados. (Laura & Saucedo, s/f)
- Pruebas activas: utiliza un programador de subprocesos asignados al azar para verificar si las advertencias comunicadas por un análisis predictivo de programa son errores reales. (Laura & Saucedo, s/f)
- Fuzz testing: Estimular el sistema bajo prueba, utilizando datos aleatorios o mutados queridos, con el fin de detectar comportamientos no deseados como violación de confidencialidad. (Laura & Saucedo, s/f)

## 2.2 Ataques en los últimos 3 años

### 2.2.1 Ataque del grupo Guacamayas Leaks a Sedena

En septiembre del 2022 el grupo llamado Guacamayas Leaks lograron hackear a la Secretaria de la Defensa Nacional (Sedena) donde vulneraron 6 terabytes de información clasificada y miles de correos electrónicos, de esta forma dejo en evidencia la vulnerabilidad que tiene el gobierno de México, este grupo denominado como Guacamayas aprovecho la evolución de Proxy Shell que ha sido una flaqueza del servidor Microsoft Exchange y fue detectada en el primer semestre del año anterior pero debido a la falta de recursos el Gobierno de México no logro corregir a tiempo, ya que antes de que hackeara a la Sedena, ya existían varios parches para la protección de esta vulnerabilidad. (Forbes Staff, 2022)

### 2.2.2 Ataque cibernético a The Guardian

En diciembre del 2022 el periódico The Guardian del Reino Unido sufrió un ataque de ransomware y esto hizo que esta empresa pidiera a su personal que trabajara

de forma remota en lo que desconectaban y clasificaban los sistemas internos, hasta los sistemas de comunicación interna del personal se vieron afectados. El periódico únicamente dijo 'Ciberataque altamente sofisticado que implique el acceso no autorizado de terceros a partes de nuestra red', la empresa *KnowBe4* fue la encargada de investigar este caso y dijo que el vector del ataque inicial fue por phishing por medio del correo electrónico. (BCS, 2023)

### 2.2.3 Incidente de la FAA

En enero del 2023 Estados Unidos suspendió sus vuelos por un problema con un sistema critico operado por le Administración Federal de Aviación (FAA) aunque no se confirmó si fue un ataque cibernético, es importante mencionarlo ya que, si fue un ataque cibernético y no se detectó como tal, nos habla de que puede haber alguna falla de seguridad cibernética en su sistema y no se pueda observar o encontrar dicha falla. (BCS, 2023)

### 2.2.4 Ataque de ransomware Royal Mail

A inicios de enero de 2023 el Royal Mail fue objeto de ataque de ransomware ya que un afiliado usaba LockBit Ransomware-as-a-Services (RaaS), el ataque afecto al centro de distribución cerca de Belfast, Irlanda del Norte, aquí fue donde se iniciaron a imprimir las demandas de la banda de ransomware. Este ataque afecto a las entregas internacionales y usaron transportistas alternativos, esto hizo que el Reino Unido declaro a Royal Mail como parte de la Infraestructura Nacional Critica (CNI) de la nación, los usuarios o afiliados cifran los datos en los servidores destino y los filtran para obtener dos palancas de extorsión y esto fue lo que sucedió con Royal Mail. (BCS, 2023)

## 2.3 Estadísticas

En las estadísticas siguientes se mostrará la posición en que se encuentra México con respecto a otros países, como se encuentra en temas de ciberseguridad.

National Cyber Security Index (NCSI) nos da una lista de 48 países donde México se encuentra en el lugar 39, Global Cybersecurity Index se encuentra en el lugar 52,

en el E-Government Development Index se encuentra en el lugar 62 yen el Network Readiness Index se encuentra igual en el lugar 62. El NCSI nos da este top recopilando los datos que están disponibles públicamente por parte de cada país. (NCSI, s/f)

En la Ilustración 2 se observa el porcentaje que México tiene de cumplimiento de NCSI y los porcentajes son los siguientes:

- Política de Ciberseguridad: 20%
- Contribución Global a la Ciberseguridad: 67%
- Educación y Desarrollo Profesional: 60%
- Investigación y Desarrollo en Ciberseguridad: en este campo no se ha realizado alguna aportación ni desarrollo.
- Ciberseguridad de las Infraestructuras Criticas de Información (CII): 50%
- Ciberseguridad de los Habilitadores Digitales: 17%
- Análisis de Amenazas Cibernéticas y Concienciación: 25%
- Protección de Datos Personales: 100%
- Respuesta a Incidentes Cibernéticos: 57%
- Gestión de Crisis Cibernéticas: 22%
- Lucha contra la Ciberdelincuencia (Policía): 38%
- Ciberdefensa Militar: 33%


*Ilustración 2.- Estadísticas de México en tema de Ciberseguridad (NCSI, s/f)*

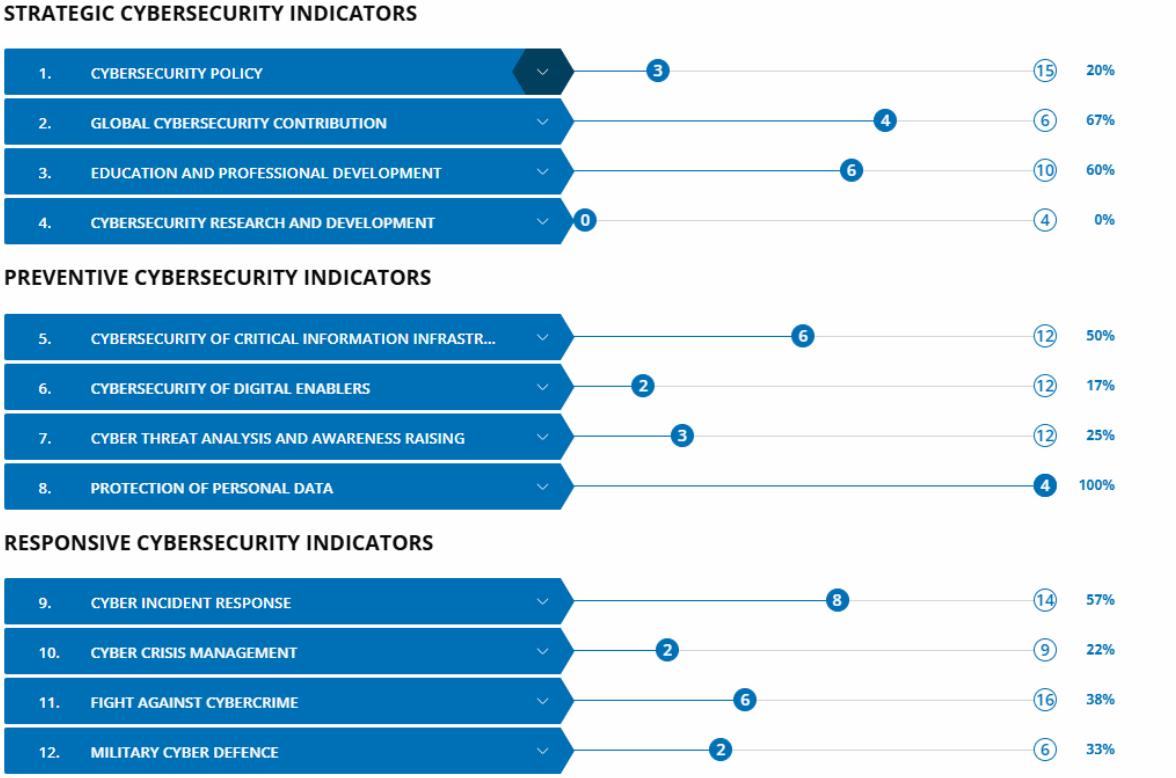


*Ilustración 3.- Indicadores de Ciberseguridad de México (NCSI, s/f)*

En la ilustración 3 se muestran los siguientes indicadores:

Indicadores de estrategia: en este apartado se abarca las políticas de ciberseguridad, la contribución gen ciberseguridad global, la educación y desarrollo profesional e investigación y desarrollo en tema de ciberseguridad.

Indicadores preventivos: se abarca ciberseguridad de la infraestructura, ciberseguridad de los habilitadores digitales, análisis de amenazas cibernéticas y conciencia y por último protección de datos personales.

Indicadores receptivos: se abarca la respuesta a incidentes cibernéticos, gestión de crisis, lucha en contra de cibercrimen y por último la ciberdefensa militar.

Analizando estas estadísticas es evidente que en México hace falta más educación en cuanto a temas de Ciberseguridad, aunque se tiene un buen porcentaje de educación en temas de Protección de Datos Personales, aun hace falta mucho trabajo en cuento a ciberseguridad dentro del países y un claro ejemplo es el ataque a SEDENA. El robo de identidad, hackeo a varias empresas como Coppel, robo de información por medio de phishing, hackeo a redes sociales por falta de contraseñas fuertes, vulnerabilidades en páginas del gobierno, entre otras vulnerabilidades dentro de los sistemas.

En los siguientes gráficos se muestra el top 5 de este ranking de ciberseguridad y México para poder dimensionar el lugar en que se encuentra con respecto a estas potencias y como es que estos 5 países se encuentran en temas de ciberseguridad.

En la Ilustración 4 observamos la línea del tiempo del ranking de estos 6 países donde podemos observar que México ha decrecido durante el 2023 y este año tuvo un aumento en sus estadísticas significativo sin embargo parece que todo esto está decreciendo nuevamente con respecto a los demás países.

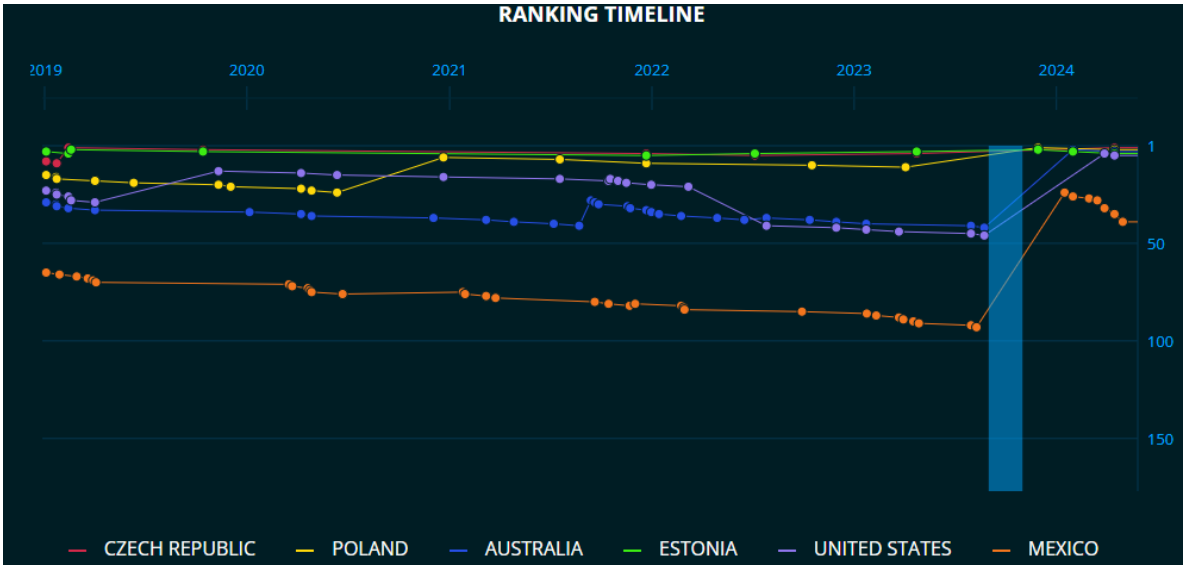


*Ilustración 4.- Diferencia de México con relación a los 5 países con mejor ciberseguridad (NCSI, s/f)*

En la ilustración 5 podemos observar cómo se encuentra el ranking con respecto a estos 5 países y podemos observar el porcentaje NCSI, el Desarrollo Digital y la diferencia que existe entre cada país incluyendo México ubicándolo en el lugar 39 con un total de 38.33% de Ciberseguridad.

| Rank | Country | National Cyber Security Index | Digital development | Difference |
|---|---|---|---|---|
| 1. | Czech Republic | 98.33 | 72.04 | 26.29 |
| 2. | Poland | 92.50 | 72.29 | 20.21 |
| 3. | Australia | 87.50 | 82.21 | 5.29 |
| 4. | Estonia | 85.83 | 80.02 | 5.81 |
| 5. | United States | 84.17 | 84.21 | -0.04 |
| 39. | Mexico | 38.33 | 62.16 | -23.83 |

*Ilustración 5.- Ranking de los 5 mejores países y diferencia con México (NCSI, s/f)*

En la Ilustración 6 se observa cómo están ubicados los países en cuanto a los indicadores de ciberseguridad.

En los Indicadores Estratégicos de Ciberseguridad se observar cómo se encuentra México en cuanto al Top 5 que nos ofrece NCSI y es una realidad que México no cuenta con las mejores estrategias de ciberseguridad en el mundo y tenemos una gran deficiencia en el ámbito de la ciberseguridad.

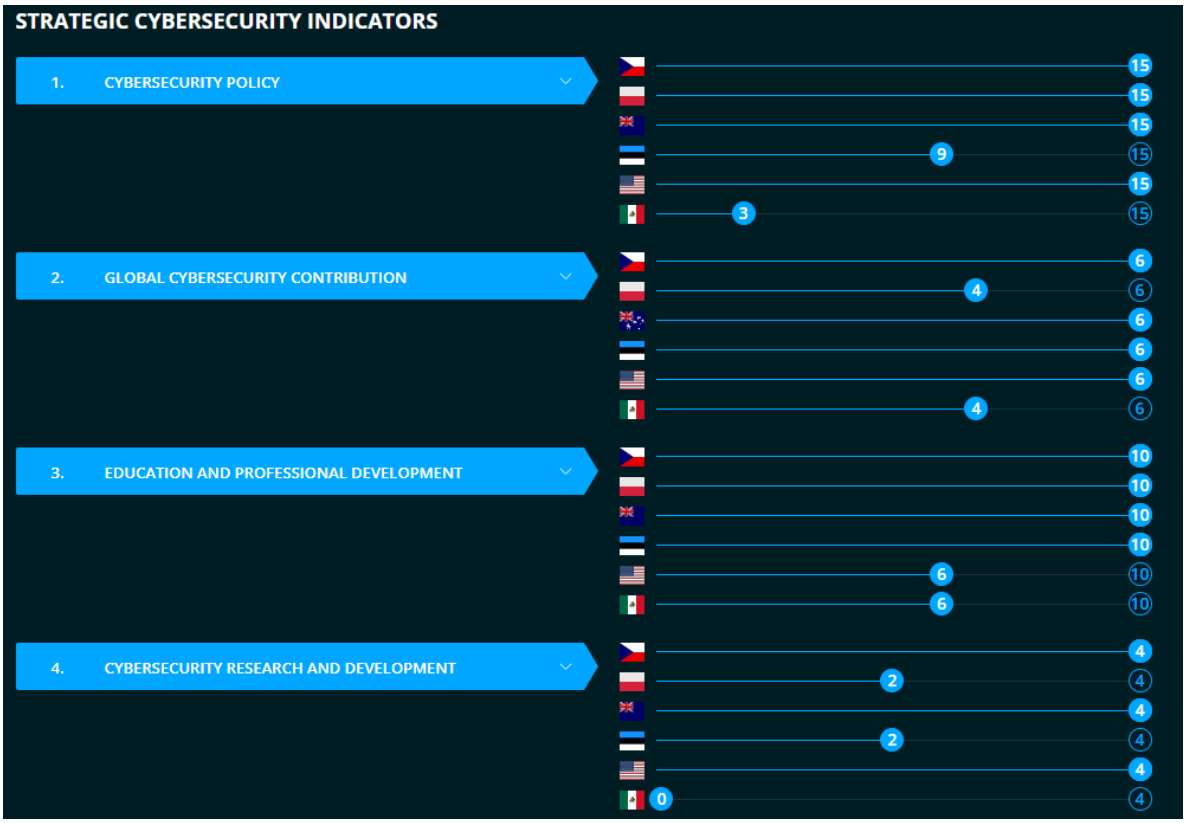


*Ilustración 6.- Diferencias entre México y los 5 mejores países en cuando a los indicadores estratégicos (NCSI, s/f)*

En la Ilustración 7 se pueden observar los indicadores Preventivos de Ciberseguridad donde México únicamente iguala en temas de Protección de Datos Personales a los demás países del top 5 y es una realidad que no tenemos una buena estrategia preventiva ante ataques y vulnerabilidades que pudiera tener un sitio web o una aplicación.


*Ilustración 7.- Diferencias entre México y los 5 mejores países en cuando a los indicadores preventivos (NCSI, s/f)*

En la Ilustración 8 se muestran los indicadores de Ciberseguridad Receptivos esta gráfica nos muestra cómo es que como país no tenemos la mejor respuesta a los ataques, no contamos con la suficiente gestión ante una crisis cibernética y tampoco tenemos las mejores herramientas para poder luchar contra la ciberdelincuencia que esto es una gran problema ya que si no contamos con las mejores herramientas no se puede determinar con rapidez y eficiencia detectar de donde fue el ataque, no se puede identificar con rapidez a los atacantes o en su defecto no se tiene la eficacia y certeza de que provocó un ataque a un sitio y esto nos trae como consecuencia que la policía cibernética no pueda actuar ante una situación de vulnerabilidad . (NCSI, s/f)

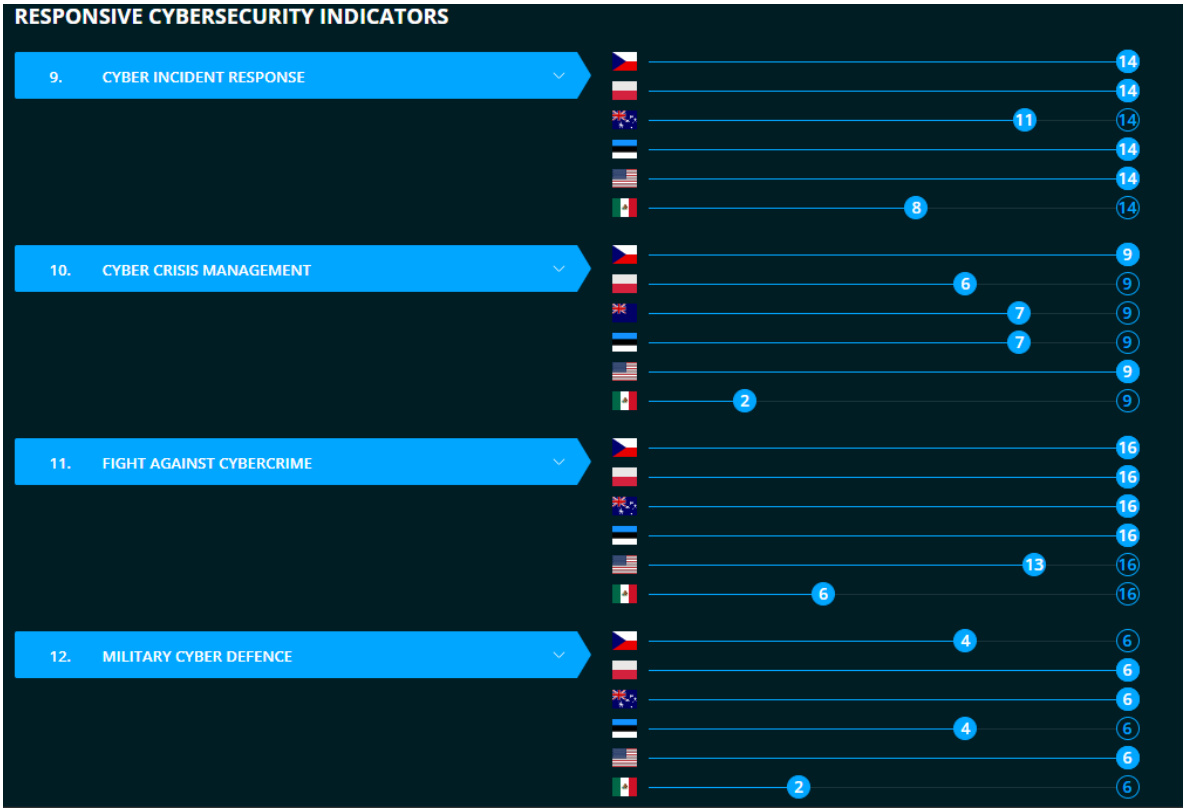


*Ilustración 8.- Diferencias entre México y los 5 mejores países en cuando a los indicadores receptivos (NCSI, s/f)*

*CVE details* creada por la empresa *SecurityScorecard* y esta ofrece ciberseguridad para empresas y tiene diferentes paquetes y productos que ofrece, pero lo más importante es que en *CVE details* nos ofrece datos que van recopilando y asignando el tipo o la categoría a las vulnerabilidades y lo hace mediante identificadores y palabras clave. Ofrece la siguiente tabla en la ilustración 9 y se puede observar el número de incidentes que se tuvieron y el total de incidentes que ha habido durante 11 años hasta el año en curso. (SecurityScorecard, s/f)

| Year | Overflow | Memory Corruption | Sql Injection | XSS | Directory Traversal | File Inclusion | CSRF | XXE | SSRF | Open Redirect | Input Validation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2014 | 832 | 627 | 304 | 1099 | 207 | 3 | 266 | 67 | 10 | 48 | 535 |
| 2015 | 1073 | 1104 | 221 | 776 | 152 | 6 | 249 | 50 | 8 | 46 | 382 |
| 2016 | 1214 | 1174 | 97 | 497 | 99 | 12 | 88 | 41 | 16 | 33 | 532 |
| 2017 | 2494 | 1555 | 505 | 1500 | 283 | 155 | 334 | 109 | 57 | 97 | 972 |
| 2018 | 2100 | 1748 | 504 | 2043 | 573 | 112 | 479 | 189 | 118 | 85 | 1285 |
| 2019 | 1213 | 2057 | 554 | 2389 | 491 | 127 | 560 | 139 | 103 | 122 | 927 |
| 2020 | 1222 | 1903 | 466 | 2203 | 441 | 110 | 416 | 119 | 132 | 101 | 832 |
| 2021 | 1677 | 2566 | 744 | 2726 | 560 | 93 | 520 | 126 | 197 | 133 | 704 |
| 2022 | 1886 | 3420 | 1790 | 3407 | 735 | 101 | 769 | 127 | 235 | 147 | 823 |
| 2023 | 1762 | 2809 | 2158 | 5179 | 808 | 138 | 1398 | 138 | 248 | 188 | 797 |
| 2024 | 1159 | 1436 | 1128 | 3009 | 431 | 113 | 698 | 46 | 183 | 66 | 313 |
| Total | 16632 | 20399 | 8471 | 24828 | 4780 | 970 | 5777 | 1151 | 1307 | 1066 | 8102 |

*Tabla 1.- Lista de incidentes en los últimos 11 años CVE Details (SecurityScorecard, s/f)*

CVE muestra en la Tabla 1 con colores más intenso los años en que esa vulnerabilidad fue mayormente usada por los hackers. Además, muestra que, aunque son vulnerabilidades concurrentes no se hace algo para erradicarlas. (SecurityScorecard, s/f)

En la Tabla 2 se observan las vulnerabilidades por tipo de impacto y como ha incrementado o disminuido en estos años.

| Year | Code Execution | Bypass | Privilege Escalation | Denial of Service | Information Leak |
|---|---|---|---|---|---|
| 2014 | 1041 | 165 | 186 | 1597 | 356 |
| 2015 | 1430 | 177 | 255 | 1793 | 602 |
| 2016 | 1239 | 469 | 608 | 2050 | 704 |
| 2017 | 1870 | 857 | 1027 | 3372 | 1394 |
| 2018 | 1728 | 665 | 849 | 2207 | 1418 |
| 2019 | 1534 | 670 | 916 | 1699 | 1326 |
| 2020 | 1691 | 817 | 1387 | 1677 | 1094 |
| 2021 | 2087 | 806 | 1121 | 2297 | 925 |
| 2022 | 2067 | 944 | 1527 | 2437 | 1144 |
| 2023 | 2581 | 1072 | 1538 | 2560 | 1546 |
| 2024 | 1987 | 521 | 619 | 1071 | 641 |
| Total | 19255 | 7163 | 10033 | 22760 | 11150 |

*Tabla 2.- Lista de vulnerabilidades por impacto en los últimos 11 años (SecurityScorecard, s/f)*

En la Ilustración 9 se observa cómo está distribuida cada vulnerabilidad y cuáles son las que más afectan a los usuarios y a cuáles se les debe poner una mayor atención para evitar la pérdida de datos tanto a empresas como las personas.

Se debe tener en cuenta que XSS es la menor vulnerabilidad que se presenta es Open Redirect.

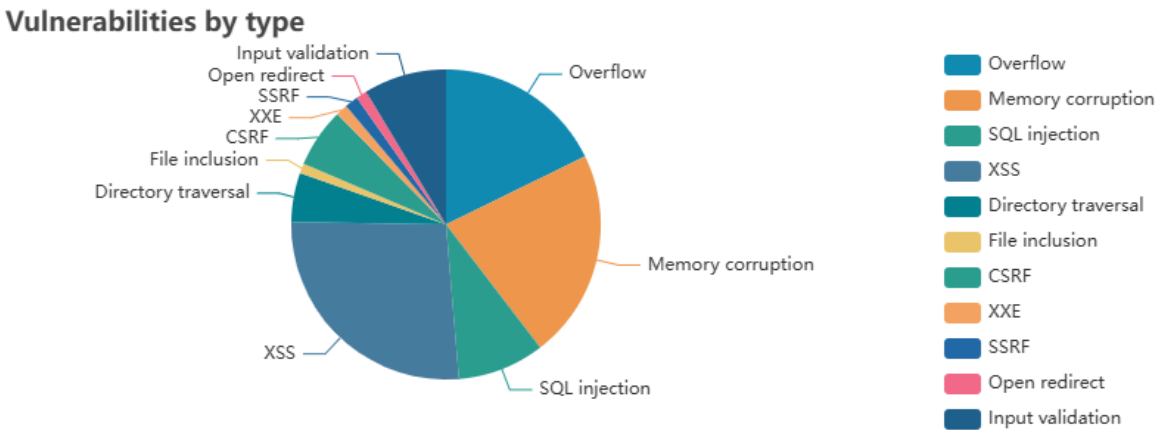


*Ilustración 9.- Distribución grafica de las vulnerabilidades (SecurityScorecard, s/f)*

# Capítulo 3

# Evaluación de Vulnerabilidades en Aplicaciones Web

## 3.1 Descripción de las herramientas

Una herramienta de ciberseguridad sirve como una armadura ya que ayuda a prevenir y poder protegernos contra amenazas o vulnerabilidades y estas amenazas pueden ser dentro de nuestras redes, activos, programas o datos. (Natali Valle, 2024)

Existen distintos tipos de herramientas de ciberseguridad en la actualidad que son:

- Corta fuegos o firewalls: ayudan a controlar el tráfico que entra y sale y está basado en las reglas de seguridad predefinidas. Estos funcionan inspeccionando los paquetes de datos que entran o salen de la red y son las encargadas de decidir si bloquean el tráfico o no. (Natali Valle, 2024)
- Sistemas de Detección de Intrusos (IDS): se encargan de monitorear el tráfico en la red en donde busca las actividades sospechosas y violaciones políticas y alerta a administradores de las posibles amenazas. (Natali Valle, 2024)
- Redes Privada Virtuales (VPN): estas se encargan de hacer una conexión segura y encriptada por medio de internet y esto permite a los usuarios remotos acceder a la red de una forma segura. (Natali Valle, 2024)
- Antivirus: ayuda a proteger del malware, virus, gusanos, troyanos, entre otros. (Natali Valle, 2024)
- Herramientas de Detección y Respuesta de Puntos Finales (EDR): monitorea constantemente actividades en los puntos finales esto buscando señales de comportamiento sospechoso y poder responder a las amenazas en tiempo real. (Natali Valle, 2024)
- Firewalls de Aplicaciones Web (WAF): se encarga de proteger las aplicaciones web filtrando y monitoreando las solicitudes HTTP/HTTPS y bloquea cualquier tráfico malicioso. (Natali Valle, 2024)

- Pruebas de seguridad de aplicaciones estáticas y dinámicas (SAST/DAST):se usan para la identificación de vulnerabilidades en el software en las fases de desarrollo y prueba. (Natali Valle, 2024)
- Herramientas de cifrado: ayudan a proteger los datos transformándolos a un formato ilegible y la única forma de decodificarlos son con las claves de descifrado. (Natali Valle, 2024)
- Solución de Prevención de Perdida de Datos (DLP): ayuda a la prevención de que se filtren o salgan datos de una organización. (Natali Valle, 2024)

Estas herramientas las podemos encontrar en distintos softwares, podemos descargarlas de forma independiente o podemos encontrarlas ya sea en un sistema operativo Linux ya sea en Kali o Parrot.

### 3.1.1 Software para realizar auditoría

**ZAP PROXY**: es una herramienta que ayuda a realizar pruebas de penetración para aplicaciones web, esta herramienta es flexible y extensible. (ZAP 2.15 Getting Started Guide, s/f)

Los requisitos que necesitamos para instalar esta herramienta es Java 11 para la última versión de ZAP 2.12.0 y versiones posteriores, Windows 11, mínimo 4 GB en RAM, pero lo recomendado son 8 GB en RAM, 100 MB para la instalación.

Es conocido por ser un proxy manipulador en el medio, es decir, este se interpone entre el navegador y la aplicación de esta forma intercepta e inspecciona los mensajes enviados del navegador si es necesario los modifica y reenvía los paquetes al destino. En caso de que ya se tenga un proxy de red ZAP se puede conectar a ese proxy. ZAP nos proporciona funcionalidad para una variedad de niveles de habilidad, es decir tiene una funcionalidad para desarrolladores hasta especialistas de pruebas de seguridad, además, tiene una gran variedad de versiones para cada sistema operativo y Docker. (ZAP 2.15 Getting Started Guide, s/f)

ZAP tiene una funcionalidad de escaneo pasivo y ataque automático que nos sirve para iniciar una evaluación de vulnerabilidades, pero tiene algunas limitaciones que son:

- SI la página tiene inicio de sesión no se puede detectar durante un análisis pasivo, pero podemos realizarla configurando la funcionalidad de autenticación de ZAP.

- No tiene mucho control sobre la secuencia, exploración y escaneo pasivo o los tipos de ataques que se llevan a cabo en el ataque automático.

El uso de arañas (spiders: es una herramienta que ayuda a descubrir nuevos recursos de forma automática) es una excelente forma de explorar el sitio y es más efectiva si se combina con la exploración manual, las arañas solo ingresan datos básicos predeterminas en los formularios de la aplicación web, pero el usuario puede ingresar información relevante y de esta forma exponer una mayor parte de la aplicación web a nuestra herramienta. Esto es real con formularios de registro en donde requerimos de un correo electrónico y nuestra araña puede introducir una cadena aleatoria y esto puede causar un error por lo que algún usuario reaccionario al error y dar la cadena correcta y esto provocaría que se exponga la mayor parte de la aplicación cuando se envía y acepta el formulario.(ZAP 2.15 Getting Started Guide, s/f)

- Evaluación de vulnerabilidades: se escanea y analiza buscando problemas de seguridad.

- Pruebas de penetración: el sistema se somete a un análisis y ataque por lo que se usan atacantes maliciosos simulados.

- Pruebas en tiempo de ejecución: se somete al sistema a un análisis y pruebas de seguridad por el usuario final.

- Revisión de código: el código del sistema es sometido a una revisión y análisis detallado donde se buscan las vulnerabilidades de seguridad.

**RECON-NG:** es un framework que se desarrolló en Python y se maneja por medio de comandos, además su objetivo principal es poder realizar reconocimiento basado en la web, los datos se almacenan y pueden ser exportados.

Se puede usar en cualquier sistema operativo, se necesita tener Python instalado en la versión 3.7.6 o superior. Para Linux su instalación es sencilla, pero depende de la distribución ya vendrá instala en sus paquetes o se tiene que clonar el repositorio en GitHub e instalar las dependencias como indica el repositorio.

Este framework utiliza lo que son módulos y nos proporciona diferentes categorías en donde estos módulos se agrupan y son las siguientes:

- Discovery: esta categoría contiene dos módulos que nos ayudan a obtener información interactuando directamente con el entorno objetivo y los módulos que tiene son: el primer módulo busca archivos en la web indicada y el segundo modulo sirve para buscar en el cache del DNS los dominios que son visitados esto con el fin de intentar determinar el antivirus que la organización usa. (Perez Herrero Luis, 2022)

- Exploration: tiene dos módulos pensado para poder explotar las vulnerabilidades en la web.

- Recon: esta categoría engloba más módulos que van más enfocados al reconocimiento de diferentes aspectos. Tiene módulos para resolución de nombres y direcciones IP, módulos para realizar búsquedas en distintos motores de búsqueda, acceso a bases de datos de credenciales expuestas en internet, entre otros. Un punto a tener en cuenta es que para muchos de estos necesitamos configurar una API key, por lo que es necesario un registro en los sitios correspondientes. (Perez Herrero Luis, 2022)

- Reporting: esta categoría nos proporciona la posibilidad de exportar información en diferentes formatos. (Perez Herrero Luis, 2022)

**SOCIAL ENGINEER TOOLKIT:** es una herramienta de código abierta que se basa en Python destinada a la realización de pruebas de penetración. (Kennedy David, s/f)

Esta herramienta solo es compatible con Linux y Mac OS X (experimental).

Tiene una serie de vectores de ataque personalizado que nos permite realizar un ataque creíble de forma rápida.

-Vector de ataque de spear-phishing: se envían correos electrónicos dirigidos con archivos maliciosos adjuntos. (Kennedy David, s/f)

- Vector de ataque de applet de Java: se crea un applet de java malicioso para comprometer a la víctima, con SET puede clonar todo un sitio web y una vez que la víctima haga clic esto la redirigirá de vuelta al sitio original lo que hace que el ataque sea más creíble. (Kennedy David, s/f)

- Vector de ataque Full Screen: se tienen dos opciones de ataque, la primera es hacer que el usuario haga clic en un enlace que fue creado con texto de información sobre las herramientas del navegador falso, cuando el usuario pasa el cursor por el enlace y es lo que hace creer que es realmente el sitio y el otro es cuando hace clic en un script, se detecta el tipo de navegador en el que se está ejecutando el usuario e implementa imágenes que coinciden con el navegador y el sistema operativo.

- Método de explotación del navegador Metasploit: se importan vulnerabilidades del lado del cliente de *Metasploit* y tiene la capacidad de clonar el sitio web y usar las vulnerabilidades basadas en el navegador.

- Método de ataque Credential Harvester: se usa cuando se quiere realizar ataques phishing para obtener nombre de usuario y contraseña del sistema. Funciona clonando el sitio web y cuando la víctima ingresa las credenciales de usuario, los nombres de usuario y contraseñas se publicarán de nuevo en su máquina y lo redirigirá al sitio legitimo.

- Método de ataque Tabnabbing: este método es usado cuando un usuario tiene varias pestañas abiertas y da clic en un enlace le aparecerá el mensaje “Espere mientras se carga la página”. Cuando la víctima cambia de pestaña, el sitio web detecta que hay una pestaña distinta y la reescribe en un sitio web que se le especifique. La víctima al hacer clic nuevamente en la pestaña piensa que se cerró

la sesión de su correo electrónico y escribe nuevamente las credenciales, en este momento se recopilan y el usuario se redirige de nuevo al sitio.

- Método de ataque de Web Jacking: se clona un sitio web y le presenta a la víctima un enlace que indicia que el sitio web fue movido. Al pasar el cursor sobre el enlace, la URL que se muestra es una URL real porque cuando el usuario da clic sobre el enlace movido, se abre la página y es reemplazada por el servidor web malicioso.

- Vector web multiataque: Se permite activar y desactivar distintos vectores de ataques y/o una combinación de estos a una sola página web. Cuando la víctima da clic al enlace, se vuelve objetivo de cada uno de los vectores de ataque que se especifiquen. Se debe tener en cuenta que con el vector de ataque no se puede utilizar Tabnabbing, Cred Harvester o Web Jacking.

- Generador de medios infecciosos: este vector de ataque es físico crear un ejecutable malicioso o uno de los que existen dentro de *metasploit* para crear un DVD/CD/USB que tenga un *autorun*.inf.. Se puede también hacer un exploits de formato de archivo para desencadenar un desbordamiento y se comprometa el sistema.

- Vector de ataque de suplantación de identidad por SMS: este vector te permite falsificar tu número de teléfono y enviar un SMS, es sumamente benéfico para ataques de ingeniería social que usa el *Credential Harvester.*

- Fast-Track Exploitation: es un vector de ataque que contiene exploits, vectores de ataque y ataques adicionales que se pueden usar durante pruebas de penetración.

## 3.2 Diseño de prototipo de laboratorio

Este trabajo de tesis se implementa con software para visualizar distribuciones de Linux sobre Sistema Operativo Windows.

En la ilustración 12 se observa la estructura del sistema que se diseñó y comprende el hardware - laptop Asus con Windows 11 y dentro se instaló Virtual Box versión 7.0.18 en donde se instalaron las máquinas virtuales con el sistema operativo de Kali en versión 2024.2 y otra con el sistema operativo de Parrot OS versión 6.1.

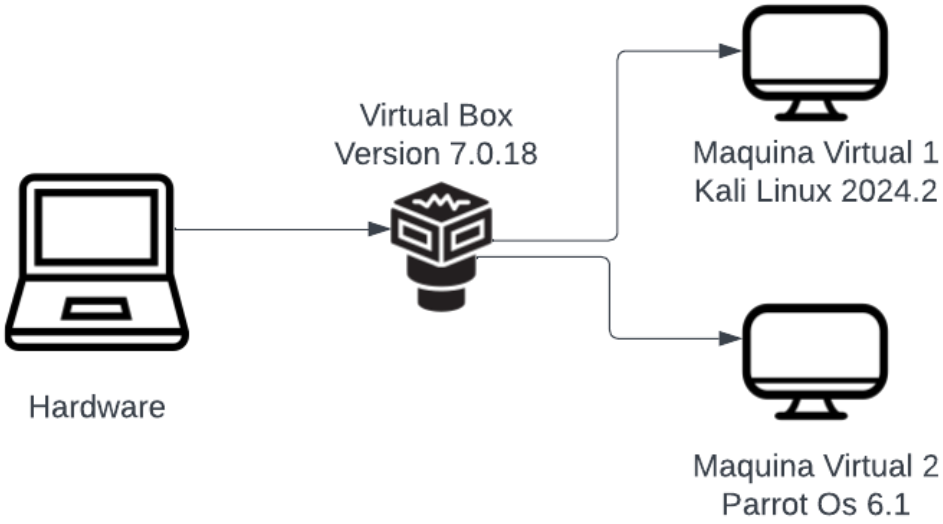


*Ilustración 9.- Diseño de distribución (Elaboración Propia)*

En la ilustración 13 podemos observar cómo es que esta la estructura para poder realizar la identificación de riesgos en la web, la estructura se inicia en tener instalado en el hardware el virtualizador VirtualBox y sobre este una máquina virtual, dentro de ella se instala el sistema operativo de Kali Linux versión 2024.2, dentro de este sistema operativo se tiene una base de datos y un sitio web que contiene html, css y javascript  y otro sistema operativo Parrot OS 6.1 aquí es donde se tienen las herramientas Zap proxy, Recon-ng y Social Engineer Toolkit que nos ayuda a realizar pruebas y chequeos al sitio web sobre ciberseguridad.

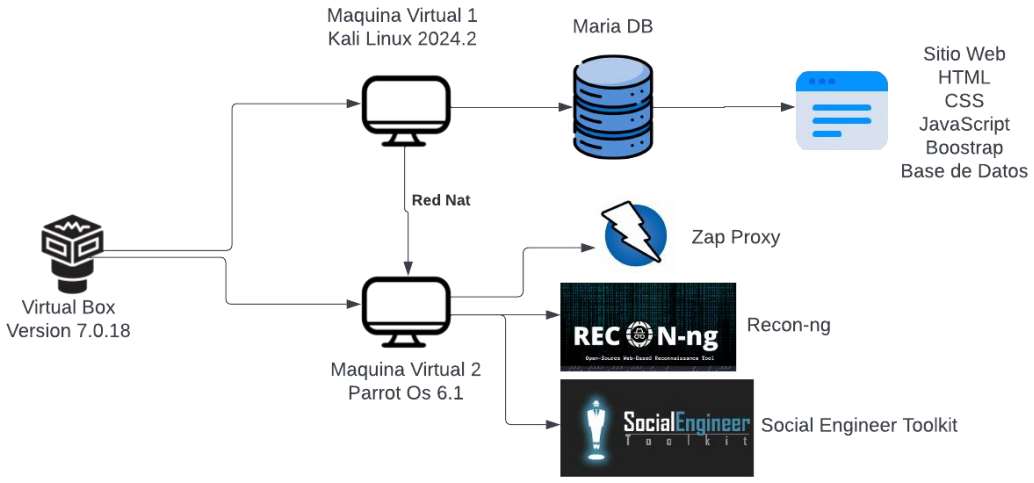


*Ilustración 10.-Diseño de identificación de Riesgos en la Web (Elaboración Propia)*

En la ilustración 14 se puede observar cómo es el diseño de identificación de riesgos de forma local es decir teniendo la herramienta de revisión de aplicaciones web en el hardware principal sin tener que usar una máquina virtual y el sitio web si se aloja dentro de una máquina virtual usando virtual box. Una vez instalado y configurado se hace ping entre el hardware principal y la máquina virtual, una vez que la comunicación está establecida se puede hacer uso de la herramienta para hacer un escaneo a la página web.

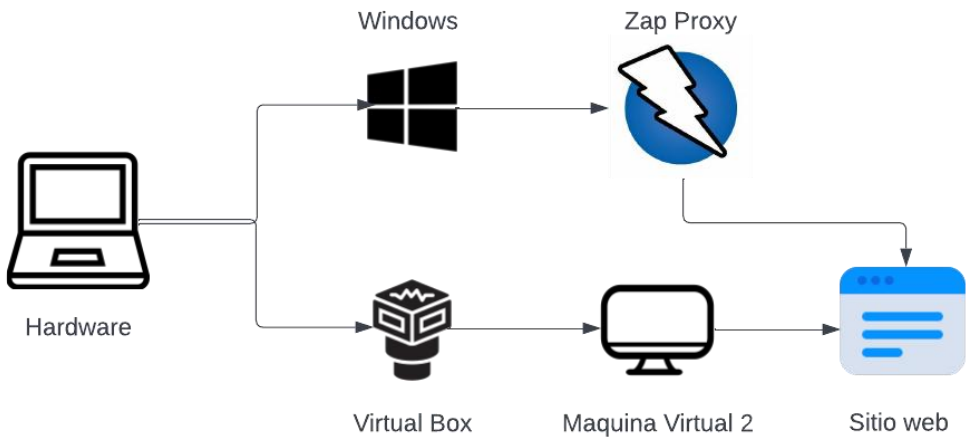


*Ilustración 11.- Diseño de identificación de riesgos de forma local (Elaboración Propia)*

En la ilustración 15 podemos ver el diagrama de la página web dentro del host, se observa que el hardware donde se tiene instalado virtual box y máquina virtual con Parrot es donde haremos los escaneo y también se puede observar el sitio web en la nube y dentro de un host, esto sirve para poder visualizar la página web en el navegador de su preferencia, esto funciona conectándose desde Parrot al sitio web y este recibe las peticiones y el escaneo y regresa la información a la máquina virtual.

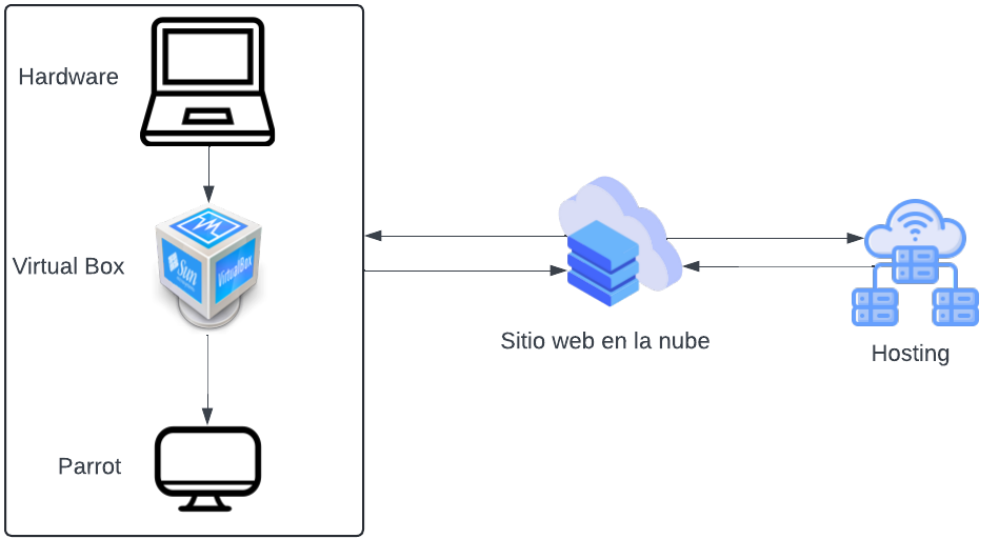


*Ilustración 12.- Diagrama de la Pagina web en un host. (Elaboración Propia)*

## 3.2 Software (Máquina Virtual)

Se usará Virtual Box versión 7.0.18 en donde se tienen dos máquinas virtuales con las siguientes especificaciones:

**Máquina Virtual 1**

En esta máquina virtual se va a usar la distribución de Kali Linux

Versión: 2024.2

Sistema operativo: Debian de 64 bit

Almacenamiento: Kali-linux-2024.2-virtualbox-amd64.vdi (Normal, 80.09 GB)

Adaptador Red: Intel PRO/1000 MT Desktop (Red Nat, NatNetwork)

**Máquina Virtual 2**

En esta máquina virtual se usará la distribución de Parrot OS Security Edition

Versión: 6.1

Sistema Operativo: Debian 12 Bookworm 64-bit

Almacenamiento: Parrot Security 6-disk001.vdi (Normal, 64.00 GB)

Adaptador Red: Intel PRO/1000 MTDesktop (Red NAT, NatNetwork)

## 3.2 Pruebas del sitio web

A continuación, se muestran las pruebas correspondientes, usando las herramientas mencionadas que son ZAP, Recon-ng y Social Engieerie toolkit.

CASO 1: PRUEBAS ZAP DE MANERA LOCAL

En la ilustración 13 se observa la interfaz de ZAP que se instaló previamente en nuestra maquina principal y se observa también todas las opciones que proporciona ZAP.

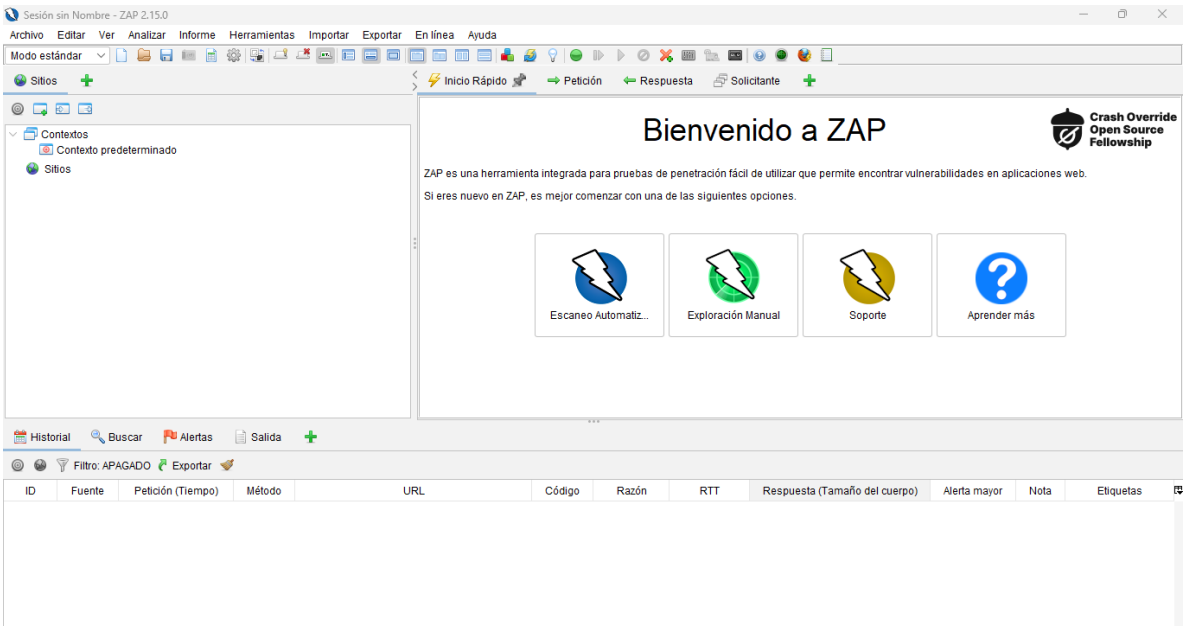


*Ilustración 13.- Inicio de ZAP*

De las opciones que nos da ZAP se usa la opción de escaneo automatizado y este es un inicio rápido y en la ilustración 14 se observa la configuración que se necesita.

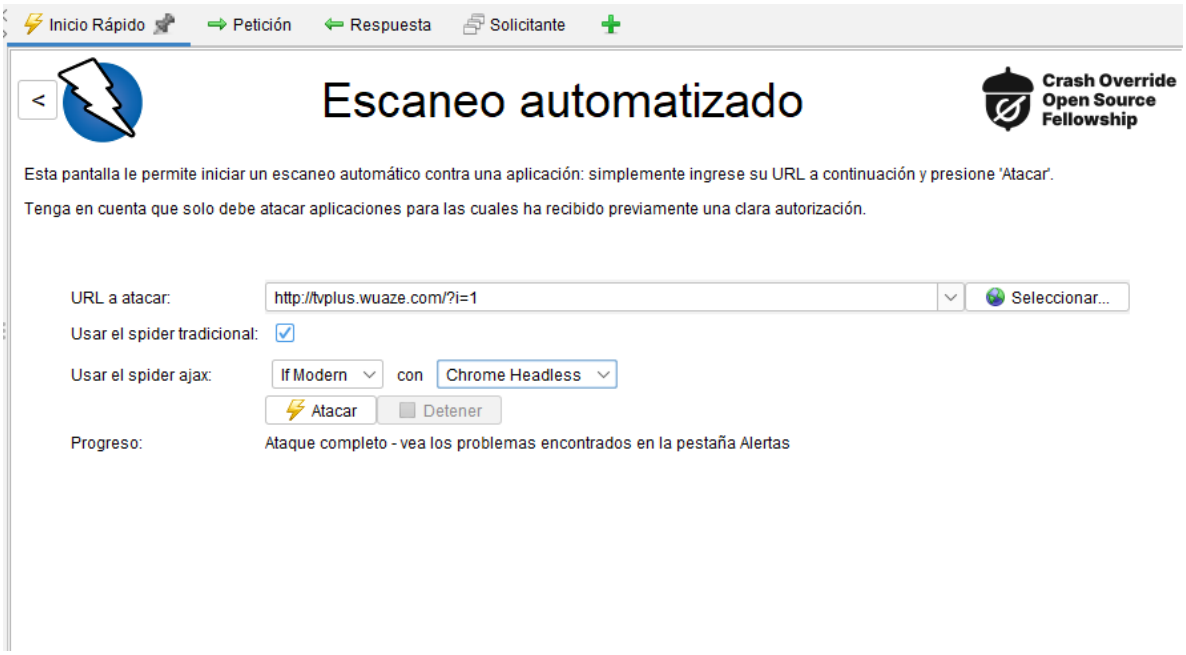


*Ilustración 14.- Configuración de ZAP para un Escaneo Automático*

Una vez que se inicia el escaneo automatizado da los resultados en una sección de Alertas y esto se observa en la Ilustración 15. Las alertas que salen son:

- Alta: Metadatos de la nube potencialmente expuestos
- Media: Encabezado de la política de seguridad de contenido (CSP) no configurado
- Media: Encabezado anti-clichacking faltante
- Baja: Falta encabezado X-Content-Type-Options(2)
- Información: Aplicación web moderna
- Información: Agente de usuario Fuzzer (12)

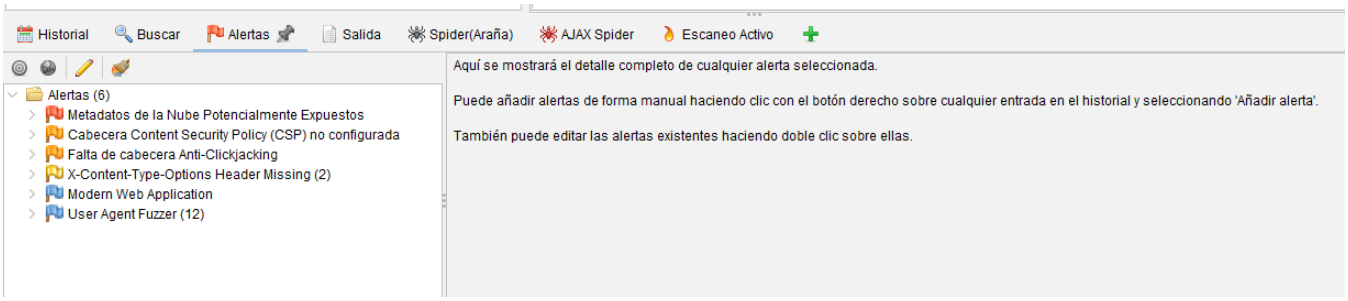


*Ilustración 15.- Resultados de las Pruebas de ZAP*

## CASO 2 PRUEBAS ZAP

Al encender la máquina virtual se usa el sistema operativo Parrot OS en su versión 6.1, se busca la herramienta ZAP para iniciar de forma rápida usando el análisis automático que trae por defecto como se observa en la ilustración 16.

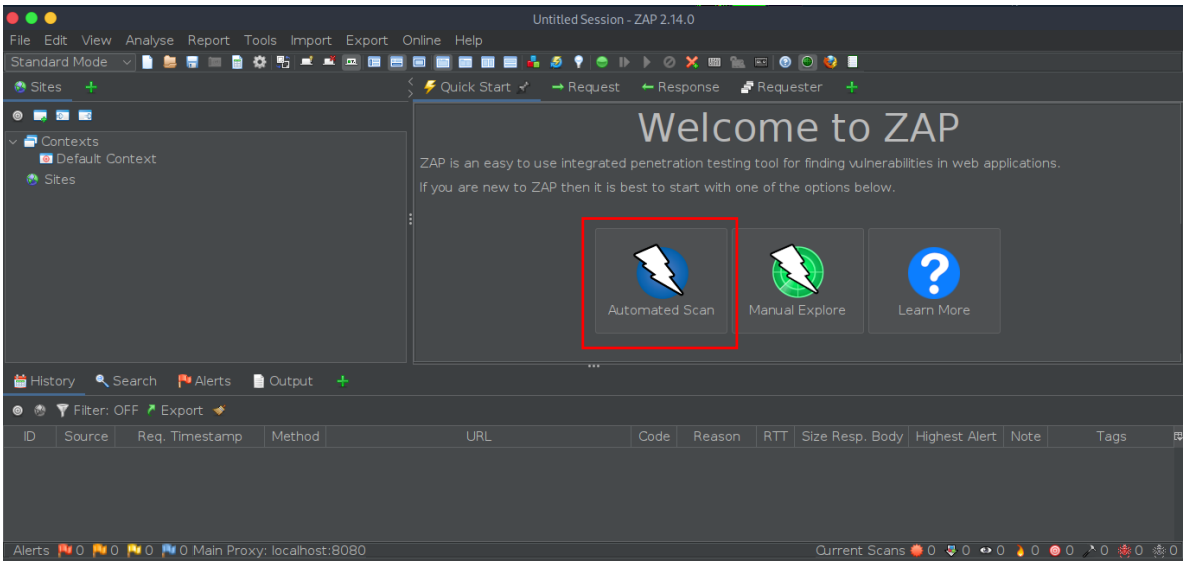


*Ilustración 16.- Escaneo automático*

Ya que se seleccionó el escaneo automatizado se tiene que agregar la URL del sitio web a auditar, se puede escoger el navegador a usar y por último se da clic en el botón que dice *attack* como se observa en la ilustración 17.

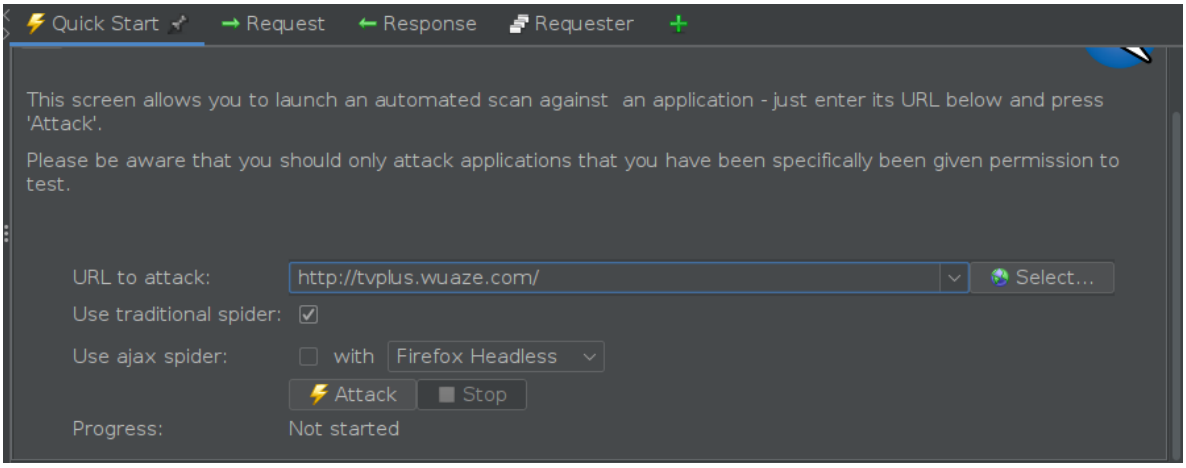


*Ilustración 17.- Configuración para Ataque Automático*

En la ilustración 18 se observa cómo una vez que inicia el ataque desde la interfaz de ZAP a la página web empieza a realizar distintas pruebas y da el porcentaje que lleva de ataque.

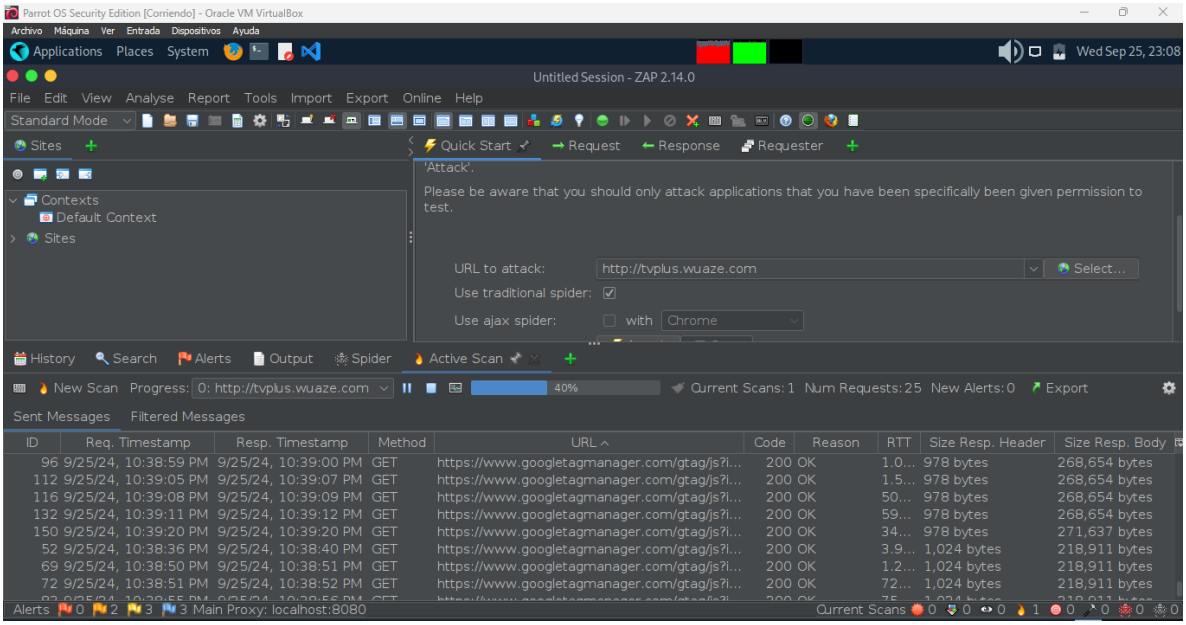


*Ilustración 18.- Ataque Visualización*

En la ilustración 19 se observan los resultados de las pruebas y las alertas que encontró, por medio de una clasificación indicada con las palabras Alta, media, baja e información. Las que se encontraron son:

- Alta: Metadatos de la nube potencialmente expuestos

- Media: Encabezado de la política de seguridad de contenido (CSP) no configurado
- Media: Encabezado anti-clichacking faltante
- Baja: Falta encabezado X-Content-Type-Options(2)
- Información: Aplicación web moderna
- Información: Agente de usuario Fuzzer (36)

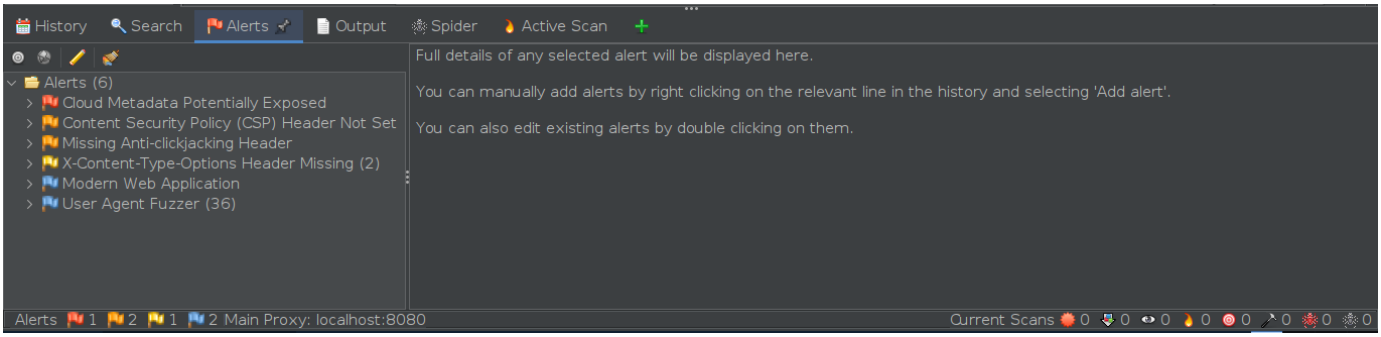


*Ilustración 19.- Resultado de Pruebas*

CASO 3 PRUEBAS RECON-NG

Al encender la máquina virtual see busca *Recon-ng* en las aplicaciones y se ejecuta.

Se debe crear un espacio de trabajo con el comando:

```
Workspace create nombre_espacio_de_trabajo
```

En la Ilustración 20 se observa el resultado del comando anterior.

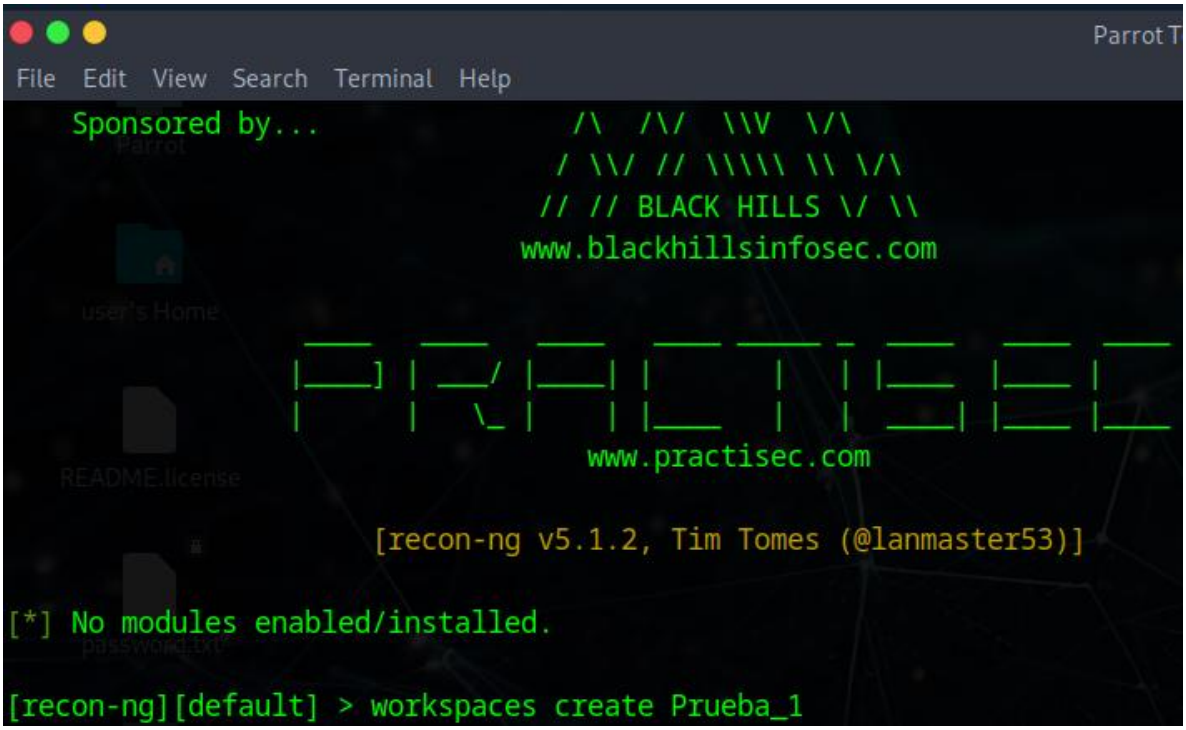


*Ilustración 20.- Creación del Espacio de Trabajo*

Se procede a ver el mercado para revisar los módulos que ofrece *recong-ng* principalmente para revisar los módulos instalados ya que estos se deben de instalar antes de usar con el comando:

“ *Marketplace help*”

En la ilustración 22 se observa el mercado y los módulos disponibles. Además de que se tienen al final dos variables que son D y K y significan:

D = Tiene dependencias.

K = Requiere claves.

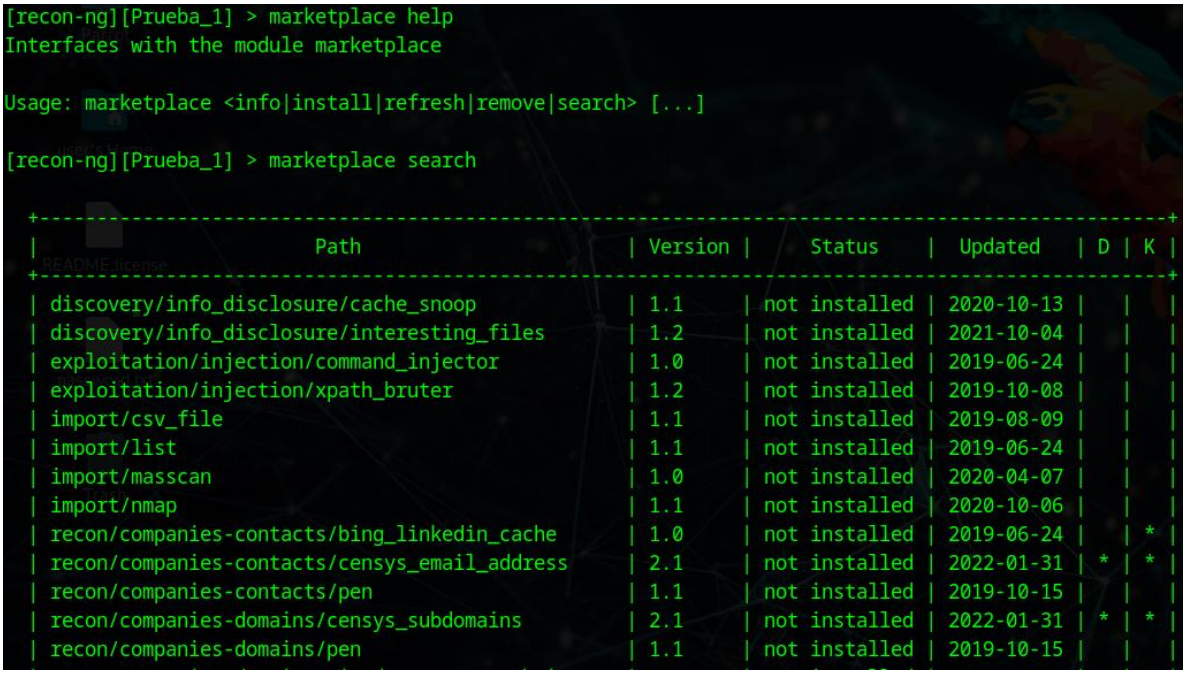


*Ilustración 21.- Mercado de Rencon-ng*

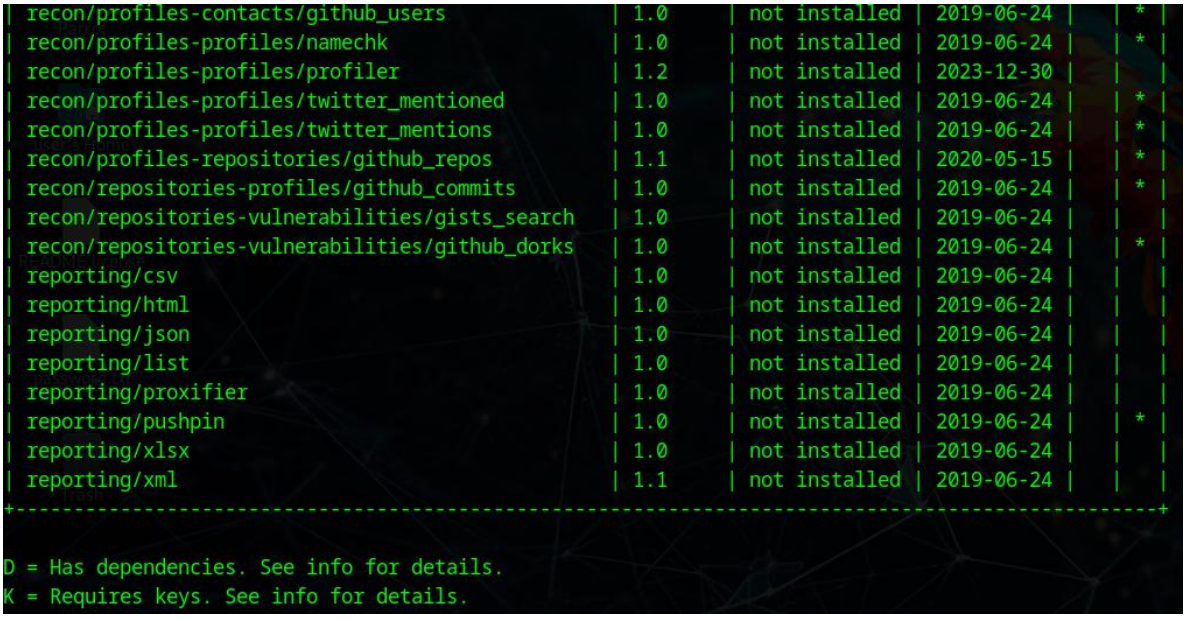


*Ilustración 22.- Mercado de Rencon-ng*

Una vez seleccionada la herramienta se crean los módulos necesarios con los siguientes comandos:

```
Marketplace install hackertarget
```

Comando para cargar los módulos:

```
modules load hackertarget
```

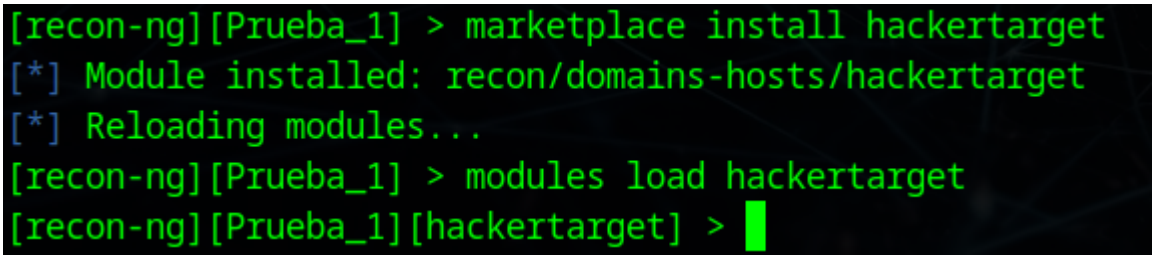


*Ilustración 23.- Instalación de hackertaget y carga de sus módulos*

En la ilustración 24 se muestra cómo se debe configurar la fuente con el nombre del dominio que se va a auditar y se usa el siguiente comando indicando la URL del dominio a investigar:

```
options set SOURCE tvplus.wuaze.com
```

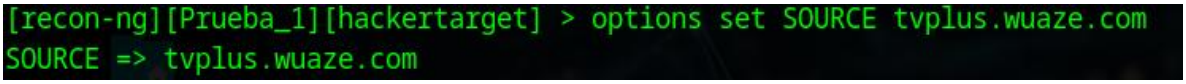


*Ilustración 24.- Configuración de la fuente con el dominio*

Si se requiere más información se usa el siguiente comando:

```
Info
```

En la ilustración 25 se observa el resultado de la ejecución del comando.

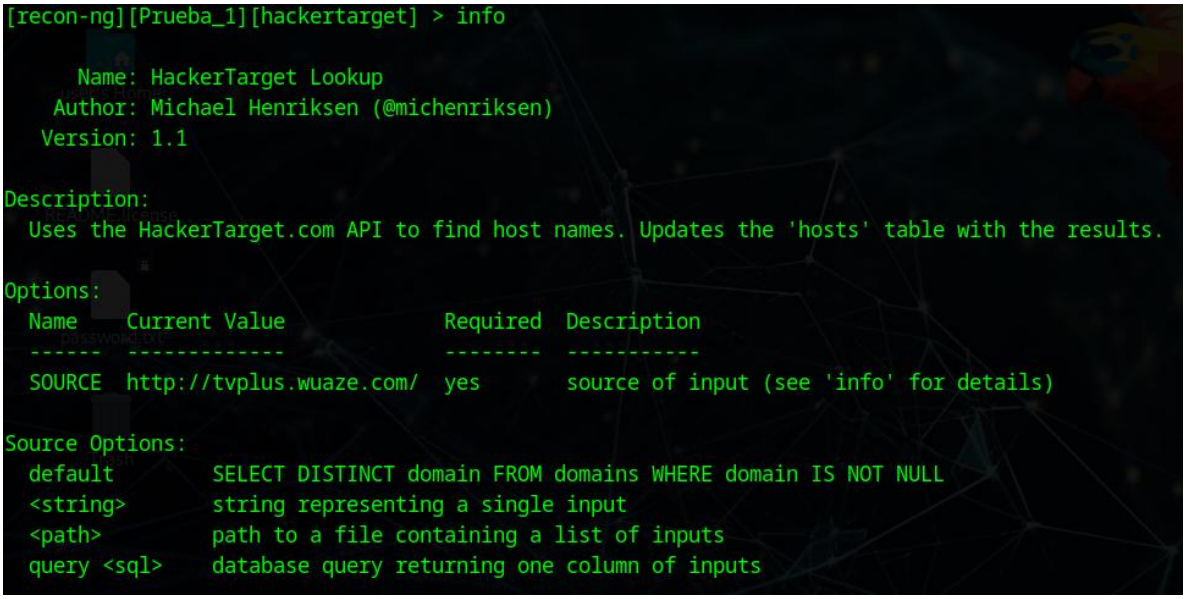


*Ilustración 25.- Información de la fuente*

Para ejecutar el módulo se ejecuta el comando run y este se ejecuta mostrando en la ilustración 26 el resultado:

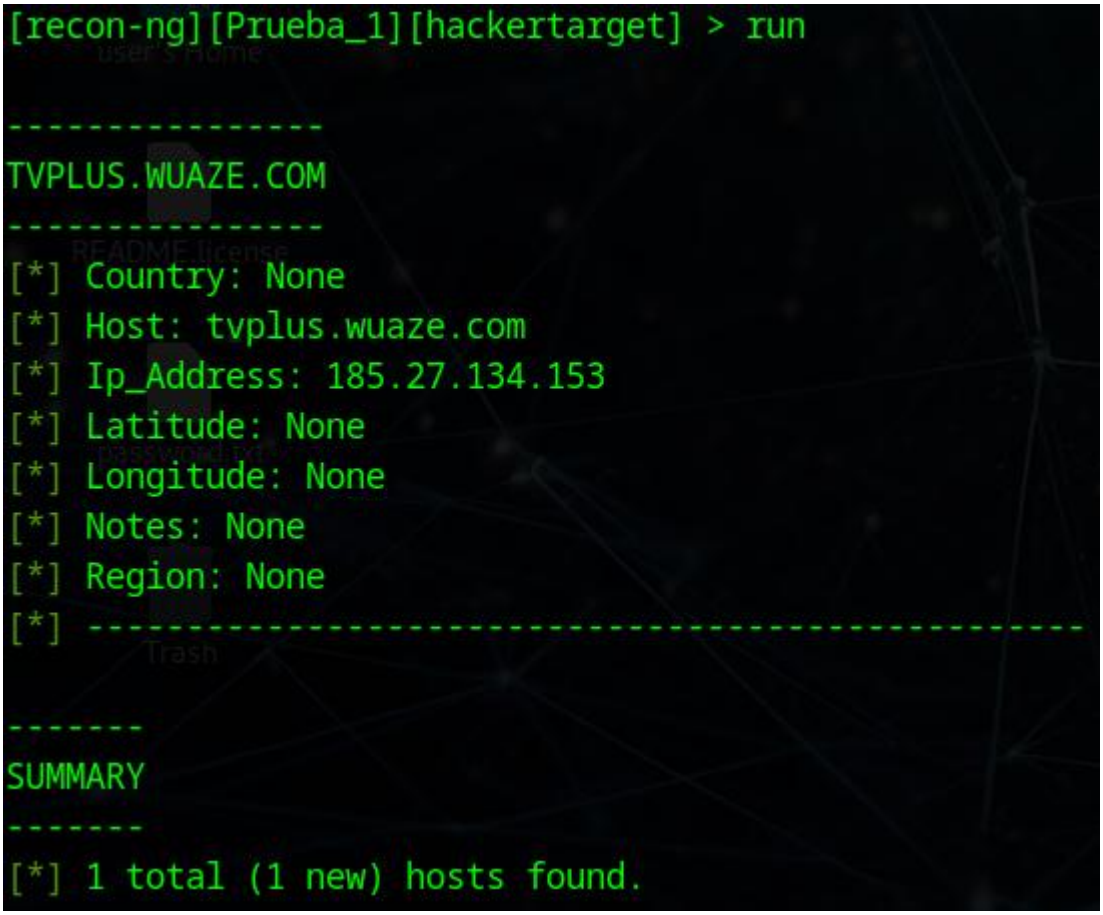


*Ilustración 26.- Ejecución del módulo*

Ahora para observar un resumen de lo obtenido se usa el comando

`show host.`

En la ilustración 27 se observa el resumen obtenido.

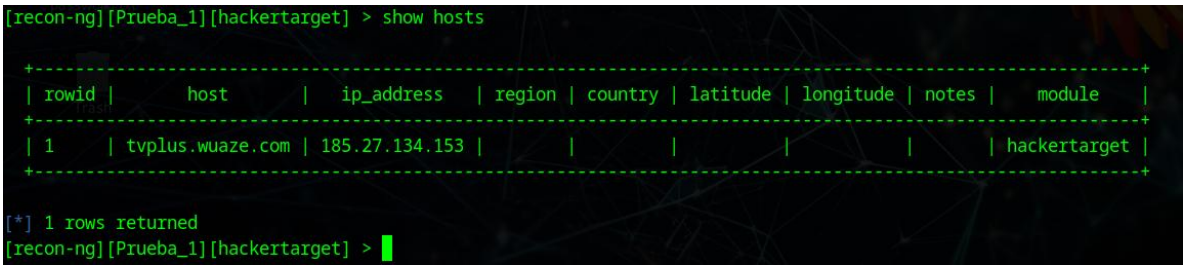


*Ilustración 27.- Resumen del módulo*

A continuación, se describen los diferentes ejercicios que se implementaron.

CASO 4 DE PRUEBAS: SOCIAL ENGINEERIE TOLKIT

En la ilustración 28 se observar el menú que nos da nuestra herramienta al abrirla en donde podemos seleccionar lo que queremos realizar y nos ofrece las siguientes opciones:

1.- Ataques Ingeniería Social

2.- Testeos de Penetración(Vía Rápida)

3.-Modulos de Terceros

4.- Actualizar el Kit de Ingeniería Social

5.- Actualizar la configuración de SET

6.- Ayuda, Créditos y Acerca de

99.- Salir del Kit de Herramientas de Ingeniería Social

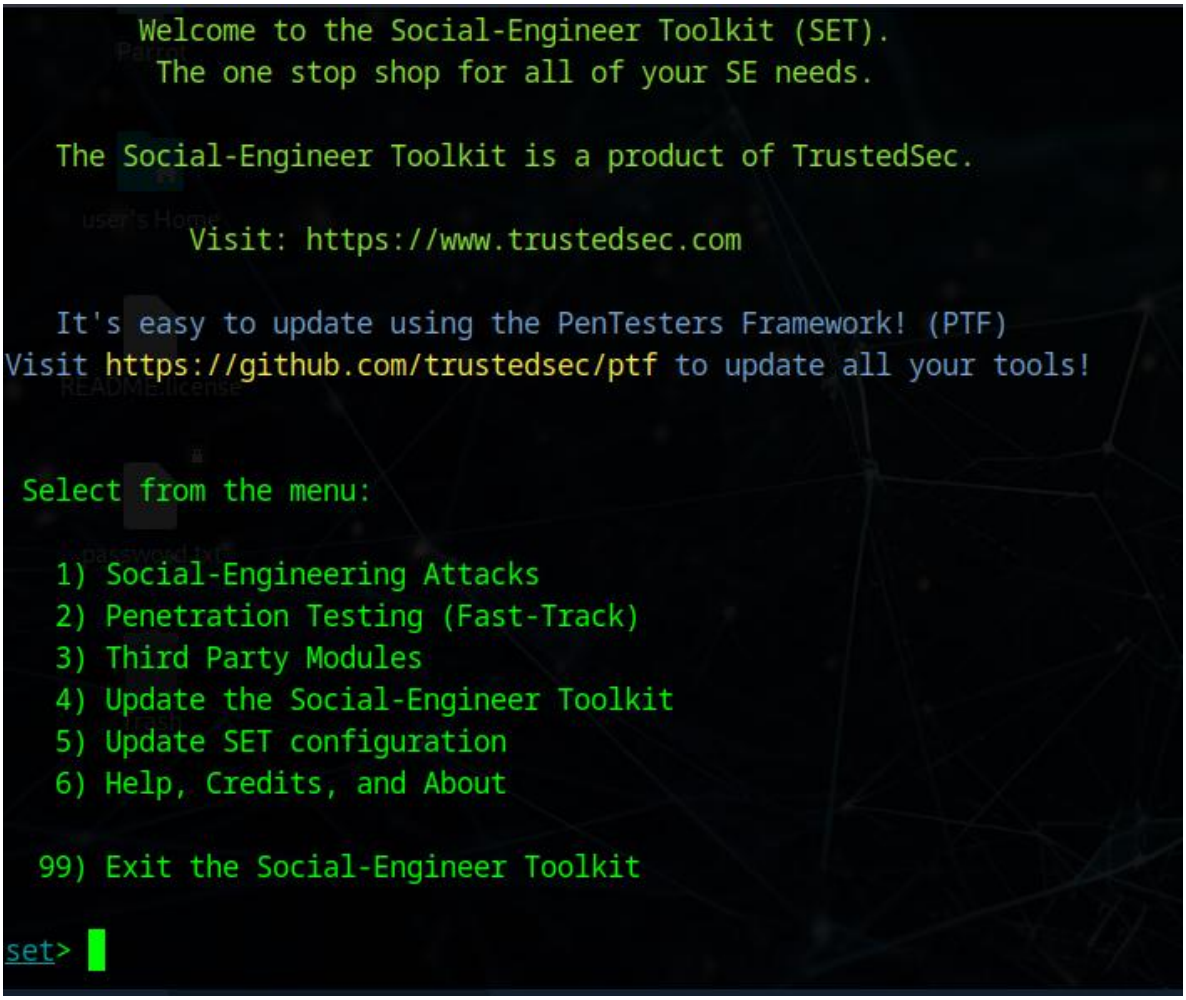


*Ilustración 28.- Menú de Social Engineer*

Se selecciona 1.- Social-Engineering Attacks y aparece el siguiente menú visible en la ilustración 29.

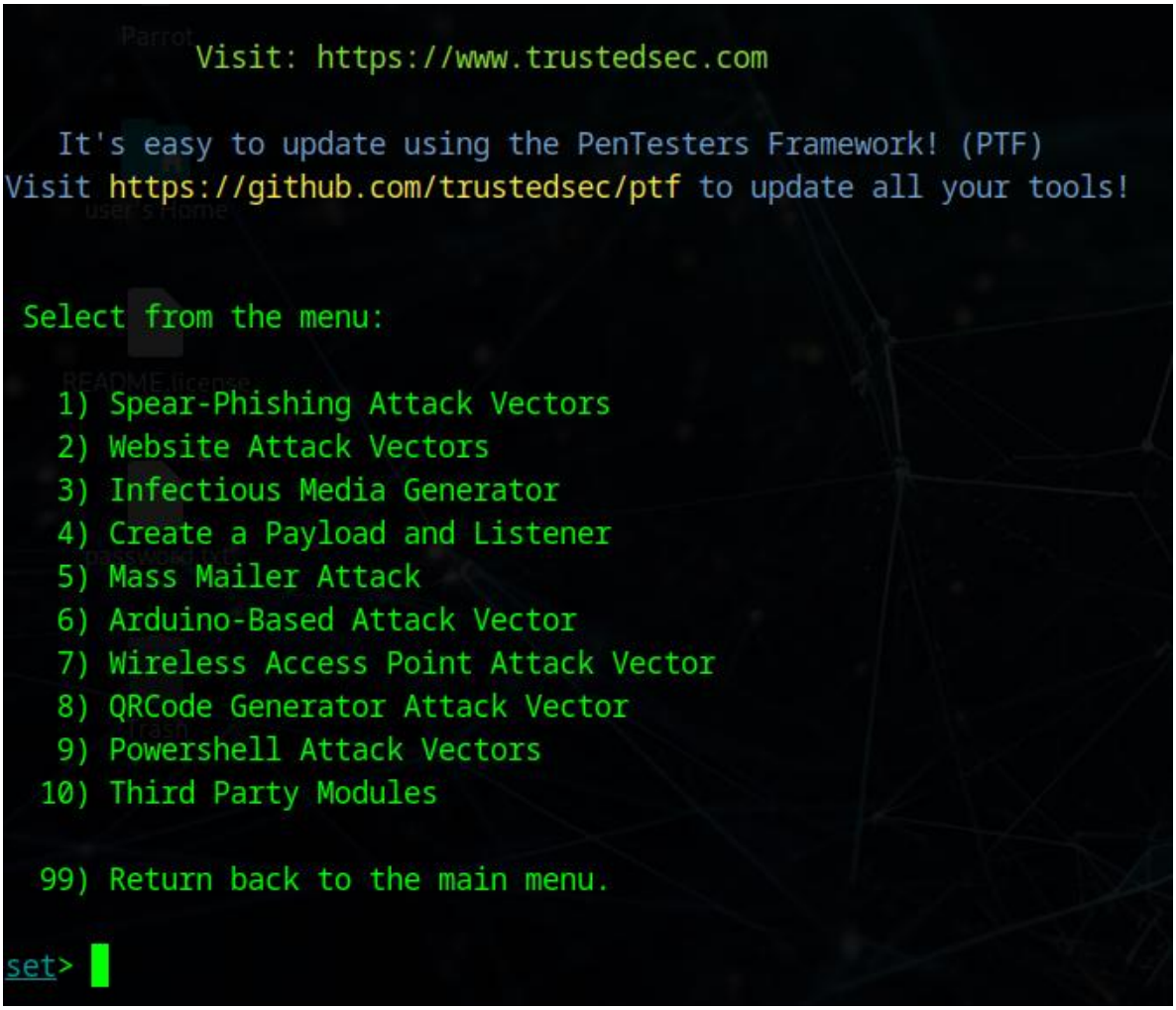


*Ilustración 29.- Menú de Social-Engineering Attack*

Se selecciona el 2.- *Website Attack Vectors* que arroja el siguiente menú y lo e observa en la ilustración 30.

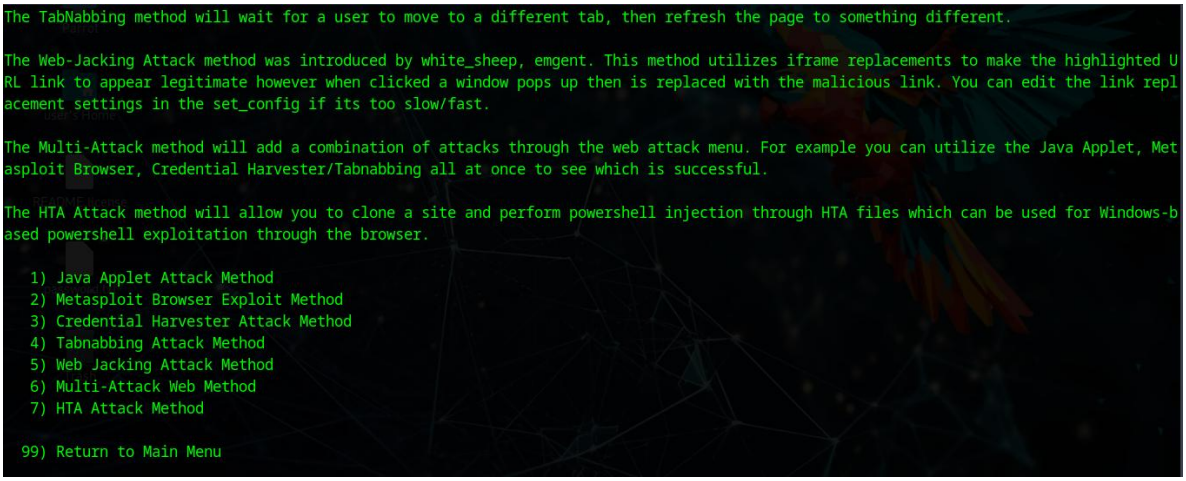


*Ilustración 30.- Menú de Website Attack Vectors*

En la ilustración 31 se observa que se seleccionó el 3.- *Credential Harvester Exploit Method* y se observa el menú con las opciones que se pueden usar.

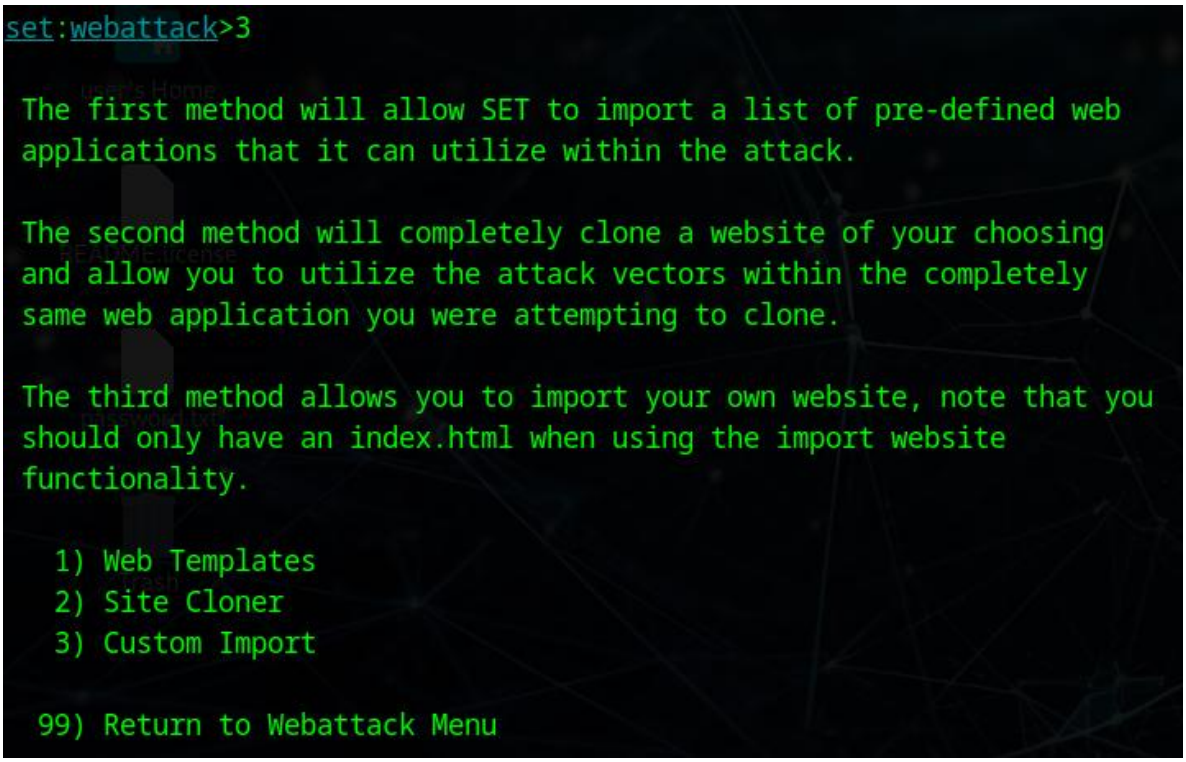


*Ilustración 31.- Menú de Credential Harvester Exploit Method*

En la Ilustración 32 se seleccionó el 2.- *Site Cloner* y se observa que da una descripción, también se observa que pide una dirección IP, esta es en donde se

alojará el sitio web clonado. Con esa misma IP se puede acceder en la web. Se elige la IP que nos da por defecto solo dando *enter*.

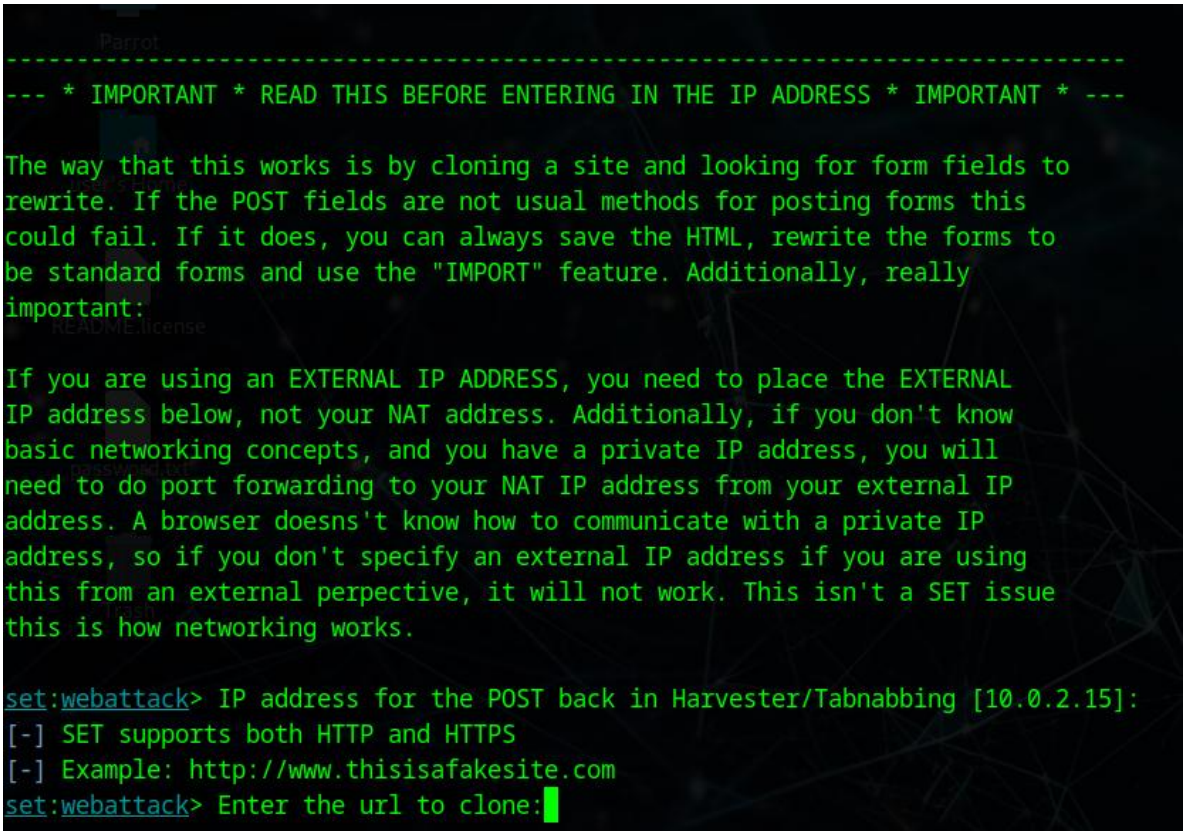


*Ilustración 32.- Información y selección de IP*

En la ilustración 34 se observa que una vez que se ingresa la URL del sitio a clonar y se ejecuta, permite acceder al sitio con la IP de la máquina virtual en este caso es 10.0.2.15


*Ilustración 34.- Resultado de que nos deja ingresar al sitio clonado*

En las ilustración 35  se observa que como resultado de la clonación de la página web se pudo recopilar el *username* de un usuario que intento iniciar sesión.

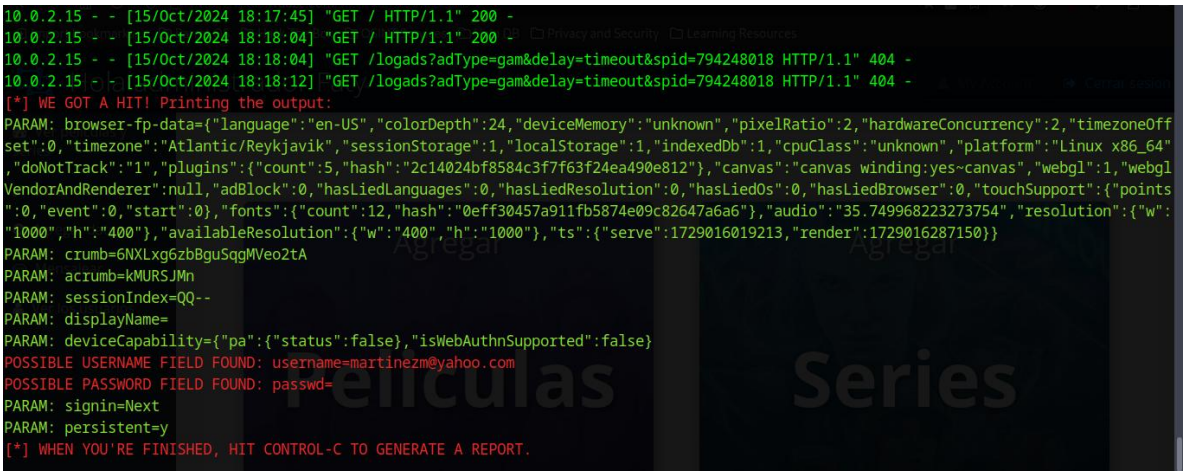


*Ilustración 35.- Resultado de hacer login en la página clonada*

En las ilustraciones 36 y 37 se observa como se ve la página de Yahoo! y la página web clonada, se puede observar que se hizo una copia tal cual el sitio que queríamos.

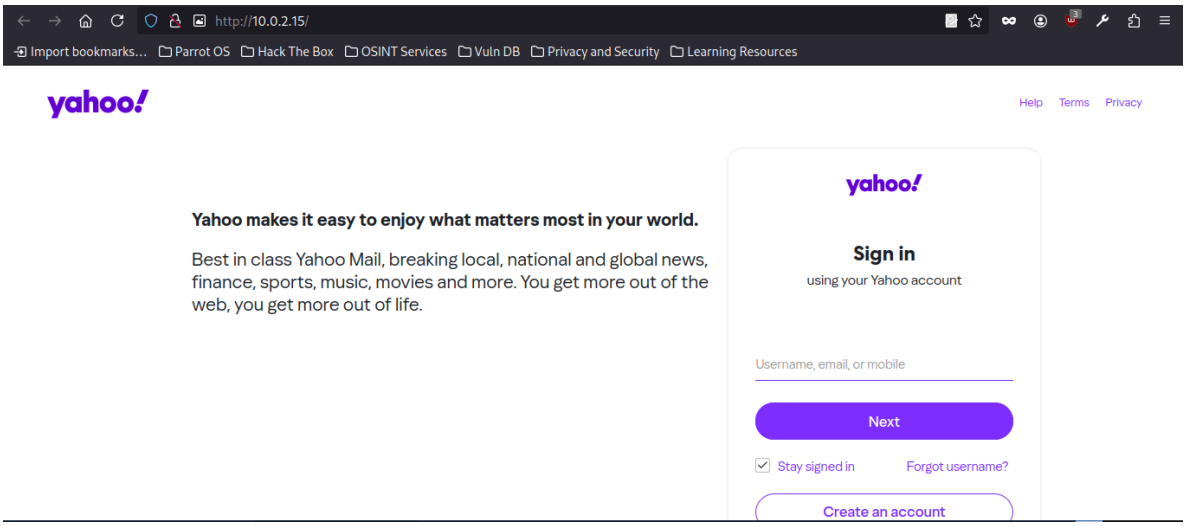


*Ilustración 36.- Pagina Clonada en el sitio local*

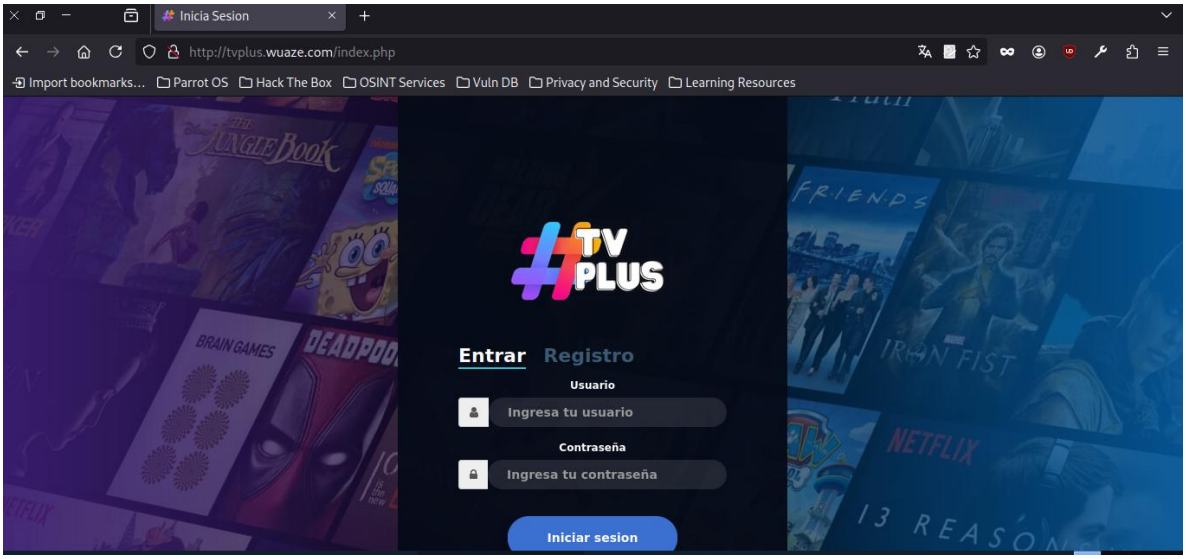


*Ilustración 37.- Pagina Clonada*

# Capítulo 4

# Estrategias de Mitigación y Protección de Datos

## 4.1 Propuesta General

En este punto vamos a dar solución a las problemáticas que se presentan durante las pruebas realizadas en las distintas herramientas a la página web y cabe destacar que es importante poner atención a cada una de estas soluciones ya que la página web se podría ver expuesta y se puede tener una fuga de información muy importante que puede hacer perder clientes o visitantes.

- ❖ Propuesta de recomendaciones a los resultados arrojados por la herramienta ZAP

- **Alta: Metadatos de la nube potencialmente expuestos**

  Solución: No confíe en ningún dato de usuario en las configuraciones de NGINX. En este caso, probablemente sea el uso de la variable $host que se establece desde el encabezado (header) 'Host' y puede estar controlado por un atacante.

- **Media: Encabezado de la política de seguridad de contenido (CSP) no configurado**

  Solución: Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy.

- **Media: Encabezado anti-clichacking faltante**

  Solución: Los navegadores web modernos admiten los encabezados HTTP Content-Security-Policy y X-Frame-Options. Asegúrese de que uno de ellos esté configurado en todas las páginas web devueltas por su sitio/aplicación.
  Si espera que la página esté enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET), querrá usar SAMEORIGIN; de lo contrario, si nunca espera que la página esté enmarcada, debe usar DENY. Alternativamente, considere implementar la directiva "frame-ancestros" de la política de seguridad de contenido.

- **Baja: Falta encabezado X-Content-Type-Options(2)**

  Solución: Asegúrese de que la aplicación o el servidor web configuren el encabezado Content-Type de forma adecuada y que configuren el

encabezado X-Content-Type-Options como 'nosniff' para todas las páginas web.

Si es posible, asegúrese de que el usuario final utilice un navegador web moderno y compatible con los estándares que no realice rastreo Extensiones Multipropósito de Correo de Internet (MIME) que la aplicación o el servidor web puedan indicarle que no realice rastreo MIME.

- **Información: Aplicación web moderna**
  Solución: Esta es una alerta informativa y por lo tanto no se requieren cambios.
- **Información: Agente de usuario Fuzzer (12)**
  Solución: Esta es una alerta informativa y por lo tanto no se requieren cambios.

❖ Propuesta de recomendaciones a los resultados de Recon-ng

Para solucionar hackertarget serevisa la seguridad del servidor, es decir se revisa que el servidor cuente todas las medidas de seguridad para que no puedan obtener su información, ya que hackertarget se encarga de recuperar información como longitud, latitud, altura y todo esto puede revelar la ubicación del servidor y que sea más fácil poder realizar ataques físicos o dirigidos de una forma más efectiva.

Entre las medidas de seguridad recomendadas para implementar en un servidor se encuentran:

- Llaves SSH: son un par de llaves criptográficas y se usan para autenticarse en el servidor SSH, es una alternativa para las contraseñas. Consiste en crear una llave publica puede ser compartida y una llave privada que la conserva el cliente.
- Firewalls o Cortafuegos: controlan los servicios que se encuentran expuestos en la red, esto significa que bloquean el acceso a ciertos puertos.
- VPN o redes privadas: Red Privada Virtual (VPN) estas son redes que están habilitadas únicamente para ciertos servidores o usuarios.

- Llaves públicas y certificados SSL/TLS: las llaves públicas o PKI nos ayuda a diseñar, crear, administrar y validar los certificados para identificar individuos y encripta la comunicación. Los certificados SSL o TLS se pueden usar para autentificar diferentes entidades., una vez que se hace la autenticación podemos usarlos para hacer una comunicación encriptada.
- Auditoria de Servicio: podemos usar este proceso para revisar que servicios están ejecutándose en los servidores, los puertos que usan y los protocolos que usan y de esta forma podemos complementar los parámetros de los cortafuegos.

❖ Propuesta de recomendaciones a los resultados de Social Engineer Toolkit.

Con esta herramienta se clona la página web y se pueden obtener las credenciales de algún administrador. Esto supone una falla grave para el sitio web y se puede solucionar con:

- Crea una infraestructura web robusta
- Monitoriza dominios con tu marca
- Rastrea potenciales clonaciones
- Implementa soluciones antifraude avanzadas
- Crea una red de enlaces internos
- Vigila dominios sospechosos

Estas herramientas pueden ser de gran ayuda para las empresas o personas que tienen un negocio propio y quieren tener su propia página web, ya que con la seguridad adecuada no podrán ser vulnerados por ciberdelincuentes que buscan robar información de personas o que tienen otros fines al atacar una pagina web en concreto.

Es importante poner atención a la ciberseguridad de las páginas web ya que actualmente muchas personas prefieren comprar en línea y es importante darles la mejor ciberseguridad para no perder clientes y sobre todo para proteger los datos sensibles de las personas.

# Conclusiones

Actualmente la ciberseguridad en México sigue siendo un tema que solicita atender acciones a los procesos que se llevan a cabo en cualquier empresa u organización. Aunque México cuenta con el equipo de Respuesta a Incidentes de Ciberseguridad (CIRT), aun hace falta implementar otros mecanismos que incluyen educación y buenas prácticas, ya que éste presenta limitaciones en cuanto al acceso a tecnología avanzada y profesionales capacitados. Esto da como resultado que sea difícil dar respuestas prontas y eficaces a los ataques. Otra limitante es que los atacantes son cada vez más sofisticados y más complicados de detectar y erradicar de los sistemas. En México, también existe una brecha en cuanto a la cultura de seguridad cibernética, es decir, la sociedad y las empresas no están educadas sobre los riesgos cibernéticos que existen en el mundo y como protegerse ante ellos.

México aún sigue un país importante en desarrollo en tema de transformación digital y ciberseguridad, este mes se lanzó el Plan Nacional de Ciberseguridad y Nube, en donde mencionan que se busca traer e implementar protocolos avanzados para poder resguardar la información pública y poder disminuir los riesgos de amenazas. Se contempla también el desarrollo de las capacidades locales en tema de tecnología de la información y ciberseguridad. Además de esto aún existe un problema inminente y son las leyes ya que la Ley de Protección de Datos esta rezagada y no se adapta a nuevas amenazas.

La finalidad de este trabajo fue mostrar cómo funcionan los ataques y como es que un ciberdelincuente puede atacar a una persona y a los sitios web que ha desarrollado, además, como aportación de este trabajo se brindan recomendaciones de como mitigar tres problemas importantes en el ámbito de la ciberseguridad y son:

- Realizar pruebas a nuestra página web en donde va a hacer ataques con arañas (spiders) y dar un reporte de todas las vulnerabilidades que encuentre en páginas web, esto ayuda a poder saber en qué partes de la página web

se puede recibir un ataque, además de que da consejos de cómo se puede solucionar ese problema.

- La clonación de una página web, como recomendación al usuario es que siempre revise la URL, que no se recargue la página principal o el inicio de sesión y en caso de que esto suceda cambiar contraseña de forma inmediata. A las empresas estar en constante búsqueda de sitios que tengan una URL parecida a la suya y pueda tener su página clonada y así evitar que sus clientes o usuarios puedan ser víctimas de un robo de credenciales.
- El poder obtener la ubicación exacta del host, como recomendación a las empresas es que cuando usen cualquier host revisen con detenimiento toda la seguridad que este ofrece y hagan uso del host de paga para mayor fortalecimiento de este.

Si no se siguen estas recomendaciones generales, la organización podría quedar vulnerable a ataques más precisos y dirigidos, lo que aumentaría el riesgo de sufrir una grave pérdida de información. La falta de medidas adecuadas de seguridad puede llevar a una exposición significativa de datos sensibles, lo cual no solo afecta la confianza y la reputación de la empresa, sino que también puede tener consecuencias legales y financieras serias. Implementar estas prácticas de seguridad no solo protege la información, sino que también brinda tranquilidad y seguridad a todos los que dependen de la integridad de los datos.

# Trabajo Futuro

Con la llegada de la computación cuántica, muchos de los paradigmas y arquitecturas que actualmente se implementan podrían quedar obsoletos, por lo que seguir en constante actualización es vital para mantener la seguridad de los datos. Así que la vigilancia, actualización y/o evolución del software es importante ya que los nuevos marcos que traerán estas computadoras va a cambiar la forma de protegernos ante cualquier ataque y como es que estos se actualizan y adaptan a estas nuevas tecnologías.

En cuanto a las herramientas empleadas en este trabajo se debe mantener vigilancia en su evolución, así como estar pendiente de nuevas estrategias y herramientas que permitan identificar y erradicar nuevas formas de ataques que seguramente surgirán más adelante con la llegada de nuevas tecnologías y herramientas para la creación y gestión de páginas web.

# Referencias Bibliográficas


Amazon Web Services. (s/f). *¿Que es la ciberseguridad?* https://aws.amazon.com/es/what-is/cybersecurity/.

BCS. (2023, noviembre 3). The biggest cyber attacks of 2023. *https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2023/*.

Belcic, I. (2023). ¿Qué es el malware y cómo protegerse de los ataques? ¿Qué es el malware y cómo protegerse de los ataques?; Avast. *https://www.avast.com/es-es/c-malware*.

Coronel Suárez, I., & Quirumbay Yagual, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE*. https://doi.org/10.26423/rctu.v9i2.672

Felipe Bueno Carranza. (2022). *Ataques a servidores web: estudio experimental de la capacidad de detección de SIDS*. Universidad de Sevilla.

Forbes Staff. (2022, septiembre 30). Hackeo masivo a Sedena evidencia vulnerabilidad de ciberseguridad; así fue el ataque. *https://forbes.com.mx/hackeo-masivo-a-sedena-evidencia-vulnerabilidad-de-ciberseguridad-asi-fue-el-ataque/*.

Free Software Foundation, Inc. (2014, agosto 16). *El estándar de ejecución de pruebas de penetración*. http://www.pentest-standard.org/index.php/Main_Page.

Hdco. (2014, septiembre 9). *Tipos de Ataques Mas Comunes A Sitios Web y Servidores*. https://blog.hostdime.com.co/tipos-de-ataques-mas-comunes-a-sitios-web-y-servidores/.

Herzog Pete. (2010). *OSSTMM.3*.

ISACA. (n.d.). ISACA. (2024). *COBIT | Control Objectives for Information Technologies | .* https://www.isaca.org/resources/cobit.

Kaspersky. (2024, enero 28). *Los Tres Ciberataques que han marcado el inicio del 2024*. https://www.kaspersky.es/about/press-releases/los-tres-ciberataques-que-han-marcado-el-inicio-de-2024.

Kennedy David. (s/f). *Information Security Made Simple SET User Manual Made for SET 6.0*. http://www.social-engineer.org

Laura, A., & Saucedo, H. (s/f). *Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web*.

Mesquida, A. L., Mas, A., Amengual, E., & Cabestrero, I. (2010). Sistema de Gestión Integrado según las normas ISO 9001. *REICIS*, *6*(3), 24–35.

MITRE ATT&CK®. (s/f). *Matrix-Enterprise* . https://attack.mitre.org/matrices/enterprise/.

Natali Valle. (2024, agosto 19). *Herramientas de ciberseguridad: tipos, métodos de evaluación y consejos de implementación*. https://blog.invgate.com/cybersecurity-tools.

NCSI. (s/f). *Clasificacion de Países en Ciberseguridad*. https://ncsi.ega.ee/ncsi-index/?order=rank.

OWASP. (2023a). *A04:2021 – Diseño Inseguro*. https://naramsim.github.io/Top10/es/A04_2021-Insecure_Design/.

OWASP. (2023b). *A10:2021 – Falsificación de Solicitudes del Lado del Servidor (SSRF)*. https://owasp.org/Top10/es/A10_2021-Server-Side_Request_Forgery_(SSRF)/.

Perez Herrero Luis. (2022). *Hacking Etico* (Perez Herrero Luis, Ed.; Ra-Ma 2022). https://books.google.com.mx/books?id=Ec64EAAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

SecurityScorecard. (s/f). *Vulnerabilidades por categoría* . https://www.cvedetails.com/vulnerabilities-by-types.php.

*The NIST Cybersecurity Framework (CSF) 2.0*. (2024). https://doi.org/10.6028/NIST.CSWP.29

*ZAP 2.15 Getting Started Guide*. (s/f). https://www.zaproxy.org/download/