BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN

IHCAS.web: IMPLEMENTACIÓN DE HERRAMIENTAS PARA EL CONTROL Y ANÁLISIS DE SEGURIDAD DE UNA PÁGINA WEB.

TESIS

QUE PARA OBTENER EL GRADO DE:

LIC. INGENIERIA EN CIENCIAS DE LA COMPUTACIÓN

PRESENTA:

SOSA CRUZ MARIA DE LOURDES

DIRECTOR DE TESIS

M.C. ANA CLAUDIA ZENTENO VÁZQUEZ

MARZO 2022 PUEBLA. PUE

AGRADECIMIENTOS

Me gustaría comenzar agradeciéndome a mí misma por la paciencia que me he tenido a lo largo de este camino. Seguido a esto me gustaría agradecer a mis papás ya que ambos pusieron de su parte lo que pudieron ofrecerme, mi madre por su parte con cariño y paciencia velando junto a mi cada noche que era necesaria y a mi padre por su apoyo, aunque lejano, pero siempre presente con sus consejos.

A mis abuelos que con fe me animaban a seguir a delante y no detenerme en este arduo camino. También a un ser que ya no se encuentra en este mundo pero que fue parte de mi inspiración para no rendirme, impulsándome con su ejemplo y demostrándome que se puede hacer lo que uno ama mientras aún se respire.

A mis hermanos que estuvieron ahí para alentarme.

A mis amigos que me animaron y compartieron de sus conocimientos para poder crecer juntos.

A una persona muy especial e importante hasta este momento en mi vida, quién me impulso a continuar cuando yo ya no creía poder continuar, y que me ha ayudado a crecer constantemente y mejorar.

Agradezco a Dios que a pesar de poner en duda mi fe hacia él, pues la ciencia te muestra otros caminos, siempre demostró estar ahí de alguna manera.

Y por su puesto a mi asesora que con paciencia y amor estuvo pendiente de mi proceso.

ÍNDICE

RESUMEN

“Aprender de un error cometido en el pasado da la oportunidad de mejorar el futuro”.

Recordando un poco el primer medio avanzado de comunicación fue el telégrafo, inventado en los años 40, su finalidad era emitir señales eléctricas las cuales viajaban por medio de cables denominados como Origen/Destino.

Para los años 80’s comenzó el desarrollo exponencial de INTERNET y gracias a este novedoso invento la humanidad comenzó a desarrollarse de una manera inimaginable, ayudando al crecimiento del mercado laboral y claro está, a la economía. Desde que todo esto surgió, la información también comenzó a ser más accesible para todo tipo de público, creando así un arma de doble filo ya que, si bien se sabe contar con datos a cualquier momento y desde cualquier lugar en la actualidad es exageradamente bueno, para mejorar procesos, rendimientos, costos, tiempos, etc. Pero también es sabido que no toda la información debe ser conocida y menos a todo el público, ya que puede ser perjudicial.

En esta investigación se tratará de uno de los temas más importantes de hoy en día, se trata de la seguridad de la información que viaja a través de internet por medio de las plataformas más utilizadas, las páginas web. Ya que éstas son un medio de comunicación que está en constante movimiento, éstas tienen distintos fines y usos, entre los objetivos que se tiene al hacer uso de estas plataformas es hacer llegar información entre dos extremos que no están en el mismo espacio y tiempo, logrando así una interacción.

El mundo está vasto de sistemas informáticos, los cuales en cada uno de sus centros alojan la información de miles de millones de usuarios, todos los datos almacenados van desde datos personales como: nombre, apellidos, dirección física, edad, etc. Y que pueden llegar a ser morales: como identidad empresarial, clientes, servicios, inventarios, etc. Pero no menos importante para ambos tipos de perfiles; cuentas de usuarios, contraseñas y correos electrónicos.

¿Por qué es importante este tema? Bien, desde que el comercio en la industria de las tecnologías ha crecido, la información se ha vuelto el **activo** más **importante**, con esto se quiere decir que si no es tratada con la suficiente responsabilidad y sobre todo si no se le da la importancia que merece se puede estar en riesgo de cualquier tipo. Algunos ejemplos de esto son; robo, modificación o eliminación de información, además de infiltración en los sistemas, denegación de servicios (DNS), etc.

Actualmente se han presentado casos de grandes compañías que han sido expuestas y robadas, algunas por no tener las medidas adecuadas y muchas otras han sido "vencidas" en el ámbito de protección. El robo de información no es algo que se deba tomar a la ligera, conlleva años de trabajo y esfuerzo de muchas organizaciones que han sabido crecer, secretos importantes de marketing etc. Se ha llegado al grado más grave que ahora es nombrado como "Secuestro de información" que más se espera si la finalidad de crecer tecnológicamente era reducir tiempos y agilizar procesos.

El objetivo principal de este estudio es presentar herramientas de análisis de vulnerabilidades en los sitios web, para así lograr una concientización empresarial, social y académica para tomar medidas de acción que permitan mejorar los sistemas con los que se cuente y en caso de no tener un plan de acción, crearlo.

1. INTRODUCCIÓN

“El ser humano es precavido por naturaleza ya que desde su creación por mera intuición ha tenido que adaptarse a cambios constantes de su entorno, y con ello, incluida su seguridad”

A lo largo de la historia la humanidad ha ido evolucionando de una manera impresionante, la adquisición de algún tipo de lenguaje fue el principio de la necesidad de comunicación y entendimiento con otros seres de la misma especie. Trayendo consigo una necesidad de expandirla, pero al mismo tiempo de protegerla.

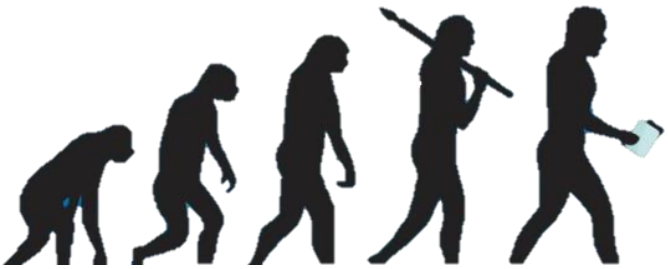


FIG 1. REPRESENTACIÓN DE LA EVOLUCIÓN DEL HOMBRE ANTE LA TECNOLOGÍA

En la figura 1 se puede observar el proceso evolutivo del hombre, pasando de ser una criatura cavernaria a un hombre enteramente tecnológico. El tiempo que se estima de transición es de entre 200.000 y 150.000 años desde su primera aparición en África, lugar donde se cree que hizo su primera aparición el hombre moderno. (Aleph, 2021)

1.1 EL VALOR DE LA INFORMACIÓN A TRAVÉS DE LA HISTORIA.

Hace muchos años existieron reinos en distintos lugares del mundo; cada uno de ellos tenía necesidades específicas y diferentes, pero la principal consistía en obtener el poder de toda tierra a como diera lugar. Esto origino enemistades entre distintos gobernantes

llevando consigo a guerras tratando de mostrar la fuerza y la debilidad (vulnerabilidad) el uno del otro.

Una de las probables razones principales que originaban las peleas fue la curiosidad e inseguridad, pues al querer saber qué pensaba o planeaba el otro, nacía el **riesgo** de exposición de información muy sensible, pero muy oportuna. Uno de los riesgos más grandes que existió en aquel tiempo fue la exposición de los planos de un palacio, pues con estos era más fácil encontrar túneles secretos o simplemente conocer la cantidad de guardias, sus posiciones o las zonas aisladas y solitarias más menos concurridas por la monarquía, etc. Expuesta y filtrada la información de la forma de intercomunicación constante de las actividades de la monarquía, eran el mejor armamento que se podía tener. Con esto se quiere decir que entre gobernantes deseaban conocer las técnicas y/o tácticas que tenían otros y a su vez conocer las debilidades de estos. Al lograr obtener la información del rival se podía saber cómo transgredir su reino y hacer el mayor número de atrocidades posible, un ejemplo sencillo podría ser que con la información obtenida que ya se mencionó anteriormente es, al conocer los planos de la estructura del reino cualquier persona podía entrar a tierras en las cuales no tenía autorización de ingresar y robar o atacar por sorpresa. (Singh, 2001)

Una forma de obtener información consistía en filtrar personal de cualquier área en un reino, dicho infiltrado (traidor) proporcionaba todos los datos necesarios, por un intercambio económico, trueques e incluso por la mera protección de sus familiares (eran amenazados).

FIG 2. EJEMPLO DE REUNIÓN CON POSIBLES INFILTRADOS.

En la figura 2 se muestra una reunión en la era medieval, en donde se puede ver a miembros de la realeza y algunos empleados. El objetivo de esta ilustración es mostrar como posiblemente lucían las reuniones que tenían como finalidad llegar a acuerdos importantes entre los miembros reunidos, además de dar un claro ejemplo que al estar múltiples personas incluida la servidumbre, la fuga se información podía llegar a ser grave.

Antes de contar con internet y un PDA (*Personal Digital Assistant* por sus siglas en inglés, Asistente Digital Personal) en la palma de la mano, existieron otros medios de comunicación como; la mensajería instantánea, los métodos conocidos y utilizados en ese entonces eran variados; cartas postales, mensajeros, palomas, etc. Algunas otras técnicas para poder obtener la información necesaria, en la actualidad podría parecer algo exagerado, pero para aquellos tiempos era la mejor manera, además de que se desarrollaba una habilidad que hoy en día no se practica a menudo, “la paciencia”. A continuación (J.M. Sadurní, 2020), algunos de los acontecimientos que durante algún periodo de tiempo fueron utilizados para poder mantener la (Singh, 2001) información confidencial:

- **Rapar a una persona:** Aunque puede parecer algo extremo y exagerado, esta fue una de las técnicas más utilizadas por siglos pasados para mantener un

mensaje oculto y poderlo "transportar" además de no levantar sospechas de terceros. La técnica consiste en, rapar la cabeza de la persona portadora del mensaje, posterior a esto se escribía un mensaje con tinta especial sobre la piel lisa de la cabeza, luego de esto se esperaba a que el cabello creciera para que dicha persona (mensajero) pudiese llevar a cabo su tarea, y llegar con un receptor (persona que recibe el mensaje) y hacer la entrega, sin correr el riesgo de que el mensaje cayera en manos inapropiadas. Una vez que el mensaje estuviese en su destino se procedía a rapar su cabellera nuevamente para poder leer el mensaje.

- **Escribir el mensaje en un cinto (cinturón)**: Para esta técnica lo principal era tener un acuerdo entre emisor y receptor, en cuestión de contar con los materiales apropiados y con las mismas características para poder redactar y leer los mensajes, es decir, para poder llevar a cabo esta actividad se necesitaba un palo de cierto grosor y forma, un cinturón y tinta para piel o que se adhiriera al material del mismo. Una vez teniendo los materiales adecuados, se procede (por parte de la persona que enviará el mensaje) a enredar el cinturón en el palo y luego escribir el mensaje, una vez seco se lo coloca la persona de manera normal. Posteriormente una vez que el mensaje estuviera en su destino, la persona a leer el mensaje debía enrollar el cinturón en el palo para poder leer el contenido.
- **Escribir un mensaje en un huevo cocido**: Este proceso es un tanto extraño, pero para esta técnica se necesitaba tener conocimiento de las propiedades de los materiales utilizados. Para este método se debía escribir en un huevo con una tinta especial, compuesta por alumbre y vinagre, en la cáscara el mensaje y posteriormente exponerlo al calor para descubrir lo escrito. Esto era posible

debido a que la combinación de dicha solución hacia una tinta que al secarse era invisible y con la exposición al fuego tornaba un color marrón.

- Uno de los medios utilizados en el México antiguo, fueron los **Painanis**, que eran personas encargadas de hacer entregas de mensajes recorriendo kilómetros corriendo.

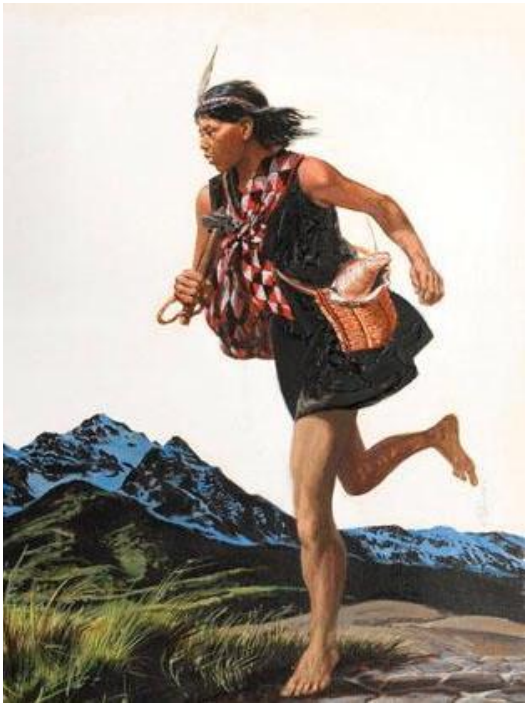


FIG 3. ALUSIÓN A UN PAINANI

En la figura 3 se muestra un hombre que en el México de aquel tiempo era llamado Painani, denominación que proviene del Náhuatl que significa **corre veloz**. Se le denominaba de esta forma a las personas que hacían entrega de noticias de guerra o paz. Estas personas recorrían grandes distancias para hacer entrega de sus mensajes. (Ayala, 2019)

Como se puede ver, la información ha sido orientada y manejada con distintos fines, en su mayoría para beneficio propio. Es importante remarcar épocas pasadas ya que de ahí emerge la necesidad de ir incrementando las técnicas de protección de cualquier tipo

de información y en cualquier contexto, sea significativa o no. Es increíble que en aquellas épocas a pesar de que en esos momentos no se contaba con tecnología tan avanzada como hoy en día, existieron métodos o mañas para poder estar a salvo (por decirlo de alguna manera). A pesar de que las técnicas que se hablaron antes daban resultados, el tiempo era un factor que se debía tomar en cuanta, por consiguiente, surge la necesidad de intercambiar información de una manera instantánea pero no solo eso, sino que, también la de protegerla aún más ya que en el transcurso del tiempo se ha ido evolucionando en esta rama y la información ha ido incrementando en sus diferentes contextos.

1.2 HISTORIA DE INTERNET

Internet ha sido una base importante para la mensajería instantánea y ha mantenido la comunicación alrededor del mundo, por ello es importante hacer un énfasis en su evolución, pero antes de ello, se define internet como la red de redes. Pero ¿Qué es una red? bien, una red es la conexión de múltiples ordenadores entre sí los cuales están compartiendo información simultánea en un mismo tiempo. (Hallberg, 2007)

FIG 4. INTERNET

En la figura 4 se muestra la interconexión que existe hoy en día a nivel mundial, mostrando todos los tipos de dispositivos desde los que se tiene acceso a internet. En los siguientes puntos se pretende mostrar la cronología del crecimiento de Internet a lo largo del tiempo:

- 1936, Konrad Zuse crea la primera computadora programable de la historia, calculadora mecánica binaria. (Xataka, s.f.)
- 1943 John William Mauchly y John Presper Eckert, crean la ENIAC *(Electronic Numerical Integrator and Computer),* aunque este equipo tenía un propósito de carácter militar, su principal objetivo se encontraba dentro del área de la balística, durante la segunda guerra mundial su objetivo fue desencriptar código alemán. (Valencia, 2011)
- 1960 ARPA (*Advanced Research Projects Agency-Energy*) inicia un proyecto en donde a las computadoras se les da un uso orientado dentro del campo de la investigación, a este proyecto se le llamó ARPANET. Consistía en la conexión de ordenadores, en 1971 ya se tenían conectados aproximadamente 23 puntos (ciudades) en todo Estados Unidos.

Después surgieron algunos otros proyectos que dieron inicio a INTERNET, dichos proyectos fueron:

- Telnet en 1974, la cual fue una versión comercial del proyecto ARPANET. (futuro, s.f.)
- Usenet en 1979, un sistema cuyo objetivo se centraba en el e-mail, hoy en día utilizado. (futuro, s.f.)

- Bitnet en 1981, este proyecto conectaba universidades estadounidenses utilizando sistemas IBM. (futuro, s.f.)
- Eunet en 1982, este proyecto unió a tres países en conexión, Reino unido, Escandinavia y Holanda. (futuro, s.f.)

Gracias a la creación de estos proyectos se dio pie a una nueva era, la cual en ese entonces fue muy criticada ya que en aquellos días se decía que era la herramienta del futuro, es decir, que todo el mundo estaría conectado. Aunque no se tenía certeza de este suceso fuera así, con el paso de los años y gracias a los antecedentes que hoy en día se tiene del INTERNET y el acceso a una gran masa de información que años atrás era inimaginable tener al alcance de la mano, a cualquier hora y desde cualquier sitio en el mundo.

Con la llegada de esta poderosa herramienta se comparte en la actualidad un gran tráfico de información día a día, desde foros web hasta clases en línea, mensajes instantáneos, correos etc. Pese a que hoy en día la información se obtiene de manera instantánea y aparentemente “segura”, esto sigue siendo un tema con un valor altamente considerable y cuestionable, ya que dicha experiencia a pesar de haber disminuido el tiempo de entrega y haber aumentado la instantaneidad, trajo consigo nuevamente al robo e infiltración de información así como al desarrollo de muchas nuevas formas de protección que continúan en desarrollo, debido a que la seguridad no es suficiente y nunca lo será ya que nunca se está 100% seguro. En la figura 5 se muestra a un usuario que tiene inseguridad de navegar pues no sabe si la información es certera.

FIG 5. ¿SEGURIDAD?

Nadie se libra de estar en la zona de vulnerabilidad, desde un simple usuario hasta el empresario más poderoso ha experimentado actividad sospechosa o inclusive haber sido saboteado. Un dato curioso es que en pleno siglo XXI la tecnología se ha apoderado de la humanidad y ha traído consigo muchos beneficios, pero también muchos problemas, y eso es bueno porque siempre hay algo en que estar ocupados. Pero las complicaciones no vienen en tener un problema y tener una solución; sino, en trabajar en ello. Pues el tiempo que transcurre en resolver determinado problema es el factor más importante y por el que se apuesta absolutamente todo, debido a que la velocidad de la comunicación actualmente ha crecido de una manera inimaginable, tanto que para los que consideran como “un minuto no es nada” para otros la mitad de ese tiempo puede significar todo. (Canal, 2006) ¿Por qué?, bien pues un atacante utiliza ese tiempo y lo invierte de la mejor manera posible, aprovechándolo al máximo, nunca se sabe todas las cuentas bancarias que podrían quedarse sin fondos en ese periodo de tiempo, además de toda la cantidad de información que puede ser robada con fines de lucro o maliciosos.

Este tema es de vital importancia para empresas y personas físicas, nadie escapa de un ataque, las redes están en todos lados. Un simple mensaje de texto puede estar

viajando a Italia para poder ser recibido en tu mismo país, por lo tanto, con los conocimientos necesarios y con la gente adecuada se puede saber el contenido de ese mensaje. Las personas físicas a pesar de no contar con los recursos económicos "suficientes" o una posición social alta, corren el riesgo de ser atacados de distintas maneras. Dichas amenazas pueden ser; extorsión telefónica, correos falsos afectando empleos, premios e incluso de corroboración de cuentas, y aun siendo empleados pueden ser flancos de acceso para las personas que se dedican a infiltrarse dentro de una compañía, estos y muchos otros métodos son parte de lo que se conoce como ingeniería social. (Canal, 2006)

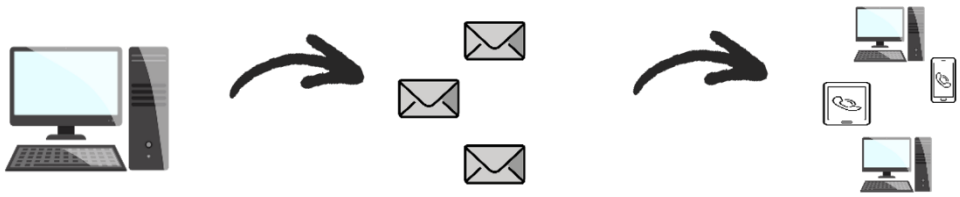


FIG 6. ENVÍO DE MENSAJES A TRAVES DE INTERNET

En la figura 6 se ilustra el envío de un mensaje (paquete) teniendo un origen (salida) y un destino (llegada), según el protocolo TCP/IP, al ser enviado un paquete, este es fragmentado durante su trayecto para hacer una entrega eficiente, algo que cabe mencionar es que cada fragmento lleva consigo información que le permitirá llegar con éxito a su destino. (HALLBERG, 2007)

Una compañía sea pequeña, mediana o grande está en riesgo constante de ser atacada, pero los **delincuentes cibernéticos** (de los que hablaremos más adelante) se enfocan con más frecuencia en las pequeñas empresas y el motivo principal es que al ser pequeñas no cuentan con los recursos suficientes para contratar un sistema de seguridad o contar con el personal adecuado para protegerse, pero esto no quiere decir

que las grandes empresas no son atacadas ya que incluso los gobiernos lo han sido. Para enfocar más el tema, se debe tener en claro el significado de seguridad, ya que no para todos, el significado es el mismo y sobre todo no tiene el mismo valor.

1.3 CONCEPTOS DE SEGURIDAD

Con el fin de enfatizar más en el tema de seguridad se plantean los siguientes conceptos para poder hacer más digerible la información al lector. Cabe mencionar que se darán ejemplos en caso de que sea necesario para ser más explícitos en el contexto y que quede claro el concepto que se pretende explicar.

- **Seguridad:** ¿Qué es la seguridad? ¿A qué se refiere? "E*s un servicio encargado de la seguridad de una persona, empresa y/o un edificio etc.*" (RAE, 2021) Sin embargo, este término es más general ya que la seguridad engloba miles de prioridades en todos y cada uno de los aspectos de la vida cotidiana de un individuo. La seguridad puede variar entre, tener seguridad en un empleo e incluso la escuela, así como de gozar de salud médica, tener una cuenta bancaria segura, finanzas protegidas, datos privados y entre muchos otros, todo depende del contexto, la situación y sobre todo de sus necesidades. Por tanto, la seguridad puede ser definida como **la ausencia del peligro, disminuir el riesgo de perder un bien**, o la **ausencia de errores** (Salazar, 2019), esto como un término neutro y general de todos los contextos posibles y existentes. Este término ha sido vivido por millones de años, pero no se tenía una certeza concreta de la definición y la importancia de esta. Como ya se mencionó antes, el ser humano por naturaleza es precavido y provee por respaldar y garantizar su existencia, así como de proteger lo que considera suyo.

- **Confidencialidad:** Impide la divulgación de información a individuos, entidades o procesos no autorizados. Es decir, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización. (SGSI, 2018)
- **Integridad:** Busca mantener los datos libres de modificaciones no autorizadas, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados. (Veiga)
- **Disponibilidad:** Es el acceso a la información y a los sistemas, por personas autorizadas en el momento que así lo requieran. (SGSI, 2018)

Las siguientes definiciones hacen un hincapié, enmarcando el correcto significado de las definiciones establecidas en este documento de investigación, ya que a lo largo de los años se les ha destinado de una manera errónea y se ha satanizado en cierto grado cada uno, y tener claros los conceptos ayudará a comprender mejor el desarrollo de este trabajo.

- **Vulnerabilidad:** Hace referencia a los puntos débiles o puntos rotos de un sistema, en los cuales este no podrá mantener una defensa ante un ataque. (Canal, 2006)
- **Riesgo:** Se refiere a la exposición a sufrir un ataque o ser dañado. (Canal, 2006)
- **Atacante:** Persona o grupo de personas que intentan aprovechar las vulnerabilidades para obtener una ganancia personal o financiera en todo; tarjetas de crédito, diseños de producto, específicamente todo aquello que le aporte un valor directa o indirectamente.
- **Hacker:** Es una persona con un profundo interés en el área técnica y en el cómo funcionan las cosas. Aunque existen distintas clasificaciones de hackers este

trabajo de tesis tiene como objetivo principal tomar como referencia el trabajo de los hackers White Hat (sombrero blanco). (Canal, 2006)

Algunos de los intereses de los White Hat son:

- Aprender constantemente y ser reconocidos por personas con intereses similares. a los de ellos mismos.
- Buscan únicamente un beneficio social.
- No pretenden causar daño ni obtener beneficios de otros (de la mala manera).
- Se enfocan en encontrar puntos vulnerables.
- Dan soporte a las fallas en los sistemas.

- **Hacking Ético:** Tipo de estrategia mediante la cual se realizan ataques para poder localizar vulnerabilidades dentro del sistema, las personas que realizan estos ataques (simulacro) deben ser personas que cuenten con los conocimientos para infiltrarse en el sistema. Esta tarea la realiza un *Hacker ético*, pero para poder decir que lo es debe contar con las siguientes cualidades:
  - Realiza su trabajo como si fuera para él, es decir, de la mejor manera posible.
  - Sus reportes son excelentes.
  - El valor de su trabajo debe ser justo.
  - Es una tumba, es decir, respeta los secretos que se le confíen.
  - Jamás habla mal de su equipo de trabajo.
  - No impone o manipula.
  - No acepta ninguna clase de soborno.
  - No altera resultados o análisis.

- Las tareas que asigna deben ser dirigidas al personal que esté altamente capacitado.
- Dice la verdad con respecto a lo que puede o no realizar.
- Debe ser responsable.
- Tiene control sobre sus recursos y los administra adecuadamente. (Canal, 2006)

- **Cracker:** Son personas que pueden tener el mismo o mayor nivel de conocimientos que un hacker, pero lo que marca la diferencia entre ellos son los intereses que estos tienen como:
  - Actúan en beneficio propio, no les interesa el bienestar social.
  - No les importa que existan consecuencias.
  - Pueden dañar la integridad de terceros. (Canal, 2006)
  - **Auditor:** Persona encargada de comprobar de manera independiente un sistema, esta persona es especialista en determinado tema y por ello puede dar observaciones claras del panorama real que se está viviendo.
    - Cumple regulaciones.
    - Cumple estándares p.e ISO 90000 (Canal, 2006).
  - **Cliente:** Destinatario del producto o servicio ofrecido o contratado. (Canal, 2006)
  - **Suministrador:** Persona que proporciona suministros que se precisan para realizar las operaciones dentro del sistema. (Canal, 2006)

- **Malware:** Código malicioso (programas que dañan el sistema). Generalmente estas amenazas son detectadas por los antivirus. Algunos ejemplos de ellos son:
  - Gusanos (*worms*).
  - *Spyware.*
  - Troyanos.
  - Virus.
  - Scripts malintencionados. (Canal, 2006).
- **Exploit**: 0 exploit es un programa de prueba de concepto que puede estar en código fuente para compilar (fuente .C) o formato binario tipo .exe, sirve para aprovechar o demostrar una vulnerabilidad en aplicación y puede estar escrita en varios lenguajes de programación. (Canal, 2006)

1.4 TIPOS DE ATACANTES.

Anteriormente se ha mencionado el término hacker, pero hay diversos enfoques y distintas prácticas para las personas que se enfocan en esta labor. Existe en el campo de la administración un término denominado sombreros, el cual hace referencia al tipo de personalidad que adquiere un individuo dentro de una organización, esta personalidad describe las acciones que realiza para aportar o perjudicar a una empresa o grupo de personas en el cual se encuentra emergido. Y ese término también es conocido para la parte de la informática, los famosos "*Colors Hats*", en la figura 7 se hace alusión de los tres tipos de hacker más comunes en el mercado.

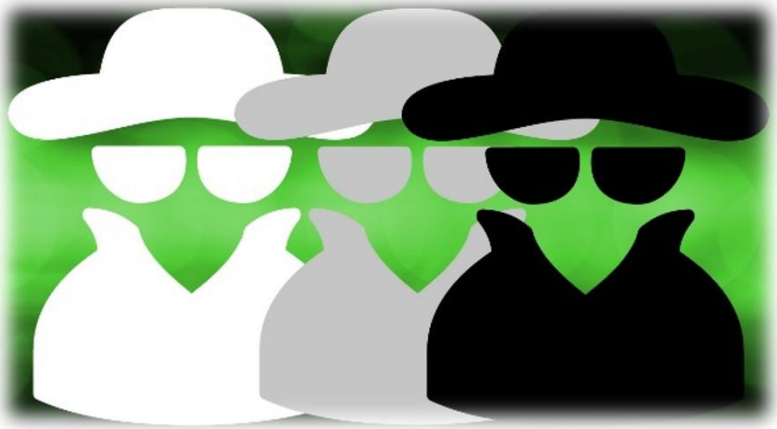


FIG 7. TIPOS DE HACKER

A continuación, se hace una breve descripción de cada uno de ellos y haciendo énfasis en la clasificación de los hackers.

- **Hacker de sombrero blanco (*White Hat*):** Utilizan sus habilidades de programación con buenas intenciones, éticas y legales. Pueden realizar pruebas de penetración de redes con la finalidad de comprometer sistemas y las redes haciendo uso de sus habilidades y conocimientos de sistemas de seguridad informática para descubrir las vulnerabilidades en la seguridad que hay en este mismo. Una vez detectadas todas las vulnerabilidades, se informa a los desarrolladores para que las corrijan antes de que puedan ser amenazadas. En algunas ocasiones las organizaciones otorgan premios o cierto tipo de recompensas a este tipo de hackers cuando dan un informe por alguna vulnerabilidad.
- **Hacker de sombrero gris (*Gray Hat*):** Estas personas cometen delitos y hacen cosas poco éticas, pero no para beneficio personal, más bien para causar daño. Un *Gray Hat* divulga la información que obtuvo acerca de las vulnerabilidades que encontró en un sistema informático dentro de una organización, posteriormente

puede darle la información después de haber puesto en peligro su propia red. Lo cual puede permitir solucionar los problemas, es muy parecido a una extorsión. (Canal, 2006)

- **Hackers de sombrero negro (*Black Hat*):** Son personas con casi nada de ética, que violan la seguridad de un sistema informático para beneficio propio, por motivos maliciosos, venganza o por contrato. Estos delincuentes atacan las vulnerabilidades para comprometer por completo un sistema. (Canal, 2006)
- ***Script Kiddie*:** Este término es utilizado para referirse a personas inexpertas (especialmente para jóvenes novatos) que no cuentan con las habilidades suficientes para escribir un script o que utilizan algunos ya publicados en la red e inclusive algunas otras técnicas con la única finalidad de impresionar a sus amigos. (CICESE, 2017)

1.5 TIPOS DE IDENTIDAD DE UN USUARIO

Una persona o un grupo de personas (llámese organización) en el mundo actual cuenta con dos tipos de identidad con los cuales se hace presente en un tiempo y espacio o bien dentro de una realidad. Estos son denominados **en línea** y **fuera de línea**, pero ¿qué quiere decir esto? Bueno dentro de internet se debe tener un perfil con el cual otros usuarios (personas) podrán encontrar y con el que se podrá estar en interacción con ellos, es decir se ocupa un espacio y se ocupa una identidad dentro del mundo de internet, no importa la plataforma que se use incluyendo; Facebook, Instagram, Telegram, etc. Lo único importante es estar presente dentro de este entorno, buscar y

ser encontrados. A continuación, se presentan las características de cada una de las identidades. (Canal, 2006)

El **usuario en línea** cuenta con:

- Cuenta de correo.
- Redes sociales.
- NickNames (sobre nombres)
- No hay información personal.
- etc.

El **usuario fuera de línea** cuenta con:

- Dirección física (donde vive).
- Nombre Real.
- Edad.
- Números de contacto.
- Cuentas bancarias.
- etc.

1.6 TIPOS DE PROTECCIÓN DE LA INFORMACIÓN.

Para poder proteger la información se debe tener en cuenta que la seguridad de la información durante años ha sido muy importante, pero a partir de marzo del año 2020 incrementó su valor gracias al trabajo remoto, debido a la pandemia ocurrida en el mismo año, dependencias gubernamentales, empresas públicas y privadas, así como instituciones educativas entre algunos otros sectores e incluso personas físicas migraron al modelo "**Home Office**". Cabe mencionar que este modelo no estaba en consideración de ser utilizado por algunas de ellas, ya que no se tenía la confianza o seguridad del

rendimiento de los empleados y estudiantes. Y aunque en algunos países de primer mundo ya se comenzaba a implementar este modelo, tras este acontecimiento la migración fue tan rápida que causo estrés por falta de preparación para este tipo de desarrollo pues tomando en consideración que la información puede ser manipulada de diversas maneras y se le puede ser tratada en múltiples direcciones para el beneficio propio de quien la obtenga, ya sea bueno o malo.

Algunas de las **consecuencias** de que la información (Canal, 2006) esté en mentes/manos equivocadas son las siguientes:

- **Divulgación:** Dependiendo de quien se trate y de qué tipo de datos se tengan, esta puede ser exhibida con fines de dar a conocer: vulnerabilidades, secretos empresariales, datos de personal, cuentas bancarias, claves de accesos, etc.
- **Mal utilizada:** en relación con el punto anterior, si un cracker tuviera en su poder cuentas bancarias, este podría hacer uso de ellas para pagarse lujos o realizar transferencias.
- **Robada:** al ser robada se le puede dar diversos usos, entre ellos el famoso secuestro de información, con el cual se llegan a pedir rescates a cambio de liberar la información.
- **Borrada:** Al ser eliminada la información, ya no se puede tener acceso a ella a menos que la organización o la persona atacada cuente con respaldos de esta, y es por esto que la empresa, persona o entidad debe contar con una estrategia de respaldos de su información, para poder garantizar su disponibilidad e integridad.
- **Saboteada:** en este punto se puede tener grandes problemas al igual que con los puntos anteriores, ya que al modificar o utilizar esta información contra los dueños

de las empresas, se pueden crear malentendidos o incluso se puede llegar a ganar unas elecciones presidenciales, ya que se manipula la información a beneficio propio.

Los puntos anteriores muestran algunos de los usos ventajosos que se le puede dar a la información afectando así su disponibilidad y poniéndola en riesgo.

La información se **clasifica de tres maneras**, las cuales ayudan a apreciar su valor verdadero.

- **Crítica:** Es indispensable para la operación de una empresa.
- **Valiosa:** Es un activo de la organización, por ende, es lo más valioso.
- **Sensible:** Sólo la debe conocer el personal indicado y autorizado.

Dentro de una empresa/organización se debe tener en cuenta, que al ser el activo más valioso para ellos deben contar con políticas de seguridad para la información, un control sobre ella, monitoreo, y programas que ayuden a la gestión de esta. Además de capacitar constantemente al personal al que se le deposito la confianza de acceso y protección de los datos.

1.7 CONSECUENCIAS DE UNA VIOLACION DE SEGURIDAD

Algo que hay que dejar bien claro, es que, ninguna persona ni organización está protegida en un 100% ya que hay múltiples factores que se suelen salir de las manos de las personas o entidades que solicitan protección:

1. **Costo:** la seguridad tiene un precio bastante elevado y no solo por el hecho de pagar a alguien por el servicio, sino, porque además de las personas se necesitan herramientas especializadas para poder tener un control de monitoreo, entre

muchas otras actividades, mantener la red segura es un reto grande. (Canal, 2006)

2. **Actualización de los atacantes:** Los delincuentes están en constante capacitación, un gran porcentaje de su día está dedicado a la exploración y explotación de vulnerabilidades de los sistemas, y para poder tener una protección al nivel de un atacante el protector de la red debe estar al mismo nivel del atacante. Se podría preguntar, ¿por qué no contratar un atacante y que proteja mi red?, pero esto es un juego de azar ya que los **crackers** no tienen (en su mayoría) ética, por lo tanto, no se podría tener una garantía de que la información estará protegida y tampoco se tendrá la seguridad de que el individuo contratado no divulgará o hará un mal uso de los datos que le fueron confiados. (Canal, 2006)

Aquí además de los puntos que ya se tocaron entra otro factor muy importante, "**El tiempo",** pero ¿por qué? bueno el atacante es una bomba de tiempo que si no se controla a tiempo puede arrasar con todo a su paso y a su vez cumplir con su propósito. Para realizar un ciberataque avanzado y bien dirigido, se requiere tener la mayor precisión posible en cuanto a análisis, tiempo de ejecución y tiempo de escape.

Aquí podría plantearse una pregunta bastante interesante, ¿Con qué rapidez su equipo de seguridad puede responder al ataque para minimizar la pérdida de datos, tiempo de inactividad, pérdida de ingresos, apagones, transacciones, etc.?

Como se mencionó a partir del año 2020 incrementó el tráfico de información en la nube y en múltiples plataformas digitales, pero esto puede tener más desventajas que ventajas, ya que al menos México no es un país que esté listo para el trabajo de esta manera y no solo México sino también muchos otros países. La taza de usuarios en

internet mundialmente hoy en día es del 81.5% con espera de crecimiento en un 8% más para el año 2024 (Fernandez, 2021) tal como se ve en la figura 8.

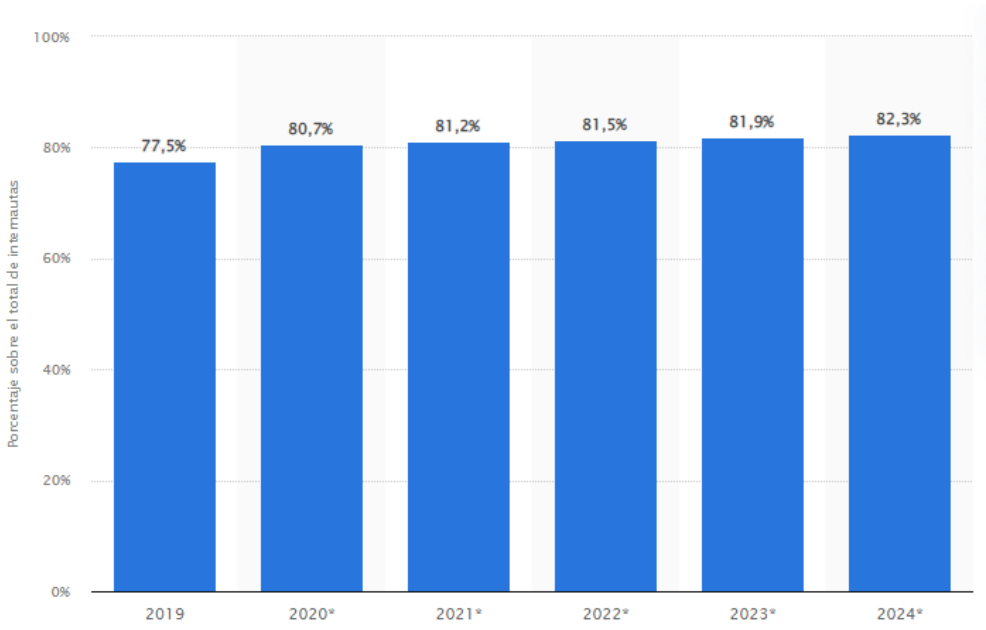


FIG 8. PORCENTAJE DE INTERNAUTAS MENSUALMENTE AL REDEDOR DEL MUNDO

Hoy en día la información se concentra en “la nube”, como ya se ha hecho mención, esto quiere decir que nuestra identidad en línea ya sea representando a una persona moral o a una persona física está en constante riesgo de ser saboteada o extorsionada. Cuando una persona moral hace público cierto tipo de datos acerca de su negocio está tomando la decisión de salir a la jauría de lobos, sobre todo cuando se hacen públicas páginas web con la finalidad de vender en línea, lo cual no está mal pues la finalidad de que la tecnología se encuentre en constante desarrollo es facilitar la llegada de información entre extremos, pero si se debe tener precaución o conocimiento de las consecuencias que pueden surgir tras el uso de internet, porque es ahí donde entran diversas situaciones como las que ya se mencionaron anteriormente. En muchas otras situaciones algunas organizaciones toman como opción mantener respaldos de su

información en la nube por miedo a tener algún infiltrado dentro de la misma, pero esto también representa un riesgo a pesar de tener contratados los servicios de un servidor virtual ya que nada garantiza que estos no vayan a ser vulnerados.

1.7.1 CONSECUENCIAS DE LA INFILTRACION A UN SISTEMA.

Existen diversas situaciones e infinidad de escenarios, así que se debe ser muchísimo muy inteligentes para evitarlas, los acontecimientos (Canal, 2006) pueden ser:

- Publicación de información falsa.
- Arruinar la reputación de la organización o persona.
- Tirar el sitio web (dejarlo fuera de servicio).
- Pérdida de ingresos e identidades
- Pérdida de credibilidad (periodos largos de tiempo sin actividad).
- Fuga de documentos confidenciales o información personal.
- En caso de ser entidad empresarial revelación de secretos comerciales o industriales.
- Robo de propiedad intelectual.

En caso de ser una organización, al ocurrir alguno de estos sucesos, se pierde la confianza por parte de los clientes, socios o personas que crean profundamente en esta entidad e incluso en casos muy extremos se podría llegar a la ruina debido a que al irse los clientes no existirán ingresos ni manera de sostenerla. Por otro lado, cuando se es una persona física, los problemas podrían llegar a ser más de chisme, y arruinando la reputación de la persona.

2. ANTECEDENTES

"La información es poder."

2.1 ATAQUES IMPORTANTES DE LA ACTUALIDAD.

Antes de mencionar algunos de los hechos más relevantes que han marcado la vida de muchos en distintos aspectos de su vida, haciendo énfasis en que para la computación estos acontecimientos son los que han ayudado a evolucionar e ir desarrollando nuevas habilidades y así poder crear nuevas tecnologías o métodos de protección. A continuación, se presentan algunos bugs (errores) que han marcado la historia.

- 9 de septiembre de 1947 ocurrió una falla en el Harvard Mark II, a las 15:45. Grace Murray Hopper registró el primer error en la historia de la computación, el error encontrado por la almirante de la marina era una polilla que se encontraba atrapada en un relé de una máquina, En la figura 9 se muestra la polilla encontrada.

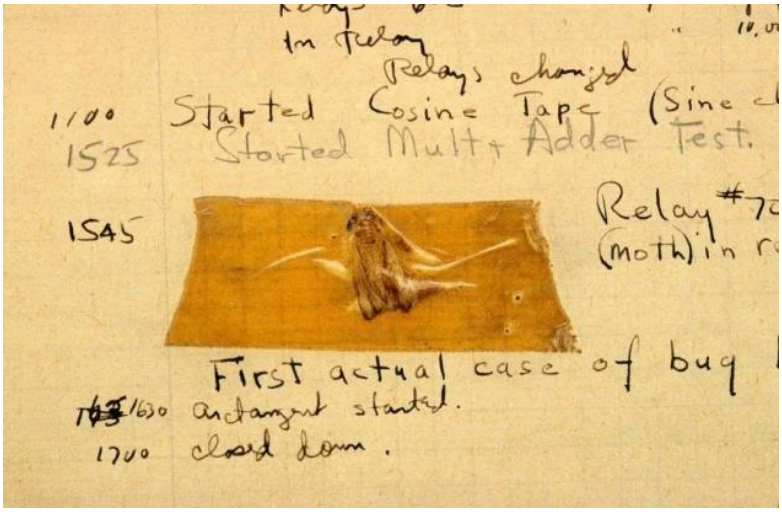


FIG 9. POLILLA ENCONTRADA POR GRACE HOPPER, PRIMER BUG DE LA HISTORIA.

- Misil de Dhahran ocurrido en febrero de 1991 (misil iraquí) logró llegar a la base de Dhahran en Arabia Saudí, quitándole la vida a 28 estadounidenses. “.0.33seg representan el tiempo en el que un radar tarda en localizar un misil Scud-Al Hussein cuya velocidad alcanza 1.5km/s, este micro retraso supone 687 metros de error aproximadamente” lo que quiere decir que al no haber sido localiza en el tiempo estimado preciso, provocó un margen error considerable, en la figura 10 se muestra gráficamente la trayectoria del misil.

FIG 10. REPRESENTACIÓN DEL BUG QUE PRESENTO UN RETRASO DE 0.33SEG.

- Existe un error conocido hoy en día como el error del milenio el cual tuvo bastante importancia ya que gracias a este suceso se detuvieron cientos de comunicaciones alrededor del mundo. La causa de esto fue por una mala práctica por parte de los programadores ya que al querer ahorrar memoria omitieron la centuria del año para el almacenamiento de fechas.

- Otro acontecimiento importante es el famoso pantallazo azul *(Blue Screen of Death),* el cual ocurrió tras la presentación de Windows 98, aunque actualmente sigue apareciendo este pantallazo en los dispositivos que cuentan con el sistema operativo Windows.

Aún continúan los ataques, por descuidos o simplemente porque las personas que han logrado realizarlos han sido bastante insistentes. Hace no mucho tiempo ocurrieron dos acontecimientos relevantes (año 2020), uno en la red social de esta época Facebook y otra en la industria petrolera mexicana más grande de México, PEMEX (Jiménez, s.f.). Los ataques fueron sorprendentes pues el primer acontecimiento tuvo fines de robo de identidad porque robaron cuentas de usuarios las cuales fueron vendidas y el propósito que esto tenía consistió en ganar una contienda electoral en USA, lo cual fue considerado como manipulación electoral. En el segundo caso fue uno de secuestro de información, penetrando en la red de la empresa petrolera, logrando así desconectar los servidores. El intercambio solicitado por los atacantes para liberar los servicios fue de aproximadamente 4.9 MDD. Y estos no son los únicos ataques a los que se puede hacer referencia, existen algunos otros que también han dejado huella en la historia de la tecnología.

- Hackeo a el hombre más rico del mundo, Jeff Bezos: este ataque fue ejecutado con ayuda de un software malicioso conocido con el nombre de Pegasus 3, este ataque fue realizado en su dispositivo personal móvil y el ejecutor fue el príncipe saudí Mohamed Bin Salman. (Mundo, 2020)
- Yahoo!: la plataforma fue atacada y el precio a pagar por este incidente fue de 300 millones de cuentas de usuarios que utilizan esta plataforma. Las

consecuencias fueron exposición de información personal y sensible como: números de teléfono, nombres, apellidos, direcciones de correo electrónico, contraseñas, cumpleaños, entre otros más. (MUNDO, 2016)

- Equifax: esta empresa perdió datos personales y entre los datos robados se detectaron miles de documentos de seguridad social, pasaportes, carnés de conducir, entre otros de identificación. Estos datos los habían subido usuarios a la plataforma de la compañía de forma “confidencial y segura”. (AFP, 2020)
- Telefónica: una de las compañías más importantes de España fue afectada por un malware llamado “Wanna Cry”, aunque esta compañía cuenta con un extraordinario equipo de seguridad en IT fueron víctimas de los ciberdelincuentes, así que con esto podemos llegar a la conclusión de que para los atacantes no hay descanso ya que siempre se encuentran trabajando para poder obtener vulnerabilidades de sus sistemas. (Toledano, 2017)
- Policía de Minneapolis USA: el 25 de mayo del año 2020 surge un acontecimiento en Minneapolis, Minnesota, la muerte de George Floyd. Luego de este acontecimiento en el mes de junio del mismo año ocurrió un ataque al gobierno de USA. Pues todo el territorio nacional estaba indignado tras esta y otras muchas muertes y no solo por las muertes si no las razones que originaron las agresiones, una de ellas es racismo. Esto incluyendo a los famosos hackers “A*nonymous*”, quienes lanzaron una advertencia al gobierno. Luego de esta amenaza, pública, por cierto, la policía de Minneapolis sufrió un DNS (denegación de servicios). (Mundo, BBC News Mundo, 2020)

El año 2020 ha traído consigo una gran oportunidad para el tráfico en la nube usándolo para el trabajo/escuela remota, lo cual ha sido de gran utilidad debido a los protocolos de sanidad que se han llevado a cabo a consecuencia de la pandemia (COVID 19) Aunque ha sido de gran apoyo para la salud y el bienestar de billones de personas, también se han suscitado consecuencias, la población en general no estaba preparada para dar un salto tecnológico tan apresurado en tan solo un día. Así como dar uso a estas herramientas puede resultar beneficioso y aplicándolo específicamente en mayor insistencia a fines educativos e incluso laborales también existen consecuencias. Al realizar estas modificaciones tecnológicas en muchas instituciones educativas y empresas de cualquier giro (siempre y cuando su trabajo les permita realizar este tipo de cambio) han surgido dudas miedo e incertidumbre acerca de la redirección de sus vidas cotidianas y de manera presencial, algunas de ellas se enfocan hacia el uso de las herramientas correctas y seguras para poder llevar a cabo sus actividades logrando un cierto porcentaje de satisfacción. Y es normal tener miedo sobre qué es lo adecuado, en muchas instituciones se migró a realizar transferencias bancarias y si se recuerda un poco las personas apenas comenzaban a adaptarse a estos métodos de pago, la desconfianza era y sigue estando presente al realizar principalmente está actividad.

Contando además que el paseo de la información en la red está muy presente y con mayor demanda. Esto abre paso a que los ataques tengan mayor ventaja ya que ellos logran ver “oportunidades” con base a la ignorancia de los usuarios. Algo cierto es que el índice de delitos ha migrado a internet, ahora los ladrones no están en las calles esperando a quien victimizar, sino que ahora están pasando a estar tras un ordenador.

Ellos no tienen piedad del conocimiento de los demás usuarios sobre las plataformas, solo roban lo que les interesa y listo ahora tienen efectivo.

2.2 CRECIMIENTO DE ATAQUES DURANTE LA PANDEMIA 2020

Tras migrar al trabajo desde casa (*Home Office*), muchos usuarios fueron afectados directa e indirectamente, esto a consecuencia de la falta de preparación y capacitación para el uso adecuado de la tecnología, como ya se mencionó anteriormente. En una situación como la que está enfrentando el mundo es más sencillo aprovecharse de la población que está migrando a realizar sus actividades desde "la comodidad de su hogar". No solo el internet está siendo vulnerado sino también las personas, que tienen miedo, desesperación, angustia, etc. Entre los ataques que han ocurrido los criminales han jugado con las emociones de las personas, como se sabe una pandemia trae consigo escasez en muchas áreas especialmente la de alimentos, productos básicos del hogar e incluso medicamentos, pero en este caso uno de los recursos más importantes para las personas contaminadas, es el hecho de contar con tanques de oxígeno. Los criminales no han tenido ninguna consideración ni piedad en este aspecto jugando así con el bienestar, salud física/emocional de las personas poniendo en riesgo la economía de estas.

Los ataques más reportados (MariaJose, 2020) en este periodo de tiempo son:

- ***Phishing***: Esta actividad ha existido durante mucho tiempo, y en la actualidad ha tenido el protagonismo directo, debido a que las actividades no son presenciales en un cierto porcentaje de la población, se ha tenido que recurrir a la entrega de información vía e-mail, como se conoce el *phishing* es una actividad en donde se envían correos electrónicos falsos, poniendo en riesgo, archivos, cuentas, pagos

etc. Cuando no se está lo suficientemente capacitado o al menos no detienen los conocimientos básicos para detectar cuando un correo en la bandeja de entrada e incluso en el *spam*, no es bueno.

Ya que si se abre o se cliquea en algún enlace se podría comprometer el equipo de cómputo y perjudicar de diversas maneras a la persona directamente afectada (esto en alguno de los casos). Por ejemplo, si en la bandeja de alguna persona hay un correo de alguna institución Bancaria colocando como asunto "Confirmación de información" o "Urgente", el usuario inmediatamente abrirá el correo por impulso, y posteriormente encontrará un texto en donde se le pide que verifique su información por cualquier "situación" que presenta el banco. Algunos de los datos que el delincuente estaría solicitando serían; correo, contraseña, número de cuenta bancaria, nombre completo, *NIP*, entre otros datos que, reflexionando ninguna institución pediría vía email. Lo que sucede aquí es que al pedir estos datos el usuario está entregando automáticamente el acceso para que sea desfalcado. Es por ello que se debe tener mucho cuidado a la hora de abrir correos electrónicos y acceder a las peticiones que trae consigo el contenido.

- **Estafas**: este tipo de actividad se puede manifestar de diversas maneras, pero cuando no se está consciente del lugar en el que se está navegando, pueden ocurrir muchas cosas. Existen algunas aplicaciones en las que se realizan las actividades de compra/venta de productos, algunos ejemplos de ello son Facebook, Amazon, Mercado libre, entre otros más que están surgiendo. Los usuarios publican anuncios colocando precios a sus productos o servicios, en algunos casos los paquetes suelen llegar a su destino en tiempo y forma, en otros

casos el producto no es lo que el cliente esperaba, pero en otros casos solo el vendedor gana, debido a que solo cobra, pero jamás entrega la mercancía/servicio.

- **Falsas oportunidades de empleo:** Tristemente el año 2020 trajo consigo una taza muy alta de desempleos formales e informales, tanto en las redes sociales como en el mismísimo Google (entre otras plataformas con demanda de ofertas laborales) se ven anuncios solicitando trabajos por horas cortas, trabajos fáciles y desde casa ganando cantidades de dinero, poco realistas. Los anunciantes publican maravillas sobre empleos (en algunos casos como estrategia de mercado) realmente o que van a ser perjudiciales para los postulantes, y es complicado distinguir entre un anuncio verdadero y uno que no lo es. Las plataformas no tienen un control o alguna política de privacidad en donde indique que debe ser 100 % real la oferta. Algunas de las consecuencias en este escenario son estafas, desfalcos, en algunos casos prostitución, etc.
- Ataques a entidades públicas y gubernamentales: conforme a avanzado la humanidad han nacido nuevas formas de molestar a otros, en este caso las entidades públicas o gobiernos, hoy en día han incrementado los ataques, exponiendo vidas públicamente o secuestrando servidores.
- **Hospitales**: Es otro de los casos más tristes y es que, ¿cuándo se había imaginado alguien, que un hospital sería atacado por delincuentes cibernéticos? La única finalidad de estos criminales ha sido la de detener los servicios (DNS), teniendo como principal ventaja la presión que se ejerce sobre el personal médico, pues al depender del equipo médico y el sistema de registro de pacientes, además

las operaciones que se realizan diariamente en los quirófanos entre muchas otras actividades realizadas en las instituciones de salud. Una vez que se obtuvo crear un clima de desesperanza es más fácil cobrar una recompensa y obtenerla, pues las funciones desempeñadas por los médicos es 100% veinticuatro siete. Este caso es uno de los más vergonzoso, ya que nos deja en un concepto nada humanitario.

Los criminales han olfateado el miedo de la ciudadanía y de los gobiernos, han sabido cómo aprovecharse de la situación que el mundo entero está pasando. Es por lo que se debe estar preparado para poder competir o solemos poder tener una defensa.

2.3 SEGURIDAD EN LA WEB

El ***World Wide Web (www)*** es un aliado potencial para cualquier tipo de comercio ya sea educativo, comercial o lucrativo incluso para el uso personal. La navegación web se ha convertido en una de las actividades cotidianas de hoy en día, tanto como respirar o comer. A través de esta herramienta se pueden realizar diversas actividades como; pagar una cuenta, hacer una transacción, una video llamada al extranjero, entre otras muchas actividades. Sin embargo, ofrece muchas “facilidades/oportunidades” a todo tipo de usuarios especialmente al sector delictivo.

A pesar de la gran gama de información con la que se cuenta actualmente aún hay quien ignora el riesgo que existe al navegar en un sitio web y no solo al trasladarse de una página a otra, sino en la estadía o en el simple acceso a él. A continuación, se exponen algunas de las sorpresas que se pueden encontrar:

- ***Ransomware*:** cifrado de información almacenada en el ordenador, por lo general se reclama un pago monetario a cambio de restablecer el servicio que haya sido bloqueado. (Kaspersky, s.f.)
- ***Adware* y/o *spyware*:** Múltiples ventanas de publicidad abiertas, en la mayoría de los casos realiza un seguimiento de la actividad que se realiza en la navegación web. (Lab, s.f.)
- ***Browsers Hijackers* (Secuestradores de navegador):** toma el control del navegador, de manera remota, y lo utiliza para fines maliciosos. Comúnmente agrega varios favoritos a la lista de marcadores del Browser. (Kaspersky, Kaspersky, s.f.)
- **Barras de utilidades:** barras de botones y/o complementos que se agregan a nuestro navegador, por lo general ocurre durante la instalación de algún software gratuito y que por lo general esconde malware. (Canal, 2006)

Además de estos peligros también se debe tomar en cuenta otro tipo de ataques, que es conocido como ingeniería social, con la cual los atacantes intentan engañar a las personas para que revelen información confidencial o realicen ciertas acciones, como descarga de contenido, aplicaciones o archivos que pueden tener una apariencia buena pero que en realidad no lo son. Los ataques más conocidos son:

- ***Phishing***: este es un método de ataque que regularmente se hace vía e-mail enviando información falsa para así poder obtener información del usuario. (Tapia, 2018)
- ***Smishing*:** esto sucede cuando un usuario recibe mensajes de texto en su teléfono celular (SMS), este puede incluir redireccionamiento de ligas (sitios web),

avisos de confirmación falsos, o incluso pedir al usuario que llame o mande un mensaje para comunicarse a otro número. (Tapia, 2018)

- ***Vishing*:** este tipo de ataque es común, en este caso se recibe una llamada engañosa tratando de suplantar la identidad de otra persona, los temas más comunes son secuestro, encarcelamiento y falta de dinero para llegar a un destino. (Tapia, 2018)

Es importante saber detectar cuando algo no está marchando bien en ordenador y tener a todos los contactos de interés registrados bajo un nombre reconocido ya que así se podrá identificar lo que ha cambiado o cuando se está siendo víctima de una suplantación de personalidad. En la figura 11 se muestra un mapa con algunas características de ataques comunes.

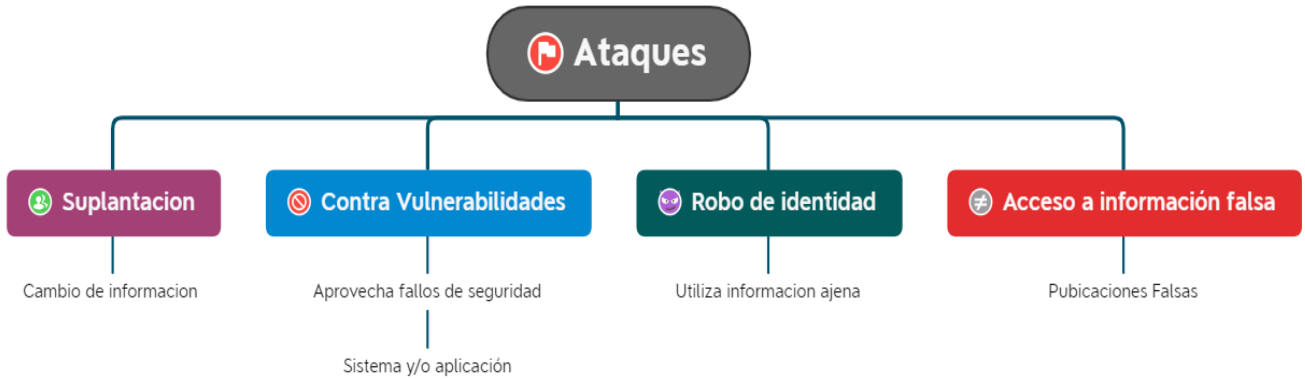


FIG 11. TIPOS DE ATAQUES

Es común ver a usuarios ingresar a páginas web falsas en las que se les muestra una URL “similar” a una original, esto puede variar en una letra, para poder hacer que el usuario no identifique a primera vista el cambio, por ejemplo https://www.google.com/ puede ser suplantada por https://www.googlle.com/ . Alguno de los peligros a los que se está expuesto pueden ser robo de información, un método bastante conocido es a través

de TypeScript, esto hace que el usuario entre en la página web falsa, comience a navegar, buscar e introducir información en esta. Si la página cuenta con un algoritmo de tipado de información una vez que el usuario esté interactuando con el sistema se va almacenando cada una de las palabras que fueron ingresadas con lo cual se logra obtener datos de interés para el delincuente.

Algunos otros atacantes suelen irse por **las vulnerabilidades** que estén en los sistemas y/o aplicaciones**.** Al detectar las vulnerabilidades será muy fácil para el sujeto infiltrarse y hacer lo que desee. Por ello también se recomienda mantener contraseñas actualizadas y lo suficientemente seguras además de que todos los equipos que disponga el usuario se encuentren bloqueados.

2.3.1. ¿QUÉ PASA CUANDO NO SE ES CAPAZ DE PROTEGERSE DE UN ATAQUE CIBERNÉTICO?

En apartados anteriores ya se hizo mención a algunos de los acontecimientos que pueden surgir tras no protegerse de un ataque. La información es poder y está convirtiéndose en el oro negro del siglo. Debemos saber que la información debe ser confidencial y está centralizada así que su valor es alto y continuará creciendo. La información puede ser manejada de diversas maneras, sobre todo cuando se trata de lucrar con ella, tenemos que puede ser:

- **Divulgada:** existe información que no debe ser expuesta a cualquier usuario por lo tanto al no tenerla en bien gestionada, esta puede llegar a usuarios no autorizados.
- **Mal utilizada:** la información en manos equivocadas no tendrá el uso adecuado y esto es perjudicial para el usuario/compañía.

- **Robada:** se obtiene un acceso para un usuario que no está autorizado.
- **Borrada:** esto afectará al sistema que dependa de esta información ya que no estará disponible.
- **Saboteada:** puede mostrarse información modificada al beneficio del criminal, con fines de perjudicar al usuario o compañía.

Afectando así su disponibilidad y poniéndola en riesgo, pero no solo la información, también se pone en riesgo la identidad personal o la persona misma, hablando en términos laborales, se estaría perdiendo tiempo valioso de productividad, y peor aun planteándonos en un escenario en donde sea afectado el sector salud se estaría poniendo en juego la vida de las personas que dependan de ciertos servicios que dependan a su vez de tecnología.

Tener marcado el terreno es como ir al bosque y saber identificar con precisión cuando existe una trampa, y justo debería ser cuando estamos en un sitio que no es el adecuado o que no tiene buena pinta, de esto dependerá la seguridad y la garantía de salir “vivos de ahí”.

Durante un descuido ya sea siendo atacados o no, se corre el riesgo de perder. La pérdida va a diferir dependiendo el contexto en el que sea vulnerada lo que puede involucrar diversos aspectos, la figura 12 muestra algunas de las facetas que pueden surgir si no se es capaz de protegerse de un ataque cibernético, ya sea que se esté en una empresa, casa, o que alguna de las empresas a las que se contrata un servicio sea atacada. (Canal, 2006)

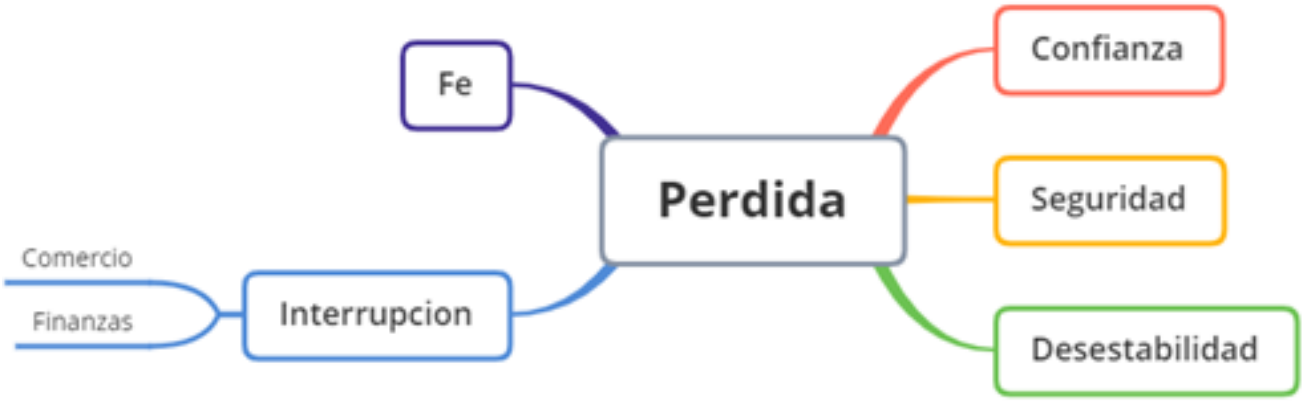


FIG 12. PERDIDAS DE UNA EMPRESA U ORGANISMO.

- **Confianza**: Es uno de los lazos más fuertes que existen y es esta alguna de las razones por las que un usuario se anima adquirir algún bien o servicio. Imaginarse estar en un escenario en donde se contrata un servicio para el almacenamiento de fotografías de **NATGEO** y de pronto un atacante se filtra y comienza a hacer públicas fotografías confidenciales o las que no se publicaría porque la empresa tiene motivos para no hacerlo. Al ser publicadas, **NATGEO** no querrá contratar más un servicio con la misma compañía ya que le falló y no solo eso expuso datos que no eran oficiales. Es aquí en donde se entra en un tema de desconfianza la cual es difícil de restaurar. (Canal, 2006)
- **Seguridad**: Se perderá automáticamente después de ser víctima. Esto dependerá del nivel de importancia que tenga la información para el usuario-blanco. Por lo regular la seguridad está ausente cuando no tenemos completo algo o bien cuando no se tiene una amenaza o riesgo. (Canal, 2006)
- **Desestabilidad**: la ausencia de estabilidad, pero… ¿qué es estabilidad? la estabilidad es mantener el equilibrio en todos los aspectos, así como evitar en

mayor parte los errores en los sistemas informáticos, entonces tener un robo o falla en el sistema se comienza a ser desechables o sustituible. (Canal, 2006)

- **Fe**: la pérdida de la fe se ve representada en muchos ámbitos, suponiendo la vida de cualquier individuo se puede direccionar principalmente en el ámbito religioso. Perder la fe en un sistema nos lleva al primer término, "pérdida de confianza", se deja de creer en algún producto o servicio. (CICESE, 2017)
- **Interrupción**: Pérdida del flujo constante de trabajo, almacenamiento, descargas entre muchas otras actividades. Estas operaciones afectan mayoritariamente a los sectores financieros, comerciales y de salud. (CICESE, 2017)

2.4. GESTIÓN DE LA SEGURIDAD.

"La administración es un arte que se lleva a cabo en distintas áreas".

Abriendo un panorama general, esta actividad se realiza desde el entorno del hogar al tratar de salir una quincena o tratar de distribuir o administrar correctamente los flujos de efectivo y los alimentos básicos, garantizando que cada uno de los integrantes de la familia obtenga los suficientes recursos para sobrevivir. Entonces enfocarnos al entorno tecnológico no cambia del todo, solo es cuestión de enfocarlo o redireccionarlo a este entorno, siendo cautelosos, observando y tratando de dar una garantía de que todo irá bien y que cada proceso tendrá la garantía de cumplir con su objetivo sin ser interrumpido y que además cuenta con los recursos suficientes para realizarlo. Una de las cosas que se debe tener presente es que no se puede estar seguro al 100% pero si se puede trabajar para tener una garantía lo más estable posible que se pueda.

La información manejada en cualquier tipo de plataforma o entorno debe ser:

- **Confidencial:** No divulgación de información a terceros, entidades o procesos que no estén autorizados. Esto asegura el acceso a la información por únicamente las personas que estén autorizadas. (Canal, 2006)
- **Íntegra:** Se busca mantener libre la información de modificaciones que no estén autorizadas. Mantiene con exactitud los datos tal cual fueron generados o recibidos, sin ser manipulados o alterados por personas o procesos que no estuvieron autorizados. (Canal, 2006)
- **Disponible:** Hace referencia a que está al alcance de la mano, en el momento y lugar que sea solicitada la información siempre y cuando se tenga una autorización para su acceso.

La sociedad está altamente informada incluso se podría decir que tiene acceso a información que no debería conocer por su propio bien o incluso tiene al alcance de la mano tecnología o aplicaciones que no son aptas para su conocimiento, haciendo referencia al buen uso de estas, y esto es lo que marca una de las diferencias entre los que tienen acceso a las nuevas tecnologías y los que no tienen acceso a ellas. (Canal, 2006)

Por ello se recomienda que los usuarios generales (los que no son desarrolladores o que son personas “normales”) desarrollen habilidades informacionales y digitales. Así sabrán como leer o gestionar algún documento digital, entre muchas otras actividades realizadas a través de un medio electrónico. Algunas recomendaciones que seguir se mencionan a continuación:

- Escribir la URL en la barra de direcciones, verificando que se ingresó la correcta, además de asegurarse que estamos accediendo al enlace que se desea.
- Asegúrese que está accediendo a sitios oficiales.
- Leer bien antes de darle clic a cualquier enlace, en caso de que este enlace solicite publicación, notificaciones o instalación de accesos directos, se debe salir y no intentar acceder ya que estos sitios en ocasiones instalan herramientas en el navegador que no necesitamos o que pueden estar para realizar acciones indebidas.
- En caso de que se esté accediendo a internet desde un ordenador no propio, se recomienda no guardar contraseñas y cerrar las sesiones que se hayan abierto, en caso de haber olvidado hacerlo cambie su contraseña.
- En caso de que esté accediendo a un sitio a través de un enlace, asegúrese que realmente el destinatario es usted y que conozca al remitente. Podría preguntar al remitente si ha enviado el enlace y corroborar con el que sea correcto. No proporcione información tan fácil, cuestione si los datos que se le están pidiendo son necesarios y ¿por qué? se le está pidiendo esto si algo no cuadra pregunte directamente a la compañía que ha enviado este mensaje.
- Mantener todos los dispositivos con los que se cuente, bloqueados para así evitar el acceso a curiosos.
- Cambie sus contraseñas cada 3 meses al menos. No coloque nombres, *NickNames*, fechas de nacimiento, números seguidos.

- Mantenga sus contraseñas resguardadas en algún lugar, que no sea de simple acceso. Podría usar una app que administre sus contraseñas, así solo se recuerda una sola vez.

Hablar de gestionar seguridad para el entorno social, es decir para personas que no son programadoras, que son directamente el usuario a interactuar es muy extenso y amplio ya que influye un contexto educativo, es más debería ser una de las materias impartidas en los colegios. Por tanto, se podría deducir en las recomendaciones anteriores. Por otra parte, se tienen algunos consejos para la parte que está directamente en contacto con la tecnología y el desarrollo web, la parte que corresponde a los creadores, así es los programadores.

- Validación de Entradas: Limitar la entrada a ciertos tipos de datos en las cajas de texto es un buen comienzo y se mataría dos pájaros de un tiro, pues se estaría evitando información que no se necesita para hacer operaciones durante el desarrollo y se estaría bloqueando el acceso a otras líneas como código.
- Codificación de Salidas.
- Prácticas criptográficas: Encriptar la información al enviarla por la red o al almacén de la base de datos.
- Estilo de programación.
- Manejo de errores y Logs.
- Manejo de Archivos.
- Manejo de memoria.
- Estandarización y reutilización de funciones de seguridad.

- Aseguramiento basado en riesgos.
- Inspección de Código por Fases.
- Pruebas de Caja Blanca y Caja Negra (después de cada cambio)

En la tabla 1 se da una sugerencia de planificación de un sistema. En este se muestran tres interfaces y cuatro acciones que llevara cada una de ellas, tomando en cuenta los requerimientos de cada interfaz.

TABLA 1 EJEMPLO DE ANÁLISIS DE REQUERIMIENTOS SEGURO.

	Validación de Entradas	Validación de Salidas	Controles Criptográficos	Manejo de Archivos	Manejo de Memoria
Interfaz 1	Aplica	No Aplica	Aplica	Aplica	-----
Interfaz 2	- -	- -	No Aplica	Aplica	Aplica
Interfaz 3	Aplica	Aplica	Aplica	No aplica	Aplica

Un equipo de fútbol no es bueno cuando cada una de las partes involucradas no hace el trabajo que le corresponde de la mejor manera posible, eso mismo pasa cuando en este contexto no se hace lo que le toca a cada parte involucrada, no será posible mantener una seguridad buena. Los usuarios deben aprender a manejar las herramientas y los desarrolladores deben aprender que no se puede saltar el proceso para desarrollar un sistema y que cada paso es indispensable, aunque sí se podría no es lo ideal.

2.5. TIPOS DE PROTECCIÓN DE LA INFORMACIÓN

Para poder proteger la información no basta con simplemente parchar un sistema, es este caso también se ve involucrado el sector humano, pues es uno quien crea un

sistema. Ciegamente se cree en la perfección y es lo que se busca al crear un sistema, que contenga la menor cantidad de errores posibles.

La capacidad de envío y administración de datos aumenta, así como el flujo de consumo de información y esto está embebido en distintos sectores si no es que en todos. En este punto lo interesante no está en centrarse únicamente en quienes están dentro del ámbito tecnológico, aunque sí es un factor, sino en la cantidad de información que se maneja día con día, hora por hora. Los usuarios gestionan, editan, envían, borran etc. Ante el desborde de información no controlada y sobreexpuesta a otros, el usuario queda desprotegido.

"*La identidad es una construcción compleja, personal y social, consiste en parte en quien creemos ser, como queremos que los demás nos perciban, y como de hecho, nos perciben*" (Smith, 2005)

Se tienen dos tipos de identidad, **online y offline**. Cada una de ellas define al individuo dependiendo el entorno en el que se encuentre:

Identidad online: define como percibe el mundo en internet al usuario a través de lo que el usuario aporta a este entorno, si bien es cierto no todo lo que está en las redes o internet es cierto, existe un grado de falsedad de información y noticias. En el entorno online el usuario miente acerca de sí mismo y de su propio estilo de vida o exponiéndola, jugando así con su privacidad. Ejemplos claros de esto se encuentran en las redes sociales como **Instagram, Twitter o Facebook** entre otras. Cada usuario cuenta y expone información principalmente fotografías, ubicaciones o lugares de alta frecuencia marcando así un historial fuertemente atractivo para un atacante cibernético o

delincuente físico (ladrón). Aquí algunos de los datos más expuestos en la web o redes sociales: (Canal, 2006)

- Fotografías.
- Ubicaciones (lugar de trabajo, rutas concurridas, etc.).
- Lugares concurridos.
- Amigos.
- Familiares.
- Posición económica.
- Ocupación
- Estados emocionales (lo cual también es un flanco rojo, ya que representa una debilidad y puede ser usada en la ingeniería social por los delincuentes).
- Etc.

Identidad Offline: definida como la vida común de un individuo, aquí la información es real, en donde la persona cuenta con casa, identificaciones oficiales y más.

Aunque son dos tipos de identidades en la que aparentemente la información está dividida, mientras más avanza el tiempo se van unificando al grado de existir usuarios principalmente nuevas generaciones, que ya no distinguen cuál es la real. (Canal, 2006)

Existen tres tipos de (Canal, 2006) protección:

- **Personal:** asociada a la protección de identidad, dispositivos y datos.
- **Corporativa:** asociada a la protección de datos, clientes y reputación.
- **Nivel estado:** protege el bienestar de la población, la seguridad nacional y la seguridad social.

2.6 IMPORTANCIA DE LA ENCRIPTACIÓN

La encriptación no es más que el hecho de ocultar los datos cuando viajan a través de la red, es decir hacerlos invisibles para los ojos de los que puedan estar atentos a lo que está sucediendo. En el principio de los capítulos se hizo mención sobre hechos que marcaron la historia y algunas técnicas que en aquellos tiempos solían usarse para proteger los mensajes o la información que se estaba enviando. Y esto es lo que se logra con este método de encriptación, que la información llegue al destino deseado sin que nadie más pueda leerlos o informarse de ellos. Han sido desarrolladas gran cantidad de metodologías para poder generar distintos y numerosos tipos de cifrado y encriptación, algunos son muy seguros y otros no tanto. La tecnología SSL *(Secure Sockets Layer*), crea un código entre dos computadoras distintas, es decir; entre el cliente y el servidor, generando así una comunicación más segura, éste es un protocolo de internet que permite la encriptación de información sensible, véase la figura 13.

FIG 13. PROTOCOLO SSL

Existen dos tipos de cifrado, **criptografía semántica y asimétrica.** La criptografía semántica utiliza la misma clave para ambos extremos de la comunicación, es decir para el receptor (quien recibe) y el emisor (quien envía). la criptografía asimétrica hace uso de dos claves una publica y una privada, la primera pude ser utilizada por todos los que

necesiten información cifrada y la segunda jamás es revelada. Otra técnica utilizada para mayor seguridad al paso de información en la web es el uso de una **VPN (*Virtual Private Network*).**

Dentro de la aplicación de la criptografía asimétrica según (Crespo, s.f.) se puede mejorar la seguridad de las comunicaciones digitales, enfocándose en la operación especial de las **funciones hash**. Según (Vazquez, 2018) las funciones hash son funciones que utilizan un algoritmo matemático, transformando un conjunto de datos en un código alfanumérico con una longitud fija, sin importar la cantidad de datos que utilice, el código saliente siempre tendrá la misma longitud de caracteres.

Las funciones Hash más populares son **MD5 y SHA-256.** Una función hash es un tipo de operación que toma una entrada de datos arbitraria y mapea una salida de un tamaño en específico, este tamaño se especifica en bits de datos. La función hash criptográfica ideal debe ser **determinista**, lo que significa que el mismo valor de entrada debe devolver siempre el mismo resumen hash de salida. Un pequeño cambio en la entrada debería dar como resultado una salida totalmente diferente, tratando de evitar que se produzca el mismo resultado entre dos entradas de datos diferentes, conocidas como **colisiones hash,** en la figura 14 se muestra un ejemplo de estas colisiones**.**

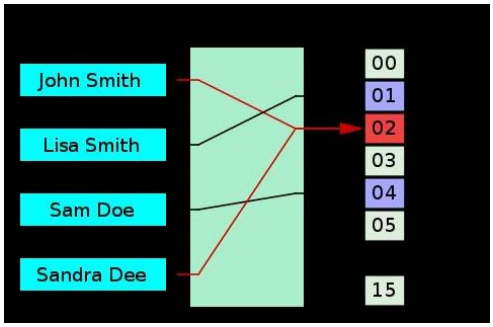


FIG 14. EJEMPLO DE COLISIÓN HASH

2.6.1 MD5 y SHA.

Estas son dos funciones hash muy conocidas las cuales cumplen con las características necesarias para alcanzar el nivel de protección deseado. MD5 trabaja con 512 bits generando resúmenes hash de 128 bits durante años este método era puesto en práctica, pero tras la detección de múltiples vulnerabilidades es recomendable utilizar SHA-256, PBKDF2, bcrypt y script. SHA-1 también una de las funciones de SHA popularmente conocida por trabajar con 512 bits y generando un resumen hash de 160bits, pero tras las mismas circunstancias que MD5 se recomienda utilizar SHA-256. MD5 comprueba la autenticidad de un archivo, es decir hace una verificación de modificaciones o se trata de una descarga corrupta, incompleta o si alguien modificó el mismo para introducir **malware,** en la figura 15 se ejemplifican estos modelos de encriptado.

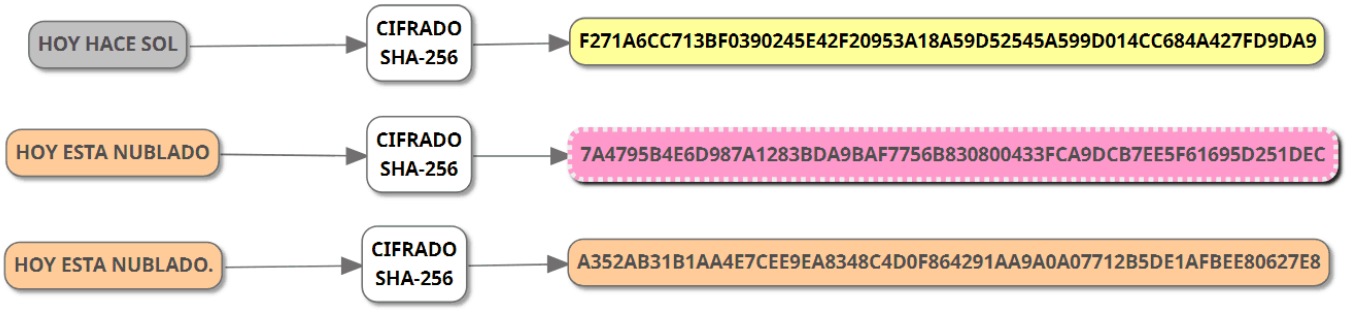


FIG 15. EJEMPLIFICACIÓN DE ENCRIPTACIÓN CON SHA-256

PBKDF1 y PBKDF2 son funciones de derivación de claves con un costo computacional, comúnmente utilizadas para reducir vulnerabilidades a los ataques de fuerza fruta. PBKDF2 es parte de la serie PKCS (*Public-Key Cryptography Standars)*, produce claves derivadas con un alcance de hasta 160 bits. Aplica una función

pseudoaleatoria, a la contraseña/información de entrada, junto con un valor de salida, el proceso es repetido múltiples veces hasta generar una clave derivada. (Guardo, 2019)

2.7 DERECHO INFORMÁTICO

Ley de mínimos privilegios (PoLP)

La asignación de permisos a un usuario, más allá de los derechos necesarios para llevar a cabo una acción determinada, puede permitirle llevar a cabo acciones para las cuales no está autorizado, como acceder, obtener o modificar información. Además, los privilegios deben estar considerados para las entidades o servicios puedan cumplir con sus objetivos, sin comprender la privacidad o la seguridad; sin embargo, en esta tarea, recae una importante responsabilidad de los usuarios para conocer y otorgar los permisos necesarios y suficientes. (Mendoza, 2018)

2.7.1 PROTECCIÓN DE DATOS PERSONALES.

Ataques a las vías de comunicación y violación de correspondencia.

Articulo o 166 bis Código Penal Federal Mexicano.

Titulo Quinto. - Delitos en Materia de vías de Comunicación y Correspondencia (Reubicado, antes Titulo Sexto, mediante Decreto publicitario en el diario oficial de la Federación el 29 de julio de 1970)

Capitulo I.- Ataques a las vías de comunicación y violación de correspondencia (Reforma la denominación mediante Decreto publicado en el Diario Oficial de la federación el 15 de enero de 1951)

A las personas que, por razón de su cargo o empleo en empresas de telecomunicaciones, ilícitamente proporcionen informes acerca de las personas que

hagan uso de medios de comunicación, se les impondrá pena de tres meses a tres años de prisión y serán destituidos de su cargo.

En el caso anterior, se aumentará la pena hasta en una mitad cuando el delito sea cometido por un servidor público en ejercicio de sus funciones. Asimismo, se le impondrán, además de las señaladas, la destitución del empleo y se le inhabilitara de uno a diez años para desempeñar cargo o comisión públicos. (Cuervo, 2018)

Artículo de 168 bis Código Penal Federal Mexicano

Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho:

I. Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas.
II. Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas (Cuervo, 2018)

Articulo 173 Código Penal Federal Mexicano.

Titulo Quinto. - Delitos en Materia de vías de comunicación de correspondencia.

Capitulo I. Ataques a las Vías de comunicación y violación de correspondencia.

Capítulo II.- Violación de correspondencia.

Artículo 173.

Se aplicarán de tres a ciento ochenta jornadas de trabajo en favor de la comunidad: (reformado mediante decreto publicado en el diario oficial de la federación el 10 de enero de 1994)

I. Al que abra indebidamente una comunicación escrita que no esté dirigida a él.

II. Al que indebidamente una comunicación escrita que no esté dirigida a él. Aunque la conserve cerrada y no se imponga de su contenido. (Cuervo, 2018)

3. MARCO METODOLÓGICO.

3.1 METODOLOGÍAS A CONSIDERAR PARA CREAR UNA PÁGINA WEB.

Al escuchar la palabra programación, la mayoría de las personas o programadores automáticamente piensan en código e incluso en cosas que seres de otros planetas pueden hacer, porque tienen capacidades sobrehumanas, y la verdad es que si es una práctica un tanto compleja pero solo tanto como el equipo de desarrollo o el desarrollador se lo proponga.

Programar es más que sentarse a tipar código, realizar una buena aplicación móvil, de escritorio o web requiere más que solo eso, ya que la programación, así como muchas artes requiere de dedicación y creatividad. Planificar adecuadamente las necesidades de la interfaz y su funcionalidad, esquemáticamente debe llevarse de la mano de un buen análisis de información, análisis de requerimientos, diseño UI/UX entre algunas otras facetas, una de las más importantes es el análisis de **casos de uso** como del tanto del lado del cliente lado del **cracker** pues esto ayudará a enfocar los puntos ciegos del sistema. Existen dos ramas de la informática que pretenden auxiliar el desarrollo de las aplicaciones o sistemas, uno es la **ingeniería de software** y el otro la **ingeniería web** (Goytía, 2017) en la figura 16 puede apreciarse la estructura de la ingeniería de software y en la figura 17 la estructura de la ingeniería web.

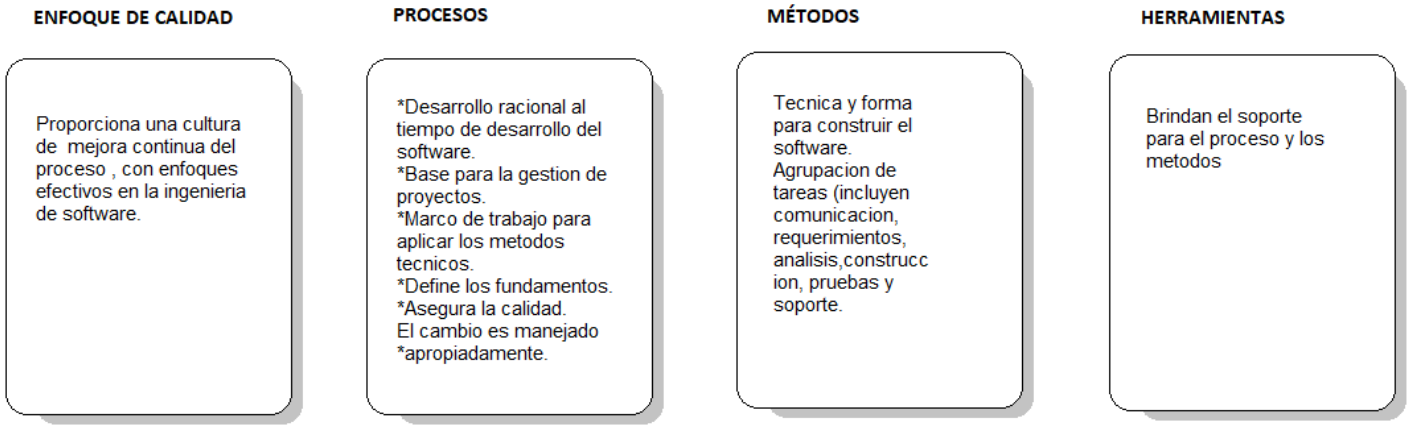


FIG 16. INGENIERÍA DE SOFTWARE. (GOYTÍA, 2017)

Esto abre un panorama más amplio de visualización a la persona o grupo de personas que se encuentren en el desarrollo de una herramienta web o de cualquier otra índole. La seguridad implica diversas medidas técnicas en la programación web, como acomodar cadenas bajo ciertas reglas para evitar ataques por XSS, inyección SQL o incorporar *Triggers* (disparadores), *Cross Site Request Forgery* (falsificación de formularios), mala gestión de cookies, sesiones o formularios y DDOS (denegación de servicios). (Goytía, 2017)

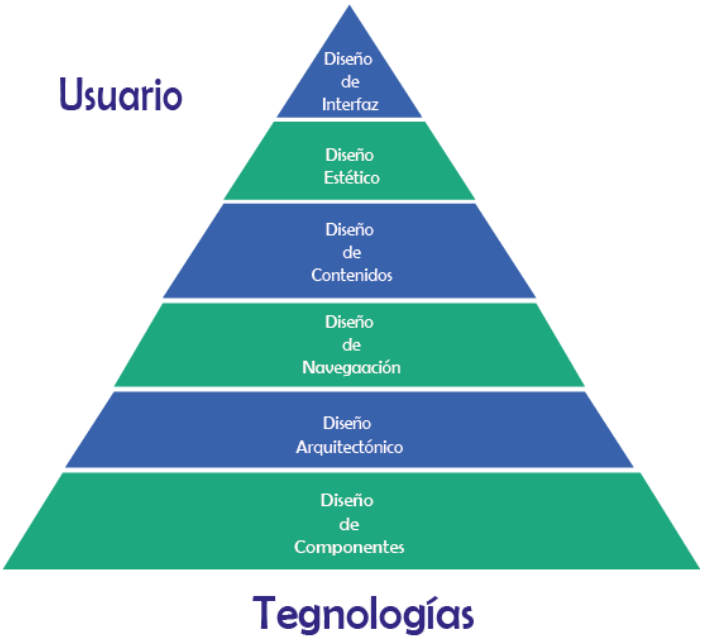


FIG 17. INGENIERÍA WEB. (GOYTÍA, 2017)

Existen ocho fases que auxilian el desarrollo de un sistema web las cuales son importantes considerar, estas son las (Goytía, 2017) siguientes:

1. **Estudio/análisis:** en esta fase se definen los objetivos del proyecto, por ello se llama fase de estudio ya que se analiza, la viabilidad del proyecto, las estrategias a utilizar, la funcionalidad que tendrá ,los alcances, los requerimientos tanto económicos como técnicos sin olvidar el capital humano necesario para la implementación del mismo, también se hace un análisis del tiempo (el cual debe ser considerable y alcanzable), sin olvidar contemplar las necesidades y los objetivos y las necesidades de la organización.
2. **Fase de planeación:** se define el "plan" de acción a tomar en cuenta para lograr el objetivo del mismo, el proyecto es asignado a un líder de proyecto el cual estará encargado de gestionar de manera adecuada cada uno de los recursos a tomar en cuenta y así garantizar que cada una de las tareas se cumplirán.

3. **Fase de análisis de requerimientos:** determina con detalle los requerimientos, tomando en cuenta el hardware a usar (tecnología a utilizar, dispositivos, servidores, periféricos y la infraestructura de red, etc.) y el software (sistema operativo, licencias, el lenguaje de programación a implementar, entre otros). Ya que es una aplicación web se debe considerar el dominio en el que será alojada la página web.
4. **Fase de diseño:** es importante considerar esta fase ya que aquí se establecen todos los elementos a utilizar. Se tendrá conocimiento de las entradas y salidas del sistema. Esto nos aportará el comportamiento que tendrá el sistema y se tendrá en conocimiento la usabilidad y accesibilidad en el sistema web.
5. **Fase de elaboración y creación de contenidos:** tener una buena estructura y planeación no van a garantizar el éxito de la aplicación, así que, si el contenido no es bueno o atractivo para el usuario, la plataforma no tendrá tanto auge como se espera, por ello es importante plantear estratégicamente el contenido de esta.
6. **Fase de Desarrollo:** esta fase se divide en dos ya que la programación de un sitio web lo requiere. Se tiene la programación por parte del cliente y por parte del servidor.
7. **Fase de pruebas:** se encarga de llevar un análisis del correcto funcionamiento del sistema, tomando en cuenta distintos tipos de navegadores, sistemas operativos y dispositivos. Además, se debe considerar el tiempo de ejecución de cada proceso que se encuentre en la página. En este apartado es conveniente comenzar con el análisis de vulnerabilidades del sistema y llevar un control para

poder hacer de conocimiento al programador y pueda solucionar los problemas encontrados.

8. **Control de Calidad:** es una etapa final en la que se hace un repaso del paso anterior y se garantiza la funcionalidad del sistema tanto para el cliente como para el usuario.

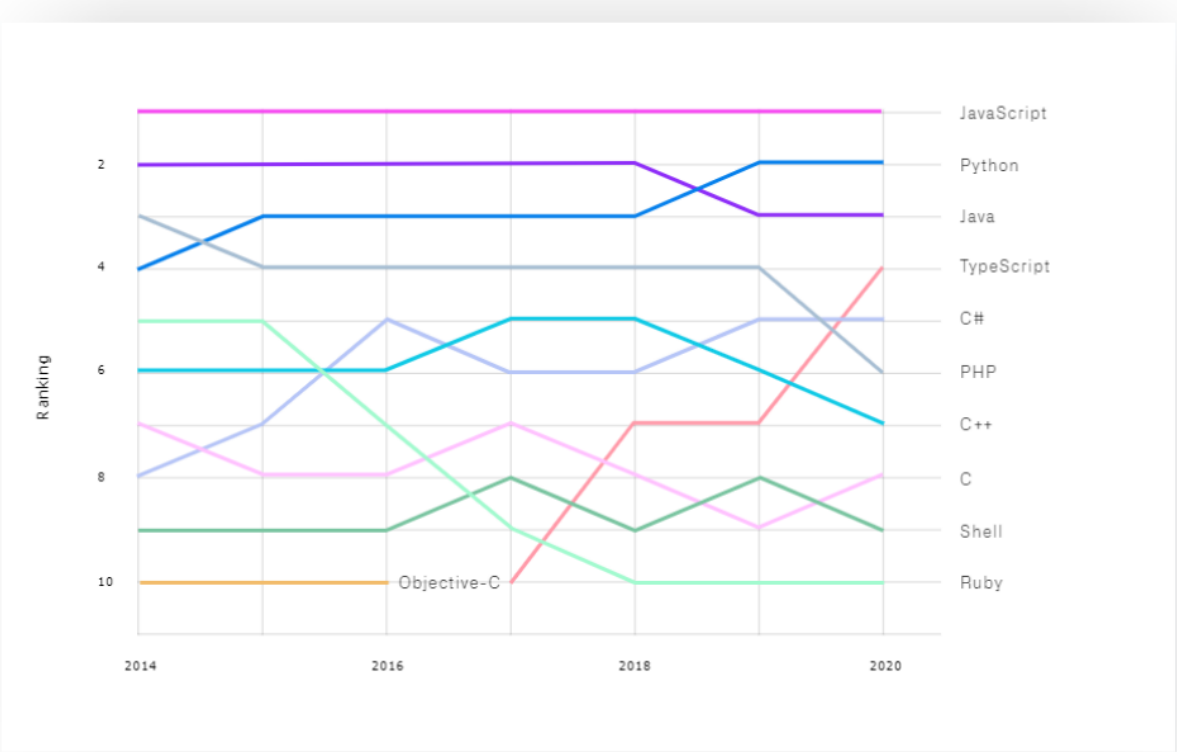


FIG 18. TENDENCIA DE LENGUAJES DE DESARROLLO (CASTELÁN, 2021)

En la figura 18 se muestra una gráfica de los lenguajes de programación en tendencia para el desarrollo de aplicaciones tanto en ambiente web como en desarrollo en general.

3.2 PROPUESTA DE SITIO PARA ANALIZAR

Se llevará a cabo el desarrollo y análisis de un sitio web contemplando cada una de las partes que se deben estimar para un buen desarrollo, contemplando que se da una descripción general de las funcionalidades del sistema completo para medir la importancia y la cantidad de información que esta plataforma es capaz de procesar, sin embargo, el análisis de vulnerabilidades se centra en dos apartados con la finalidad de enfocar el proceso al objetivo de esta investigación, que es demostrar la importancia de un análisis de vulnerabilidades y adquirir las herramienta que pueden ser utilizadas para realizar esta actividad.

3.2.1 DESCRIPCIÓN DE LA PLATAFORMA A ANALIZAR.

La empresa **ASENEG**, requiere de un sistema enfocado a FREELANCERS y EMPRESAS de cualquier giro, el propósito general y principal de este sistema es poder fungir como un despacho intermediario el cual llevará el control de proyectos o actividades que requiera alguna empresa y a su vez, que alguna persona pueda desempeñar sus habilidades como un trabajador freelance, evitando así la relación subordinada de jefe-empleado, dando un beneficio para todos los involucrados (empleador/empleado).

La estructura principal del sistema consiste en:

1. **REGISTROS:** por medio de formularios para ambos tipos de usuarios (empresas y Freelance), la información que se almacenara dependerá de acuerdo con el rol/privilegio que tenga el tipo de usuario registrado.
2. **ACCESO**: el usuario independientemente de su privilegio puede ingresar al sistema direccionando a la vista correspondiente de acuerdo con el privilegio asignado.

3. **EMPRESAS** en el perfil de empresa se tendrá el siguiente menú:

    a) **Configuración de perfil** en este apartado la empresa visualizara toda información de registro y si lo requiere puede hacer algunas modificaciones.

    b) **Proyectos** en este apartado la empresa podrá agregar n proyectos por medio de un formulario, los cuales serán vistos por los freelances, eliminar algún proyecto, editar algún proyecto, buscar algún proyecto en particular e imprimir la relación que se genera con las acciones antes mencionadas.

    c) **Agregar independiente** en este apartado la empresa podrá visualizar información de sus proyectos creados y de todos los Freelances interesados en cada uno de los proyectos y decidir si quiere que sea parte del proyecto o declinar la solicitud, así mismo puede realizar búsquedas particulares e imprimir la información visualizada.

    d) **Seguimiento** este apartado está disponible siempre y cuando haya sido aceptado un freelance por parte del despacho, es decir, ya es un empleado. Una vez esto será posible asignarle tareas o procesos a realizar del proyecto, aquí podrá la empresa visualizar la fase en la que se encuentra la tarea (asignada, en proceso, realizada o vencida) también puede imprimir esta información.

    e) **Traslados** en este apartado la empresa visualizara información desglosada del pago del servicio que se le realizara al freelance por medio del despacho, debido a que el despacho se encargara de distribuir el monto correspondiente al freelance.

f) **Contratos** puede visualizar a los empleados que ya forman parte del equipo y que a su vez tienen asignado un proyecto.

4. **FREELANCERS** en el perfil de freelance se tendrá el siguiente menú:
   a) **Configuración de perfil**: visualizara toda su información de registro y si lo requiere puede hacer algunas modificaciones.
   b) **Proyectos** podrá subir su currículo si así lo prefiere para poder crear un historial más concreto de su información personal y profesional, de la misma manera podrá visualizar todos los proyectos en los cuales se podrá postular dependiendo de su área de interés con la que se registró al sistema en un principio.
   c) **Mis postulaciones** se visualizarán todas las postulaciones que realizo el freelance y el estado en el que se encuentran (pendientes, aceptadas o rechazadas).
   d) **Seguimiento tareas** se visualizarán las tareas/actividades que le fueron asignadas por la empresa en el momento que fue aceptado para elaborar el proyecto, el será el encargado de iniciar y finalizar las tareas para que los interesados lleven el seguimiento de las mismas.
   e) **Mis pagos** en este apartado se le mostrara un desglose con la información relacionada al pago que recibirá de acuerdo al trabajo realizado en el proyecto y el acuerdo que haya tenido con el despacho.
   f) **Mis contratos** podrán ver los proyectos en los que esa participando y su estado.
5. **DESPACHO** en este perfil el (los) despacho(s) tendrá(n) el siguiente menú:
   a) **Configuración de perfil** visualizara toda su información de registro y si lo requiere puede hacer algunas modificaciones.

b) **Empresas** en este apartado el despacho podrá visualizar en un registro general todas las empresas que se han registrado de manera autónoma, en otro apartado visualizara a las empresas que el cómo despacho ha registrado, de la misma manera puede realizar búsquedas particulares e imprimir la información mostrada.

c) **Freelances** podrá visualizar en un registro general todo el freelance que se han registrado de manera autónoma, en otro apartado visualizara a los freelances que el cómo despacho ha registrado, de la misma manera puede realizar búsquedas particulares e imprimir la información mostrada.

Como este proyecto es muy extenso, el primer análisis para éste se realizará en el primer y segundo apartado que corresponden al acceso y al registro, ya que el objetivo principal es demostrar la importancia de la seguridad y como puede afectar esto a un sistema, en este caso web. El objetivo de mostrar la descripción general es para mostrar que este trabajo contiene el paso y almacenamiento de información altamente sensible, ahora se hará una descripción muy general de lo que los módulos de acceso y registro necesitan para poder proseguir al análisis de requerimientos de los módulos que se analizaran sus vulnerabilidades.

Para poder ingresar al sistema los usuarios deberán ingresar su correo y una contraseña con mínimo ocho caracteres, todo esto en su apartado de *login*. Si el usuario no cuenta con un previo registro, este podrá realizar su alta en el sistema en el apartado “Registrarse”, los todos que se solicitan son: nombre completo (en caso de ser un freelance y en caso de ser una empresa el nombre de la empresa), correo, contraseña, edad(en caso de ser freelance), dirección, teléfono celular, teléfono de casa u oficina,

para ambos casos se requiere de un comprobante fiscal de su RFC, y así mismo el RFC validando el tipo de RFC si es para persona física o moral, para las empresas se requiere su razón social y tipo de empresa, para los freelance se requiere saber su edad, especialidad, años de experiencia, además de su fecha de nacimiento. En la tabla 2 se describen los requerimientos del sistema desarrollado para este trabajo de tesis.

TABLA 2 REQUERIMIENTOS DEL SISTEMA.

ACCIÓN QUE REALIZARÁ EL SISTEMA	REQUERIMIENTOS
Login (ambas categorías)	▪ Correo ▪ Password
Registro Morales (Todos los tipos a excepción del Administrador y el Despacho)	▪ Correo ▪ Password ▪ Tipo de Usuario ▪ Nombre empresa ▪ RFC ▪ Dirección ▪ Teléfono ▪ Etc. ▪ cfdi
Registro FreeLancer	▪ Correo ▪ Teléfono ▪ Password

	▪ Cfdi ▪ Fecha de nacimiento ▪ Edad ▪ Teléfono móvil ▪ Etc.

Mockups

Los mockups son propuestas de diseño que se presentan ante un cliente para darle una vista de cómo lucirá su producto al finalizar (Bravo, s.f.). En las figuras 19, 20 y 21 se muestran los mockups utilizados para las páginas en las que se realizara el análisis de vulnerabilidades y la pagina de presentación del sistema.

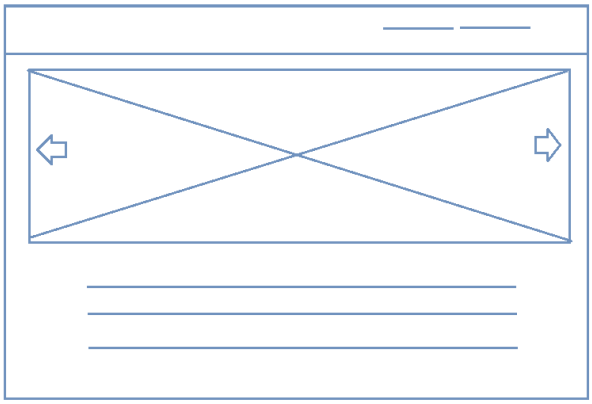


FIG 19. PÁGINA PRINCIPAL SITIO DE PRUEBA.

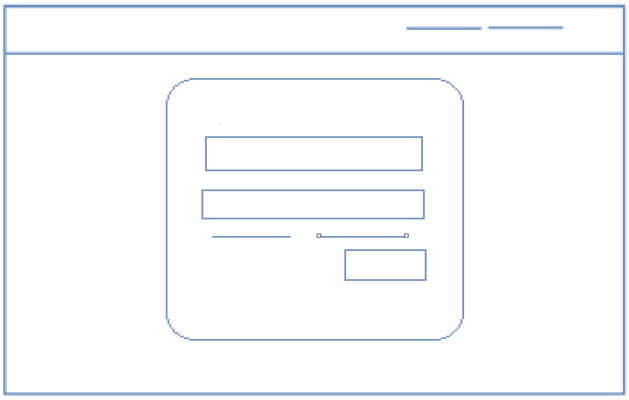


FIG 20. LOGIN PARA AMBOS CASOS.

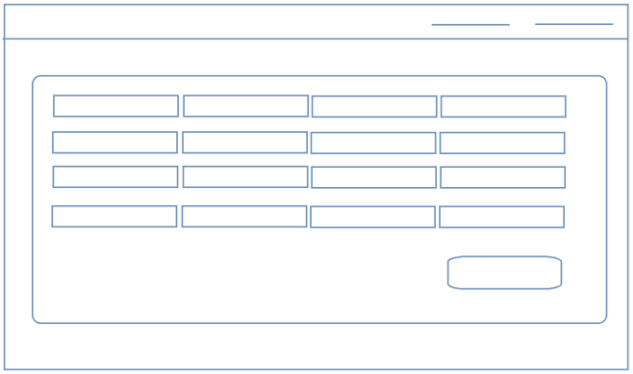
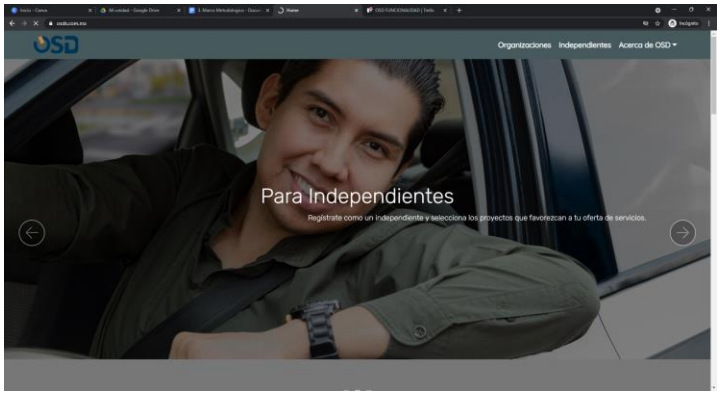
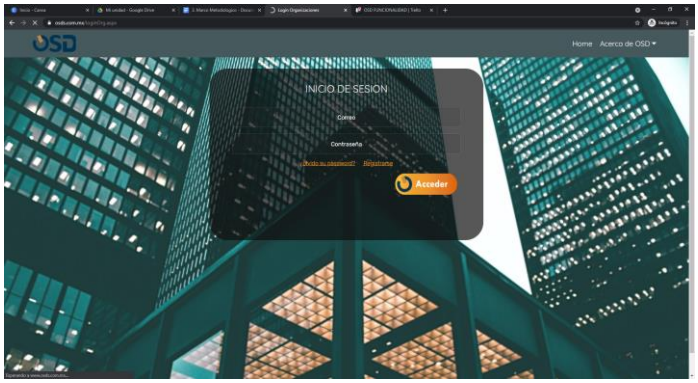


FIG 21. REGISTRO PARA AMBOS CASOS





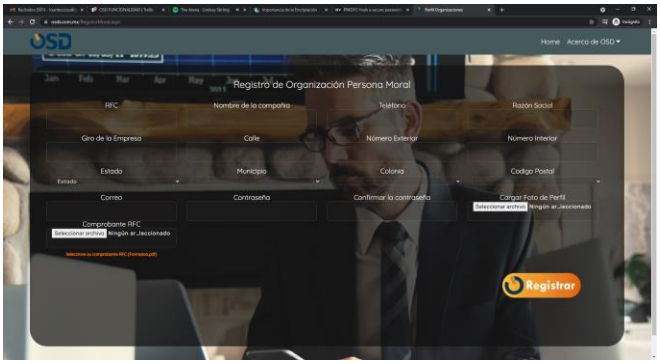


FIG 22. IMÁGENES DEL SISTEMA DE MUESTRA A PROBAR.

3.3 CASOS DE USO Y CASOS DE USO INDEBIDO

Los siguientes casos de uso están basados en los requerimientos que fueron solicitados por el cliente. En la figura 23 se muestra la interacción que tendrán los dos tipos de usuarios, tanto el Administrador como el Usuario “Persona Moral”, asignado cada una de las actividades que cada uno puede realizar. En el caso de la figura 24 se muestra la misma interacción, pero esta vez con un sospechoso que está en espera de actividad para atacar, mostrando los posibles puntos de vulnerabilidad que se tengan en el sistema en caso de no a ver trabajado de forma adecuada.

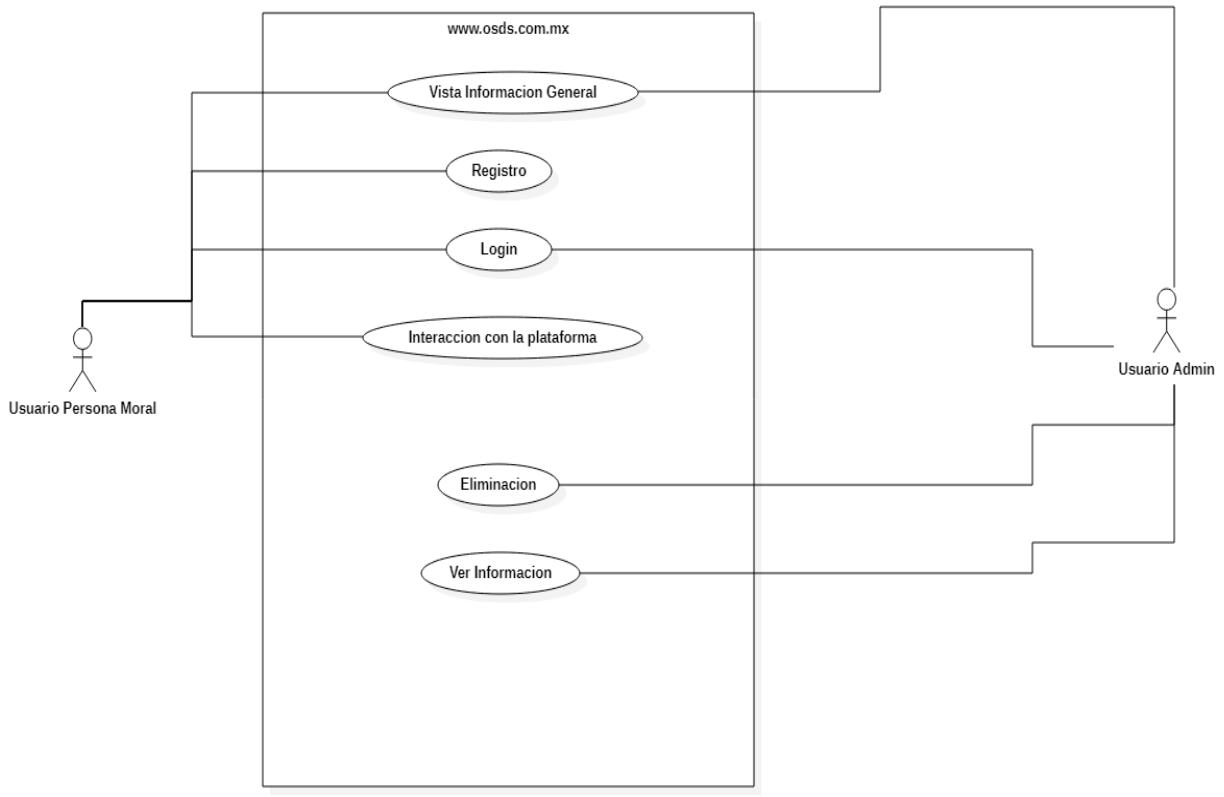


FIG 23. CASOS DE USO

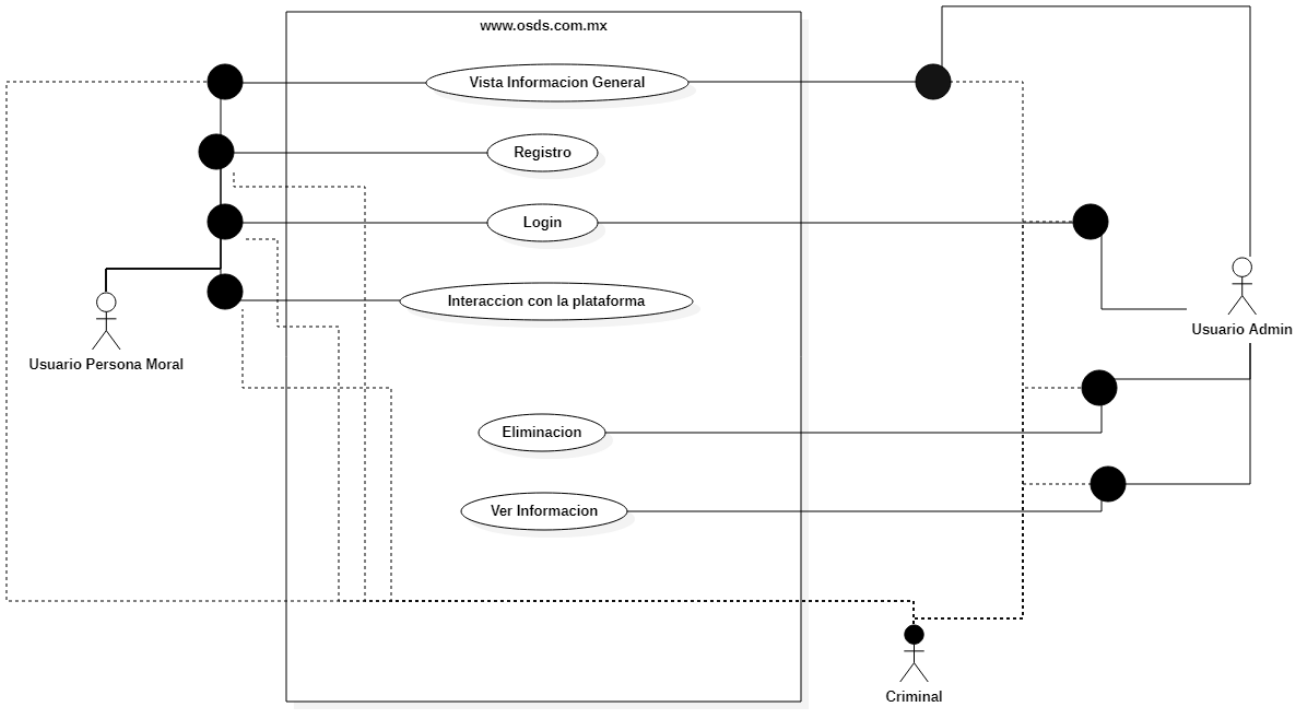


FIG 24. CASOS DE USO DE VULNERABILIDADES.

Tomar en cuenta esta parte de la información es una de las iniciativas que deben tomarse en cuenta, es decir un buen programa de seguridad debe pedir la documentación de la aplicación: Arquitectura, diagramas de flujo de datos, casos de uso. Pues además de ser una de las mejores prácticas como desarrolladores, ayudará a facilitar el trabajo y tener un mejor enfoque de lo que se pretende realizar.

3.4 FASES DE SEGUIRDAD (ATAQUE INFORMÁTICO).

En la vida lo más importante y esencial es comprender como opera o funciona una situación, un evento o un prospecto, esto facilita las tareas además de contribuir a la mejora y solución de las problemáticas que se presenten en un presente o futuro ya sea cercano o lejano. Por esta razón uno de los pasos más importantes que deben ser

considerados al momento de querer realizar un análisis o investigación es comprender cual es el mecanismo que está siendo aplicado por un delincuente cibernético (aunque esto también es aplicable en un crimen físico), pensar con una mentalidad muy similar a la de un ciberdelincuente no es del todo descabellado ya que esto permitirá ir a la par o incluso pensar en el acto siguiente a realizar por el mismo. Hace algún tiempo leí una novela en la cual cuentan las crónicas de un asesino serial en donde la narradora (la detective que llevaba el caso). Durante dicha trama ella mencionó este punto, la equivalencia o la ventaja de asemejar la mentalidad a la del criminal (Pierce, 2015), lo cual me pareció cordial después de analizar lo que había leído. Situándonos en un escenario esto podría poner al Analista de seguridad en sincronía con un posible paso a dar por la persona que intente atacar o vulnerar un sistema y así ahorrar tiempo e incluso detener el paso siguiente.

Cabe mencionar que existe una diferencia entre seguridad informática y seguridad de la información, la primera se encarga de la seguridad del medio por el que se está pasando la información, y la segunda no solo se ocupa de la seguridad por el medio de transmisión sino también del contenido que se entrega. (SGI, 2017)

Con esto entendido la seguridad puede clasificarse en tres; usuarios, información e infraestructura. Lo cual queda de la siguiente manera:

1. **Usuarios**: este es el primer filtro por el que para el sistema antes de considerar directamente a un cracker, el usuario está considerado como una zona de riesgo ya que no es un objetivo manipulable o controlable, este puede quitar poner y

jugar como el disponga y llegar a “romper” algo que conllevo mucho tiempo de trabajo.

2. **Información**: principal activo por el que se está trabajando en tener ausencia de peligro.

3. **Infraestructura**: como se mencionó antes, éste es el medio por el que la información viaja.

En el principio de este subcapítulo se mencionó la importancia que tiene conocer cómo trabaja un ciberdelincuente, por tanto, es conveniente conocer primero las fases que lleva un ataque informático. (Castro, 2018).

1. **Reconocimientos:** se recaba la información necesaria la cual corresponde al entorno en el que se estará trabajando, detectando el punto u objetivo altamente potencial. Lo cual puede variar desde una simple búsqueda en internet, la práctica de **ingeniería social** e incluso comprender el paso de información a través de una red ya sea local o no.

2. **Escaneo e investigación:** se lleva a cabo un análisis de los datos que el delincuente tiene en su poder. Con la finalidad de detectar las vulnerabilidades que tiene un sistema informático/web o una red.

3. **Acceso:** una vez que se tiene detectada cada una de las debilidades el atacante procede a manipular los accesos a su favor.

4. **Manteamiento del acceso:** el objetivo principal de esta fase es colocar un **backdoor (**puerta trasera**)**, esto permitirá al atacante entrar y salir en el momento que este lo solicite.

5. **No dejar rastro:** sin más que explicar este punto es exactamente como se entiende, el no dejar un rastro de quien fue, que medio utilizó por donde navegó o algunos datos para el posible rastreo como lo son la dirección IP, MAC, compañía de internet.

Existen tres aspectos de seguridad a considerar, principalmente porque son la mina de oro buscada por los criminales; **confidencialidad, integridad y accesibilidad de los datos.** En un apartado anterior se hizo mención del significado de estos conceptos. Además, se tiene en cuenta este tipo de ataques en los sistemas para entorno web, los cuales también deben estar contemplados a la hora de hacer el análisis, la codificación y la publicación de dicha herramienta.

Los ataques informáticos más populares y conocidos actualmente son: **DOS (ataque de denegación de servicios), Ping Flood, Ping de la muerte, Escaneo de puertos, ARP Spoofing, ACK Flood, Ataque FTP Bounce, TCP Session Hijacking, Man-In-the-Middle, Ingeniería social, Os Finger Printing, Puertos expuestos, KeyLoggers, ICMP Tunneling, Ataque loki, Secuencia TCP, CAM Table Overflow.** Como esta investigación hace referencia a la seguridad web será más conveniente centrarse en los ataques más concurrentes e intrusivos aplicados (Ramiro, 2018) en este campo:

1. **Inyección SQL**: ejecución de código, presencia de vulnerabilidad en la capa base de la aplicación web, este código puede obtener datos confidenciales, como; rutas, nombre del servidor, claves, usuarios, etc.
2. **Cross-Site Request:** como se mencionó en un apartado anterior este método es una falsificación de solicitudes en un sitio web.
3. **Ataque de envenenamiento de cookies:** implica la modificación de los contenidos de una cookie (información personal almacenada en la computadora de un usuario web) para eludir los mecanismos de la seguridad. Con este tipo de ataques se puede obtener información no autorizada sobre el usuario y robar su identidad.
4. **Robo de cookies:** se realiza por medio de scripts del lado del cliente, por ejemplo, JavaScript. Cuando el usuario da clic en un enlace, el script busca la cookie almacenada en la memoria de la computadora para todas las cookies activas y las envía al atacante.
5. **Phishing:** uno de los ataques más comunes, el cual es un crimen fraudulento, el cual intenta obtener información importante y sensible de la víctima, como su nombre, correo, contraseña, datos bancarios etc. Todo esto haciéndose pasar por alguna entidad confiable para el usuario.
6. **Web Defacement:** se suplanta el sistema montado en un servidor por uno propio del cracker, con la finalidad de arruinar la reputación de la compañía ya que esta suplantación cambia la visibilidad del que fue suplantado.
7. **Buffer Overflow:** Un desborde de Buffer, es una anomalía que almacena procesos en el búfer fuera de la memoria que fue reservada por el programador

para el trabajo del sistema, los datos son sobrescritos en la memoria. Esto puede ocasionar error de acceso a memoria, datos y resultados erróneos, finalización de un programa entre otros. Es común que el error se presente por error el programador y no del cracker.

8. **Negación forzada:** su objetivo es enumerar y acceder a los recursos que la aplicación no referencia, pero que aún tienen acceso. Por ejemplo, un Backus, directorios config, logs a los que se pueda acceder etc. (Ramiro, 2018)
9. **División de respuesta HTTP:** este tipo de ataque abre puerta al ataque XSS de las palabras Cross-site scripting o en español Secuencia de comandos en sitios cruzados. (Ramiro, 2018)
10. **Defectos de inyección:** permite a un atacante retransmitir código malicioso a través de una aplicación web a otro sistema el uso de programas externos a través de comandos Shell. Así como llamadas a las bases de datos en el *backend* a través de SQL. (Ramiro, 2018)

Ahora que ya se conocen los tipos de ataques más frecuentes, se realizará un análisis para la implementación de las estrategias que se tomarán en cuenta para prevenir un ataque en un sitio web. Lo más recomendable es hacer uso de mejores prácticas, para proteger a los usuarios y a su información y datos personales. Realizar monitoreos y revisión de código podrá ayudar a encontrar errores o vulnerabilidades al inicio del desarrollo de software. Implementar escáneres de códigos dinámicos y estáticos, estos son sistemas de software desarrollados para llevar a cabo una búsqueda de vulnerabilidades dentro de un sistema (Luz, 2021). Hacer uso de procedimientos

almacenados que permitan el paso de parámetros automáticos, hacer uso del captcha contribuye a la detección de éstas.

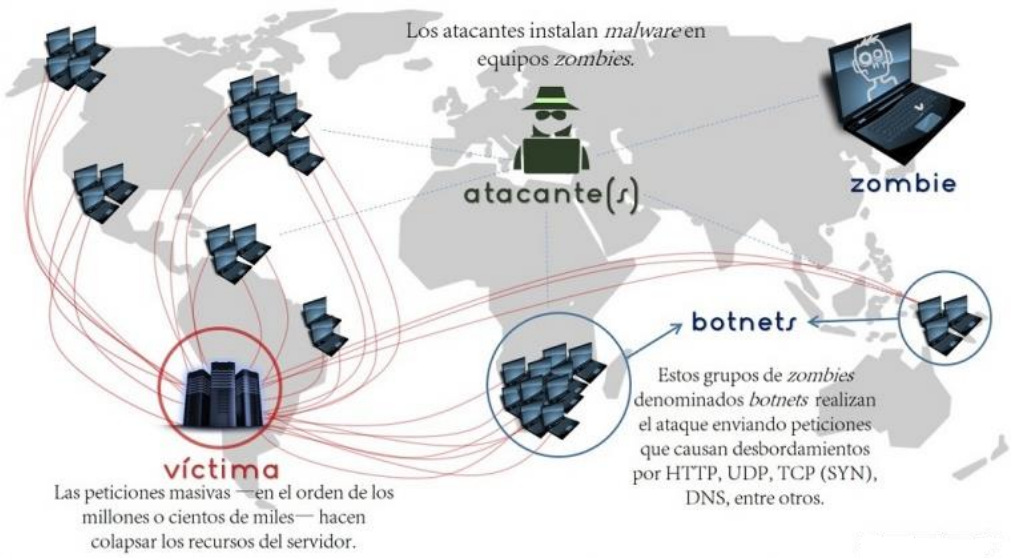


FIG 25. ATAQUE DDOS (DENEGACIÓN DE SERVICIOS).

3.4 SOFTWARE DE ANÁLISIS DE SEGURIDAD PARA SISTEMAS WEB

Actualmente existen diversas herramientas que sirven de apoyo para el escaneo y detección de vulnerabilidades. Antes que nada, hay que tener claro el concepto y el contexto en el que se enfatiza la palabra herramienta. En este escenario una herramienta hace referencia al conjunto de líneas de programación/código, lo cual automatiza un proceso de escaneo, recolección o explotación de información, logrando con esto acortar el tiempo de aplicación de algún método o técnica ***step by* step** de una prueba de pentesting.

Las herramientas tienen una clasificación acorde al tipo de trabajo que se realiza en este trabajo de investigación, se hace mención de nueve clasificaciones de las herramientas de trabajo de *pentesting,* así como una explicación del enfoque de cada

una de ellas, así como en el campo de clasificación en el que es más conveniente utilizarlas:

- **Recolección de Información:** esto depende de si el escaneo es para una infraestructura, aplicación web o un sitio web. Este tipo de herramientas obtienen información como el servidor en él se está trabajando, respuestas, tecnologías de desarrollo, etc.
- **Análisis de Vulnerabilidades:** proceso que consiste en identificar brechas de seguridad, evaluando su criticidad y corrigiendo los errores para hacer más seguro un sistema. Dos herramientas que pueden ser utilizadas son:
    - **Nessus Vulnerability Scanner:** detecta amenazas en tiempo real, es una herramienta muy precisa y evita la generación de falsos positivos durante el escaneo.
    - **Open Vass (Open Vulnerability Assessment Scanner):** es un scanner de vulnerabilidades, realiza pruebas no autenticadas, pruebas autenticadas, ajuste de rendimiento para escaneos, protocolos industriales e internet bajo y alto nivel.

  Ambas herramientas pueden ser utilizadas en infraestructuras o en la web, estas herramientas permiten el análisis de vulnerabilidades, es decir que no realizan ataques como por ejemplo de fuerza bruta o no explotan los datos.
- **Análisis Forense:** conjunto de técnicas que permite la extracción de información de discos y memorias de un equipo, sin alterar su estado. Esto ayuda a la búsqueda de datos, tratando de detectar un patrón o descubrir información que no puede ser visualizada a simple vista.

- ***Cellebrite*:** Se encarga de crear hardware y software para hacer análisis en teléfonos móviles. Proporciona recolección, preservación y análisis forense de datos de dominio público como; ubicación, perfiles, imágenes, archivos etc.
- **Encase:** análisis forense a dispositivos, usb's, discos duros etc.

- **Aplicaciones Web:** existen diversas herramientas para el escaño de vulnerabilidades, pero se hablará de dos herramientas de trabajo muy populares que son auxiliares en las auditorias webs.
  - **Burp Suite:** Sus diversas herramientas trabajan en conjunto para apoyar el proceso completo de pruebas, desde el mapeo inicial y análisis de la superficie de ataque de la aplicación web, hasta encontrar y explotar sus vulnerabilidades de seguridad.
  - **Owasp Zap:** herramienta de penetración integrada, fácil de utilizar para encontrar vulnerabilidades en aplicaciones web.

  Mas adelante se hablará de todas las características de estas herramientas ya que estas son las que se están utilizando para hacer las pruebas en el sistema propuesto para analizar.
- **Auditoria Wifi**
  - **Aircrack-Ng:** permite auditar diferentes protocolos dentro de la tecnología wifi.
- **Explotación:** es la cuarta fase de una auditoria de pentesting, y es una de las más complejas pues el evaluador o el intruso, debe buscar aprovecharse de alguna de las vulnerabilidades identificadas en las etapas anteriores de la

auditoria y así poder completar la intrusión en el sistema objetivo. Una de las herramientas utilizadas es:

- **Metasploit:** es una herramienta enfocada para auditores de seguridad. Contiene *exploits* que son vulnerabilidades conocidas que contienen *payloads* los cuales ayudan a la explotación de vulnerabilidades.

- **Sniffing**: es una técnica para escuchar el tráfico que corre a través de una red interna o una intranet e incluso se puede aplicar en internet, ya sea cableada o vía wifi.
  - **WireShark:** analizador de paquetes de red. Presenta los datos de los paquetes capturados con el mayor detalle posible.
- **Fuerza Bruta**
  - **John the Ripper:** es un software *crackeador* de claves muy eficaz es multiplataforma y su principal función es detectar claves débiles, pero también es capaz de analizar clave hash. Algunos de los algoritmos que entiende son; DES, MD5, BLowfish, Hash, MD4, LDAP y MySQL.
  - **Hydra:** consigue acceder al sistema o redes no autorizadas, es de código abierto y totalmente gratuita.
- **Ingeniería Inversa**
  - **Olly Dbg:** depurador de código ensamblador de 32 bits para sistemas operativos Microsoft Windows.
  - **Dbugger:** prueba y depura (elimina) errores de otros sistemas.

Acorde a los términos mencionados con anterioridad hoy en día se utilizan dos poderosas herramientas para el análisis vulnerabilidades en la categoría **Aplicaciones Web** las cuales son **Owasp ZAP Proxy** y **Burp Suite,** ambas permiten realizar un escaneo y lograr un análisis de la aplicación WEB que se desee supervisar. Para ayudar al lector a entrar en contexto de la capacidad de análisis de estas herramientas, se describen a continuación sus principales características:

OWASP ZAP *(Zet Attack Proxy)* herramienta de código abierto y gratuita, diseñada para la prueba de aplicaciones web, conocida como "Proxy intermediario". Se encuentra entre el browser (navegador) y la aplicación web. Es capaz de conectar a otro proxy que se encuentre en la red. Pertenece a la compañía **OWASP** (*Open Web Application Security Project*) esta compañía se encarga de trabajar en la seguridad del software. Está conformada por personas alrededor del mundo tratando de promover la seguridad de los sistemas. La empresa cuenta con un **Top Ten** de las vulnerabilidades destacadas, la versión más actual es Owasp top Ten 2017. Este top permite a la comunidad de desarrolladores estar al tanto en la situación que se está viviendo en cuanto a las vulnerabilidades de los sistemas, esto contribuye a mejorar el desarrollo de los sistemas y a mejorar la protección de la información que está siendo trabajada.

Según (Owasp, 2017) "Las empresas deben adoptar este documento e iniciar el proceso para garantizar que sus aplicaciones web minimicen estos riesgos. Usar **OWASP Top 10** es quizás el primer paso más efectivo para cambiar la cultura de desarrollo de software dentro de su organización a una que produzca un código más seguro."

En la figura 26 se muestran las diez vulnerabilidades encontradas por la organización Owasp en 2017.

FIG 26. TOP 10 DE VULNERABILIDADES OWASP 2017

Zap proporciona funcionalidad para cualquier tipo de usuario ya sea que se encuentre iniciando en el mundo del pentesting o sea un experto además de contar con versiones para cada sistema operativo y Docker.

Burp Suite fue creada por la empresa *PortSwigger* y desarrollada en Java. Cuenta con dos tipos de versiones una libre y otra llamada profesional. Una de las funcionalidades de esta herramienta es un proxy, con el que se puede inspeccionar y modificar el tráfico haciendo la función de intermediario entre el navegador y la aplicación destino. Para el entorno de escritorio Windows existe un ejecutable para su instalación y para el entorno de trabajo en Linux ya se encuentra instalado por defecto. Además de esto proporciona una academia llamada "***WebSecurity Academy***" en la cual un practicante de estas técnicas puede adquirir conocimientos y mantenerse actualizado en el campo.

4. METODOLOGÍA PROPUESTA Y PRUEBAS

4.1. METODOLOGÍA PROPUESTA.

Es importante tener una guía que seguir para poder desempeñar de la mejor manera posible el trabajo que se desea realizar, para esto se propone un modelo de trabajo de pentesting. Es importante apegarse al modelo para detectar claramente las vulnerabilidades de un sistema. En la figura 27 se muestran las cinco fases que se consideran para realizar la detección.

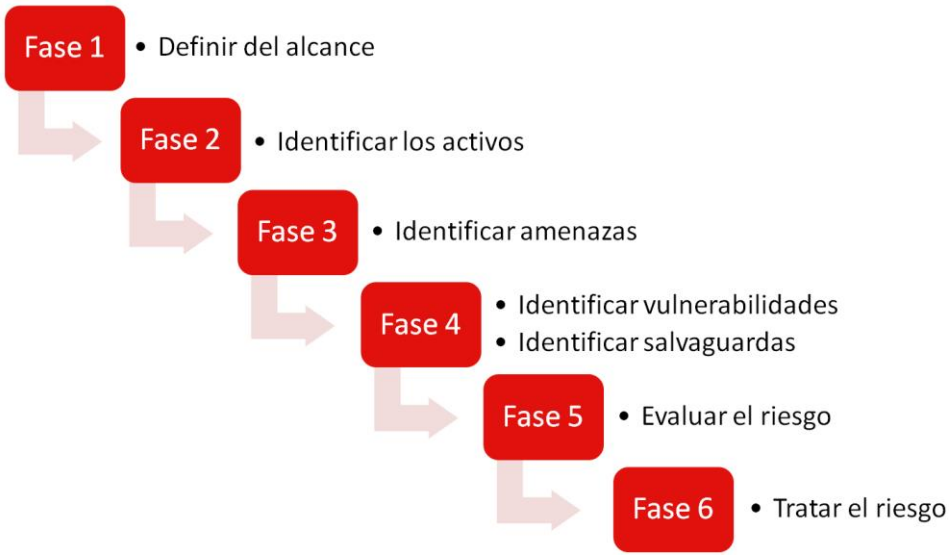


FIG 27. METODOLOGÍA PROPUESTA (INCIBE, 2017)

A continuación, se da una breve descripción de cada una de las fases de este modelo de (INCIBE, 2017)trabajo:

1. **Definición de Alcance**: Esta es la primera fase y la más importante ya que aquí se define hasta qué punto o que áreas de una organización serán las involucradas durante el análisis de vulnerabilidades.

2. **Identificar los activos:** una vez que se definió el alcance se deben identificar los activos con los con los que se trabajará, todos estos datos deben tener una relación directa con el departamento que se seleccionó para llevar a cabo el análisis, una posible opción es llevar una tabla en la que se pueda llevar el control de que activo se está trabajando, quien está asignado para llevar a cabo esa tarea, descripciones generales del activo, que tipo de activo es (software o hardware) en donde se encuentra ubicado físicamente en el departamento y si su estado es crítico o no.
3. **Identificar / seleccionar las amenazas:** se evalúan y estudian las características de los activos detectados para identificar las vulnerabilidades de éstos.
4. **Identificar vulnerabilidades y salvaguardarlas:** se realiza un estudio de los activos identificados.
5. **Evaluar el riesgo:** una vez que se tiene toda la información referente a los puntos tratados anteriormente, se debe hacer una evaluación para saber qué tan frecuente se presenta cada vulnerabilidad y que nivel de complejidad tiene, esto dará lugar para poder evaluar el impacto de las amenazas detectadas.
6. **Tratar el riesgo:** informe que es entregado al cliente, describiendo las vulnerabilidades encontradas, para que el equipo de desarrollo pueda darles solución.

Es importante comentar al lector que este trabajo considera fuertemente el análisis de la fase 2 Recopilación de información y fase 3 Identificación de vulnerabilidades, pues es necesario construir el escenario sobre el que se van a realizar las pruebas atendiendo a la construcción de un sitio web con ingreso al sistema por nombre de usuario y

contraseña, además del diseño de base de datos para identificar vulnerabilidades en estos aspectos. De tal forma que una metodología adaptada para nuestro trabajo se presenta en la figura 28.

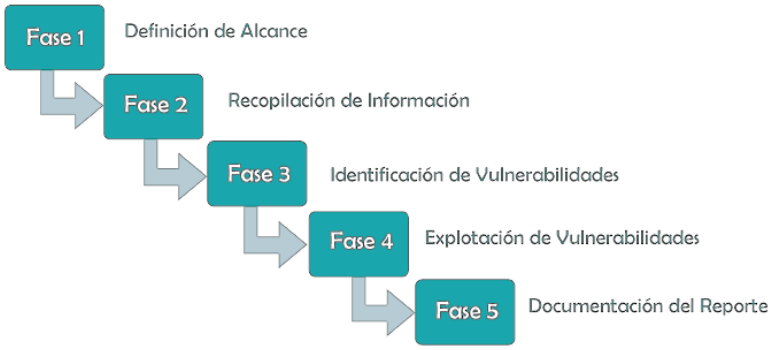


FIG 28. PROPUESTA DE METODOLOGÍA DE TRABAJO

De la metodología propuesta y la metodología que se mostró en la figura 27 se muestra la unificación entre las fases 1 y la fase 2 tomando éstas dos como los pasos más importantes para llevar a cabo el trabajo de pentesting.

4.2. PRUEBAS.

A continuación, se presentan algunos ejemplos para los que se identifica en la fase 2 los sitios web a analizar y en la fase 3 se aplican diferentes pruebas entre las que destacan las herramientas de escaneo de vulnerabilidades, Burp Suite con SQLMap para las pruebas de injection, utilizando diferentes parámetros para los diferentes métodos de análisis que se realizan con sqlmap y ZAP para pruebas generales de vulnerabilidades como análisis de sistemas de autenticación, comprobación de peticiones y respuestas cliente servidor.

Para llevar a cabo las pruebas pertinentes para este proyecto de investigación se utilizó una extensión de **Burp Suite** llamada **CO2** ésta permite la ejecución con interfaz gráfica del complemento **Sqlmap** dentro de la misma. Esta extensión cuenta con algunos módulos (pestañas) de los cuales es necesario conocer sus funcionalidades y que se listan a continuación:

- **SQLMapper**: es un ***helper*** de Sqlmap. Con el cual se puede obtener el comando a ejecutar con SQLMap ya sea desde la GUI o desde la consola de esta herramienta. El rellenado de los campos que aparecen en este apartado se llena con ayuda de la información proporcionada por el Proxy a la hora de realizar la intercepción de información del navegador.
- ***User Generator*:** hace un aproximado de combinaciones de nombres más comunes y los ordena en una lista como consecuencia. Actualmente su limitante de resultados se basa en 200,000 nombres.
- ***Name Mangler*:** dados algunos nombres y dominios, los modificara para generar una lista de nombres de usuario potenciales que pueden colocar un ***intruder*** para realizar pruebas de inicio de sesión válidos.
- ***CeWLer*:** extrae una lista de palabras de archivos HTML, esta funciona con una lista de repuestas directamente dentro de Burp.
- ***Masher*:** dada una lista inicial de palabras de la lista pronunciada, luego agrega y reemplaza caracteres para crear nuevas contraseñas.
- ***BasicAuther*:** dada una lista de nombres de usuario y una lista de contraseñas, genera cadenas de bacisauth adecuadas que luego se pueden colocar en un intruder.

De las pestañas anteriores solo se trabajó con **SQLMapper**, primera pestaña con la que se obtiene la línea de comando que será ejecutada en la consola de sqlmap, pues ésta contiene los elementos necesarios para realizar una prueba básica, de la cual se espera obtener el nombre de la base de datos, el nombre de las tablas utilizadas, algunos privilegios y/o usuarios.

4.3. PRUEBA 1 Y CONFIGURACIÓN

Antes de realizar las pruebas ver apartado de anexos (6.2) ya que en este apartado se encuentra la información necesaria para preparar el entorno de pruebas.

En la figura 29 muestra el flujo de trabajo que se tuvo entre la aplicación y el equipo de cómputo que fue utilizado para realizar las pruebas, además de que se puede visualizar en que vulnerabilidad se trabajó en base al top ten de OWASP. Observe que en el lado de la PC que ejecuta SQLMap requiere de un conjunto de software que funciona en los niveles más bajos (Hardware- SO Windows 10- Burp Suite - SQLMap).

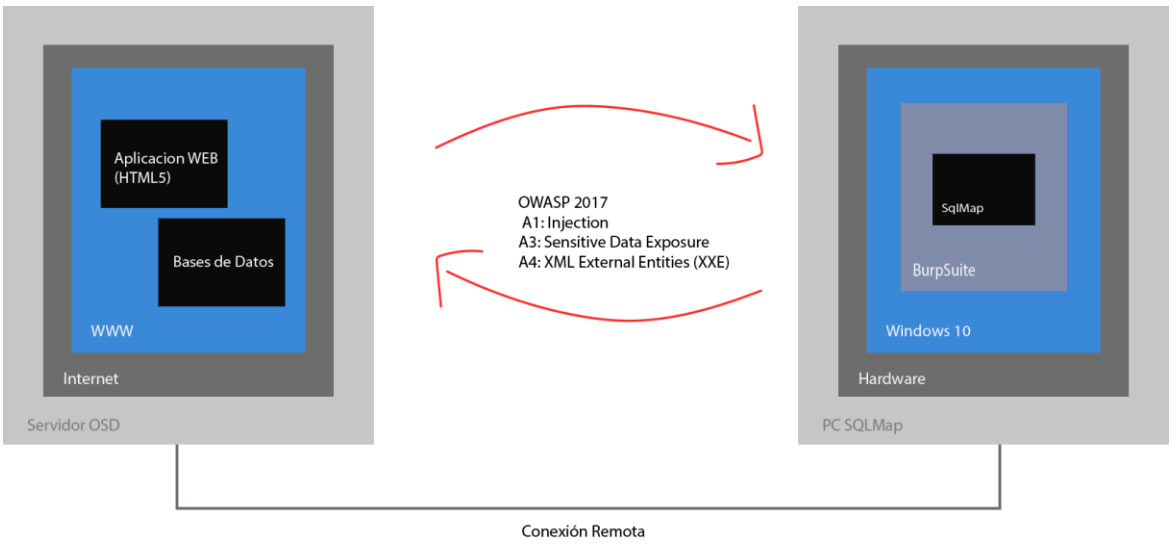


FIG 29. INTERACCIÓN PRUEBAS OSD

Para llenar algunos de los campos mostrados en la figura 30 se tiene que tomar en cuenta la información que se obtiene luego de ingresar a Burp suite (ver anexos). La información que se colocará en Basic → URL tomando en cuenta el Host que fue regresado en los apartados ya mencionados, el host retornado en la pestaña de Proxy que fue **www.osds.com.mx** ver figura 31.

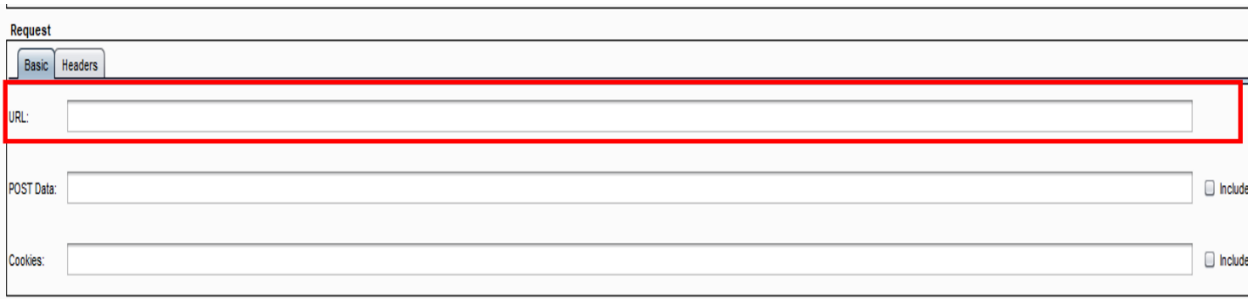


FIG 30. PRIMERA CONFIGURACIÓN DE INFORMACIÓN

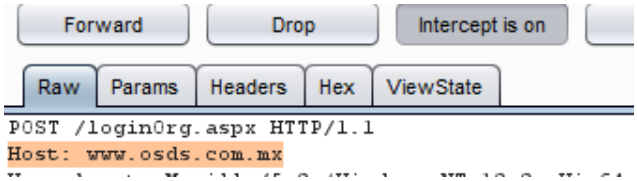


FIG 31. HOST DE LA APLICACIÓN

Luego de haber llenado el espacio de la **url,** se llenará en automático el apartado SQL Command. Conforme se vayan agregando los argumentos en la configuración dentro de la pestaña CO2, el apartado **SQLMap Command** que se encuentra en esa misma ventana mostrada en la figura 30.

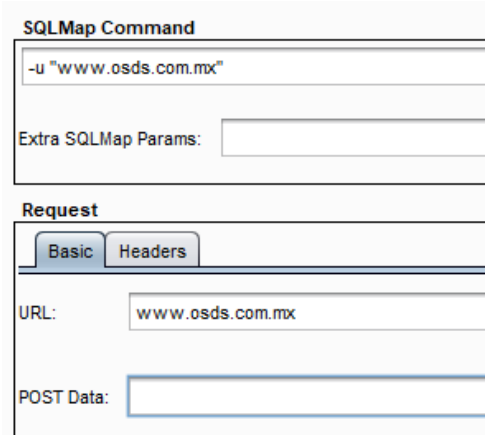


FIG 32. LLENANDO DE SQLMAP COMMAND

Así como se copió el **Host** para agregarlo en URL, ver figura 32. También se deberá copiar **Post**, ver figura 33, para continuar con la configuración, y este se pegará en el mismo apartado de URL, como se pude observar se está formando la **url** que se escaneará.

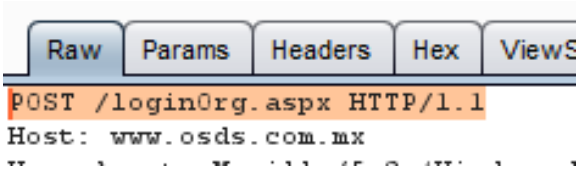


FIG 33. POST DEVUELTO EN LA INTERCEPCIÓN

Como se mencionó SQLMap Command seguirá modificándose conforme se agreguen instrucciones, en la figura 34 se puede ver la modificación, la configuración anterior solo pertenece a la línea URL.

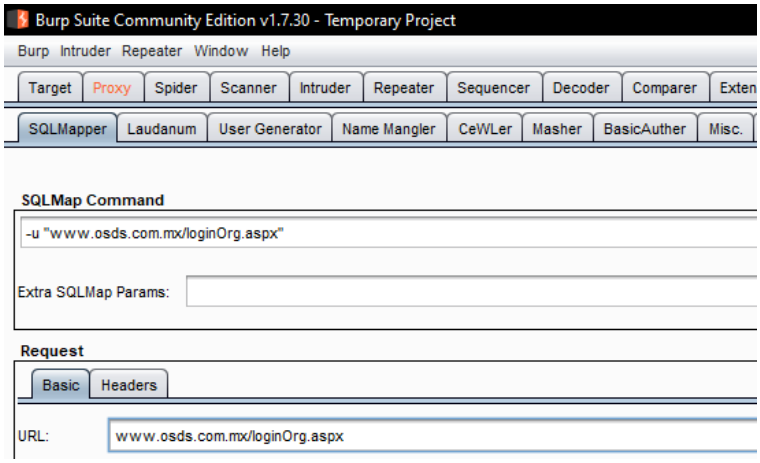


FIG 34. MODIFICACIÓN SQLMAP COMMAND

Después de URL se encuentra un apartado llamado POST en el cual se insertará la información obtenida en ***Proxy-Intercept*****,** generalmente se muestra encriptada o devolviendo los controladores/cajas de donde se está enviando la información al servidor como se muestra en la figura 35 pero para que esta sea tomada en cuenta se debe dar clic en el check que se encuentra a un lado de POST.

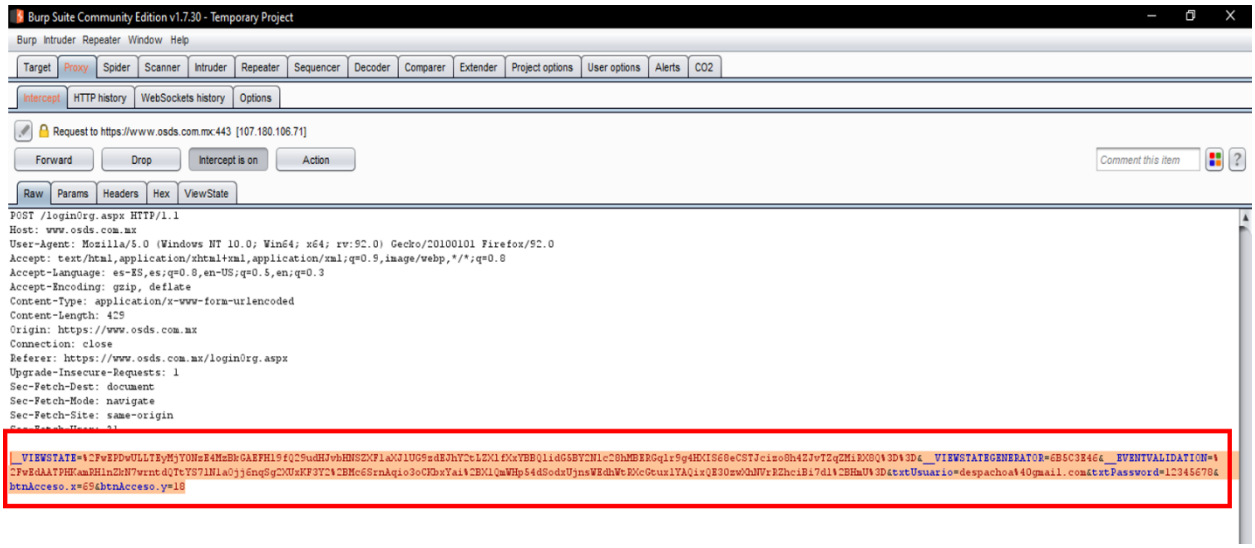


FIG 35. INFORMACIÓN QUE SE ADJUNTARA EN EL APARTADO POST

Después de agregarla POST Data lucirá como se muestra en la figura 36.

FIG 36. RESULTADO DESPUÉS DE AGREGAR INFORMACIÓN POST

La información seguirá agregándose en SQL Map Command la cuál lucirá como se ve en la figura 37.

FIG 37. SQLMAP COMMAND MODIFICADO.

Sabiendo que con SQL Map puede obtenerse diversa y gran variedad de información del servidor tales como: lo son tablas, privilegios, contraseñas etc. Se tiene la opción de configurar el apartado **Enumeration** figura **38** en el cual se indica que tipo de información se espera encontrar u obtener. Esta configuración se realiza en la misma pestaña que se ha estado trabajando.

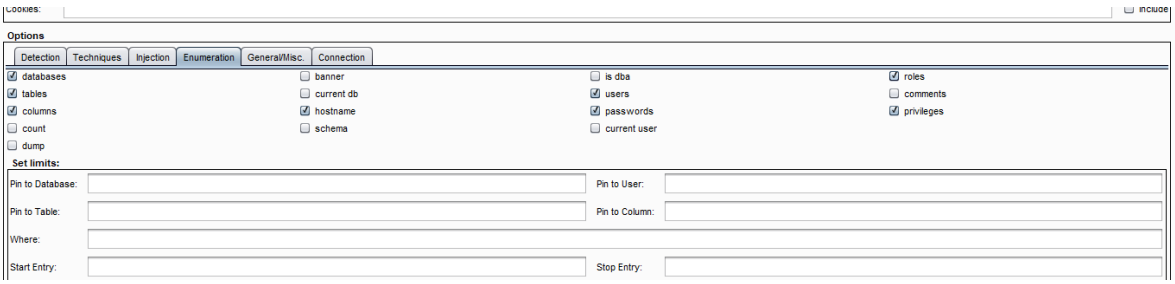


FIG 38.APARTADO ENUMERATION

En la figura 38 se puede observar los campos que fueron seleccionados para ejecutar esta prueba**; databases, tables, columns, hostname, users, passwords, roles y privilegios**. Toda esta información específica es la que se desea recuperar una vez finalizado el análisis. Mencionando la última configuración la cual en la primera prueba se dejará por defecto, CO2 cuenta con **5 niveles de análisis** y **3 niveles para el Risk figura 39.** los valores default son para el primer nivel en ambos casos.

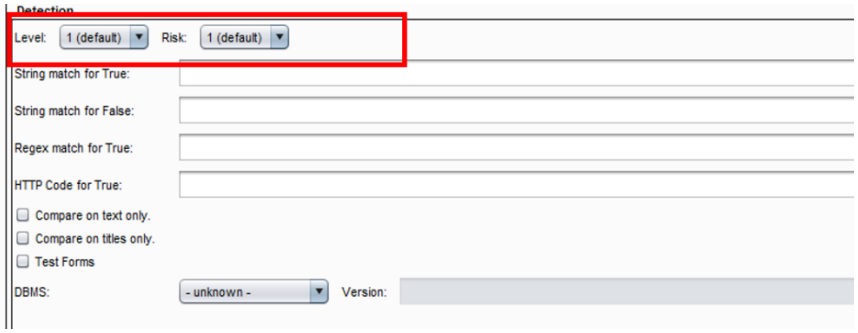


FIG 39. NIVELES DE DETECCIÓN.

Una vez que se terminó la configuración básica, es momento de dar clic en el botón RUN figura 40 que se encuentra a un lado de SQL Map Command.

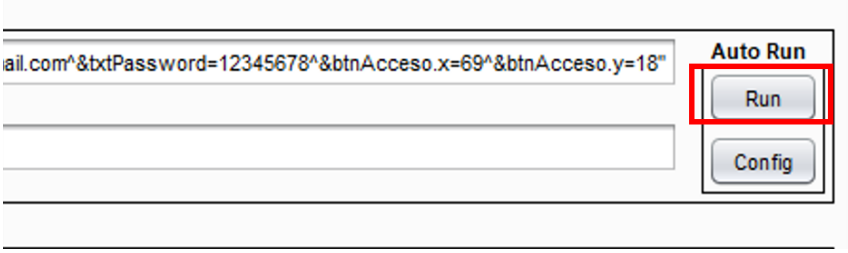


FIG 40. BOTÓN DE EJECUCIÓN

Después de esto se cargará una consola, correspondiente a la herramienta SqlMap.py con la cual se ejecutará la cadena **SQL Map Command** obtenida después de la configuración en Burp. La figura 41 muestra la primera línea de ejecución que indica una prueba de conexión hacia la base de datos.

FIG 41. CONSOLA SQLMAP

En la figura 42 linea 2 se muestra remarcado en rojo el letrero **CRITICAL** debido a aque no se ha podido establecer la conexión con la URL de destino por lo que el sistema

intenta nuevamente hacer la perticion para poder establecer una conexión, además de mostrar una sugerencia en la linea 3. Después de haber terminado el proceso anterior es mostrará una sugerencia para intentar regresar la solicitud como un agente aleatorio o un conmutador switch.

FIG 42. CONEXIÓN INESTABLE

Luego de haber intendado establecer la conexión nuevamente se muestra el mensaje “no se pudo establecer conexión con la url destino” y una vez más sqlmap realiza un intento para conectarse, seguido de esta acción se muestra un mensaje diciedo “ la conexión con la url destino no es estable…” indicando en este caso que se procedera con un comparador de secuencias. Preguntando si se desea continuar, encadenar hacer un regex o salir del analisis. Para este escenario se dio la instrucción de continuar con el proceso introduciendo la **letra c** y dando enter para continuar. Una vez ejecutada la instrucción se despliega la respuesta obtenida siguiente, “No se ha podido comprobar el contenido dinamico debido a la falta de contenido de la pagina”, procediendo asi con la ejecucion y dando respueta a las siguentes peticiones realizadas por sqlmap.

Iniciando el escaneo por parametros, los cuales fueron ingresados en la configuracion como metodo post. En este caso indica que se estan ignorando tres parametros que son; __VIEWSTATE, VIEWESTATEGENERATOR y __EVENTVALIDATION. Tomando como

parametro dinamico '**txtUsuario'**, pues durante la ejecucion fue detectado con estas caracteristicas figura 43.

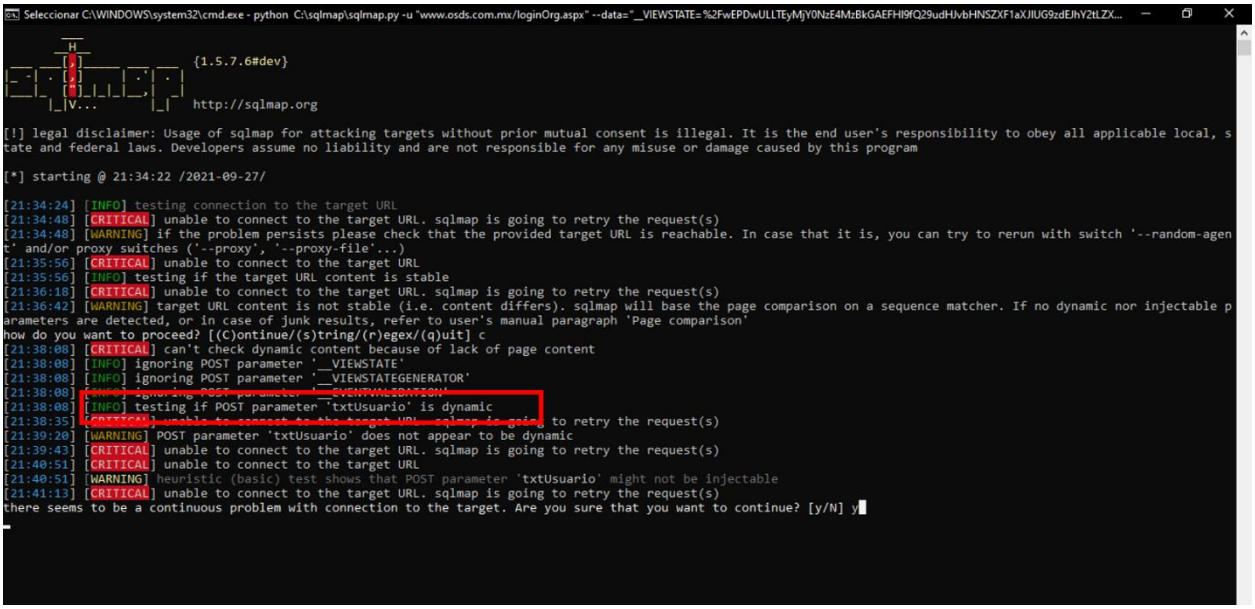


FIG 43. TESTEO

Haciendo una inspección al codigo de marcado de texto a la aplicación web figura 44 este parámetro es perteneciente a la caja de texto en donde se introduce el correo del usuario registrado para acceder al sistema.

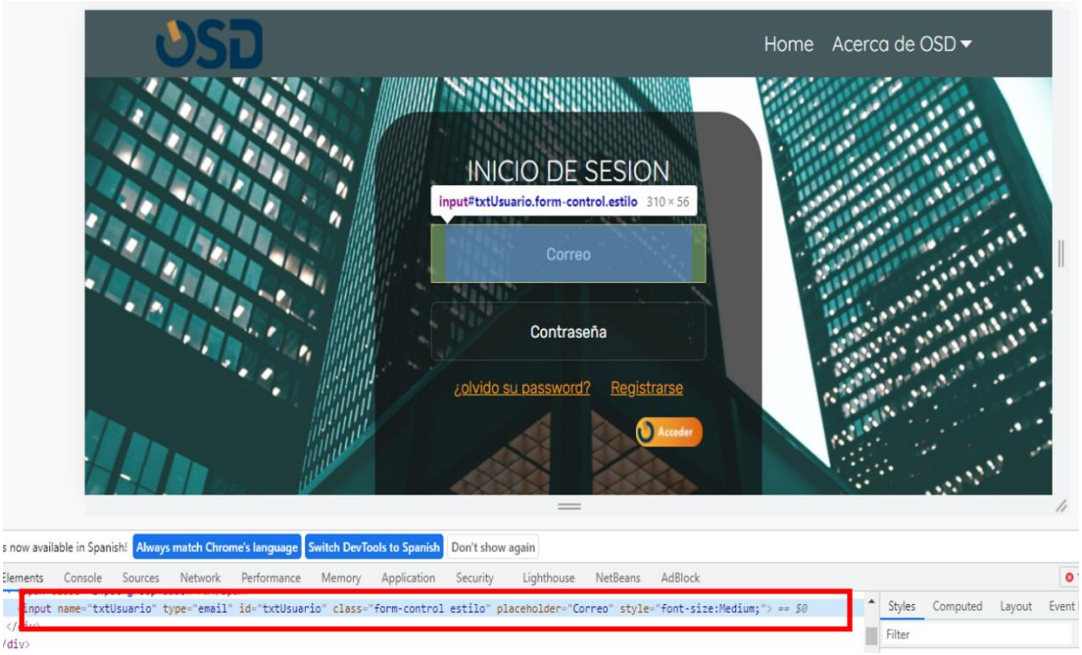


FIG 44. VERIFICACIÓN DE PARÁMETRO DINÁMICO

Procediendo con el testeo ocurrio nuevamente la desconeccion con la url destino y nuevamente la herramienta intenta reconectarse a esta, regresando la desconexion. **La linea [21:40:51] indica que la prueba heurística (básica) muestra que el parametro testeado (‘txtUsuario’) puede no ser inyectable figura 45**. Posterior a esto se vuelve a intetar la reconexion con la URL ya que ha permanecido incestable durante el proceso de testeo. Ahora la respuesta a la conexcion, fue que se encontro una conexión continua y pregunta si se desea continuar a lo que la respuesta que se le dio fue si. Iniciando asi con un testeo para SQL injection con metodo POST tomando como parametro a analizar **txtUsuario** nuevamente, y continuando con un testeo 'AND booleand-based blind -where or having clause'.

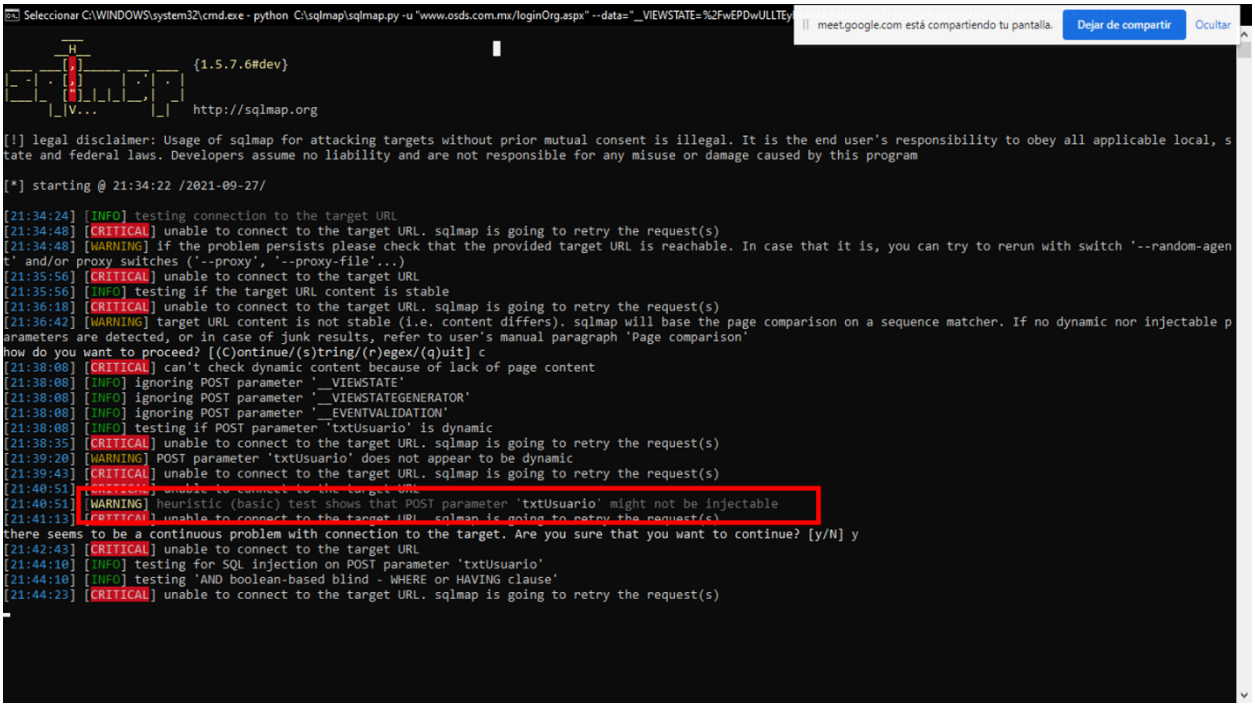


FIG 45. PARÁMETROS NO INYECTABLES.

En este punto fue detenida la ejecución pues en una prueba anterior a esta se obtuvieron los mismos resultados, y continuando a este paso ocurrió lo siguiente.

No se logró establecer la conexión después de siete u ocho intentos aproximadamente, al lograr establecerla se detecta que la aplicación posiblemente se encontraba asegurada por algún tipo de **WAF/IPS figura 46** el cuál es un tipo de protección contra ataques de **inyección SQL** y **XSS (*Cross-Site Scripting*).**

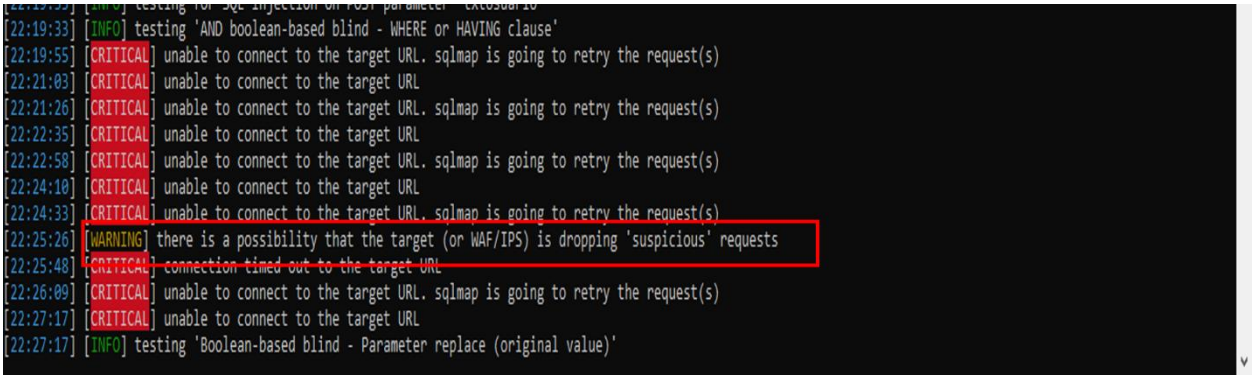


FIG 46. DETECCIÓN DE PROTECCIÓN WAF/IPS

El tiempo estimado de esta prueba inicio a las 21:34:24 terminando a las 22:27:17 con una estimación de tiempo de una hora con aproximadamente treinta minutos.

4.3 PRUEBA 2 Evaluando con --proxy=http://127.0.0.1:8080 nivel 2 y Risk 2.

Al inicio de la prueba anterior se hizo una sugerencia para la evaluación del test aplicando el parámetro/conmutador, que en este caso es la instrucción --**proxy con el cual se puede conectar a la URL destino a través del proxy** y **Risk** hace referencia a **el nivel del riesgo de las pruebas a realizar**. Dicho parámetro se coloca en **SQL Map Command → Extra SQLMap Params figura 47** en este apartado se pueden escribir algunos otros parámetros que no se encuentren gráficamente en **burpsuite,** pero que, si pueden ser ejecutados por **sqlmap**, como es el caso del conmutador proxy.

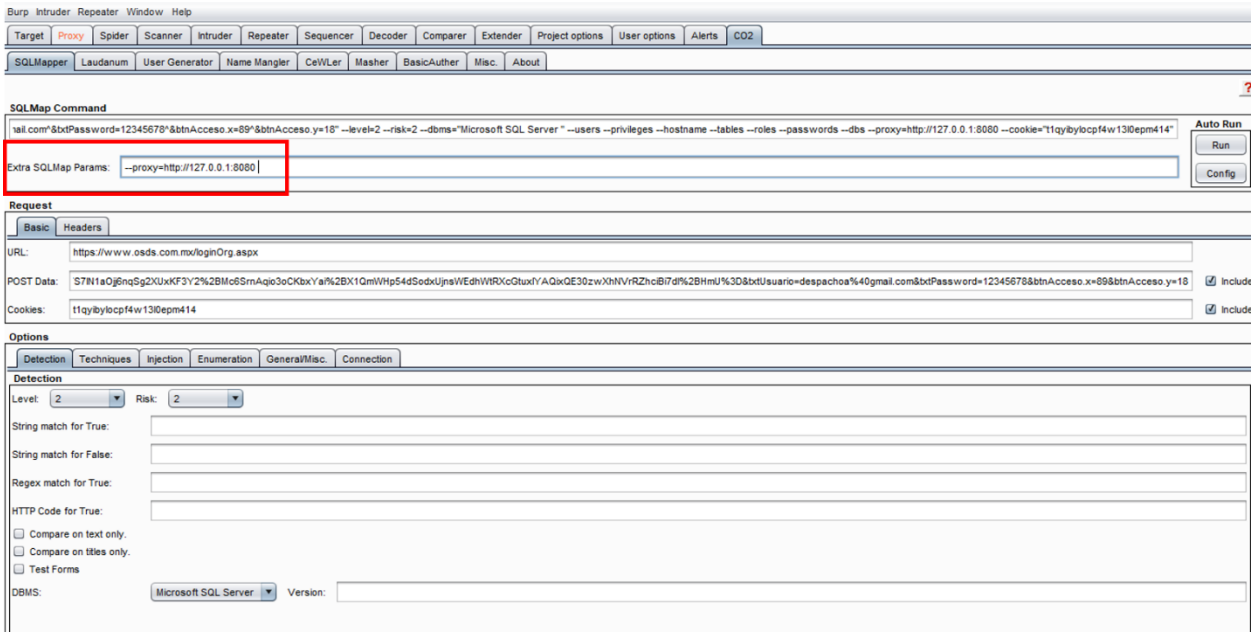


FIG 47. CONFIGURACIÓN EXTRA SQLMAP PARAMS

Para esta primera prueba se dio una explicación paso a paso como introducción a la configuración de algunos campos que fueron utilizados como parámetros en las pruebas que se llevaron a cabo. En esta solo se agregan los argumentos extras en el apartado

que ya se mencionó. Luego de escribir el o los parámetros necesarios, la línea que fue ejecutada por SQLMap fue la siguiente, cabe destacar que algunos de los atributos enviados son parte de la información que se desea obtener después del análisis:

Información enviada a través de las cajas de texto de la aplicación:

- ***txtUsuario****: envía el nombre del usuario que está siendo ingresado en el sistema por medio de su correo electrónico.*
- ***txtPassword****: clave de acceso al sistema.*

Además de la información que es ingresada para hacer las peticiones, se están estableciendo como parámetros los siguientes valores, los cuales indican el grado de complejidad del análisis:

- **Nivel de análisis**: --level 2.
- **Nivel de riesgo**: --risk 2.
- **Motor de Base de Datos**: *Microsoft SQL Server, que cual fue utilizado por el desarrollador para el alojamiento de la información del sistema.*
- --users: pretendiendo encontrar una lista de los usuarios pertenecientes al sistema.
- --privileges: lista de privilegios.
- -hostname: nombre del host.
- --tables: nombre de las tablas creadas en el motor de base de datos.
- --roles: los roles del usuario.
- Contraseñas: --paswords.

Se envió además el parámetro del proxy para poder acceder a la aplicación en caso de que se encuentre con algún tipo de protección.

- *Proxy: --proxy=http://127.0.0.1:8080*

Debido a que es común el uso de tokens o cookies para la identificación de un usuario para aprobar su acceso o mantener su sesión en todas las páginas de la aplicación web, es decir que en el navegador se queda información a la deriva, se pasó como parámetro el argumento Cookies el cual ayudara a descifrar la información adicional que está siendo utilizada en el navegador.

- *8080 --cookie="t1qyibylocpf4w13l0epm414"*

*-u "https://www.osds.com.mx/loginOrg.aspx" --data="__VIEWSTATE=%2FwEPDwULLTEyMjY0NzE4MzBkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYBBQlidG5BY2Nlc28hMBERGqlr9g4HXIS68eCSTJcizo8h4ZJvTZqZMiRX8Q%3D%3D^&__VIEWSTATEGENERATOR=6B5C3E46^&__EVENTVALIDATION=%2FwEdAATPHKamRHlnZkN7wrntdQTtYS7lN1aOjj6nqSg2XUxKF3Y2%2BMc6SrnAqio3oCKbxYai%2BX1QmWHp54dSodxUjnsWEdhWtRXcGtuxlYAQixQE30zwXhNVrRZhciBi7dl%2BHmU%3D^&**txtUsuario=despachoa%40gmail.com**^&**txtPassword=12345678**^&btnAcceso.x=89^&btnAcceso.y=18" **--level=2 --risk=2 --dbms="Microsoft SQL Server " --users --privileges --hostname --tables --roles --passwords --dbs --proxy=http://127.0.0.1:8080 --cookie="t1qyibylocpf4w13l0epm414"***

Resultado tras la ejecución de dicha linea de comandos se muestra en la figura 48.

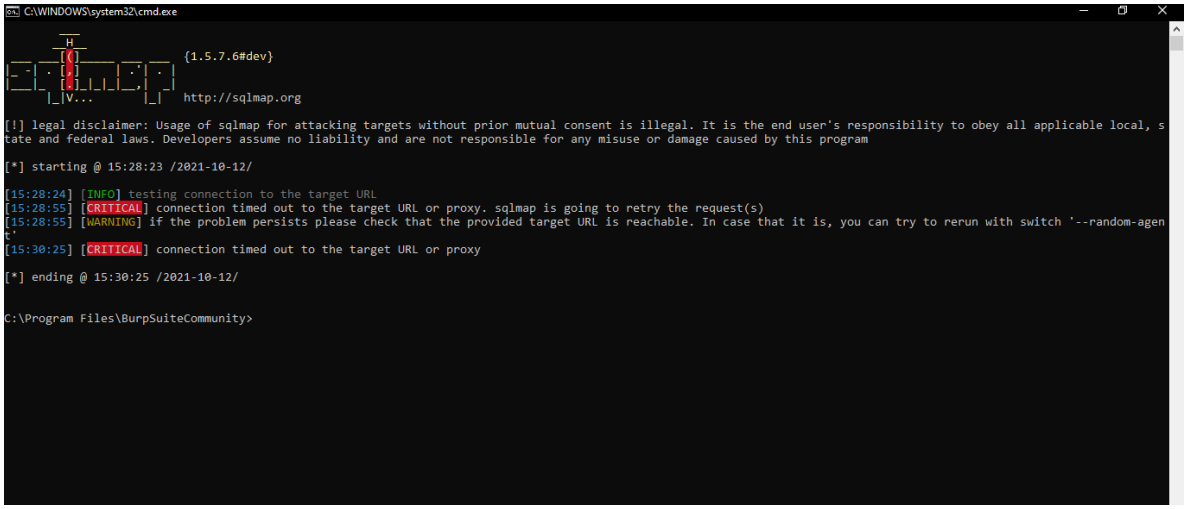


FIG 48. RESULTADO EVALUACIÓN CON --PROXY=HTTP://127.0.0.1:8080 NIVEL 2 Y RISK 2.

Tiempo de ejecución de esta prueba fue de aproximadamente 3 min.

4.4 PRUEBA 3 EVALUANDO CON COMANDO --random-agent nivel 2 y risk 2

En este caso en Extra SQLMap Params se adjunta el argumento --**random-agent** este arguento ayuda a **usar un valor del header de agente aleatorio HTTP seleccionado aleatoriamente**, además se configuran los parametros nivel y risk pasandolos de su posicion por default a un nivel 2 de ejecucion y añadiendo el motor de base de datos utilizado en la aplicación web figura 49.

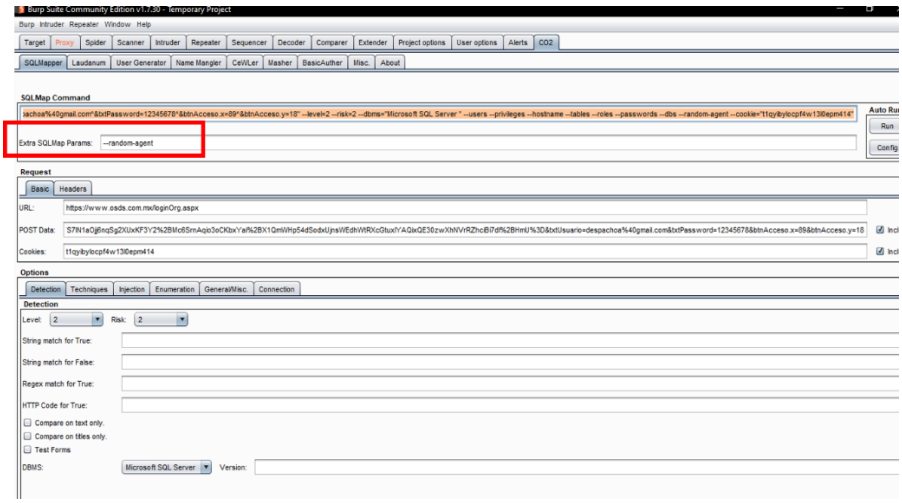


FIG 49. CONFIGURACIÓN PARA PRUEBA 3.

Comando ejecutado para prueba 3.

Los argumentos destacados de esta prueba fueron:

- *txtUsuario*
- *txtPassword*
- *--level=2*
- *--risk=2*
- *--dbms="Microsoft SQL Server "*
- *--users*
- *--privileges*
- *--hostname*
- *--tables*
- *--roles*
- *--passwords*
- *--dbs --random-agent*
- *--cookie="t1qyibylocpf4w13l0epm414"*

*-u "https://www.osds.com.mx/loginOrg.aspx" --data="__VIEWSTATE=%2FwEPDwULLTEyMjY0NzE4MzBkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYBBQlidG5BY2Nlc28hMBERGqlr9g4HXIS68eCSTJcizo8h4ZJvTZqZMiRX8Q%3D%3D^&__VIEWSTATEGENERATOR=6B5C3E46^&__EVENTVALIDATION=%2FwEdAATPHKamRHlnZkN7wrntdQTtYS7lN1aOjj6nqSg2XUxKF3Y2%2BMc6SrnAqio3oCKbxYai%2BX1QmWHp54dSodxUjnsWEdhWtRXcGtuxlYAQixQE30zwXhNVrRZhciBi7dl%2BHmU%3D^&**txtUsuario=despachoa***%40gmail.com^&***txtPassword=12345678****^&btnAcceso.x=89^&btnAcceso.y=18" **--level=2** **--risk=2** **--***

dbms="Microsoft SQL Server " --users --privileges --hostname --tables --roles --passwords --dbs --random-agent --cookie="t1qyibylocpf4w13l0epm414"

Resultado de prueba 3

En esta prueba al igual que en las pruebas anteriores el parámetro que fue detectado de tipo dinámico para realizar el análisis continúo siendo **txtUsuario**. Como se puede observar en este escenario se obtuvo mayor número de información (valores de cajas de entrada de datos, evaluaciones para inyecciones de valores booleanos, queries, etc) en los escaneos realizados figura 50 en comparación con los resultados de la prueba anterior.

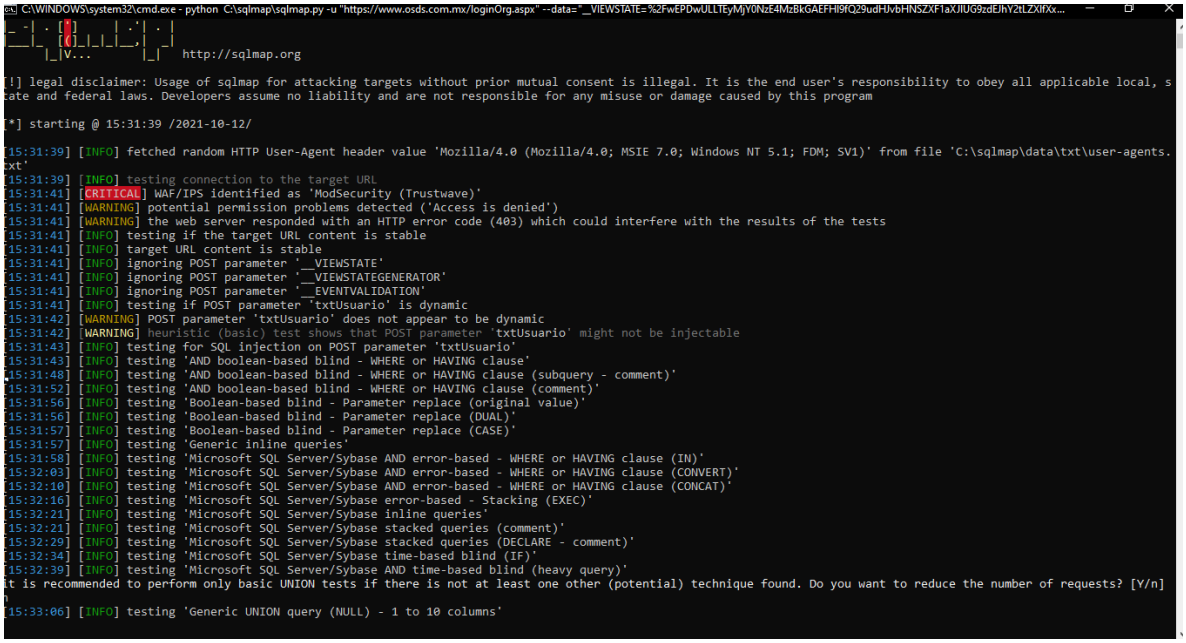


FIG 50. RESULTADO TESTEO PRUEBA 3.

En la última línea mostrada en la figura 50 se hace una observación en la cual se recomienda realizar solo una prueba de unión básica si no se encuentra al menos una técnica (potencial), preguntando si se quiere reducir el número de peticiones en este

caso se respondió negativamente para continuar con la configuración que fue establecida para esta prueba.

En la figura 51 línea [16:00:34] se envía un aviso sobre el parámetro que se analiza. En el que se informa que el parámetro parece no ser inyectable, en las siguientes 3 líneas se indica lo mismo, posteriormente se continúa analizando y se puede apreciar que se está escaneando en base al motor de base de datos que le fue configurado a esta prueba.

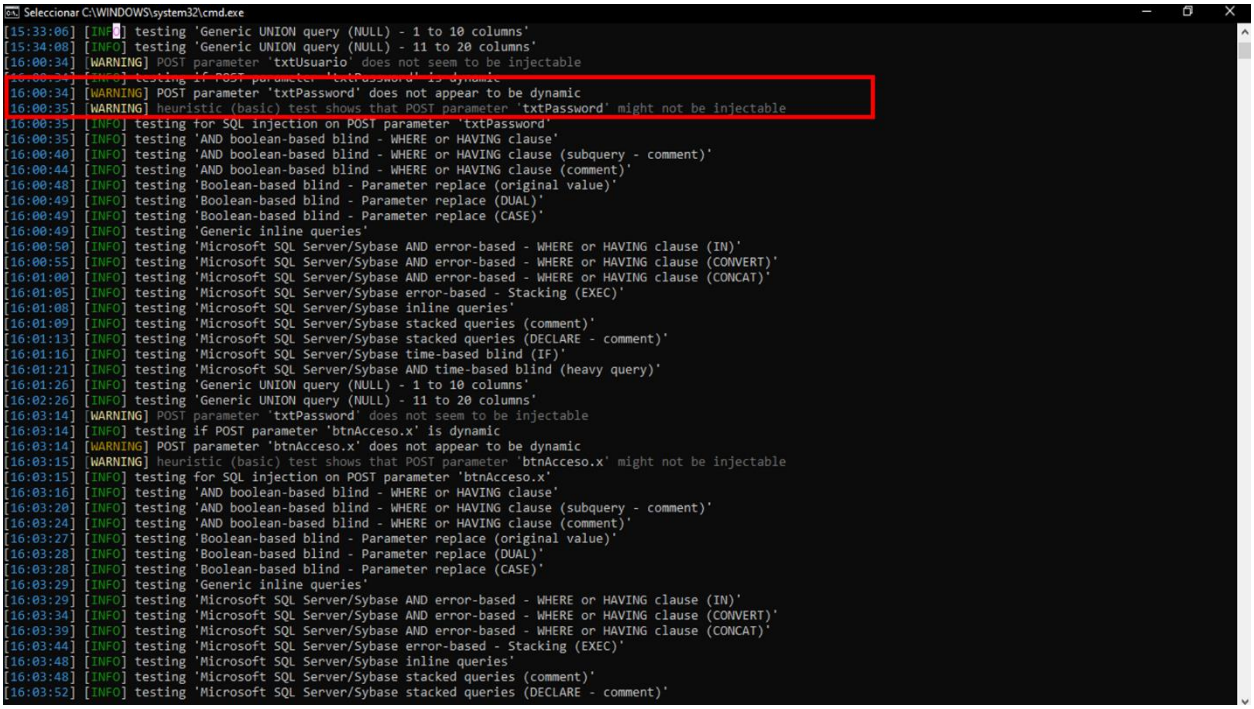


FIG 51. RESPUESTA PRUEBA 3 CONTINUACIÓN.

En la línea [16:03:14] de la figura 51 se inicia un nuevo testeo cambiando el parámetro **txtusuario** al parámetro **btnAcceso.x** este y el parámetro anterior fueron obtenidos de la información que se pasó como parámetros en el aparto POST en la configuración, y en la línea [16:05:53] también se detecta **btnAcceso.y.** Mencionando que el único valor de interés para este caso de estudio, de entre los que fueron detectados como dinámicos,

era **txtUsuario** pues pertenece a un caja de texto en donde es ingresada información y los otros dos parámetros hacen referencia al botón de acceso al sistema.

Terminando con los escaneos aparece un mensaje en donde se indica la posibilidad de que todos los parámetros analizados no son inyectables, dando una recomendación en la figura 52 de subir el nivel tanto de risk como de nivel e intentar obtener mejores resultados.

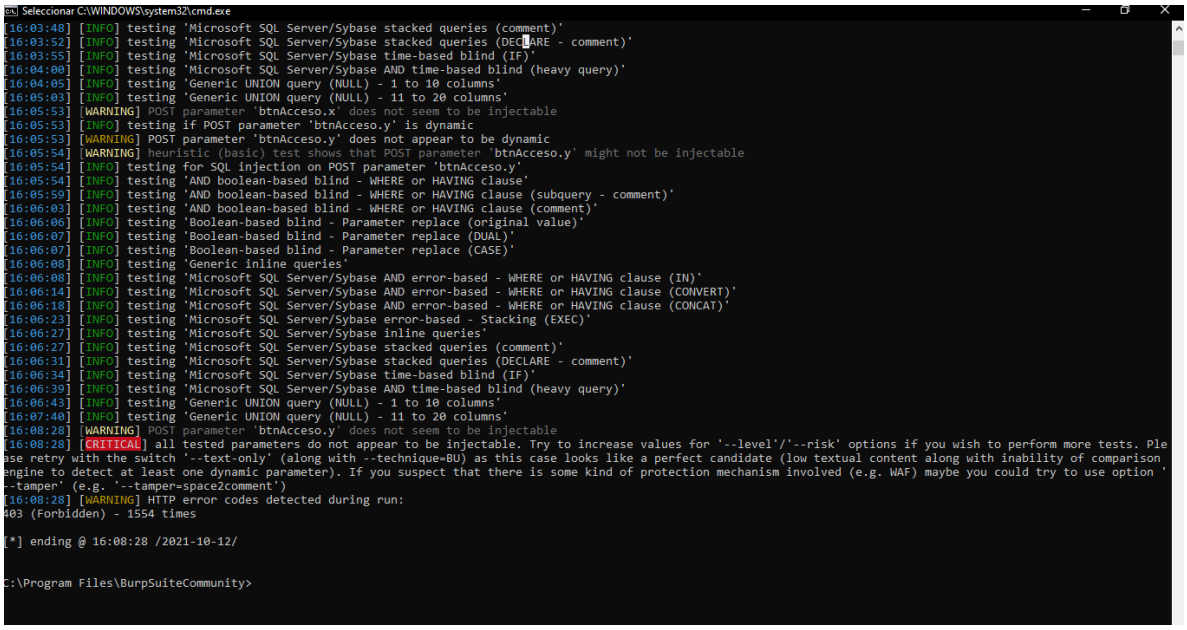


FIG 52. TERMINO DE PRUEBA 3

Tiempo de ejecución para esta prueba fue de aproximadamente de 1hr con 30min.

4.5 PRUEBA 4

Para esta prueba se utilizó un sistema web diferente con la finalidad de poder observar las diferentes conductas de los testeos dependiendo de las herramientas utilizadas para el desarrollo de las aplicaciones y las precauciones que los desarrolladores hayan tenido para la implementación de éste, en esta prueba se utilizó la página web de CIEN

Empresa. En la figura 53 se muestra el nivel de vulnerabilidades con las que se trabajaron durante las pruebas.

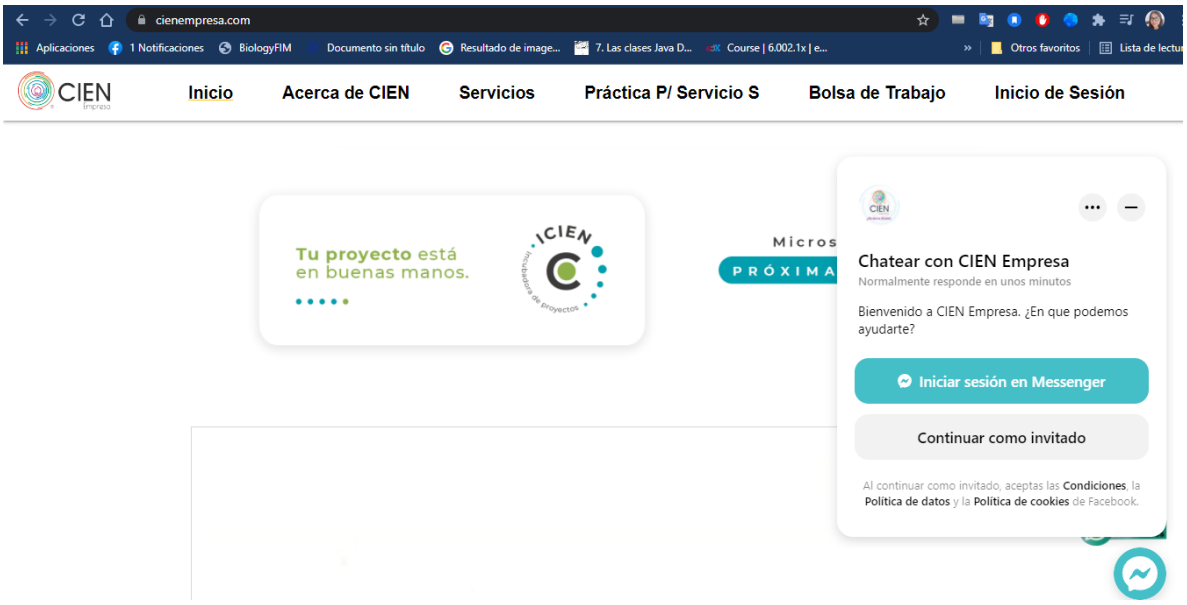


FIG 53. PAGINA CIENEMPRESA

El apartado que será analizado en esta plataforma es el de su inicio de sesión, ver figura 54, al igual que el anterior ya que tiene parámetros dinámicos. Además de que es el flanco de peticiones al servidor para ejecución de **querys**, y que puede proporcionar información como; quien es el administrador del sistema.

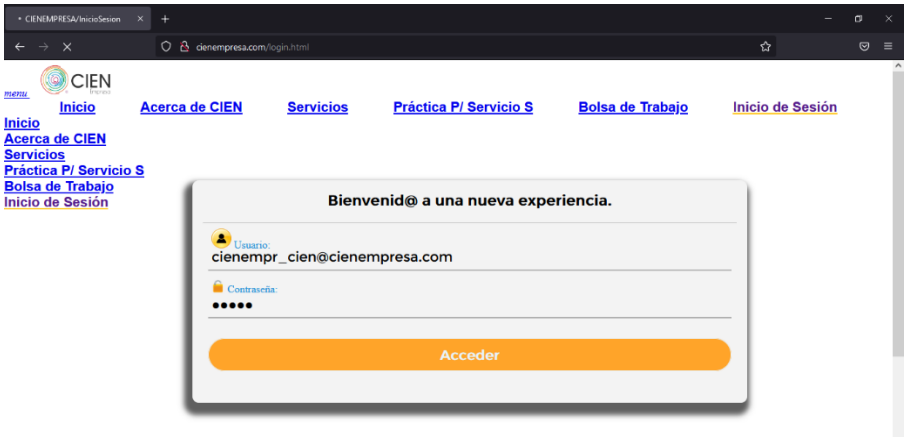


FIG 54. INICIO DE SESIÓN CIENEMPRESA

Configuración en Burp suite.

En esta prueba se desea obtener los **usuarios**, **privilegios**, **nombre** de **host**, **roles**, **tablas**, **contraseñas** y **base** de **datos** del sistema. El nivel en que se llevará a cabo el análisis es de nivel 2 y risk en nivel 2. En este escenario no se pasa el motor de base de datos utilizado como parámetro en el DBMS (*sistema de gestión de bases de datos*) puesto que no se sabe en que se desarrolló figura 55.

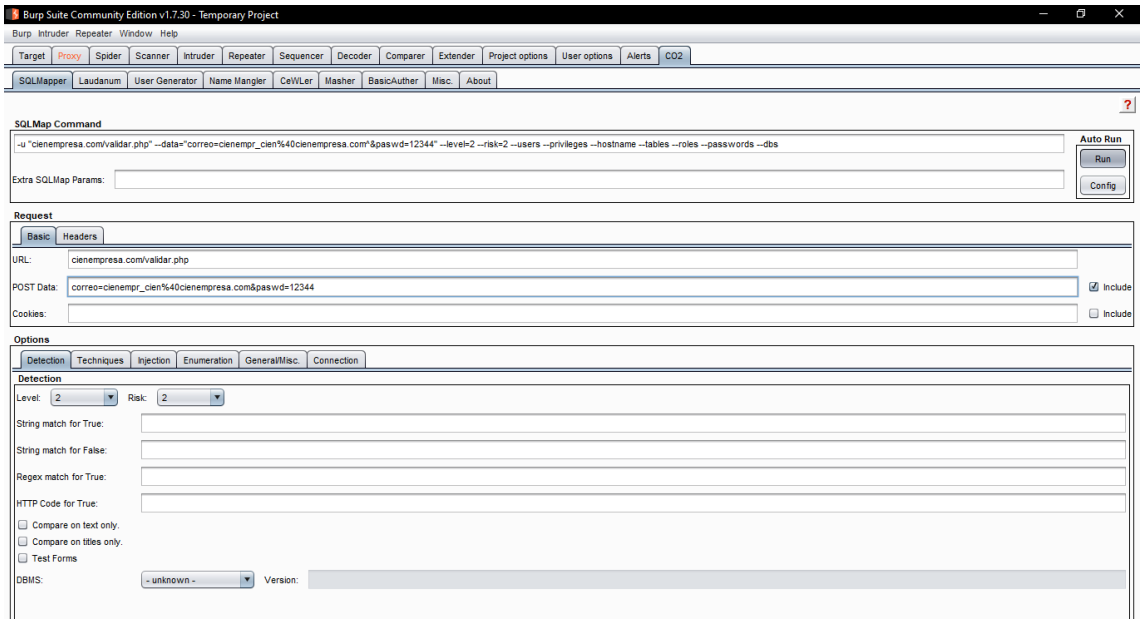


FIG 55. CONFIGURACIÓN CIEN EMPRESA

Ejecución de la prueba.

En esta prueba el parámetro que se detecta como dinámico para analizar es ‘correo’ y se inician los testeos para detección de instrucciones que retornen una respuesta booleana, además de realizar pruebas por distintos motores de bases de datos, como MySql, PostgreSQL, Oracle, Microsoft SQL figura 56.

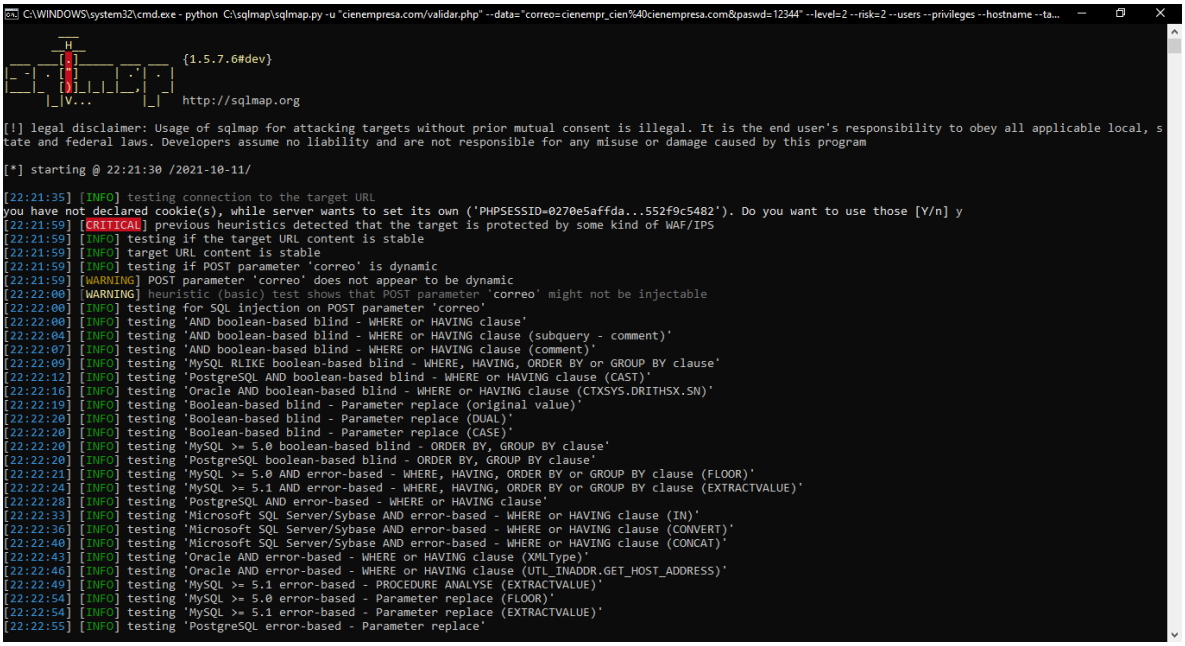


FIG 56. EJECUCIÓN DE PRUEBA CIENEMPRESA

En la figura 56 se realizan pruebas para líneas genéricas de **queries** de distintos motores de bases de datos. Encontrando el parámetro correo inyectable, lo que se observa aquí es la devolución del motor de base de datos utilizado en el back-end el cual es MySQL en su versión 5.0.12. En la línea [22:23:36] se observa esto y además se pregunta si se desea omitir las cargas útiles de pruebas específicas para otros DBMs, a lo que la respuesta fue si, el compilador regresa otra línea con la pregunta “para las pruebas restantes, ¿quiere incluir todas las pruebas para MySQL ampliando el nivel 2 y valores re riesgo 2 proporcionados?” para lo que la respuesta una vez más fue afirmativa procediendo así con el análisis extendiendo los rangos automáticos para la unión detectando 3 columnas de la URL destino inyectables. Como respuesta a este escaneo se obtuvo una inyección fallida porque los valores utilizados eran nulos, por consiguiente, se pregunta si se desea utilizar valores aleatorios para la opción **‘—union-char’**, nuevamente la respuesta fue afirmativa.

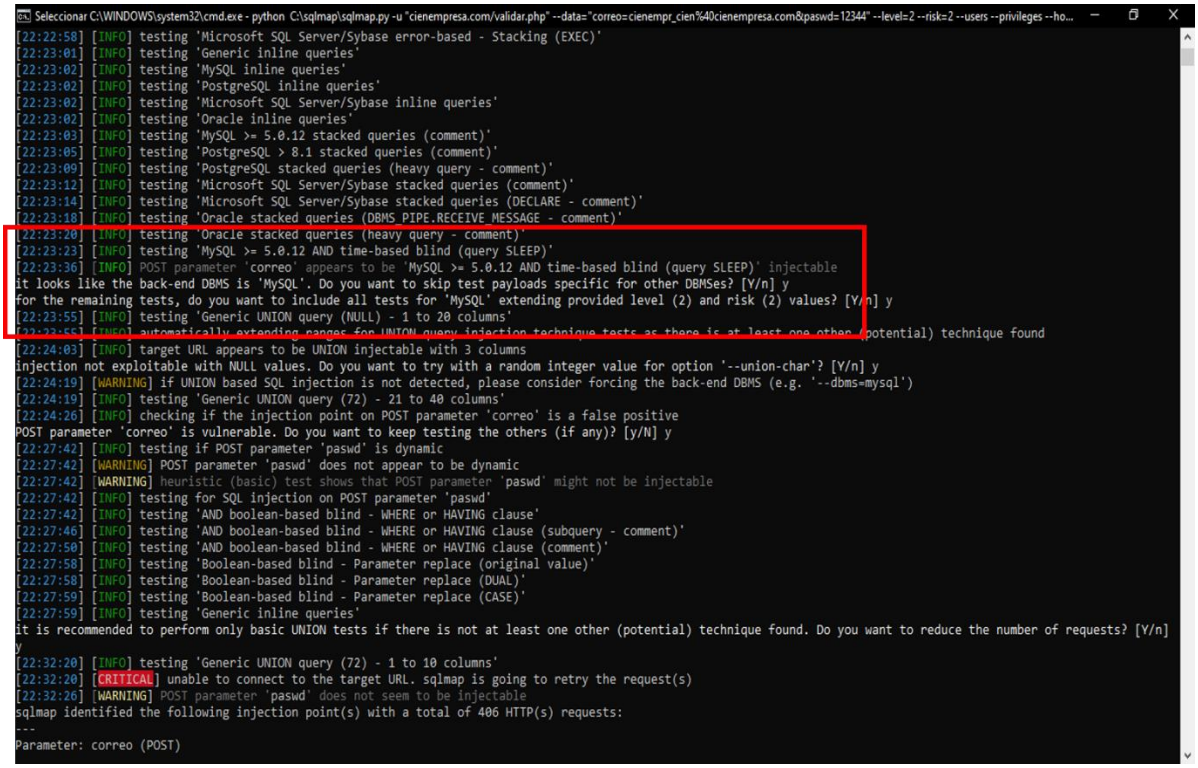


FIG 57. DETECCIÓN DE PARÁMETROS INYECTABLES

Continuando con el análisis en la línea [22:24:26] se realiza una prueba para verificar si el punto de inyección que es el parámetro **correo** es un falso positivo**, encontrando el parámetro vulnerable**, y preguntando si se quiere mantener el testeo de otros en caso de que existan, y una vez más la respuesta fue sí. Ahora el parámetro analizado es **paswd** y no parece ser inyectable. Identificando 406 solicitudes https para el punto de inyección que fue el parámetro correo con método de entrada POST figura 58.

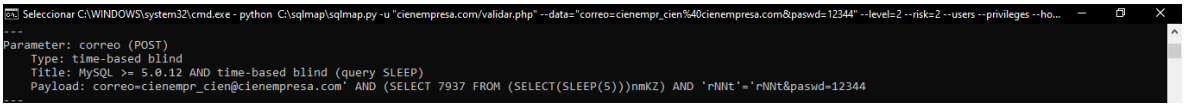


FIG 58. VALORES DEVUELTOS DEL VALOR INYECTABLE.

En la figura 58 se muestra la **tecnología** que fue utilizada para el desarrollo de esta aplicación web, el **nombre del host**, el administrador de la base de datos y algunos otros datos que serán mostrados a continuación.

- **Tecnología**: Apache, PHP.
- **Nombre del host**: sh-pro32.hostgator.mx
- **Administrador de la base de datos:** cienemp_cienempresa@localhost
- **Privilegio:** cienemp_cienempresa, verfigura 59.

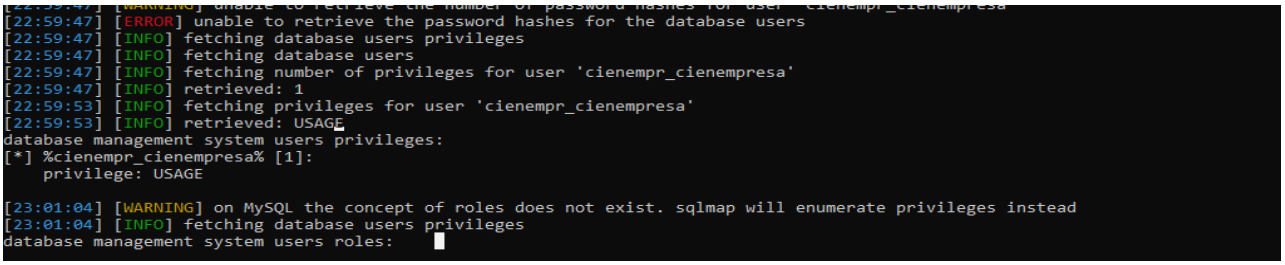


FIG 59. RESPUESTAS DE LA PRUEBA A CIENEMPRESA

En la figura 60 se muestran los nombres de las bases de datos detectadas que tienen como nombres, **cienempr_empresacien** e **información_schema.** Posteriormente se inicia la búsqueda de los nombres de las tablas para ambas bases de datos.

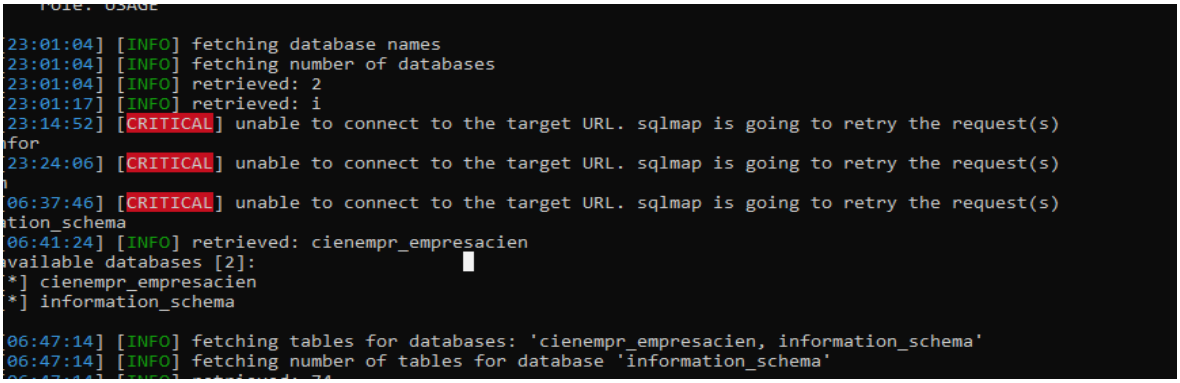


FIG 60. NOMBRES DE BASES DE DATOS.

Para **información_schema** se detectaron 74 tablas de las cuales se pueden apreciar sus nombres en la figura 61.

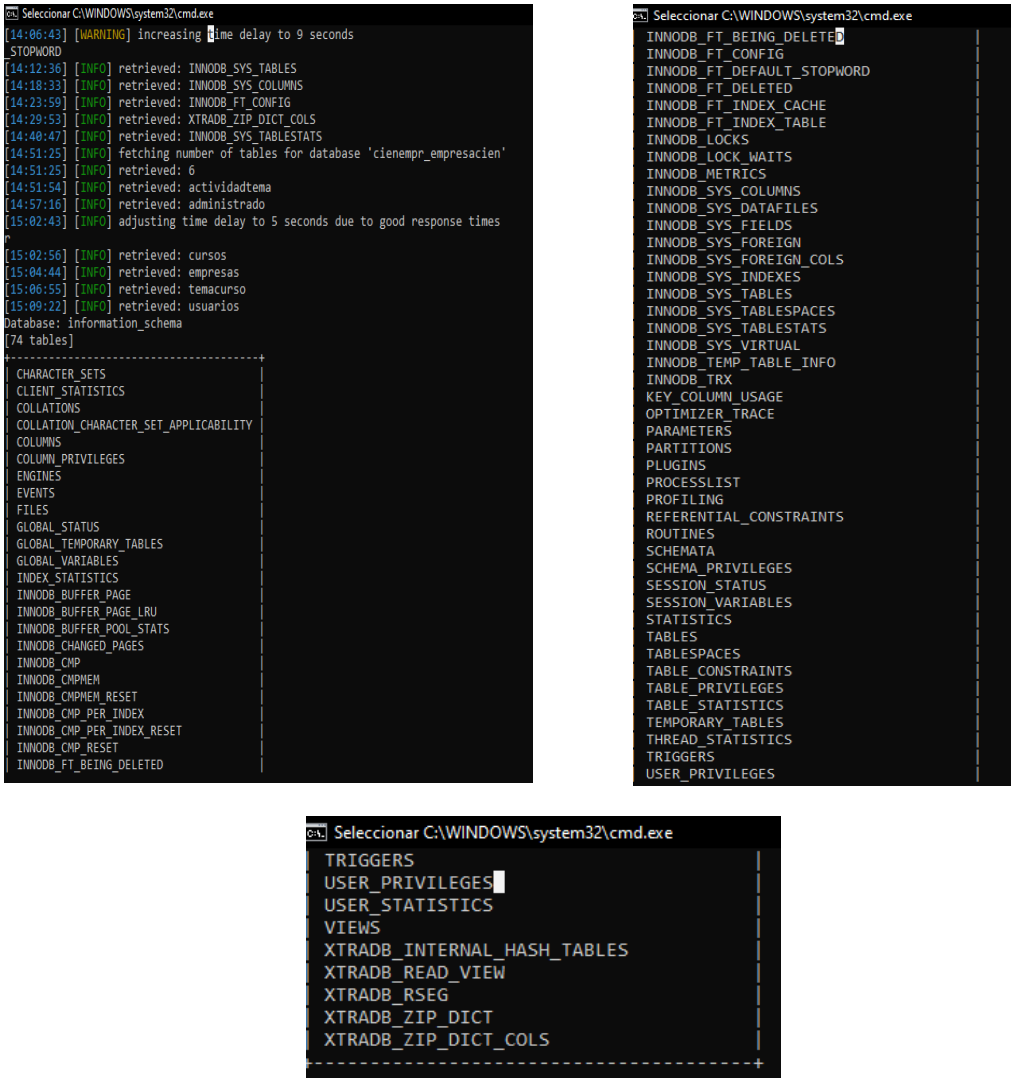


FIG 61. NOMBRES DE TABLAS PARA INFORMACIÓN_SCHEMA

Para **cienempr_empresacien** se obtuvieron 6 tablas cuyos nombres se ven en la figura 62, además de mostrar los nombres de estas tablas, en la figura se puede observar los niveles de vulnerabilidades de acuerdo al top ten de OWASP 2017, en los que se trabajó.

Observe que en el lado de la PC que ejecuta SQLMap requiere de un conjunto de software que funciona en los niveles más bajos (Hardware- SO Windows 10- Burp Suite - SQLMap).

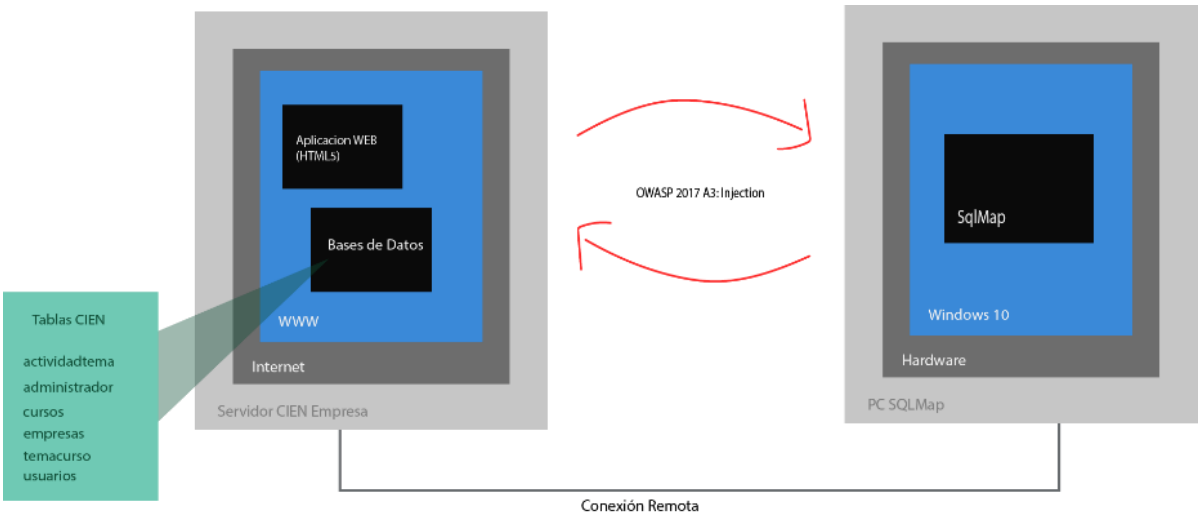


FIG 62.NOMBRES DE TABLAS PARA CIEN EMPRESA

El tiempo de ejecución para esta prueba fue aproximadamente de 10 hrs.

4.6 PRUEBA 5. ANÁLISIS CON ZAP (ZED ATTACK PROXY)

Para la siguiente prueba realizada se utilizó el ambiente de virtualización VirtualBox en el que se Instaló una máquina virtual con Kali Linux. Para iniciar la prueba se inició VirtualBox. Observe que en el lado de la PC que ejecuta ZAP requiere de un conjunto de

software que funciona en los niveles más bajos (Hardware- SO Windows 10- VirtualBox - ZAP).

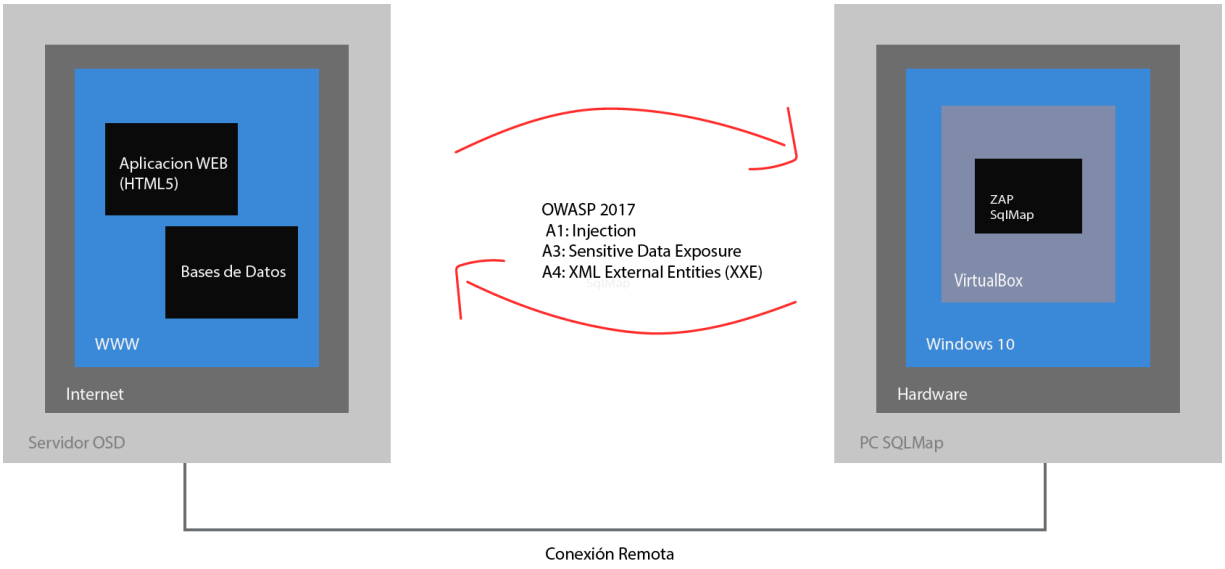


FIG 63. INTERACCIÓN DE ANÁLISIS DE VULNERAVILIDADES CON ZAP

Al iniciar Kali, se pedirán las credenciales de acceso que fueron configuradas en la instalación, puesto que es un ambiente seguro siempre se tendrá que iniciar sesión con las credenciales correspondientes.

Una vez dentro de la sesión de la máquina virtual con el sistema operativo Kali Linux, se abrió Mozilla Firefox como se ve en la figura 64. Tal como en las pruebas anteriores, también se debe configurar el navegador para hacer las intercepciones a través del proxy de Mozilla.

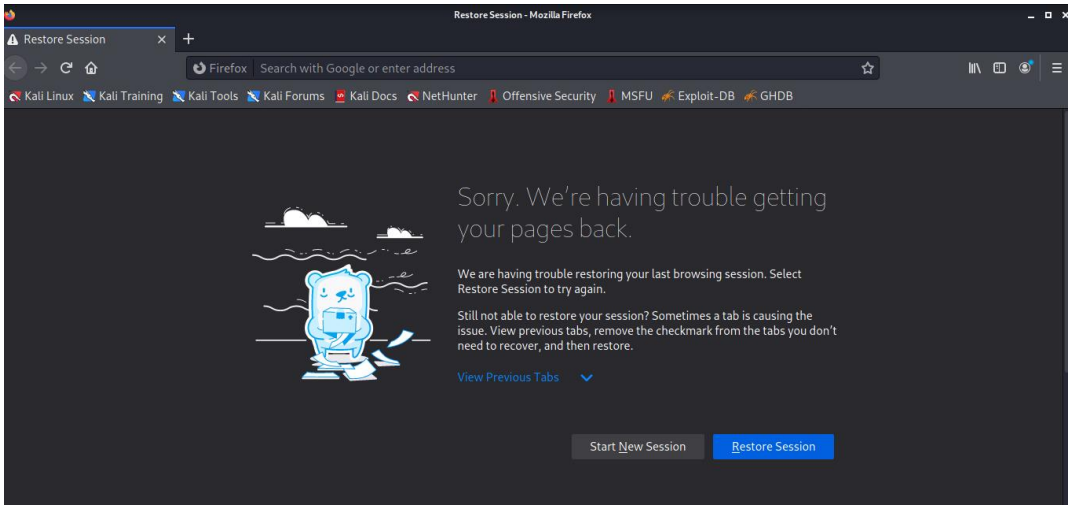


FIG 64. NAVEGADOR MOZILLA EN KALI LINUX

Una vez comprobada la configuración, también se abrió el entorno de pruebas ZAP (*Zet Attack Proxy*).

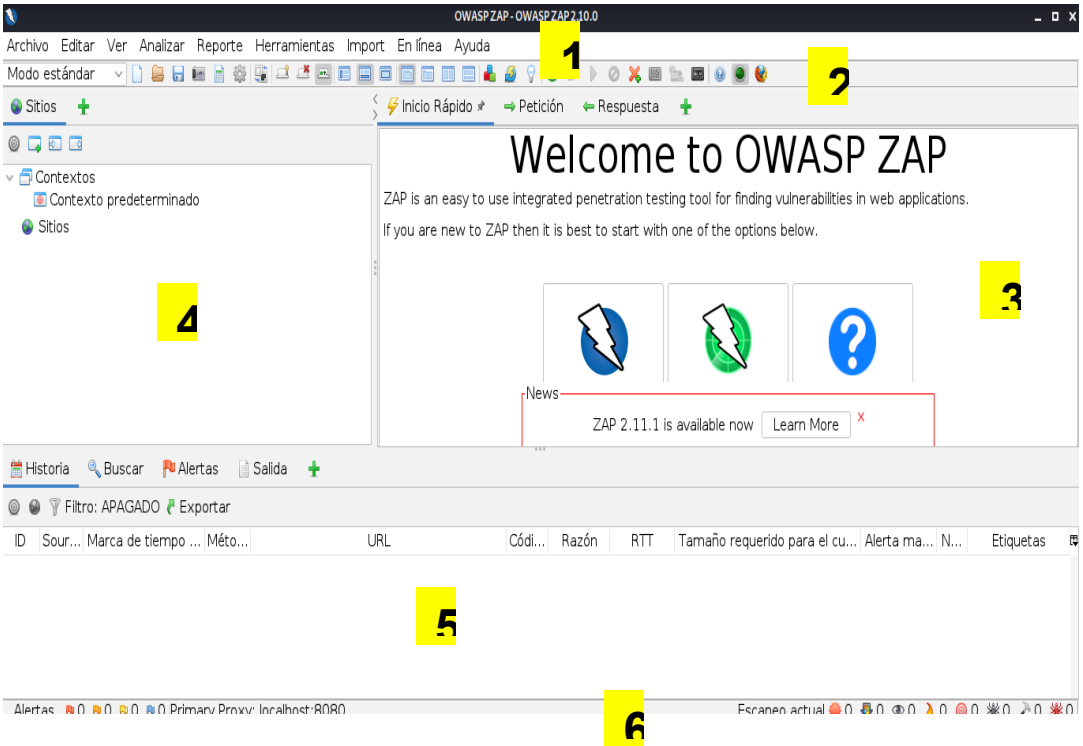


FIG 65. COMPONENTES DE ZAP

ZAP cuenta con 6 apartados como se puede ver en la figura 65.

1. **Menú**: acceso a las funcionalidades de ZAP.
2. **Barra de herramientas**: cuenta con accesos directos y funcionalidades.
3. **Espacio de Trabajo**: permite visualizar los mensajes intercambiados.
4. **Árbol de sitios**: re recogen cada una de las páginas web que se visiten.
5. **Ventana de información**: se mostrará un historial de las peticiones enviadas.
6. **Pie**: se muestran iconos con el estado de ciertas acciones.

INICIANDO PRUEBA

En el espacio de trabajo se dio clic al botón **Inicio Rápido** y luego de esto en **URL to Attack** se escribió la URL del sitio web que se va a analizar, en este caso será https://ww.osds.com.mx figura 66. Al dar clic en el botón atacar se iniciaron las peticiones y esto puede ser visto en la ventana de información en donde se muestra el estado de proceso del archivo analizado, el método que utiliza, la url que se está interceptando y las banderas.

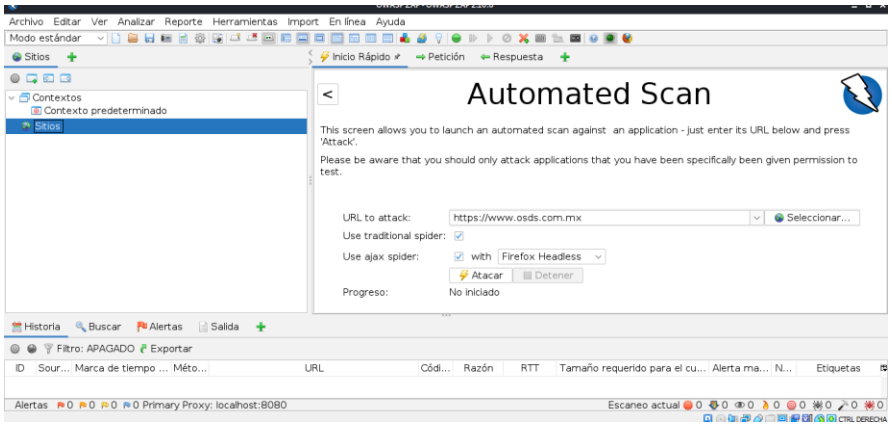


FIG 66. INICIO DE PRUEBA

Los escaneos realizados a las diversas pruebas pueden demorar un poco de tiempo, esto dependerá de la información que se esté interceptando, ver figura 67.

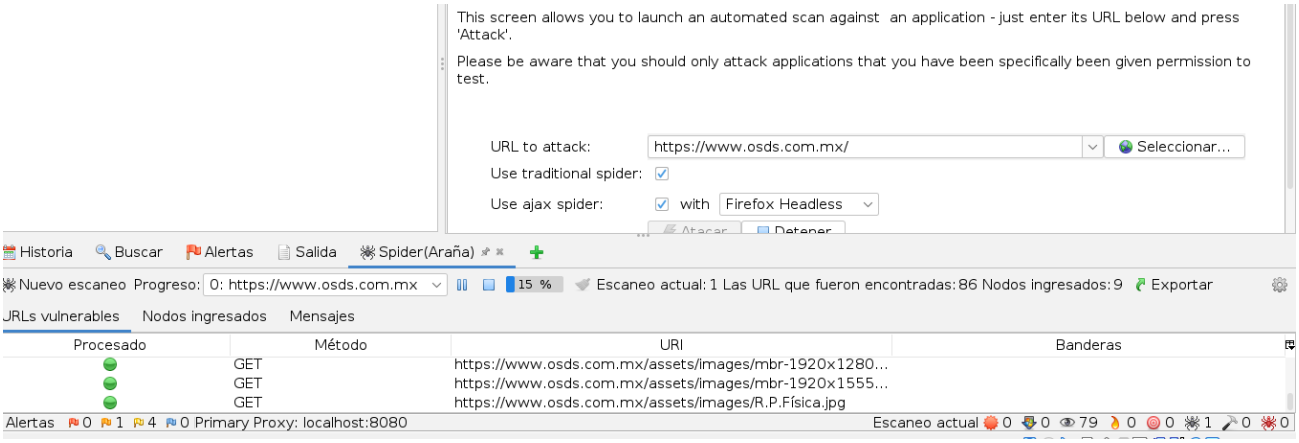


FIG 67. INICIO DE INTERCEPCIONES

Una vez terminado el análisis, el sitio o la aplicación web interceptada se podrá ver en el **árbol de directorio** (costado izquierdo) figura 68, mostrando las banderas con colores dependiendo de la complejidad de la alerta.

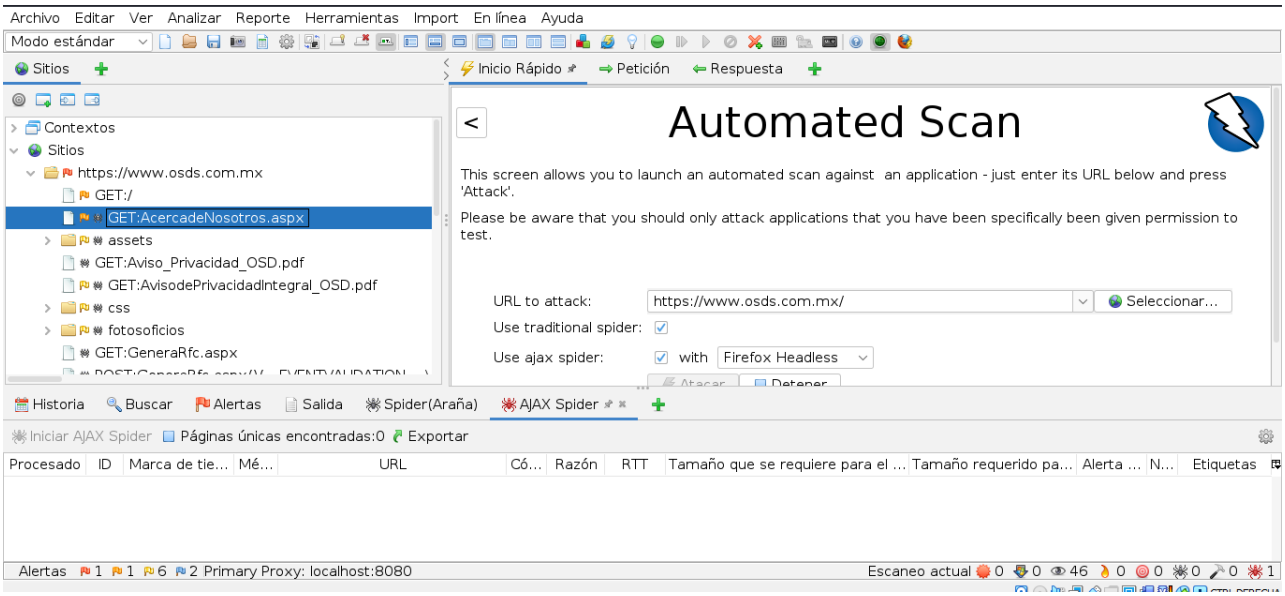


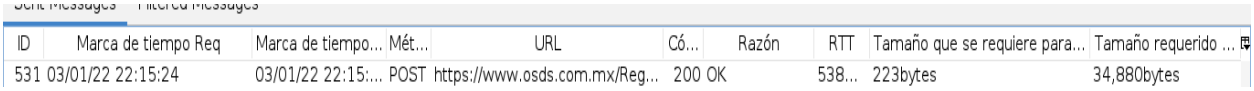
FIG 68. INFORMACIÓN EN ÁRBOL DE DIRECTORIO

Los niveles que se manejan son los que se presentan en la Tabla 3.

TABLA 3. NIVELES DE ALERTAS ZAP

NIVEL	COLOR
Bajo	Amarillo
Medio	Naranja
Alto	Rojo
Informativo	Azul

En la figura 69 de muestra la información que se pudo obtener durante la prueba, los cuáles fueron; Id de la prueba que se realizó, tiempo en el que se ejecuto la prueba, metódo de respuesta de la prueba regalizada, url perteneciente al proyecto y a la que se le esta realizando la prueba, codigo devuelto, entre otros.



ID	Marca de tiempo Req	Marca de tiempo...	Mét...	URL	Có...	Razón	RTT	Tamaño que se requiere para...	Tamaño requerido ...
531	03/01/22 22:15:24	03/01/22 22:15:...	POST	https://www.osds.com.mx/Reg...	200	OK	538...	223bytes	34,880bytes

FIG 69. INFORMACIÓN OBTENIDA DE LA PRUEBA.

Una vez que se completo la prueba al 100%, se puede ver todas las url analizadas tal como se muestra en la figura 70.

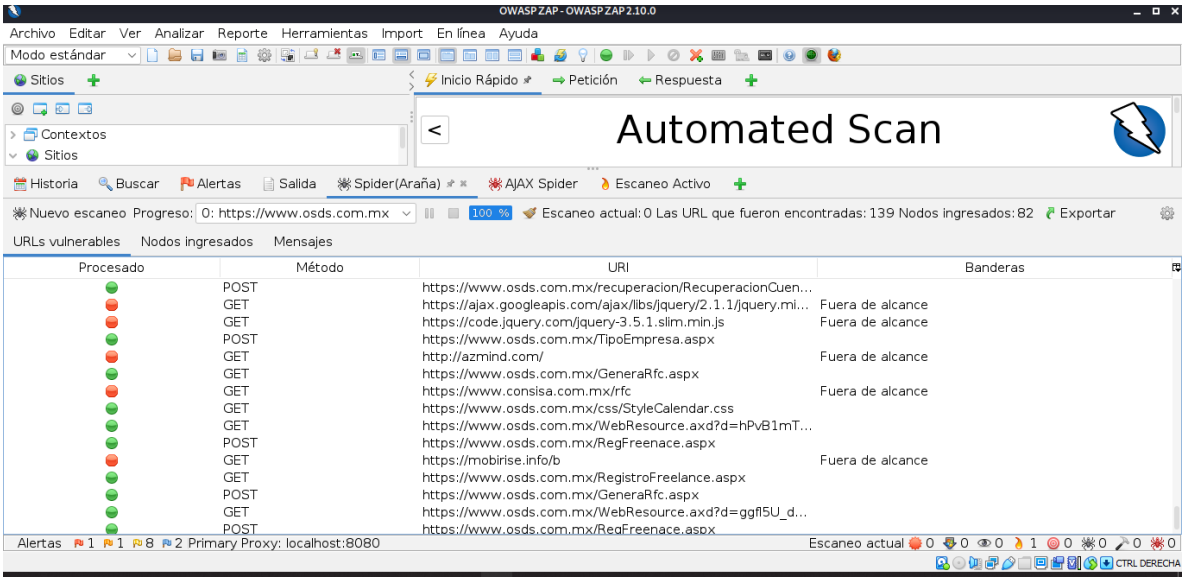


FIG 70. URL'S ANALIZADAS

En este caso se obtendrá el reporte que proporciona ZAP. Para exportarlo se debe ir al Menú se encuentra un apartado que se llama **Reporte como se puede ver en la figura 71.**

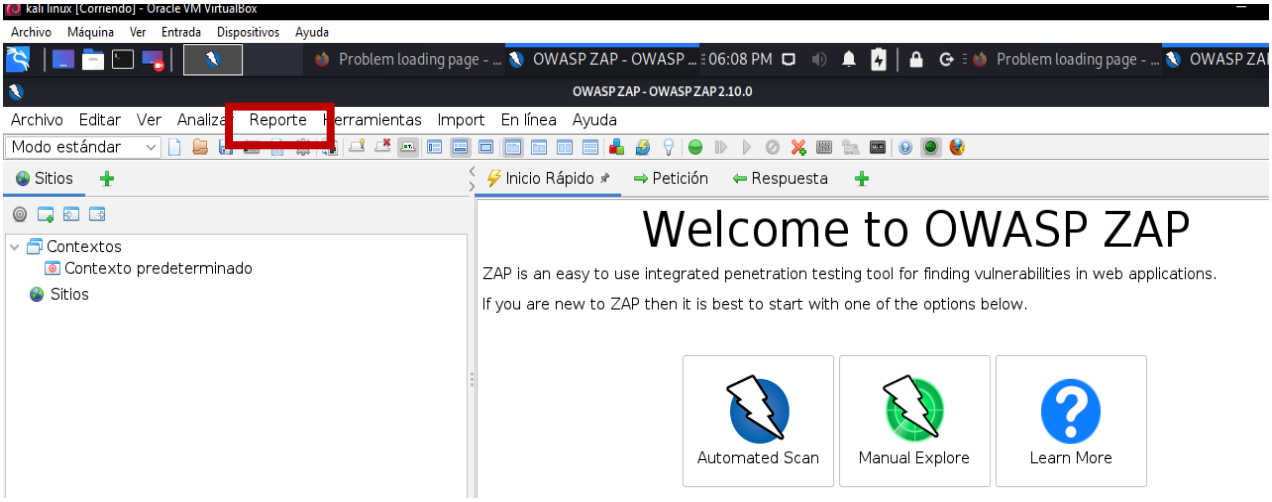


FIG 71. MENÚ REPORTE

Este reporte se puede descargar, al dar clic sobre esta opción se muestran las diversas sub opciones para obtener la información, ver figura 72.

FIG 72. MENÚ DE OPCIONES PARA OBTENER REPORTE.

En este caso se tomó el reporte como HTML, al dar clic se abrirá una ventana en la que se pedirá la ruta en donde será almacenado el archivo. La ruta en donde se almaceno es en el Escritorio, así como se ve en la figura 73.

FIG 73. ALMACENADO DE REPORTE HTML

En este caso se eligió el Escritorio como ruta de almacenamiento y el nombre que se le dio al archivo fue **reporte.html.** Una vez descargado se dio doble clic sobre el archivo y se abrió una ventana en el explorador en donde se muestra toda la información referente al análisis realizado anteriormente. En la figura 74 se muestra la siguiente información:

1. **Fecha y hora en la que se realizó el análisis.**
2. **Niveles de riesgo de las alertas y la cantidad obtenida durante el análisis.**
3. **Nombre de las alertas.**

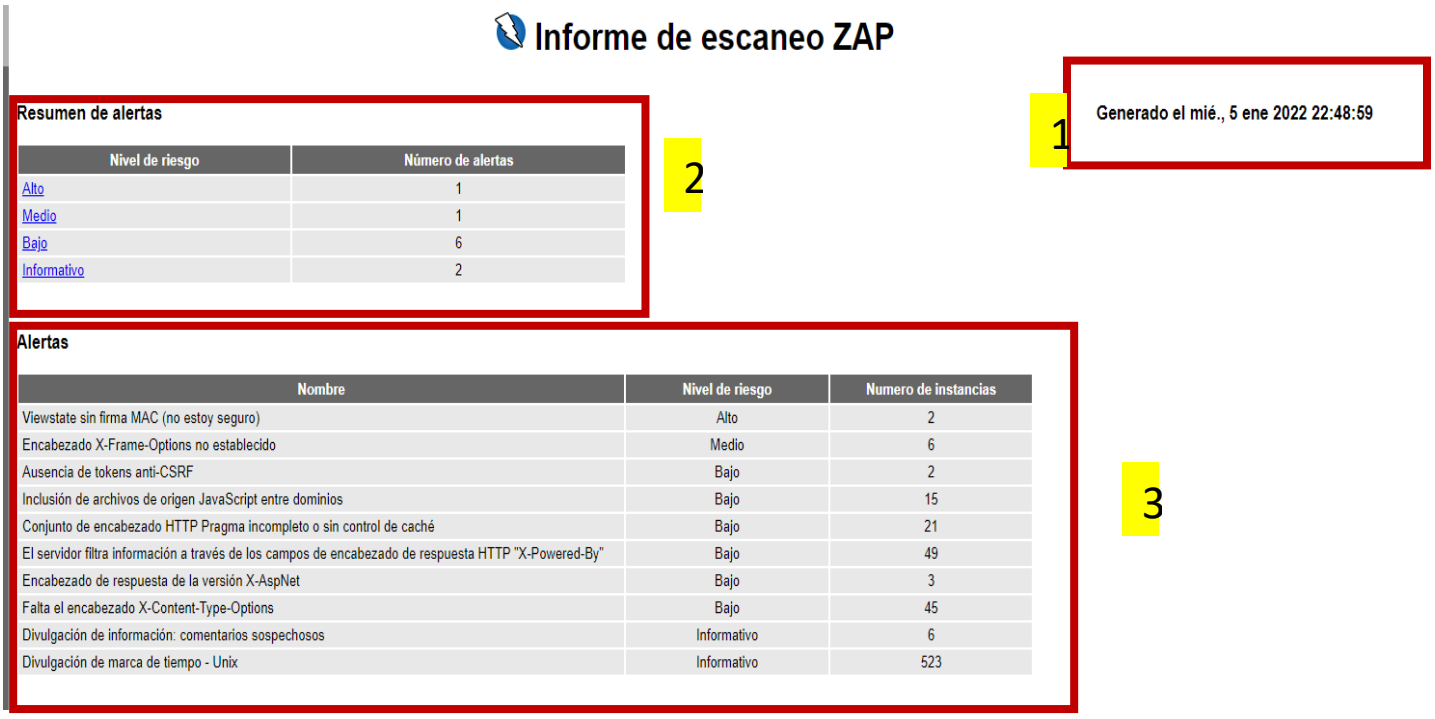


FIG 74. INFORMACIÓN PRIMARIA DEL REPORTE

A continuación, se describe cada una de las alertas resultantes.

1) **Viewstate sin firma MAC:**

a. **Descripción**: **EXPERIMENTAL** este sitio web utiliza ASP.NET pero quizá ningún MAC.

b. **Solución**: Asegúrese de que el MAC este configurado para todas las páginas de este sitio web.

2) **Encabezado X-Frame-Options** no establecido:

a. **Descripción:** El encabezado X-Frame-Opions no se incluye en la respuesta HTTP para proteger contra ataques 'ClickJacking'

b. **Solución:** La mayoría de los navegadores web modernos admiten el encabezado **HTTP X-Frame-Option**. Asegúrese de que este configurado en todas las páginas web devueltas por su sitio.

3) **Ausencia de tokens anti-CSRF**:

a. **Descripción**: No se encontraron tokens Anti-CSRF en un formulario de envió HTML. Una solicitud falsa entre sitios en un ataque compromete y obliga a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento o intención de poder realizar una acción como víctima.

b. **Solución**: Asegúrese de que su aplicación esté libre de fallas de secuencias de comandos entre sitios, ya que la mayoría de las defensas de CSRF pueden detenerse por alto por medio del uso de secuencias de comandos manejadas por ataque.

4) **Inclusion de archivos de origen JavaScript entre dominios**:

a. **Descripción**: La pagina web incluye uno o mas archivos de secuencia de comandos de un dominio de terceros.

b. **Solución**: Asegurese que los archivos de origen de JavaScript se carguen solo desde fuentes confiables y que los usuarios finales de la aplicación no puedan controlar las fuentes.

5) Conjunto de encabezado HTTP programa incompleto o sin control caché:

a. Descripción: El control de caché y el encabezado HTTP pragma no se han configurado correctamente o faltan, lo que permite que el navegador y los proxies almacenen contenido en caché.

b. **Solución:** Siempre que sea posible, asegurese de que el encabezado HTTP de control de cache este configurado con no-store, no-cache, must-revalidate y que el encabezado HTTP pragma esta configurado sin caché.

6) El servidor filtra información a través de los campos de encabezado de respuesta HTTP “X-Powered-By”:

a. **Descripción**: El servidor web / de aplicaciones está filtrando información a través de uno o más encabezados de respuesta HTTP “X-Powered-By”. El acceso a dicha información puede facilitar que los atacantes indiquen otros marcos / componentes de los que depende su aplicación web y las vulnerabilidades a las que dichos componentes pueden estar sujetos.

b. **Solución**: Asegúrese de que su servidor web, servidor de aplicaciones, equilibrador de carga, etc. este configurado para suprimir los encabezados “X-Powered-By”.

7) Encabezado de respuesta de la versión X-AspNet:

a. **Descripción**: El servidor filtra información a través de los campos de encabezado de respuesta HTTP “X-AspNet-Version”/”X-AspNetMvc-Version”.
b. **Solución**: Configure el servidor para que no devuelva esos encabezados.

8) Falta el encabezado X-Content-Type-Options:
   a. **Descripción**: El encabezado no se estableció en ‘nosniff’. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen de MIME en el cuerpo de la respuesta, lo que podría hacer que el cuerpo de la respuesta se interprete y muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales y heredadas de Firefox usaran el tipo de contenido declarado en lugar de realizar el rastreo MIME.
   b. **Solución**: Asegúrese de que la aplicación / servidor web establezca el encabezado Content-Type de manera adecuada y que establezca el encabezado X-Content-Type-Options en ‘nosniff’ para todas las páginas web. Si es posible asegúrese de que el usuario final utilice un navegador web moderno y que cumpla con los estándares que no realice ningún rastreo MIME.

Las dos siguientes con alertas con menajes informativos, pero también deben ser tomados en consideración.

1) Divulgación de información (Comentarios sospechosos):
   a. **Descripción**: La respuesta parece contener comentarios sospechosos que pueden ayudar al atacante. Nota: las coincidencias realizadas dentro de los

bloques de secuencia de comandos o archivos se refieren a todo el contenido, no dolo a los comentarios.

b. **Solución**: Elimine los comentarios que devuelvan información que pueda ayudar a un atacante y solucione cualquier problema subyacente al que se refiera.

2) Divulgación de marca de tiempo-Unix:

a. **Descripción**: La aplicación/servidor web revelo una marca de tiempo - Unix.

Solución: Confirme manualmente que los datos de la marca de tiempo no son confiables y que los datos no se pueden agregar para revelar patrones explotables.

5. CONCLUSIONES

Como aporte de este trabajo se recomienda seguir la metodología anteriormente propuesta para detección de vulnerabilidades en sitios WEB. Es importante mencionar que este trabajo de tesis se centra en las fases 1 a 3.

Los sitios con tecnología MySQL ante ataques SQL Injection presentan un riesgo sino son programados con seguridad y para ambos casos se recomienda implementar programación en capas utilizando procedimientos almacenados (conjunto de instrucciones con envío de parámetros) para la interacción entre el servidor y la aplicación web ya que de esta manera se evita la exposición de información debido a que no hay una interacción directa.

Como se mostró los resultados pueden ser diversos, siempre dependiendo del nivel de complejidad con el que sea diseñado un proyecto o plataforma web. En las pruebas realizadas en este trabajo se utilizaron niveles de ataque que no buscan exponer el total de la información de las empresas, y es importante mencionar que tampoco fueron explotadas las vulnerabilidades ya que el propósito de este trabajo de tesis se limita solo a la detección de estas.

Los resultados en detección de vulnerabilidades son variables y dependen del tipo de aplicaciones y métodos que sean utilizados para su desarrollo. Desarrollar con .NET brinda mayor seguridad con respecto a PHP en los entornos analizados cuando se realizan pruebas de inyección.

De las dos plataformas analizadas, solo con CIEN empresa se logró obtener información de las tablas de la Base de datos durante el proceso de pruebas, y se

muestra que del top ten de OWASP versión 2017 corresponde a la principal vulnerabilidad en entornos WEB.

Las pruebas de detección de vulnerabilidades en la empresa OSD mostró que la seguridad implementada contra ataques WAF/IPS es correcta y no se logró obtener información sensible.

Se pretende continuar con este trabajo ya que me fue de interés notar que uno de los complementos utilizados para llevar a cabo este análisis, se encuentra desarrollado bajo el leguaje de alto nivel Python, este lenguaje de programación ha incrementado su popularidad en los últimos años además de que es multidisciplinario pues puede trabajarse con él en distintas áreas de la industria de la tecnología como es el caso de la ciberseguridad.

6. ANEXOS

6.1. CONFIGURACIÓN DE PROXY EN MOZILLA FIREFOX.

1. Abrir el Explorado Mozilla, figura 75.

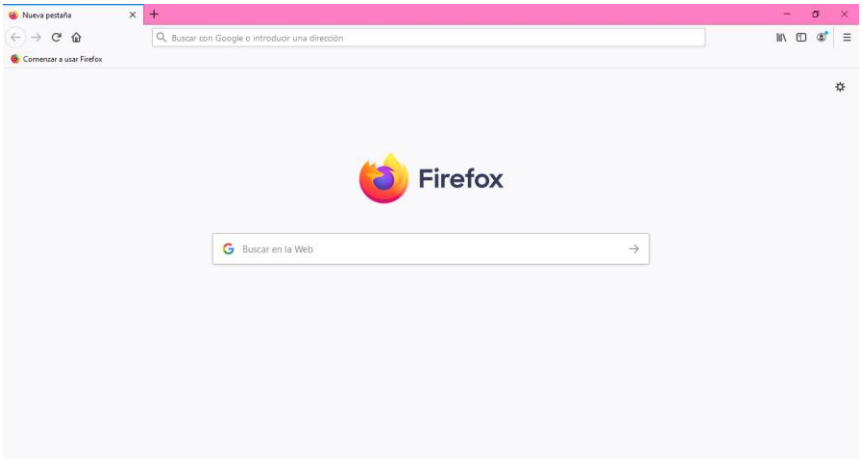


FIG 75. MOZILLA

2. Ir al menú que se encuentra en la parte superior derecha y dar clic en opciones, ver figura 76.

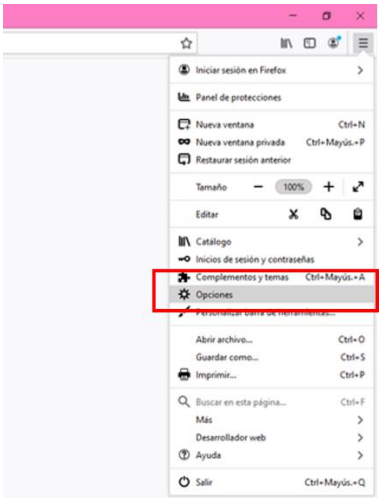


FIG 76. MENÚ

3. En la parte superior aparecerá una caja de texto de búsqueda, escribir Proxy y dar enter, esta acción mostrará un apartado llamado configuración de red, se debe dar clic en el botón configuración que aparece ahí, ver figura 77.

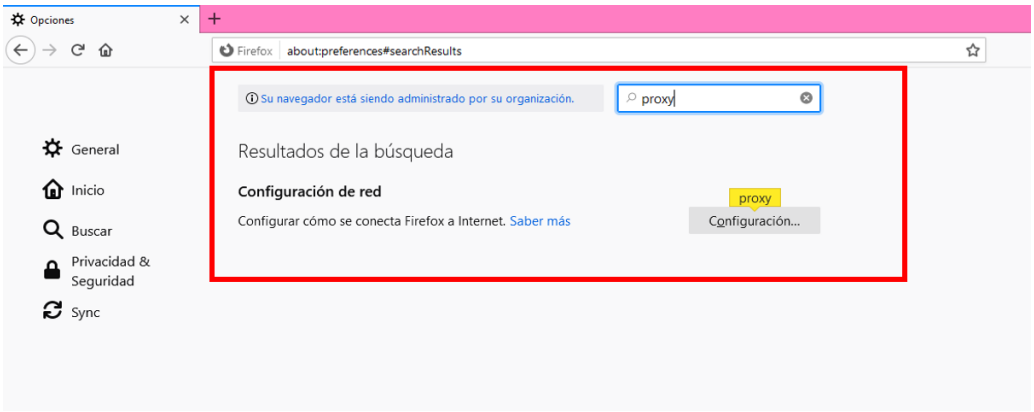


FIG 77. PROXY MOZILLA

4. Se abrirá un apartado en donde se deberá hacer la configuración correspondiente al Proxy, ver figura 78.

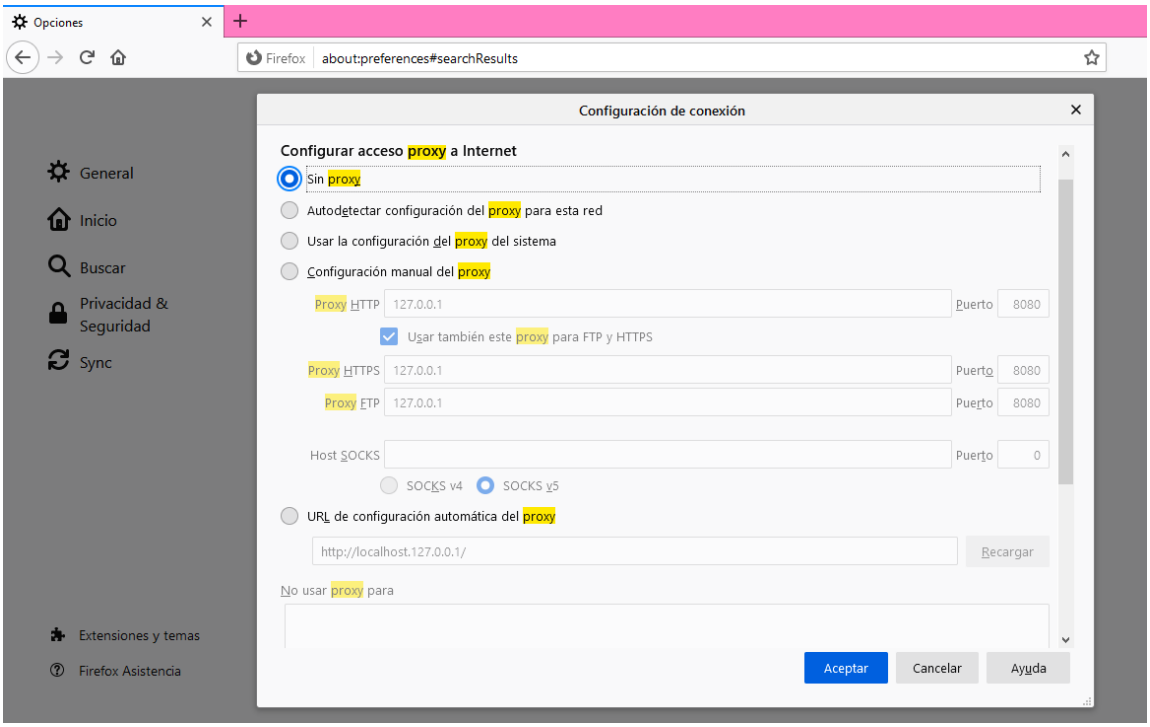


FIG 78. CONFIGURACIÓN DE PROXY

5. Dar clic en el Check “Configuración manual del proxy”, figura 79.

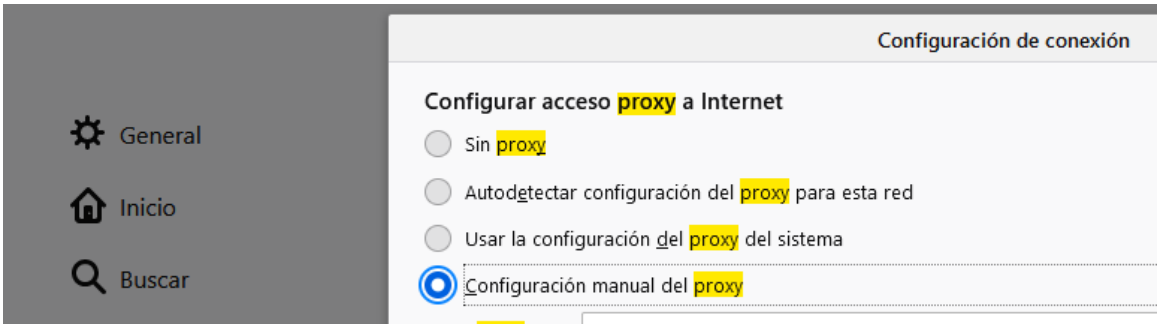


FIG 79. CONFIGURACIÓN MANUAL

6. Escribir los siguientes datos como parámetros en los apartados que se indican.
    a. Proxy HTTP: 127.0.0.1
    b. Puerto: 8080

Dar clic en aceptar y es así como queda configurado el proxy para poder trabajar.

6.2. PREPARANDO ENTORNO PARA ANÁLISIS.

Lo primero es abrir el explorador que fue configurado como proxy, en este caso Mozilla Firefox, para acceder a la aplicación mediante su ruta de acceso. En este escenario la ruta utilizada fue: https://osds.com.mx la cual al acceder muestra la pantalla como su inicio y/o presentación al usuario, tal como se ve en la figura 80.

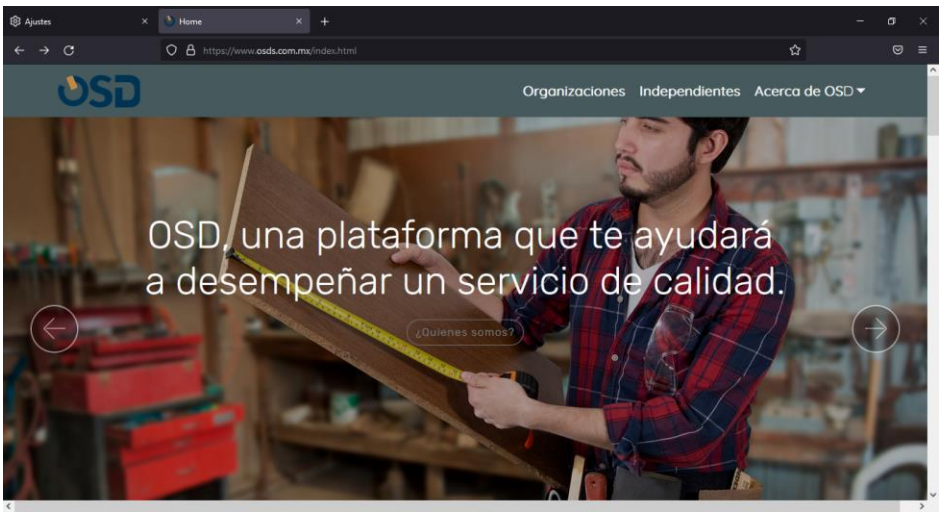


FIG 80. PANTALLA PRINCIPAL OSD

Una vez mostrada esta pantalla, se ingresó al acceso de las Organizaciones mediante el enlace mostrado en el apartado superior derecho “Organizaciones”. Luego de dar clic para su acceso el navegador lanza un mensaje de advertencia de seguridad el cual luce como se muestra en la figura 81.

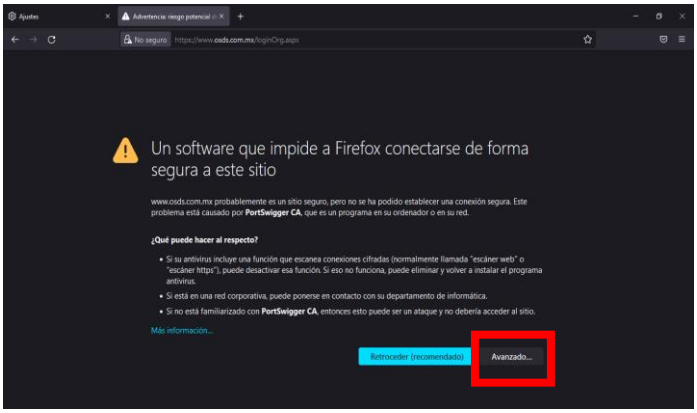


FIG 81. MENSAJE DE ADVERTENCIA

Para poder continuar con la prueba se obtuvo el acceso dando clic en aparatado con título “**Avanzado**”, seguido de esta acción se desplego un mensaje más al cual se dio clic en **Aceptar el riesgo y continuar** ver figura 82.

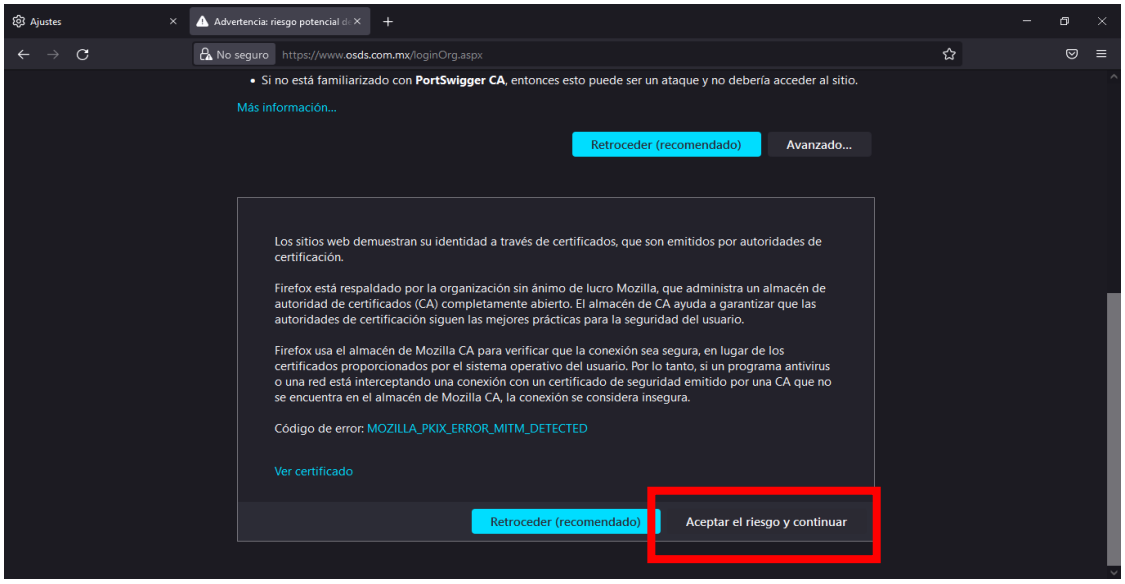


FIG 82. AVISO DE RIESGOS

Entonces se pudo mostrar la página siguiente y de interés que se desea analizar, que es https://osds.com.mx/loginOrg.aspx, un apartado en donde se lleva a cabo la acción del inicio de sesión de un usuario, como se ve en la figura 83.

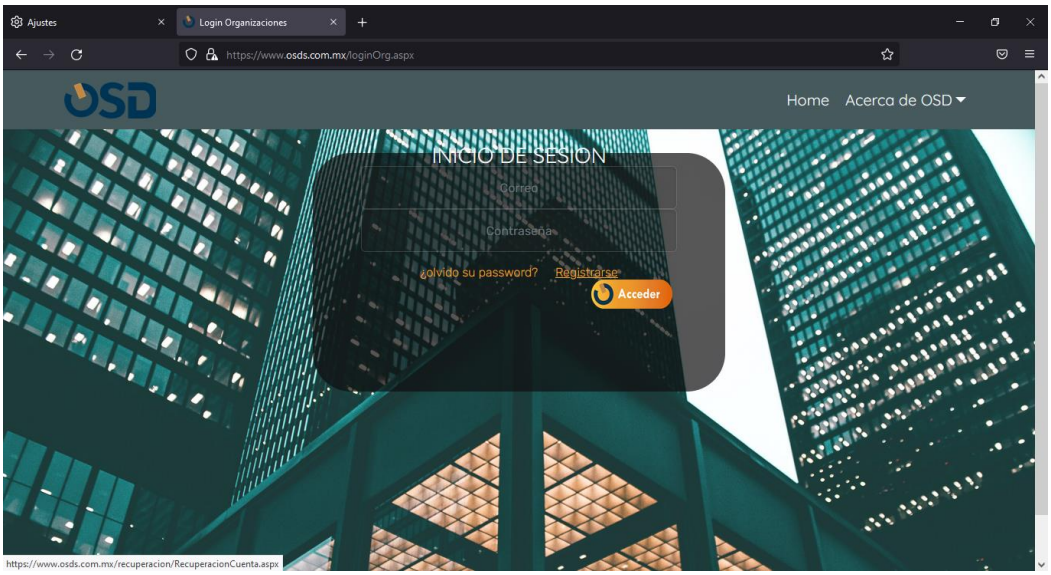


FIG 83. LOGIN ORGANIZACIONES

Hasta este momento Burp Suite y la plataforma web se encuentran desconectadas, pues la intercepción de Burp Suite se encuentra apagada y ésta es la que origina la conexión entre ambas, ya que aún no se ingresaron los datos correspondientes a cada campo solicitado en el apartado de login y así poder lanzar un llamado al servidor.

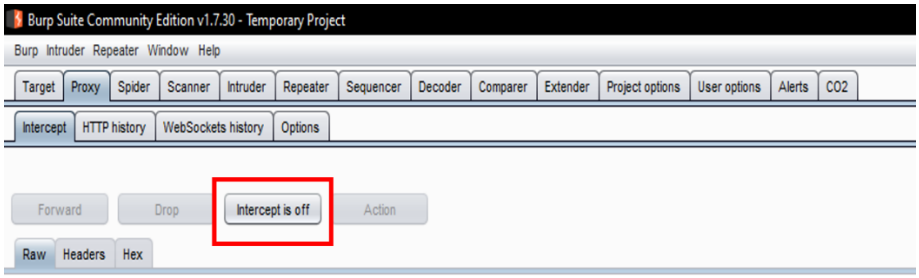


FIG 84. INTERCEPCIÓN APAGADA

Antes de encender la intercepción se deben ingresar los datos correspondientes en el formulario, ver figura 86. Ya que estos serán los parámetros que realizarán las peticiones al servidor y así poder obtener una respuesta. Esto se realiza antes de dar clic en el botón ***Intercept is off*** en Burp figura 84.

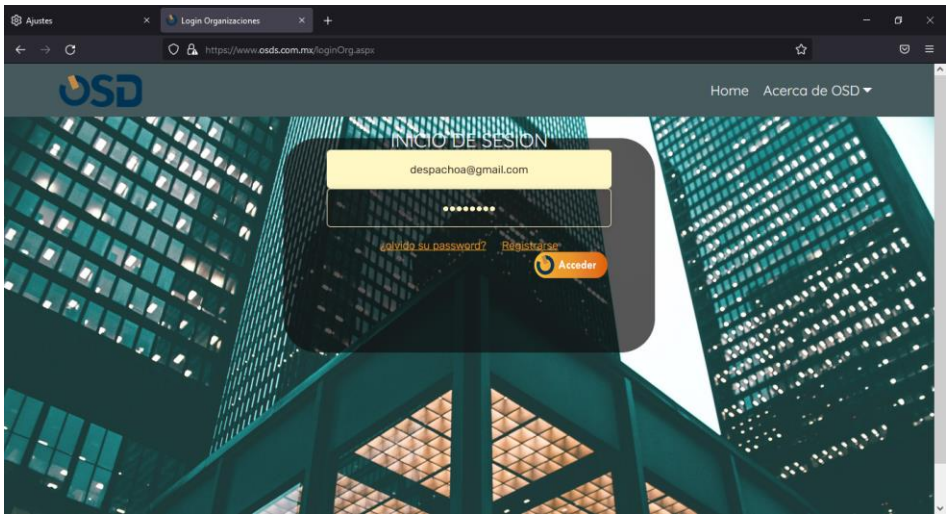


FIG 85. INGRESO DE DATOS PARA PETICIÓN

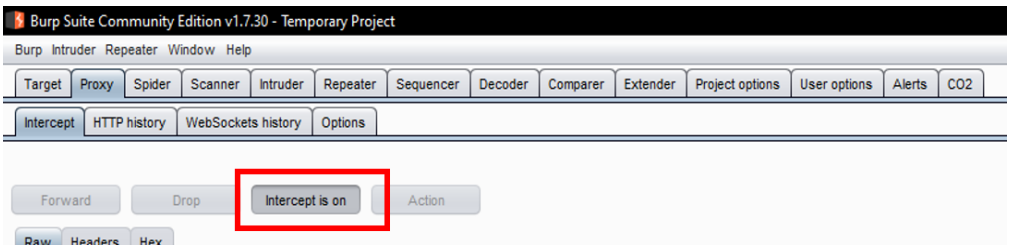


FIG 86. INTERCEPCIÓN ENCENDIDA

Después de haber llenado los campos en el formulario mostarado en la figura 84. de la aplicación web y haber encendido la intercepcion en **Burp Suite. figura 73.** Se da clic en el botón acceder (color naranja) en el apartado del formulario del login, como si se estuviera ingresando al sistema y es aquí cuando Burp Suite en su pestaña **Proxy** reflejara la información que indicara la conexión entre el sitio y el servidor indicando asi la conexión de proxy exitosa. Para comprobar que realmente

se establecio la comunicación entre ambos basta con observar ***Proxy-Intercep-Row*** aquí son devueltos algunos valores entre ellos el **Host** al que se esta conectando y este debe ser correspondiente a la url del sitio objetivo. Tal como se ve en la figura 87 en la cual se puede apreciar que el Host devuelto efectivamente correstonde a **osds.com.mx**

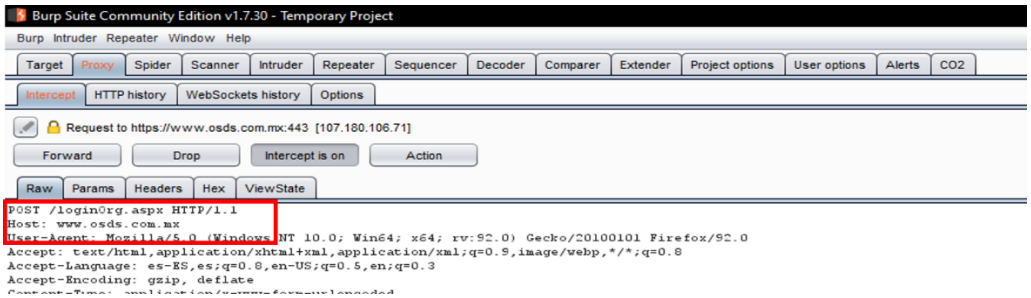


FIG 87. HOST DE CONEXIÓN

Otro apartado que también devuelve información correspondiente a la conexión de la información es en la misma pestaña de **Proxy-Intercept- Headers** en este apartado se mostrará la información con una mejor clasificación, como se ve en la figura 88 y su lectura se vuelve más digerible ya que la información se encuentra mejor distribuida. Además, parte de la información mostrada en este apartado o en el anterior sirve para ejecutar cualquiera de las extensiones proporcionadas por Burp Suite, en este caso de estudio para **CO2**, pues esta información servirá como argumentos o parámetros dependiendo del caso a analizar.

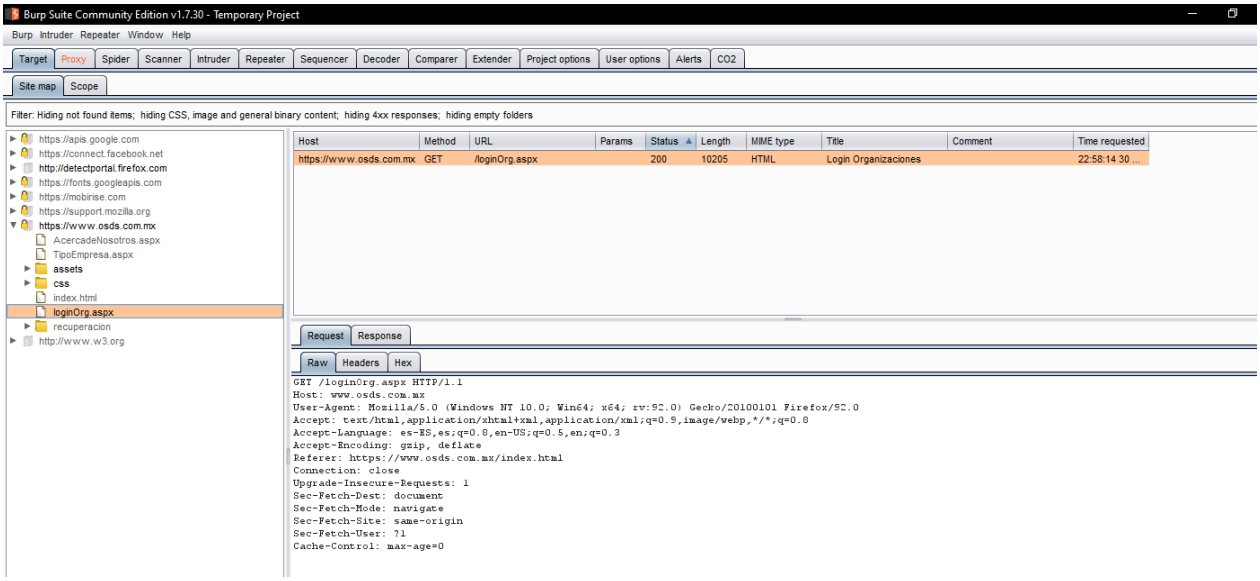


FIG 88. APARTADO TARGET, DEVUELVE EL ESQUEMA DEL SITIO WEB

Una vez que fue verificada la conexión de comunicación entre el proxy y la aplicación es momento de ir a la extensión que será de apoyo para realizar el **SQL Injection,** CO2. Este procedimiento se lleva a cabo sin apagar la intercepción después de lo anterior descrito.

INDICE DE FIGURAS

INDICE DE TABLAS

BIBLIOGRAFÍA

AFP. (10 de FEBRERO de 2020). *El Economista*. Obtenido de https://www.eleconomista.com.mx/empresas/EU-acusa-a-cuatro-militares-chinos-de-participar-en-hackeo-a-Equifax-en-2017-20200210-0044.html

Aleph. (5 de Abril de 2021). *Aleph*. Obtenido de https://aleph.org.mx/como-fue-la-evolucion-del-hombre-resumen

Ayala, R. (23 de Septiembre de 2019). *Heraldo de México*. Obtenido de https://heraldodemexico.com.mx/opinion/2019/7/23/pasion-por-correr-105896.html

Bravo, C. (s.f.). *estudiok*. Obtenido de https://estudioka.es/que-es-un-mock-up/

Canal, V. A. (2006). *Seguridad de la Información.* México: Limusa.

Castelan, J. (6 de Mayo de 2021). *Creana*. Obtenido de https://www.crehana.com/mx/blog/web/lenguajes-de-programacion-mas-usados/

Castro, I. (04 de Septiembre de 2018). *Cero Uno Software Corporativo*. Obtenido de https://cerounosoftware.com.mx/2018/09/04/las-5-fases-de-un-ataque-informatico/

CICESE, S. (2017). *Ivan Valencia Santiago*. Obtenido de https://seguridad.cicese.mx/alerta/335/Hacker,-Crackers,-Lamers,-Script-Kiddies-y-Phreakers-Quienes-son

Crespo, R. (s.f.). *Roberto Crespo Blog Personal*. Obtenido de Roberto Crespo Blog Personal: http://www.robertocrespo.net/kaizen/funciones-hash-md5-y-sha256/

Cuervo, J. (21 de Febrero de 2018). *Informatica Juridica*. Obtenido de http://www.informatica-juridica.com/codigo/articulo-166-bis-codigo-penal-federal-mexicano/

Fernandez, R. (2021). *Statista*. Obtenido de https://es.statista.com/estadisticas/635987/porcentaje-de-internautas-usuarios-de-redes-sociales-en-el-mundo/

futuro, R. I. (s.f.). *Facultat d'Informàtica de Barcelona* . Obtenido de https://www.fib.upc.edu/retro-informatica/historia/internet.html

Goytía, Á. G. (2017). *Desarrollo y programacion en entornos web.* México: Alfaomega.

Guardo, D. M. (4 de Octubre de 2019). *Dev*. Obtenido de https://dev.to/demg_dev/pbkdf2-hash-a-secure-password-5f8l

Hallberg, B. (2007). *Fundamentos de Redes.* Mexico: McGraw-Hill.

HALLBERG, B. (2007). *Fundamentos de redes.* México: McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V.

Hernandez, S. (2020). Obtenido de https://www.udemy.com/course/curso-completo-de-hacking-etico-y-ciberseguridad

INCIBE. (01 de Enero de 2017). Obtenido de https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

J.M. Sadurní. (15 de Noviembre de 2020). *National Geographic*. Obtenido de https://historia.nationalgeographic.com.es/

Jiménez, A. S. (s.f.). *La Jornada*. Obtenido de https://www.jornada.com.mx/notas/2021/05/10/economia/pemex-con-alto-riesgo-de-ser-victima-de-hackeos-asf/

Kaspersky. (s.f.). *Kaspersky*. Obtenido de https://latam.kaspersky.com/resource-center/threats/ransomware

Kaspersky. (s.f.). *Kaspersky*. Obtenido de https://www.kaspersky.com/resource-center/threats/browser-hijacking

Lab, S. (s.f.). *Software Lab*. Obtenido de https://softwarelab.org/es/que-es-adware/

Luz, S. d. (24 de Marzo de 2021). *redzone*. Obtenido de https://www.redeszone.net/tutoriales/seguridad/mejores-escaner-vulnerabilidades-gratis-hacker/

MariaJose. (2020 de Noviembre de 2020). *Grupo Fractalia*. Obtenido de https://fractaliasystems.com/los-ataques-ciberneticos-aumentan-40-en-mexico-durante-la-pandemia/

Mendoza, M. Á. (8 de Junio de 2018). *We live Security*. Obtenido de https://www.welivesecurity.com/la-es/2018/06/08/principio-menor-privilegio-limitar-acceso-imprescindible/

MUNDO, B. N. (14 de DICIEMBRE de 2016). *BBC NEWS MUNDO*. Obtenido de https://www.bbc.com/mundo/noticias-38324372

Mundo, B. N. (22 de Enero de 2020). *BBC NEWS | MUNDO*. Obtenido de https://www.bbc.com/mundo/noticias-51206264

Mundo, B. N. (26 de Mayo de 2020). *BBC News Mundo*. Obtenido de https://www.bbc.com/mundo/noticias-internacional-52815026

Owasp. (2017). Obtenido de https://owasp.org/www-project-top-ten/

Pierce, B. (2015). *Una vez desaparecido.*

RAE. (2021). *REAL ACADEMIA ESPAÑOLA*. Obtenido de https://dle.rae.es/seguridad

Ramiro, R. (20 de Enero de 2018). *Ciberseguridad Blog*. Obtenido de https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

Salazar, P. G. (2019). *El libro blanco del hacker.* Ciudad de México: RA.MA.

SGI. (16 de Enero de 2017). Obtenido de https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

SGSI. (2018). *Blog especializado en Sistemas de Gestión*. Obtenido de https://www.pmg-ssi.com/

Singh, S. (2001). *Los Códigos Secretos.* Obtenido de Libros Maravillosos: www.librosmaravillosos.com

Smith, W. y. (2005).

Tapia, E. (20 de Noviembre de 2018). *UnoCero*. Obtenido de https://www.unocero.com/como-se-hace/que-son-el-phishing-pharming-vishing-smishing-y-como-prevenirte/

Toledano, B. (12 de Mayo de 2017). *El Mundo*. Obtenido de El Mundo Tecnologia: https://www.elmundo.es/tecnologia/2017/05/12/59158a8ce5fdea194f8b4616.html

Valencia, E. T. (5 de Diciembre de 2011). *Historia de la Informática*. Obtenido de https://histinf.blogs.upv.es/

Vazquez, A. (22 de Febrero de 2018). *Cysae Legal*. Obtenido de https://www.cysae.com/funciones-hash-cadena-bloques-blockchain/

Veiga, J. M. (s.f.). *Google Books.* Obtenido de https://books.google.com.mx/books?id=suXJDwAAQBAJ&pg=PA1028&dq=Busca+mantener+los+datos+libres+de+modificaciones+no+autorizadas,+la+integridad+es+mantener+con+exactitud+la+informaci%C3%B3n+tal+cual+fue+generada,+sin+ser+manipulada+ni+alterada+por+personas

Xataka. (s.f.). *Xataka*. Obtenido de https://www.xataka.com/otros/1936-la-primera-computadora-programable-de-la-historia#:~:text=1936%2C%20Konrad%20Zuse%2C%20ingeniero%20alem%C3%A1n,entera%2C%20bastante%20grande%20por%20cierto.