ANÁLISIS DE SEGURIDAD DEL SISTEMA DE PEDIDOS WEB DE LA EMPRESA E.B. SOFTWARE LTDA. MEDIANTE PENTESTING

CIRO ALFONSO PACHECO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIAS E INGENIERIA
CEAD (BOGOTA CRA.30) JOSE ACEVEDO Y GOMEZ
SANTA FÉ DE BOGOTÁ D.C
2018

ANÁLISIS DE SEGURIDAD DEL SISTEMA DE PEDIDOS WEB DE LA EMPRESA E.B. SOFTWARE LTDA. MEDIANTE PENTESTING

CIRO ALFONSO PACHECO

Director

Ingeniero Edgar Alonso Bojacá Garavito

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIAS E INGENIERIA

CEAD (BOGOTA CRA.30) JOSE ACEVEDO Y GOMEZ

SANTA FÉ DE BOGOTÁ D.C

2018

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

La empresa E.B. Software Ltda., ubicada en la ciudad de Bogotá D.C., busca ofrecer a sus clientes una herramienta web con la confidencialidad, la integridad y la disponibilidad de la información procesada a través de su aplicativo web para la toma de pedidos en línea. Mediante el presente proyecto se pretende descubrir amenazas a las cuales este aplicativo se podría ver afectado, con el apoyo de la implementación de estrategias como las pruebas de penetración o *Pentesting* a sitios web, utilizando mecanismos y herramientas de código abierto que permitan salvaguardar la seguridad del aplicativo web y ofrecer las recomendaciones necesarias o requeridas para dicha seguridad.

Para nadie es un secreto que la tecnología ha crecido y viene en crecimiento; una muestra de ello se enfoca en lo que se refiere a los servicios orientados hacia el uso de la Internet, lo cual ha generado preocupaciones relacionadas con la seguridad y la integridad que estos puedan certificar. Desde los inicios de los años 60, con el creciente uso de las redes de comunicaciones, se han venido desarrollando estrategias y medidas para garantizar que los sistemas informáticos no se vean afectados por amenazas que inquieten el buen funcionamiento de los sistemas. De esta forma se hace importante conocer las herramientas que buscan detectar e identificar las vulnerabilidades de los sistemas para adoptar los correctivos necesarios que permitan una prevención y detección oportuna.

En la actualidad existen políticas, normas, estándares y herramientas de software que propenden por la seguridad de los sistemas informáticos. Con el desarrollo de este trabajo se busca concientizar a la empresa E.B. Software Ltda. sobre la importancia de ofrecer aplicaciones web seguras para sus clientes, realizando

pruebas de penetración, aplicando herramientas de código abierto, que permitirán determinar las vulnerabilidades de alto impacto o riesgo que afecten la integridad y el buen funcionamiento del sistema de pedidos web de la organización.

1. DEFINICIÓN DEL PROBLEMA

La empresa E.B. Software Ltda., ubicada en la ciudad de Bogotá D.C. es una compañía líder en el mercado de las aplicaciones administrativas y contables de Colombia, que cuenta con la experiencia de más de 8 años en el mercado. Actualmente ofrece una aplicación web para la realización de pedidos en línea que puede ser implementada por medianas y pequeñas empresas. Esta aplicación web está bajo una plataforma de desarrollo en .Net y bases de datos MSQL, actualmente no se puede definir con certeza la seguridad con la que cuenta, las posibles vulnerabilidades que presenta, ya que está se encuentra alojada en servidores externos a la propia compañía.

1.2 PLANTEAMIENTO DEL PROBLEMA

¿Cómo se puede determinar la confidencialidad, la integridad y la disponibilidad de la información procesada del aplicativo web para la toma de pedidos en línea de la empresa E.B. Software Ltda. y que permita fortalecer la seguridad de dicho aplicativo?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Analizar la seguridad de la aplicación web de pedidos de la empresa E.B. Software Ltda. mediante pruebas de penetración.

2.2 OBJETIVOS ESPECÍFICOS

- Realizar un análisis de los riesgos y las vulnerabilidades del aplicativo de pedidos web de la empresa E.B Software Ltda.

- Realizar pruebas de penetración o *Pentesting*, a la aplicación de pedidos web la empresa E.B Software Ltda. mediante herramientas de código abierto.

- Generar informe de las posibles amenazas encontradas a la aplicación de pedidos web la empresa E.B Software Ltda.

- Brindar información de los controles necesario para mejorar la seguridad del aplicativo de pedidos web de la empresa E.B. Software Ltda. usando la metodología Magerit.

3. JUSTIFICACIÓN

La empresa E.B. Software Ltda. Ubicada en la ciudad de Bogotá D.C., debe ofrecer a sus clientes la confianza total en el uso de su aplicativo web de pedidos en línea, garantizando la confidencialidad, la integridad y la disponibilidad de este, puesto que la información que este procesa es información de importancia para sus clientes, ya que el funcionamiento de su negocio gira en torno a las ventas que ellos pueden realizar mediante uso del aplicativo web.

Esta temática no puede ser ajena a ninguna organización, grande, mediana o pequeña, y se hace de vital importancia que la empresa E.B. Software Ltda., realice pruebas de penetración a su aplicativo web y tome las medidas necesarias para garantizar la seguridad dicho aplicativo web.

Ofrecer a los clientes de E.B. Software Ltda., un aplicativo de pedidos web en línea seguro, redunda de forma positiva en aspectos como la imagen corporativa, como además la posibilidad de ofrecer un plus adicional a la hora comercializar dicho producto, puesto que un cliente que sienta que su información está siendo tratada de la forma correcta y sobre todo de forma segura, permitirá garantizar su fidelidad, y con un porcentaje alto que la empresa sea recomendada, lo cual hará crecer la organización. Por todo esto, el proyecto pretende no solo descubrir los posibles riesgos, a los cuales el aplicativo web en mención se puede ver afectado, si no a que además pretende ser una herramienta de apoyo para brindar la seguridad necesaria que permita fortalecer la compañía comercialmente y ubicarla en una posición de liderazgo en materia de seguridad informática para su aplicación web.

4. ALCANCES Y DELMITACIÓN DEL PROYECTO

El alcance del presente trabajo pretende analizar la seguridad de la aplicación web de pedidos en línea de la empresa E.B. Software Ltda., ubicada en la ciudad de Bogotá D.C., iniciando con un análisis de riesgos y vulnerabilidades de la aplicación, llevando a cabo la realización de pruebas de penetración o *pentesting* de su aplicativo web de pedido en línea, mediante herramientas de código abierto, para generar el correspondiente informe sobre las pruebas y así brindar información relevante para la aplicación de los controles necesarios para garantizar la confidencialidad, la integridad y la disponibilidad del aplicativo web en su versión 1.2, desarrollado por el área de desarrollo de la misma.

5. MARCO REFERENCIAL

5.1 MARCO CONTEXTUAL

Desarrollo de una propuesta metodológica para determinar la seguridad de una aplicación web, por Martha Ascencio Mendoza y Pedro Julián Romero Patiño de la Universidad Tecnológica de Pereira del año 2011. Dentro de sus alcances realiza un análisis de conceptos y los fundamentos en materia de seguridad web, así como de determinar tipos de vulnerabilidades y herramientas realizando la propuesta metodológica para determinar la seguridad de las aplicaciones web.

Evaluación de seguridad a sistemas de información en cuanto a ataques maliciosos con base en normatividad, tendencias, impacto y técnicas vigentes para ambientes empresariales a nivel nacional, por David Hernando Alonso Torres de la Universidad de la Sabana del año 2014. Dentro de sus alcances identifica y estudia la legislación, normativas, estándares y circulares actuales respeto a la seguridad de la información a nivel nacional, identificando sus fuentes para su procesamiento, realiza una caracterización de los ataques informáticos comunes determinando el impacto organizacional, así como la consulta de herramientas para el *hacking* ético.

Desarrollo de metodología para hallazgos de vulnerabilidades en redes corporativas e intrusiones controladas, por Diego Fernando Ortiz Aristizábal, de la Fundación Universitaria Los Libertadores del año 2015. Dentro de sus alcances identifica errores de configuración aplicados indebidamente en las redes de comunicación de las empresas, determinar sistemas operativos con vulnerabilidades, la optimización

de recursos económicos destinados a estos procesos aplicando la metodología propuesta.

Identificación de vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental, mediante pruebas de testeo de red en la empresa INGELEC S.A.S, por Henry Aldemar Guerrero Erazo, Lorena Alexandra Lasso Garces, Paola Alexandra Legarda Muñoz, de la Universidad Nacional Abierta y a Distancia UNAD, de la ciudad de Pasto del año 2015. Dentro sus alcances están la realización de pruebas de *pentesting* a la red interna de la organización, para determinar y evaluar vulnerabilidades y así poder establecer controles que minimicen los riesgos y aumentar la seguridad del sistema de gestión documental.

Identificación de los ataques más realizados en un sitio concurrido por personas que utilizan sus dispositivos móviles y determinación de las vulnerabilidades más comunes en el sistema operativo Android, por William Steven Tavera Jaramillo y Miguel Ángel Mahecha Rivera de la Universidad Nacional Abierta y a Distancia UNAD de la ciudad Bogotá del año 2016. Dentro de sus alcances se destacan la identificación de vulnerabilidades y ataques a dispositivos con sistemas Android, detallando herramientas para la realización de pruebas de penetración en teléfonos inteligentes.

5.2 MARCO TEÓRICO

5.2.1 Seguridad informática. Es el conjunto de estrategias y normas orientadas a garantizar la seguridad de los equipos informáticos como su estructura física.

5.2.1.1 IDS/IPS. Por sus siglas en inglés, sistemas de detección de intrusos, que está diseñados para monitorear y detectar acciones sospechosas o malintencionadas que buscan afectar de una u otra manera los equipos informáticos dentro de las redes de comunicación de las organizaciones y que pueden reaccionar de forma automática para prevenir cualquier incidente de seguridad.

Su función principal es monitorear los paquetes de información dentro de las redes de comunicación para explorar y descubrir posibles intentos de intrusiones y reportarlos a los administradores de los sistemas informáticos, generando avisos como alarma que permitan reaccionar de forma preventiva ante posibles ataques de seguridad informática.

La forma que un IDS puede actuar está determinada por dos tipos de respuesta, una pasiva, donde se registra todas las actividades que puedan considerarse sospechosas, como intrusiones o simples usos de servicios y puertos de forma no habituales y reportando esta información a los administradores de los sistemas; y una repuesta activa, mediante el cual IDS puede generar bloqueos de acceso y finalización de conexiones, o finalización de servicios, reconfiguración de los cortafuegos, bloqueos de cuentas de usuarios, así como la localización de la fuente del ataque para ser reportada cono una especia de boletín informativo generalizado, de tal forma que se pueda detener cualquier posible incidente de seguridad.

Los IDS poseen una arquitectura que funciona como una aproximación estándar de diseño en el cual se pueden identificar cuatro componentes principales:

- Generador de eventos o fuentes de datos: es la fuente principal de información que bridan los eventos del sistema o la red informática.
- Base de datos: es la que almacena los patrones de comportamiento considerados como normales y además los perfiles de los tipos de ataques.
- Analizador de eventos o motor de análisis: se encarga de detectar las posibles evidencias que pueden ser una alerta de intrusión o ataque.
- Unidad de respuesta o módulo de respuesta: Definido para ejecutar acciones de prevención de ataques de acuerdo con lo reportado por el motor de análisis.

Los IDS, para su funcionamiento implementan dos tipos de modelos de detección

- De un mal uso o *misuse*, es el modelo de detección que se caracterizan por los tipos ilegales de tráficos de paquetes de información en las redes de comunicación, así como secuencias utilizadas para realizar ataques contra los equipos, estas secuencias de código son conocidos como *exploits*, como también le escaneo de puertos.
- De uso anómalo: Este modelo de detección se basa en un análisis estadístico del tráfico de red, la monitorización de procesos y del comportamiento de los usuarios cuyo objetivo es identificar los comportamientos considerados como anómalos dado los patrones generados y registrados en el uso generalizados de los sistemas informáticos dentro de los horarios de flujo normal, el tipo de servicios y puertos usados, y así, compararlos con comportamientos que pueden cambiar y que no tienen una justificación clara que pueden ser evidenciadas por uso de aplicaciones no reconocidas, el aumento de tráfico en la red.

Los IDS aunque son una herramienta útil a la hora proteger los sistemas informáticos poseen algunas desventajas que se pueden enumerar así:

- Pueden generar un gran número de falsas alarmas.
- Es compleja la monitorización del tráfico de red en topologías con *swiches*, ya que conmutan el tráfico de los paquetes de información.
- No es posible el análisis de conexiones cifradas.
- Pueden afectar en gran medida el rendimiento de la red.

5.2.1.2 Tipos de IDS. HIDS o Host IDS, este tipo de IDS está orientado a la detección de intrusiones a nivel de host, principalmente identifica cualquier alteración de los archivos fundamentales del sistema operativo, como de las aplicaciones, verificando su integridad, realizando un análisis periódico de tallado. Trabaja a bajo nivel capturando las llamadas o paso de mensajes de las funciones del sistema operativo.

MHIDS o MultiHost IDS, está orientado a la detección de intrusiones mediante el análisis de más de un host o equipos informáticos y cumple funciones idénticas al HIDS.

NIDS o Network IDS, este sistema de detección de intrusos se instala en una red de equipos informáticos con el objetivo de realizar un monitoreo del tráfico de red y llevando a cabo el respectivo análisis del mismo; es capaz de detectar acciones

consideradas sospechosas como lo es escanear puertos, los intentos de explotación de vulnerabilidades de seguridad en los servicios instalados.

Los IPS, o sistemas de prevención de intrusos, es un dispositivo orientado a brindar control de acceso a las redes de tal forma que permita proteger los sistemas informáticos de los distintos ataques e intrusiones. Trabaja analizando los datos obtenidos del ataque y procede a actuar de tal forma que puede detenerlo antes que este tenga efectos sobres los sistemas.

5.2.2 Seguridad de la información. Es el conjunto de estrategias, normas y estándares para proteger la información garantizando la privacidad, confidencialidad e integridad de esta, en todas sus formas, digitales o no digitales.

5.2.3 Aplicación web. Se entiende por aplicación, programa o *software*, el conjunto de instrucciones en algún lenguaje de programación diseñadas con el objetivo de que la computadora realice algunas tareas; adicionalmente, una aplicación web, es aquella que puede ser accedida dentro una red mediante un navegador web, y funciona como una aplicación cliente/servidor, mediante el cual un usuario, puede acceder desde un cliente, el navegador web, a un servidor web, realizando peticiones desde dicho cliente y enviando solicitudes al servidor mediante el protocolo HTTP.

5.2.3.1 Codificación y desarrollo de una aplicación web. Una aplicación web está codificada principalmente en un lenguaje de marca de hipertexto denominado HTML por su siglas en inglés *HyperText Markup Languaje*, y es el estándar más usado a nivel general, y puede desarrollarse en conjunto con un lenguaje

interpretado como el JavaScript, adicionalmente con un lenguaje de estilo para dar presentación al documento HTML, como las CSS por su siglas en inglés *Cascading Style Sheets*; la combinación de estas tres tecnologías, podrían dar origen a una aplicación web básica, aunque en la actualidad, se está popularizando otro estándar denominado HTML5, debido a su implementación para el desarrollo de aplicaciones web orientadas a dispositivos móviles. Sin embargo, para el desarrollo de una aplicación web robusta, es necesario contar con otras tecnologías que principalmente funcionan del lado del servidor y que ofrecen otros servicios como el acceso a base de datos, entre las cuales se puede mencionar PHP, Java JSP, .Net ASP y ASPX entre los más usados a nivel global, estos, son leguajes de programación orientados al desarrollo de aplicaciones web, que permiten brindar dinamismo y funcionalidades especiales, como la manipulación de datos, archivos entre otros.

5.2.3.2 Seguridad en aplicaciones web. Los tres pilares fundamentales de un sistema seguro y, por ende, de una aplicación web segura, son la confidencialidad, la integridad y disponibilidad de todos los recursos que ellos ofrecen. Es importante que los desarrolladores web, tengan en cuenta estos tres principios, ya que ello depende en gran medida el éxito de los proyectos de desarrollo. Identificar riesgos como factores que amenacen la seguridad para proteger los sistemas, es un punto vital dentro de todo el ciclo de desarrollo de cualquier tipo aplicaciones.

5.2.3.3 OWASP. Es el Proyecto abierto de seguridad de aplicaciones web, que propone una guía de buenas prácticas en la codificación de software con el objetivo de ser integrado en el ciclo de desarrollo de aplicaciones con el objetivo de minimizar las vulnerabilidades más comunes en el *software*, esta define la siguiente lista de verificación de prácticas de codificación segura:

- validación de entradas
- Codificación de salidas
- Administración de autenticación y contraseñas
- Administración de sesiones
- Control de acceso
- Prácticas criptográficas
- Manejo de errores y logs
- Protección de datos
- Seguridad en las comunicaciones
- Configuración de los sistemas
- Seguridad de bases de datos
- Manejo de archivos
- Manejo de memoria
- Prácticas generales para la codificación

5.2.3.3.1 Pentesting mediante OWASP ZAP. Del proyecto cuyas siglas en inglés son *Open Web Application Security Project*, como su nombre lo indica es un proyecto abierto, en sí, es una comunidad a nivel internacional cuyo objetivo es velar por la consecución y el desarrollo aplicaciones web seguras y de esta manera mantener la red de internet más segura. ZAP, Zed Attack Proxy, es considerada una de las herramientas de seguridad más populares y es de carácter libre, permite monitorear las aplicaciones web y facilita el trabajo de las auditorias de sistemas. Es multiplataforma, dentro de sus características están:

- Permite hacer un seguimiento a las peticiones y respuestas entre un cliente (navegador) y un servidor.
- Facilita la localización de recursos en un servidor, como archivos, enlaces, etc.
- Permite la realización de análisis tanto activos como pasivos.

- Puede realizar múltiples ataques al mismo tiempo.
- Permite la utilización de certificados SSL dinámicos.
- Permite analizar el sistema de autenticación

5.2.4 Vulnerabilidades en la web. El creciente uso de las redes de comunicación, principalmente la Internet, ha permitido que las aplicaciones web sean el foco de atención de los atacantes, no solo para afectar el funcionamiento de la misma, sino también para vulnerar la seguridad permitiendo el hurto de información. Las malas configuraciones y errores de programación son las causas más comunes que hacen vulnerables las aplicaciones web. Existen dos tipos de puntos de entrada, en otras palabras, dos vectores principales de ataque, los controles de acceso y el software de vulnerabilidades.

5.2.4.1 Trasferencia de zona. Copia del contenido de archivos de zona DNS desde un servidor DNS principal a un servidor de DNS secundario, una mala configuración de los servidores DNS, mediante la transferencia DNS, puede permitir que se obtenga la zona de dominio administrada por el DNS, la información recolectada por este proceso puede ser las direcciones IP de la red, sus servidores y estaciones conectadas a las mismas.

5.2.4.2 Banner Grabbing. La mayoría de los servidores web ofrecen como respuesta a una solicitud, datos como el tipo servidor que pueden contener un simple texto como “apache”, “nginx” o “ISS”, para los servidores Apache, servidores Nginx y Microsoft Windows Server, entre los más comunes. La técnica de Banner Grabbing, busca captura información del servidor web donde las aplicaciones web están alojadas la cual se logra con una interacción en texto plano.

5.2.4.3 Fingerprinting web. Información como el tipo y versión de servidor, permiten descubrir vulnerabilidades para la realización de los tests de intrusión.

5.2.4.4 Controles de acceso. Se pueden considerar como ataques de fuerza bruta, un ejemplo de ellos es el intento de inicio de sesión mediante el ingreso de combinaciones de nombre de usuario y contraseña, por medio de secuencias de comandos que hacen intentos continuos hasta lograr la combinación de acceso.

5.2.4.5 El *software* de vulnerabilidades. Entre las cuales se pueden mencionar: Inyección SQL (SQLi), que consiste en enviar consultas SQL mediante los campos de búsqueda, o campos de ingreso de datos o directamente en una dirección web, para lograr acceso completo al sistema, o denegar a los usuarios o a la base datos en sí; *Cross-Site Scripting* (XSS) que consiste usar página web como inicio de ejecución para ataques a otros usuarios que vistan el sitio web, esto permite al atacante acceder a las computadoras de los usuarios una vez haya logrado convencer al usuario de realizar algo que no debe. LFI y RFI, o vulnerabilidades de inclusión, en los cuales un atacante puede detectar funcionalidades en una aplicación web que le permita ejecutar código desde dentro del sistema o por fuera de él para sacar provecho, mediante dos estrategias, la inclusión de archivos locales y la inclusión de archivos remotos.

5.2.5 *Pentesting* pruebas de penetración. Es el análisis de aplicaciones, para este proyecto, de aplicaciones web, que permiten realizar evaluaciones de seguridad y brindan información relevante para determinar el nivel de seguridad establecido por las aplicaciones web, dentro de una red LAN o WLAN, mediante la simulación de ataques que podrían poner en riesgo la información o los servicios

asociados a ella y de esta manera descubrir amenazas antes de que los atacantes las localicen.

5.2.5.1 Métodos de análisis de aplicaciones web. Existen múltiples métodos para el análisis de la seguridad de las aplicaciones, y de las aplicaciones web, entre los cuales se pueden identificar los siguientes: *Network Mapping*, *Information Gathering*, CMS *Identification*, IDS/IPS *Detection*, *Open Source Analysis*, *Web Crawlers*, *Vulnerability Assessment and Exploitation*, *Maintaining Access*, a continuación, se hará una breve descripción de cada uno de ellos.

Network Mapping, consiste en el estudio de la conectividad física de las redes esto permite identificar los servidores, y los sistemas operativos que estos ejecutan para su funcionamiento.

Information Gathering, consiste principalmente en la recolección de la mayor cantidad de información de una aplicación, esto mediante del uso de herramientas como los navegadores web, escaneos o simples peticiones HTTP, de tal manera que se pueda obtener información como los mensajes de errores, versiones de la aplicación entre otros.

CMS *Identification*, Es la identificación del administrador de contenidos de las aplicaciones web usado por ella, de tal manera que se pueda aprovechar los fallos de seguridad para que un atacante pueda actuar.

IDS/IPS *Detection*, Sistemas de detección de intrusiones y sistemas de prevención de intrusiones, por sus siglas en inglés, son sistemas hardware y software que se encargan de analizar el tráfico de red con el fin detectar virus, troyanos y gusanos que puedan afectar los sistemas informáticos, los atacantes pueden vulnerar la seguridad de los cortafuegos y de esta manera evitar los obstáculos que estos proponen, este conoce como "*bypassear*".

Open Source Analysis, consisten en herramientas web, principalmente, que se pueden utilizar para recopilar información de servidores vulnerables y pueden ser utilizados por *Pen-teste'r*, personas que realizan pruebas de penetración.

Web Crawlers, es un tipo de análisis que busca detectar los archivos ocultos dentro de un servidor web, de esta localizar fallos de seguridad.

Vulnerability Assessment and Exploitation, consiste en una evaluación de vulnerabilidad del objetivo, esto permite recabar información sobre una aplicación web, en la que mediante un escaneo se puede detectar la versión de las aplicaciones instaladas en el servidor web y a partir de ahí, se pueden utilizar otras herramientas para detectar las vulnerabilidades del servidor web específico.

Maintaining Access, es principalmente la acción de mantener disponible el acceso a una aplicación web, una vez se haya logrado acceder, para realizar futuros accesos con un esfuerzo mínimo, esto se logra cargando o manteniendo las denominadas puertas traseras sobre la aplicación web.

5.2.5.2 Herramientas de test de penetración. En el área de auditoría de seguridad informática una de las herramientas respetadas era la distribución de GNU/Linux llamada BackTrack basada en Ubuntu, sin embargo, el proyecto llegó hasta la versión 5 R3 y sus desarrolladores, *Offensive Security*, ahora trabajan para una distribución denominada Kali Linux pero esta vez basada en Debian en la que se incluyen herramientas para la realización de pruebas de penetración de las cuales a continuación se listan algunas destacadas:

- NMAP, o mapeador de redes, muy útil en la auditoria de sistemas, es de código abierto, y permite realizar una detección de los equipos disponibles dentro de una red. NMAP es una aplicación que permite recolectar información de los servidores de una red, los servicios ofrecidos por cada equipo, los tipos de paquetes y corta fuegos que empelan, como además los sistemas operativos que estos emplean.
- NEFITERIA, permite el escaneo de forma activa pasiva de la red detectando los hosts de la red.
- THEHARVESTER, permite recabar información como correos electrónicos, cuentas de usuarios, nombres de hosts o subdominios desde herramientas como los motores de búsqueda.
- MALTEGO, es una herramienta que permite relacionar, como el análisis forense, información entre los usuarios, empresas, amigos, de determinadas aplicaciones como las redes sociales y de esta manera construir una relación entre dominios y nombres de DNS.
- BlindElephant, es una aplicación que permite realizar proceso para la recopilación de información como la versión del navegador o del sistema operativo, sobre aplicaciones web, un concepto más conocido como "*fingerprinting*".
- WHATWEB, esta herramienta permite identificar el sistema de gestión de contenidos implementado por las aplicaciones web. Mediante esta aplicación se puede identificar gran cantidad información de un sitio web; desde el tipo servidor,

hasta los servicios que este utilice como: la plataforma, el tipo de gestor de contenidos, tipos de scripts, si usa el sistema de Google Anlystiscs, la plataforma del servidor web, direcciones IP, entre otros. Usa un tipo de escaneo pasivo y un testeo agresivo. El escaneo pasivo obtiene información de las cabeceras HTTP, de tal forma que parezca una visita normal al sitio web. El testeo agresivo utiliza algunas consultas que permiten identificar la tecnología y realizar un escaneo de vulnerabilidades.

- WAFFIT, facilita la detección de los posibles cortafuegos que está implementando un servidor web.
- WEBSHAG, es una herramienta la auditoria de servidores web, escaneo de direcciones web y el rastreo de web.
- DIRBUSTER, es una herramienta que permite realizar el proceso conocido como “Fuerza bruta” en los directorios y archivos de los servidores web, con el fin de localizar archivos ocultos.
- JOOMSCAN, es una herramienta que permite detectar vulnerabilidades como las SQL *injections*, XSS, sobre los servidores web basados en Joomla.
- SQLMAP, esta herramienta ayuda a explorar y detectar vulnerabilidades sobre el acceso a las bases de datos de los servidores web.
- SHODAN, es una herramienta que permite identificar que dispositivos están conectados a la Internet, y se están ejecutando el dominio correcto.
- W3AF, es una herramienta de auditoría de seguridad de aplicaciones web, desde la cual se pueden usar los siguientes módulos: Ataque, Auditoria, *Exploit*, Descubrimiento, *Evasion* y *Brute Force*.
- WEEVELY, es una herramienta que se utiliza como puerta trasera y de esta maneara mantener disponibles sesiones de cuentas de usuarios disponibles.

Otras herramientas:

- GHDB, es una aplicación web que permite recopilar información sobre servidores vulnerables.
- XSSED, es un sitio que mantiene una lista de sitios web vulnerables a XSS. UNISCAN, es un escáner de vulnerabilidades web, está bajo GPL 3.
- WEBACOO, es una herramienta que permite mantener el acceso a las a los servidores web, funciona como backdoor “puerta trasera”.
- OWAS MANTRA, es un marco de trabajo de seguridad, compuesto por varias herramientas que permiten el testeo mediante un navegador web basado FireFox.

5.2.5.2.1 Fragroute. Esta aplicación es capaz de interceptar, modificar y reescribir el tráfico de salida destinado a host determinado. Este está constituido con un conjunto de reglas que retrasa, duplica, descarta, fragmenta, superpone, imprime, reordena, segmenta, enruta los paquetes de salida destinados a un host. Está diseñado para las pruebas de sistemas IDS, corta fuegos y comportamiento básico de pila TCP/IP.

5.2.6 Riesgo y control informático. En la actualidad, una de las mayores preocupaciones de las organizaciones, está relacionada con la seguridad de la información y de los sistemas informáticos, esto, a causa de los crecientes reportes de ataques perpetrados por los delincuentes informáticos. Cuyos actos se han visto reflejados desde simples accesos no autorizados a las cuentas de las redes sociales más populares, y hasta la publicación de información de entidades gubernamentales y empresas privadas, las cuales se han visto afectadas en las últimas décadas, y lo que genera un especial interés en el tema de la protección de la información dentro de las empresas.

Otro de los factores influyentes en contra de la seguridad, son los avances tecnológicos y el acceso creciente a la red de Internet, lo que permite y facilita los actos en contra de la seguridad informática y de la información.
Para facilitar el proceso de mantener buenas prácticas en materia de seguridad informática, las organizaciones cuentan con distintos estándares y metodologías para el control y gestión de riesgos, así como, para la mantención de la información y de los sistemas informáticos bajo políticas de seguridad que la protejan.

En seguridad informática y seguridad de la información, el riesgo se puede definir como la posibilidad de que ocurra algún evento que afecte la confidencialidad, la integridad, la disponibilidad de la información y en general de los sistemas informáticos.

El control, se refiere a cada una de las medidas, estrategias y procedimientos que ayuden a mitigar o a mantener en bajos niveles los riesgos de seguridad informática.

Dentro de las normas, estándares y metodologías en pro de la seguridad informática, se encuentran la norma ISO 27000, COBIT, MAGERIT.

5.2.7 Magerit Es una metodología orientada al proceso de gestión de riesgos asociados con el uso de las tecnologías de la información que ha sido desarrollada por el Consejo Superior de Administración Electrónica de España.

Esta metodología posee las siguientes características:

- El resultado se expresa en valores económicos.
- Método sistematizado para analizar los riesgos.
- Ayuda a identificar y planificar medidas necesarias para minimizar los riesgos.
- Da herramientas que ayudan a facilitar el análisis de riesgos.
- Se le atribuye con un alcance completo, tanto en el análisis como en la gestión de riesgos.
- Posee un extenso archivo de inventarios en lo relacionado a recursos de información, amenazas y tipo de activos.
- Permite un análisis completo cualitativo y cuantitativo.
- De carácter Público.
- No requiere autorización previa para su uso. Es una metodología líder en España, con buenos referentes de aplicación.

Magerit propone las siguientes fases:

- Planificación del proyecto de riesgos.
- Análisis de riesgos.
- Gestión de riesgos.
- Selección de salvaguardas.

5.3 Ataques a los sistemas de información

Uno los activos más importantes de todo sistema de información es su sistema de gestión de gestión de bases de datos, y puede ser un punto de quiebre para la seguridad informática y de la información de la organización.

5.3.1 Ataques a las bases de datos

5.3.1.1 Db-DoS. O ataques de denegación de servicios de bases de datos. Se considera uno de los ataques más comunes y se destacan los siguientes:

- ***flooding the pipes* o inundación**: Este tipo de ataque consiste en el envío de muchos paquetes de red que el equipo no es capaz de resolver consiguiendo saturarlo. Este ataque toma muchos clientes o equipos malintencionados para inundar redes grandes. Con el tráfico de red a gran volumen o con muchos datos, la información que los usuarios solicitan se confunde y no es capaz de llegar a los servidores.
- ***Exhausting servers*:** Estos ataques están dirigidos al software que corre en los servidores principalmente su sistema operativo y a los componentes de las aplicaciones web, afectando el uso de la CPU, la memoria y demás recursos del sistema. Estos ataques pueden estar orientados a las vulnerabilidades y características de las aplicaciones para saturar los servidores previniendo que el tráfico de datos acceda a las páginas web y finalice las transacciones. Al consumir más recursos de hardware y software la plataforma se vuelve menos eficiente, llevándolos al límite bloqueando la espera de recursos y retrasando su disponibilidad. En algunos casos es necesario reiniciarlos.

Las bases de datos poseen sus propias características de red y servicios que facilitan los ataques de ambos tipos.

5.4 MARCO CONCEPTUAL

La seguridad de la información: Esta se refiere a las estrategias aplicadas para garantizar la integridad, la confidencialidad y la disponibilidad de todos los elementos como datos e información almacenada de forma digital y que forman parte de la aplicación de pedidos web.

La integridad: Desde el punto de vista de la seguridad de la información, la información de un sistema tiene integridad cuando se garantiza que la información es la correcta y esta no ha sufrido cambios no esperados para los cuales fue diseñado el sistema.

La confidencialidad: Desde el punto de vista de la seguridad de la información, la información de un sistema es confidencial cuando esta es visible solo para las personas autorizadas a interactuar con el sistema.

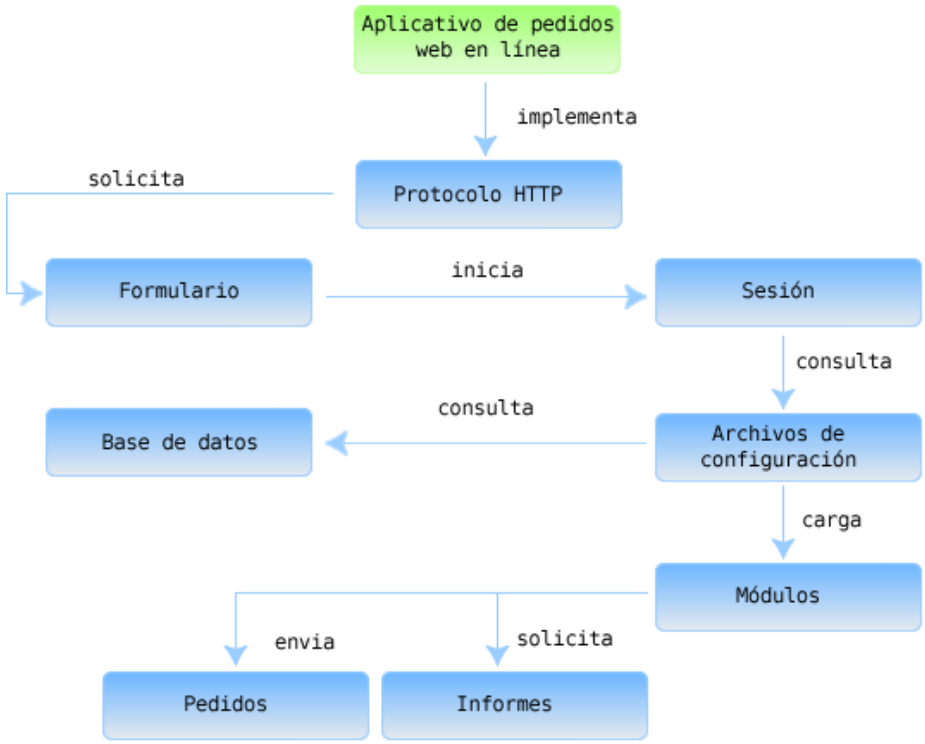
La disponibilidad: Desde el punto de vista de la seguridad de la información, la información de un sistema está disponible cuando se requiera para los efectos que el sistema haya sido diseñado, manteniendo los niveles de seguridad en los términos de accesibilidad bien definidos.

La seguridad de los sistemas informáticos: Esta se refiere a las estrategias aplicadas para garantizar la integridad, la confidencialidad y la disponibilidad de todos aquellos elementos físicos como servidores, dispositivos de red entre otros que garanticen la disponibilidad de la aplicación web.

Aplicación web: Desde el punto de vista informático, una aplicación como tal es el resultado de la codificación en un lenguaje entendible por la computadora, conocido como lenguaje de programación, diseñada con el objetivo de cumplir determinados propósitos, ya sea el registro de información o procesamiento de la misma, adicionalmente una aplicación web está orientada para su uso a través de la red Internet por medio de un navegador web.

Sistema de pedidos: Es una aplicación informática, desarrollada apara un entorno web, desde el cual un usuario puede realizar un pedido de productos por catálogo.
Análisis de riesgos: Es el estudio de todos los factores que pueden intervenir o afectar la seguridad de la aplicación web de pedidos web de la empresa.

Figura 1. Marco conceptual



Fuente: El autor

La implementación de metodología Magerit, para la realización de este proyecto, pretende ser la guía inicial para que la empresa E.B. Software Ltda., mantenga políticas de seguridad informática y de la información, así como buenas prácticas a la hora de desarrollar aplicaciones web y esta forma brindar a sus clientes confianza a la hora de elegir sus productos.

Se ha decido, una vez realizado el análisis de riesgos, detectar posibles fallas de seguridad mediante la realización de pruebas de penetración o *pent testing*, que ayuden a implementar medidas de control para prevenir posibles amenazas relacionadas con la integridad, confidencialidad y disponibilidad del sistema de pedidos web de la empresa E.B Software Ltda.

5.4.1 Norma ISO 27000. Estas normas dan una visión general de las normas que componen la serie 27000 y proporcionan un modelo de gestión para la seguridad de la información aplicable a cualquier organización.

Contiene alcance y propósitos, bases para implantar un Sistema de Gestión de Seguridad de la Información, al cual se hará referencia en este documento como SGSI, monitoreo, mantenimiento de los SGSI, buenas prácticas para la gestión de la seguridad de la información.

Función: definir requisitos para un sistema de gestión de seguridad informática, para garantizar controles de seguridad adecuados y proporcionales, protegiendo así la información.

Características:

- Confidencialidad
- Seguridad de información
- Sistema de gestión de seguridad de la información

Algunas de las normas contenidas en esta serie son:
ISO/IEC 27001, norma principal de la serie, constituida por los requisitos de seguridad de la información, mediante esta norma se certifican los sistemas de gestión de seguridad de la información.

ISO/IEC 27002, guía de buenas prácticas donde se establecen los objetivos de control y controles recomendables en cuanto a seguridad de la información, No certificable, plantea 39 objetivos de control y 133 controles.

ISO/IEC 27003, esta guía se enfoca en los aspectos críticos necesarios para el diseño e implementación de un sistema de gestión de seguridad de la información, hace una descripción del proceso y el diseño desde la definición hasta la implementación como además del proceso de aprobación por parte de la dirección para la implementación del sistema de gestión de seguridad de la información. No certificable.

ISO/IEC 27004, esta norma contiene la guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un sistema de gestión de seguridad de la información, así como los controles implementados según ISO/IEC 27001.
ISO/IEC 27005, indica directrices para la gestión de riesgos en la seguridad de la información.

ISO/IEC 27006, Establece los requisitos necesarios para que las entidades de auditoría y los sistemas de gestión de seguridad de la información puedan ser acreditados.

ISO/IEC 27017, es una guía de seguridad para Cloud Computing, computación en la nube.

ISO/IEC 27018, código de buenas prácticas en controles de protección de datos para servicios de computación en la nube.

ISO/IEC 27034, está orientada a la seguridad en aplicaciones informáticas, entre los cuales comprende validación de la seguridad en aplicaciones, estructura de datos entre otros.

5.5 MARCO LEGAL

5.5.1 ASPECTOS GENERALES DE LA LEY 1273 DE 2019 DELITOS INFORMÁTICOS EN COLOMBIA. Es la ley que se adiciona al código penal, y fue promulgada el 5 de enero de 2019. En ella se tipifican los delitos de conductas referidas a los datos personales.

Esta ley se refiere específicamente de los delitos que atentan contra las características principales de la información y los sistemas informáticos como lo son la confidencialidad la integridad y la disponibilidad de los mismos; que contiene dos capítulos, el primero con 8 artículos y el segundo con 2 artículos, dónde las penas de presión pueden ir hasta los 120 meses y las multas ascienden a los 1500 salarios mínimos vigentes.

6. MARCO METODOLÓGICO

6.1 POBLACIÓN Y MUESTRA

6.1.1 Población objetivo. La población objetivo se conforma con los usuarios de la aplicación de pedidos web de la empresa E.B. Software Ltda., ubicada en la ciudad de Bogotá D.C.

6.1.2 Tamaño de la Muestra. El tamaño de la muestra está determinado por la cantidad de usuarios logueados en el sistema de pedidos web de la empresa E.B. Software Ltda., ubicada en la ciudad de Bogotá D.C., involucra a dos (2) empleados por empresa, un (1) empleado encargado de realizar el pedido, y un (1) empleado encargado de realizar la verificación y autorización de los pedidos realizados.

6.2 METODOLOGÍA DE INVESTIGACIÓN

Este proyecto de desarrollará con un enfoque de investigación cualitativa, ya que se basará en observación directa de las pruebas de penetración para identificar las posibles fallas de seguridad, de tal forma que se puede recolectar la mayor cantidad información para posteriormente interpretar estos datos y determinar cómo se puede mejorar la seguridad de la aplicación web.

6.3 METODOLOGÍA DE DESARROLLO

Para el desarrollo del proyecto se implementará la metodología Magerit, que propone las siguientes etapas:

6.3.1 Planificación del proyecto de riesgos. Dada la importancia que representa para la empresa E.B. Software Ltda. mantenerse en el mercado ya que es de la venta de sus productos, software, su principal fuente ingresos; se determinó desde el área de desarrollo que una de las aplicaciones que podría ser destacada por el área comercial era la aplicación de pedidos web, y teniendo en cuenta que una de las mayores dificultades que presentan los asesores a la hora de ofrecer un producto distribuido en Internet, es el temor de los adquirentes a tener la información de sus productos y clientes fuera de sus instalaciones. En esta etapa se define como política desarrollar aplicaciones web seguras, cuyo objetivo principal es garantizar la integridad, la disponibilidad y confidencialidad de la información y los datos procesados en estas.

6.3.2 Análisis de riesgos. Para esta etapa, se inicia un proceso de recolección de información dentro de la empresa E.B Software Ltda. enfocada al aplicativo de pedidos web, en la que se pudo identificar qué elementos y componentes la integran, basados en la escasa documentación que el área de desarrollo reporta, como lo es el modelo de datos, arquitectura de desarrollo, lenguaje de programación, motor de base de datos empleado y herramientas utilizadas en la codificación. El capítulo 8, ítem 8.1 identificación de activos, muestra el resultado de esta etapa.

6.3.3 Gestión de riesgos. Con toda la información recolectada de la etapa anterior se procede a identificar que tan importantes son los componentes que integran la aplicación web asignando una valoración y presupuestando a qué amenazas podrían verse sometidos. El capítulo 8 de este documento, ítem 8.1.1 Valoración de activos, 8.2.1 valoración de amenazas, se recopila el resultado de esta etapa.

6.3.4 Selección de salvaguardas. Para esta etapa se indican qué medidas se pueden aplicar para mejorar la seguridad del aplicativo de pedidos web y de los componentes que la integran a nivel general, el capítulo 8, ítem 8.3 SALVAGUARDAS, registran el resultado de esta etapa.

7. PRODUCTO RESULTANTE A ENTREGAR

El resultado del proyecto será un informe con el análisis de la seguridad del aplicativo web de pedidos en línea de la empresa E.B Software Ltda., con sus respectivas recomendaciones. El cual contendrá lo siguiente:

- Resumen ejecutivo
- Descripción de los *test* de ataques
- Recomendaciones principales
- Calificación del riesgo
- Conclusiones generales

8. ANÁLISIS DE RIESGOS

8.1 IDENTIFICACIÓN DE ACTIVOS

Activos esenciales: datos / información, servicios

Cuadro 1. Activo Base de datos de la aplicación

[info] Información	
Código: EBSL1	**Nombre**: Base de datos de la aplicación
Descripción: Archivo principal que contiene los datos de la aplicación.	
Propietario: E.B. Software Ltda.	
Responsable: Ciro Pacheco	
Tipo: [info],[vr],[per],[M],[classified],[R],[service]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p.

Cuadro 2. Activo Imágenes de productos

[info] Información	
Código: EBSL2	**Nombre**: Imágenes de productos
Descripción: Archivo de imágenes en formato .jpg que son representación gráfica de los productos.	
Propietario: Cliente usuarios de la aplicación de gestión de pedidos web	
Responsable: E.B. Software Ltda.	
Tipo: [files]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p.

Cuadro 3. Activo Módulo compilado capa de datos (.dll)

[info] Información	
Código: EBSL3	**Nombre**: Módulo compilado capa de datos (.dll)
Descripción: Archivo compilado como librería de clases .dll, que gestiona el proceso de gestión con la base de datos.	
Propietario: E.B. Software Ltda.	
Responsable: Ciro Pacheco	
Tipo: [files],[int],[edi]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p.

Cuadro 4. Activo Módulo compilado envío de correos (.dll)

[info] Información	
Código: EBSL4	**Nombre**: Módulo compilado envío de correos (.dll)
Descripción: Archivo compilado como librería de clases .dll, que gestiona el proceso de envío de correos como notificaciones de pedidos nuevos.	
Propietario: E.B. Software Ltda.	
Responsable: Ciro Pacheco	
Tipo: [files],[int],[edi]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p.

Cuadro 5. Activo Intranet

[service] Servicio	
Código: EBSL5	**Nombre**: Intranet
Descripción: Red de computadoras interna, que permite la comunicación entre las estaciones de trabajo.	
Propietario: Cliente usuarios de la aplicación de gestión de pedidos web	
Responsable: Personal de TIC del cliente de la aplicación de pedidos web	
Tipo: [prp],[*file*],[edi],[www]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p

Cuadro 6. Activo Servidor de alojamiento de aplicación

[HW] Equipamiento informático (hardware)	
Código: EBSL6	**Nombre**: Servidor de alojamiento de aplicación
Descripción: Equipo servidor donde se encuentran alojadas las aplicaciones web	
Propietario: Godaddy.com	
Responsable: Godaddy.com	
Tipo: [*host*],[pc],[*network*],[MAN]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p

Cuadro 7. Activo Servidor de alojamiento de aplicación

[AUX] Equipamiento auxiliar	
Código: EBSL7	**Nombre**: Hosting de alojamiento Go Daddy
Descripción: Servicio de alojamiento de las aplicaciones web	
Propietario: Godaddy.com	
Responsable: Godaddy.com	
Tipo: [*host*],[pc],[*network*],[MAN]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p

Cuadro 8. Activo Internet

[AUX] Equipamiento auxiliar	
Código: EBSL8	**Nombre**: Internet
Descripción: Servicio de conexión a la red de internet	
Propietario: Cliente usuarios de la aplicación de gestión de pedidos web	
Responsable: Personal de TIC del cliente de la aplicación de pedidos web	
Tipo: [www], [*network*],[MAN]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p

Cuadro 9. Activo Ubicación Hosting de alojamiento Go Daddy

[AUX] Equipamiento auxiliar	
Código: EBSL9	**Nombre**: Ubicación de Hosting de alojamiento Go Daddy
Descripción: Ubicación principal del servicio de alojamiento web	
Propietario: Godaddy.com	
Responsable: Godaddy.com	
Tipo: [www], [network],[MAN], [host],[pc]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p

Cuadro 10. Activo Usuarios de aplicación

[P] Personal	
Código: EBSL10	**Nombre**: Usuarios de aplicación
Descripción: Son los usuarios que inician sesión en el aplicativo para realizar pedidos	
Propietario: E.B. Software Ltda.	
Responsable: Cliente usuarios de la aplicación de gestión de pedidos web	
Tipo: [ue],[ui],[adm] ,[com] ,[dba],[des]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p

Cuadro 11. Activo Administrador de aplicación

[P] Personal	
Código: EBSL11	**Nombre**: Administrador de aplicación
Descripción: Es el usuario encargado de la administración de la aplicación	
Propietario: E.B. Software Ltda.	
Responsable: Ciro Pacheco	
Tipo: [ue],[ui],[adm],[com],[dba],[des]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p

Cuadro 12. Activo Soporte de aplicación

[P] Personal	
Código: EBSL12	**Nombre**: Soporte de aplicación
Descripción: Es el usuario encargado del soporte de la aplicación	
Propietario: E.B. Software Ltda.	
Responsable: Ciro Pacheco	
Tipo: [ue],[ui],[adm],[com],[dba],[des]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p

Cuadro 13. Activo Mantenimiento de aplicación

[P] Personal	
Código: EBSL13	**Nombre**: Mantenimiento de aplicación
Descripción: Es la persona encargada del mantenimiento de la aplicación	
Propietario: E.B. Software Ltda.	
Responsable: Ciro Pacheco	
Tipo: [ue],[ui],[adm],[com],[dba],[des]	

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p

8.1.1 Valoración de activos

Cuadro 14. Escala para valoración de activos

Valor cuantitativo	Valor cualitativo	Descripción
0	MB	Muy bajo - No aplicable
1	B	Bajo - La pérdida de seguridad en la dimensión no impediría la actividad normal de la empresa.
2	M	Medio - La pérdida de seguridad en la dimensión causaría trastornos leves en la actividad normal de la empresa.
3	A	Alto -La pérdida de seguridad en la dimensión causaría trastornos graves en la actividad normal de la empresa.

Fuente: El autor

Cuadro 15. Dimensiones de seguridad

Código	Dimensión
[C]	Confidencialidad
[I]	Integridad
[A]	Autenticidad
[D]	Disponibilidad
[T]	Trazabilidad

Fuente: El autor

Cuadro 16. Valoración de activos

Activo	[C]	[I]	[A]	[D]	[T]	Valoración
Base de datos de la aplicación	3	3	3	3	3	15
Imágenes de productos	2	1	1	1	1	8
Módulo compilado capa de datos	3	3	3	3	2	15
Módulo compilado envío de correos	2	2	3	2	3	12
Intranet	3	3	3	3	3	15
Servidor de alojamiento de aplicación	3	3	3	3	3	15
Hosting de alojamiento Go Daddy	3	3	3	3	3	15
Usuarios de aplicación	3	3	3	3	3	15
Administrador de aplicación	3	3	3	3	3	15
Soporte de aplicación	3	3	3	3	3	15
Mantenimiento de aplicación	3	3	3	3	3	15

Fuente: El autor

8.2 AMENAZAS

De origen natural

Inundaciones, terremotos

Del entorno (de origen industrial)

Fallas eléctricas, fuego

Defectos de las aplicaciones

Errores de programación

Causadas por las personas de forma accidental

Error al ingresar datos, usuarios deja sesión iniciada en el sistema

Causadas por las personas de forma deliberada

8.2.1 Valoración de Amenazas. Para la valoración de amenazas se implementa la siguiente escala de valoración, que de acuerdo la metodología Magerit, se usa de forma habitual un año como referencia, teniendo en cuenta la siguiente tabla.

Cuadro 17. Escala de probabilidad y frecuencia

Probabilidad	Frecuencia	Valor
Muy frecuente	A diario	100
Frecuente	Mensualmente	10
Normal	Una vez al año	1
Poco frecuente	Cada varios años	1/10
Muy poco frecuente	Siglos	1/100

Fuente: MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid, octubre 2012. 127 p

Cuadro 18. Relación Amenazas – Activos

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[N.1] Fuego	HW] equipos informáticos	1				3	
	[Media] soportes de información	1				3	
	[AUX] equipamiento auxiliar	1				3	
	[L] instalaciones	1				3	
[N.2] Daños por agua	[HW] equipos informáticos	1				3	
	[Media] soportes de información	1				3	
	[AUX] equipamiento auxiliar	1				3	
	[L] instalaciones	1				3	
[N.7] Desastres naturales. 07- Fenómeno sísmico.	[HW] equipos informáticos	1				3	
	[Media] soportes de información	1				3	
	[AUX] equipamiento auxiliar	1				3	
	[L] instalaciones	1				3	

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[I.3] Contaminación mecánica	[HW] equipos informáticos	1				3	
	[Media] soportes de información	1				3	
	[AUX] equipamiento auxiliar	1				3	
[I.5] Avería de origen físico o lógico.	[S] Software – Aplicaciones informáticas	1				3	
	[HW] equipos informáticos	1				3	
	[Media] soportes de información	1				3	
[I.6] Corte del suministro eléctrico	[HW] equipos informáticos	10				3	
	[Media] soportes de información	10				3	
	[AUX] equipamiento auxiliar	10				3	
[I.7] Condiciones inadecuadas de temperatura o humedad	[HW] equipos informáticos	1/10				3	
	[Media] soportes de información	1/10				3	
	[AUX] equipamiento auxiliar	1/10				3	

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[I.8] Fallo de servicios de comunicaciones	[COM] Redes de comunicaciones	10				3	
[I.9] Interrupción de otros servicios y suministros esenciales	[AUX] equipamiento auxiliar	10				3	
[I.10] Degradación de los soportes de almacenamiento de la información	[Media] soportes de información	1				3	
[E.1] Errores de los usuarios	[D] Datos/Información	10	3	3		3	
	[S] Servicios	10	3	2		2	
	[S] Software – Aplicaciones informáticas	10	3	2		2	
	[Media] soportes de información	10	3	2		2	

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[E.2] Errores del administrador	[D] Datos/Información	10	3	3		3	
	[S] Servicios	10	3	3		3	
	[S] Software – Aplicaciones informáticas	10	3	3		3	
	[HW] equipos informáticos	10	3	3		3	
	[COM] Redes de comunicaciones	10	3	3		3	
	[Media] soportes de información	10	3	3		3	
[E.3] Errores de monitorización (log)	[D] Datos/Información [Log] registros de actividad	1		1			3
[E.4] Errores de configuración	[D] Datos/Información [conf] datos de configuración	1		3			
[E.7] Deficiencias en la organización	[P] Personal	10				3	

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[E.8] Difusión de software dañino	[S] Software – Aplicaciones informáticas	1	3	3		3	
[E.9] Errores de re encaminamiento	[S] Servicios	1	3				
	[S] Software – Aplicaciones informáticas	1	3				
	[COM] Redes de comunicaciones	1	3				
[E.10] Errores de secuencia	[S] Servicios	1		3			
	[S] Software – Aplicaciones informáticas	1		3			
	[COM] Redes de comunicaciones	1		3			

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[E.15] Alteración accidental de la información	[D] Datos/Información	1/10		3			
	[S] Servicios	1/10		3			
	[S] Software – Aplicaciones informáticas	1/10		3			
	[COM] Redes de comunicaciones	1/10		3			
	[Media] soportes de información	1/10		3			
	[L] instalaciones	1/10		3			
[E.18] Destrucción de la información	[D] Datos/Información	1/10				3	
	[S] Servicios	1/10				3	
	[S] Software – Aplicaciones informáticas	1/10				3	
	[COM] Redes de comunicaciones	1/10				3	
	[Media] soportes de información	1/10				3	
	[L] instalaciones	1/10				3	

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[E.19] Fugas de información	[D] Datos/Información	1/10	3				
	[S] Servicios	1/10	3				
	[S] Software – Aplicaciones informáticas	1/10	3				
	[COM] Redes de comunicaciones	1/10	3				
	[Media] soportes de información	1/10	3				
	[L] instalaciones	1/10	3				
	[P] personal	1/10	3				
[E.20] Vulnerabilidades de los programas (software)	[S] Software – Aplicaciones informáticas	1/10	3	3		3	
[E.21] Errores de mantenimiento / actualización de programas (software)	[S] Software – Aplicaciones informáticas	10		3		3	

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[HW] equipos informáticos	10				3	
	[Media] soportes de información	10				3	
	[AUX] equipamiento auxiliar	10				3	
[E.24] Caída del sistema por agotamiento de recursos	[S] Servicios	10				3	
	[HW] equipos informáticos	10				3	
	[COM] Redes de comunicaciones	10				3	
[E.25] Pérdida de equipos Robo	[HW] equipos informáticos	1/10	3			3	
	[Media] soportes de información	1/10	3			3	
	[AUX] equipamiento auxiliar	1/10	3			3	
[E.28] Indisponibilidad del personal	[P] Personal	1/10				3	

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[A.3] Manipulación de los registros de actividad(log)	[D] Datos/Información [Log] registros de actividad	1/100		3			3
[A.4] Manipulación de la configuración	[D] Datos/Información [Log] registros de actividad	1/100	3	3		3	
[A.5] Suplantación de la identidad del usuario	[D] Datos/Información	1/100	3	3	3		
	[S] Servicios	1/100	3	3	3		
	[S] Software – Aplicaciones informáticas	1/100	3	3	3		
	[COM] Redes de comunicaciones	1/100	3	3	3		
[A.6] Abuso de privilegios de acceso	[D] Datos/Información	1/10	3	3		3	
	[S] Servicios	1/10	3	3		3	
	[S] Software – Aplicaciones informáticas	1/10	3	3		3	
	[HW] equipos informáticos	1/10	3	3		3	
	[COM] Redes de comunicaciones	1/10	3	3		3	

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[A.7] Uso no previsto	[S] Servicios	1/10	3	3		3	
	[S] Software – Aplicaciones informáticas	1/10	3	3		3	
	[HW] equipos informáticos	1/10	3	3		3	
	[COM] Redes de comunicaciones	1/10	3	3		3	
	[Media] soportes de información	1/10	3	3		3	
	[AUX] equipamiento auxiliar	1/10	3	3		3	
	[L] instalaciones	1/10	3	3		3	
[A.8] Difusión de software dañino	[S] Software – Aplicaciones informáticas	1/10	3	3		3	

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[A.9] [Re-] encaminamiento de mensajes	[S] Servicios	1/100	3				
	[S] Software – Aplicaciones informáticas	1/100	3				
	[COM] Redes de comunicaciones	1/100	3				
[A.11] Acceso no autorizado	[S] Software – Aplicaciones informáticas	1/10	3	3			
	[HW] equipos informáticos	1/10	3	3			
	[COM] Redes de comunicaciones	1/10	3	3			
	[Media] soportes de información	1/10	3	3			
	[AUX] equipamiento auxiliar	1/10	3	3			
	[L] instalaciones	1/10	3	3			

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[A.12] Análisis de tráfico	[COM] Redes de comunicaciones	1/10	3				
[A.14] Interceptación de información (escucha)	[COM] Redes de comunicaciones	1/100	3				
[A.15] Modificación deliberada de la información	[D] Datos/Información	1/10		3			
	[S] Servicios	1/10		3			
	[S] Software – Aplicaciones informáticas	1/10		3			
	[COM] Redes de comunicaciones	1/10		3			
	[Media] soportes de información	1/10		3			
	[L] instalaciones	1/10		3			

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[A.18] Destrucción de información	[D] Datos/Información	1/10				3	
	[S] Servicios	1/10				3	
	[S] Software – Aplicaciones informáticas	1/10				3	
	[Media] soportes de información	1/10				3	
	[L] instalaciones	1/10				3	
[A.19] Divulgación de información 34 – Copia ilegal de software	[D] Datos/Información	1/10	3				
	[S] Servicios	1/10	3				
	[S] Software – Aplicaciones informáticas	1/10	3				
	[COM] Redes de comunicaciones	1/10	3				
	[Media] soportes de información	1/10	3				
	[L] instalaciones	1/10	3				
[A.22] Manipulación de programas	[S] Software – Aplicaciones informáticas	1/10	3	3		3	

Fuente: El autor

Cuadro 18. Relación Amenazas – Activos (Continuación)

Amenazas por activo							
Amenaza	**Activo**	**Probabilidad**	**Impacto por dimensión**				
			[C]	**[I]**	**[A]**	**[D]**	**[T]**
[A.23] Manipulación de los equipos	[HW] equipos informáticos	1/10	3			3	
	[Media] soportes de información	1/10	3			3	
	[AUX] equipamiento auxiliar	1/10	3			3	
[A.24] Denegación de servicio	[S] Servicios	1/10				3	
	[HW] equipos informáticos	1/10				3	
	[COM] Redes de comunicaciones	1/10				3	
[A.25] Robo 20 - Robo de soporte o documentos	[HW] equipos informáticos	1/100	3			3	
	[Media] soportes de información.	1/100	3			3	
	[AUX] equipamiento auxiliar	1/100	3			3	
[A.29] Extorsión	[P] Personal interno	1/100	3	3		3	
[A.30] Ingeniería social	[P] Personal interno	1/100	3	3		3	

Fuente: El autor

8.3 SALVAGUARDAS

Las medidas y estrategias tecnológicas dirigidas a reducir los riesgos de seguridad informática son conocidas como salvaguardas, Magerit define las siguientes.

Cuadro 19. Tipo de salvaguardas

Código	Descripción	Efecto
[PR]	Prevención	Reducir la oportunidad que incidente ocurra
[DR]	Disuasión	Impedir que los atacantes se atrevan a realizar los ataques, reducir la probabilidad antes de que ocurra.
[EL]	Eliminación	Impedir que un incidente tenga lugar.
[IM]	Minimización del impacto / limitación del impacto	Acotar las consecuencias de in incidente
[CR]	Corrección	Una vez producido un daño, esta lo repara
[RC]	Recuperación	Permitir regresar al estado anterior del incidente
[MN]	Monitorización	Verificar lo que está ocurriendo o lo que ha ocurrido
[DC]	Detección	Informar de ataques que están ocurriendo
[AW]	Concienciación	Informar a las personas anexas al sistema sobre los riesgos
[AD]	Administración	Salvaguardas de los componentes de seguridad del sistema

Fuente: El autor

Cuadro 20. Salvaguardas de activos

Código de grupo	Nombre del grupo	Código del activo	Nombre del activo	Salvaguarda
[info]	Información	EBSL1	Base de datos de la aplicación	[CR]
				[RC]
				[AW]
				[AD]
		EBSL2	Imágenes de productos	[CR]
				[RC]
		EBSL3	Módulo compilado capa de datos (.dll)	[CR]
				[RC]
		EBSL4	Módulo compilado envío de correos (.dll)	[CR]
				[RC]
[service]	Servicio	EBSL5	Intranet	[PR]
				[RC]
				[AW]
				[AD]
				[MN]
[HW]	Equipamiento informático (hardware)	EBSL6	Servidor de alojamiento de aplicación	[PR]
				[RC]
				[AW]
				[AD]
				[MN]

Fuente: El autor

Cuadro 20. Salvaguardas de activos (Continuación)

Código de grupo	Nombre del grupo	Código del activo	Nombre del activo	Salvaguarda
[AUX]	Equipamiento auxiliar	EBSL7	Hosting de alojamiento Go Daddy	[PR]
				[RC]
				[AW]
				[AD]
				[MN]
		EBSL8	Internet	[PR]
				[RC]
				[AW]
				[AD]
				[MN]
		EBSL9	Ubicación de Hosting de alojamiento Go Daddy	[PR]
				[RC]
				[AW]
				[AD]
				[MN]
[P]	Personal	EBSL10	Usuarios de aplicación	[AW]
				[AD]
		EBSL11	Administrador de aplicación	[AW]
				[AD]
		EBSL12	Soporte de aplicación	[AW]
				[AD]
		EBSL13	Mantenimiento de aplicación	[AW]
				[AD]

Fuente: el autor

8.3.1 Declaración de aplicabilidad

La declaración de aplicabilidad lista los controles de seguridad, que se relaciona con la implementación de las medidas de protección de la información, y se ha seguido para este proyecto el estándar de la Norma ISO/IEC 27002:2005.

Cuadro 21. Controles Norma ISO/IEC 27002:2013

Dominio	Subdominios	C.%	Cumplimiento %
5. Políticas de seguridad	5.1.1 Documento de política de seguridad de la información	**1 %**	**1 %**
	5.1.2 Revisión de la política de seguridad de la información	**1 %**	
Sub total (Suma de los porcentajes de cada subdominio)		**2 %**	
Promedio		**1 %**	
6. Aspectos Organizativo de la seguridad informática	6.1.1 Compromiso de la Dirección con la seguridad de la información.	**10 %**	**17.3 %**
	6.1.2 Coordinación de la seguridad de la información.	**1 %**	
	6.1.3 Asignación de responsabilidades relativas a la seguridad. de la información	**1 %**	
	6.1.4 Proceso de autorización de recursos para el tratamiento de la información.	**1 %**	
	6.1.5 Acuerdos de confidencialidad.	**40 %**	

Fuente: el autor

Cuadro 21. Controles Norma ISO/IEC 27002:2013 (Continuación)

Dominio	Subdominios	C.%	Cumplimiento %
	6.1.6 Contacto con las autoridades.	**1 %**	
	6.1.7 Contacto con grupos de especial interés.	**1 %**	
	6.1.8 Revisión independiente de la seguridad de la información.	**5 %**	
	6.2.1 Identificación de los riesgos derivados del acceso de terceros.	**20 %**	
	6.2.2 Tratamiento de la seguridad en la relación con los clientes.	**50 %**	
	6.2.3 Tratamiento de la seguridad en contratos con terceros.	**60 %**	
	Sub total	**190 %**	
	Promedio	**17.3 %**	
7. Gestión de los activos	7.1.1 Inventario de activos.	**30 %**	**20.2 %**
	7.1.2 Propiedad de los activos.	**10 %**	
	7.1.3 Uso aceptable de los activos.	**50 %**	
	7.2.1 Directrices de clasificación.	**1 %**	
	7.2.2 Etiquetado y manipulado de la información.	**10 %**	
	Sub total	**101 %**	
	Promedio	**20.2 %**	

Fuente: el autor

Cuadro 21. Controles Norma ISO/IEC 27002:2013 (Continuación)

Dominio	Subdominios	C.%	Cumplimiento %
8. Seguridad ligada a los recursos humanos	8.1.1 Funciones y responsabilidades.	**1 %**	**20.5 %**
	8.1.2 Investigación de antecedentes.	**1 %**	
	8.1.3 Términos y condiciones de contratación	**75 %**	
	8.2.1 Responsabilidades de la Dirección.	**10 %**	
	8.2.2 Concienciación, formación y capacitación	**1 %**	
	8.2.3 Proceso disciplinario.	**1 %**	
	8.3.1 Responsabilidad del cese o cambio.	**1 %**	
	8.3.2 Devolución de activos.	**75 %**	
	8.3.3 Retirada de los derechos de acceso.	**20 %**	
	Sub total	**185 %**	
	Promedio	**20.5 %**	
9. Seguridad física y del entorno	9.1.1 Perímetro de seguridad física.	**40 %**	**35.8 %**
	9.1.2 Controles físicos de entrada.	**50 %**	
	9.1.3 Seguridad de oficinas, despachos e instalaciones.	**50 %**	

Fuente: el autor

Cuadro 21. Controles Norma ISO/IEC 27002:2013 (Continuación)

Dominio	Subdominios	C.%	Cumplimiento %
	9.1.4 Protección contra las amenazas externas y de origen ambiental.	**30 %**	
	9.1.5 Trabajo en áreas seguras.	**30 %**	
	9.1.6 Áreas de acceso público y de carga y descarga.	**80 %**	
	9.2.1 Emplazamiento y protección de equipos.	**10 %**	
	9.2.2 Instalaciones de suministro.	**10 %**	
	9.2.3 Seguridad del cableado.	**50 %**	
	9.2.4 Mantenimiento de los equipos.	**40 %**	
	9.2.5 Seguridad de los equipos fuera de las instalaciones.	**10 %**	
	9.2.6 Reutilización o retirada segura de equipos.	**10 %**	
	9.2.7 Retirada de materiales propiedad de la empresa	**5 %**	
	Sub total	**465 %**	
	Promedio	**35.8 %**	
10. Gestión de comunicaciones y operación	10.1.1 Documentación de los procedimientos de operación.	**1 %**	**22.8 %**
	10.1.2 Gestión de cambios.	**1 %**	
	10.1.3 Segregación de tareas.	**30 %**	

Fuente: el autor

Cuadro 21. Controles Norma ISO/IEC 27002:2013 (Continuación)

Dominio	Subdominios	C.%	Cumplimiento %
	10.1.4 Separación de los recursos de desarrollo, prueba y operación.	**40 %**	
	10.2.1 Provisión de servicio	**50 %**	
	10.2.2 Supervisión y revisión de los servicios prestados por terceros.	**40 %**	
	10.2.3 Gestión del cambio en los servicios prestados por terceros.	**40 %**	
	10.3.1 Gestión de capacidades.	**50 %**	
	10.3.2 Aceptación del sistema.	**50 %**	
	10.4.1 Controles contra el código malicioso.	**30 %**	
	10.4.2 Controles contra el código descargado en el cliente.	**30 %**	
	10.5.1 Copias de seguridad de la información.	**60 %**	
	10.6.1 Controles de red.	**30 %**	
	10.6.2 Seguridad de los servicios de red.	**40 %**	
	10.7.1 Gestión de soportes extraíbles.	**5 %**	
	10.7.2 Retirada de soportes.	**1 %**	
	10.7.3 Procedimientos de manipulación de la información.	**20 %**	

Fuente: el autor

Cuadro 21. Controles Norma ISO/IEC 27002:2013 (Continuación)

Dominio	Subdominios	C.%	Cumplimiento %
	10.7.4 Seguridad de la documentación del sistema.	**10 %**	
	10.8.1 Políticas y procedimientos de intercambio de información.	**1 %**	
	10.8.2 Acuerdos de intercambio.	**1 %**	
	10.8.3 Soportes físicos en tránsito.	**1 %**	
	10.8.4 Mensajería electrónica.	**10 %**	
	10.8.5 Sistemas de información empresariales.	**20 %**	
	10.9.1 Comercio electrónico.	**5 %**	
	10.9.2 Transacciones en línea.	**40 %**	
	10.9.3 Información públicamente disponible.	**60 %**	
	10.10.1 Registros de auditoría.	**1 %**	
	10.10.2 Supervisión del uso del sistema.	**1 %**	
	10.10.3 Protección de la información de los registros.	**10 %**	
	10.10.4 Registros de administración y operación.	**10 %**	
	10.10.5 Registro de fallos.	**40 %**	
	10.10.6 Sincronización del reloj.	**1 %**	
	Sub total	**729 %**	
	Promedio	**22.8 %**	

Fuente: el autor

Cuadro 21. Controles Norma ISO/IEC 27002: 2013 (Continuación)

Dominio	Subdominios	C.%	Cumplimiento %
11. Control de acceso	11.1.1 Política de control de acceso.	**1 %**	**4.6 %**
	11.2.1 Registro de usuario.	**1 %**	
	11.2.2 Gestión de privilegios.	**1 %**	
	11.2.3 Gestión de contraseñas de usuario.	**10 %**	
	11.2.4 Revisión de los derechos de acceso de usuario.	**1 %**	
	11.3.1 Uso de contraseñas.	**1 %**	
	11.3.2 Equipo de usuario desatendido.	**1 %**	
	11.3.3 Política de puesto de trabajo despejado y pantalla limpia.	**10 %**	
	11.4.1 Política de uso de los servicios en red.	**5 %**	
	11.4.2 Autenticación de usuario para conexiones externas.	**1 %**	
	11.4.3 Identificación de los equipos en las redes.	**30 %**	
	11.4.4 Protección de los puertos de diagnóstico y configuración remotos.	**5 %**	
	11.4.5 Segregación de las redes.	**1 %**	
	11.4.6 Control de la conexión a la red.	**1 %**	
	11.4.7 Control de encaminamiento (routing) de red.	**5 %**	

Fuente: el autor

Cuadro 21. Controles Norma ISO/IEC 27002: 2013 (Continuación)

Dominio	Subdominios	C.%	Cumplimiento %
	11.5.1 Procedimientos seguros de inicio de sesión.	**1 %**	
	11.5.2 Identificación y autenticación de usuario.	**1 %**	
	11.5.3 Sistema de gestión de contraseñas.	**1 %**	
	11.5.4 Uso de los recursos del sistema.	**20 %**	
	11.5.5 Desconexión automática de sesión.	**1 %**	
	11.5.6 Limitación del tiempo de conexión.	**1 %**	
	11.6.1 Restricción del acceso a la información.	**5 %**	
	11.6.2 Aislamiento de sistemas sensibles	**1 %**	
	11.7.1 Ordenadores portátiles y comunicaciones móviles.	**1 %**	
	11.7.2 Teletrabajo	**10 %**	
	Sub total	**116 %**	
	Promedio	**4.6 %**	

Fuente: el autor

Cuadro 21. Controles Norma ISO/IEC 27002: 2013 (Continuación)

Dominio	Subdominios	C.%	Cumplimiento %
12. Adquisición, desarrollo y mantenimiento de sistemas de información	12.1.1 Análisis y especificación de los requisitos de seguridad.	**40 %**	**20.6 %**
	12.2.1 Validación de los datos de entrada.	**30 %**	
	12.2.2 Control del procesamiento interno.	**10 %**	
	12.2.3 Integridad de los mensajes.	**40 %**	
	12.2.4 Validación de los datos de salida.	**60 %**	
	12.3.1 Política de uso de los controles criptográficos.	**20 %**	
	12.3.2 Gestión de claves.	**60 %**	
	12.4.1 Control del software en explotación.	**40 %**	
	12.4.2 Protección de los datos de prueba del sistema.	**10 %**	
	12.4.3 Control de acceso al código fuente de los programas.	**5 %**	
	12.5.1 Procedimientos de control de cambios.	**5 %**	
	12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	**5 %**	
	12.5.3 Restricciones a los cambios en los paquetes de software.	**1 %**	

Fuente: el autor

Cuadro 21. Controles Norma ISO/IEC 27002: 2013 (Continuación)

Dominio	Subdominios	C.%	Cumplimiento %
	12.5.4 Fugas de información.	**1 %**	
	12.5.5 Externalización del desarrollo de software.	**1 %**	
	12.6.1 Control de las vulnerabilidades técnicas.	**1 %**	
	Sub total	**329 %**	
	Promedio	**20.6 %**	
13. Gestión de incidentes en la seguridad de la información.	13.1.1 Notificación de los eventos de seguridad de la información.	**1 %**	**1.8 %**
	13.1.2 Notificación de puntos débiles de seguridad.	**1 %**	
	13.2.1 Responsabilidades y procedimientos.	**1 %**	
	13.2.2 Aprendizaje de los incidentes de seguridad de la información.	**5 %**	
	13.2.3 Recopilación de evidencias.	**1 %**	
	Sub total	**9 %**	
	Promedio	**1.8 %**	
14. Gestión de la continuidad del negocio	14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	**1 %**	**1%**

Fuente: el autor

Cuadro 21. Controles Norma ISO/IEC 27002: 2013 (Continuación)

Dominio	Subdominios	C.%	Cumplimiento %
	14.1.2 Continuidad del negocio y evaluación de riesgos.	**1 %**	
	14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	**1 %**	
	14.1.4 Marco de referencia para la planificación de la cont. del negocio.	**1 %**	
	14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.	**1 %**	
	Sub total	**5 %**	
	Promedio	**1 %**	

Fuente: El autor

8.4 IMPACTO Y RIESGO RESIDUAL

8.4.1 Impacto residual

De acuerdo con Magerit al desplegar las salvaguardas, el sistema puede quedar con un posible impacto residual, puesto que se busca reducir el impacto potencial a un valor residual. Para el cálculo de este impacto residual, con la aplicación de la salvaguarda, la magnitud de degradación cambia, entonces se repiten los cálculos basados en este nuevo valor de degradación. Ver tabla 23.

8.4.2 Riesgo Residual

De acuerdo con Magerit al desplegar las salvaguardas, el sistema puede quedar un estado de riego residual, puesto que se busca reducir el riesgo potencial a un valor residual. Para el cálculo de este riesgo residual, con la aplicación de la salvaguarda, la magnitud de degradación cambia y la probabilidad de la amenaza, entonces se repiten los cálculos basados teniendo en cuenta el impacto residual y la probabilidad residual Ver tabla 23.

Cuadro 22. Relación Amenazas – Activos - Salvaguardas

Amenazas por activo aplicando las salvaguardas								
Amenaza	**Activo**	**Salvaguarda**	**Probabilidad**	**Impacto por dimensión**				
				[C]	**[I]**	**[A]**	**[D]**	**[T]**
[N.1] Fuego	HW] equipos informáticos	AUX.start AUX.power AUX.AC AUX.wires	1/10				1	
	[Media] soportes de información	AUX.start AUX.power AUX.AC AUX.wires	1/10				1	

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
	[AUX] equipamiento auxiliar	AUX.start AUX.power AUX.AC AUX.wires	1/10				1	
	[L] instalaciones	AUX.start AUX.power AUX.AC AUX.wires	1/10				1	
[N.2] Daños por agua	[HW] equipos informáticos	AUX.power AUX.wires	1/10				1	
	[Media] soportes de información	MP.A	1/10				1	
	[AUX] equipamiento auxiliar	AUX.power AUX.wires	1/10				1	
	[L] instalaciones	L.design	1/10				1	
[N.7] Desastres naturales. 07- Fenómeno sísmico.	[HW] equipos informáticos	AUX.power AUX.wires	1/10				1	
	[Media] soportes de información	MP.A	1/10				1	
	[AUX] equipamiento auxiliar	AUX.power AUX.wires	1/10				1	
	[L] instalaciones	L.design	1/10				1	

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
[I.3] Contaminación mecánica	[HW] equipos informáticos	MP.clean	1/10				1	
	[Media] soportes de información	MP.A	1/10				1	
	[AUX] equipamiento auxiliar	AUX.power AUX.wires	1/10				1	
[I.5] Avería de origen físico o lógico.	[S] Software – Aplicaciones informáticas	MP.A	1/10				1	
	[HW] equipos informáticos	AUX.power AUX.wires	1/10				1	
	[Media] soportes de información	MP.A	1/10				1	
[I.6] Corte del suministro eléctrico	[HW] equipos informáticos	AUX.power AUX.wires	1				1	
	[Media] soportes de información	MP.A	1				1	
	[AUX] equipamiento auxiliar	AUX.power AUX.wires	1				1	

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
[I.7] Condiciones inadecuadas de temperatura o humedad	[HW] equipos informáticos	AUX.AC	1/100				1	
	[Media] soportes de información	AUX.AC	1/100				1	
	[AUX] equipamiento auxiliar	AUX.AC	1/100				1	
[I.8] Fallo de servicios de comunicaciones	[COM] Redes de comunicaciones	COM.internet COM.wifi	1				1	
[I.9] Interrupción de otros servicios y suministros esenciales	AUX] equipamiento auxiliar	AUX.AC	1				1	
[I.10] Degradación de los soportes de almacenamiento de la información	[Media] soportes de información	D.A, D.I, D.C, D.DS	1/10				1	
[E.1] Errores de los usuarios	[D] Datos/Información	D.A, D.I, D.C, D.DS	1	1	1	1	1	1
	[S] Servicios	S.A	1	1	1	3	1	1

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
	[S] Software – Aplicaciones informáticas	D.A	1	1	1	3	1	1
	[Media] soportes de información	D.A	1	1	1	1	1	1
[E.2] Errores del administrador	[D] Datos/Información	D.A, D.I, D.C, D.DS	1	1	1	1	1	1
	[S] Servicios	S.A	1	1	1	1	1	1
	[S] Software – Aplicaciones informáticas	D.A	1	1	1	1	1	1
	[HW] equipos informáticos	D.A, SW.CM	1	1	1	1	1	1
	[COM] Redes de comunicaciones	SW.CM, COM.A	1	1	1	1	1	1
	[Media] soportes de información	D.A, D.I, D.C, D.DS	1	1	1	1	1	1

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
[E.3] Errores de monitorización (log)	[D] Datos/Información [Log] registros de actividad	D.A, D.I, D.C, D.DS	1/10					1
[E.4] Errores de configuración	[D] Datos/Información [conf] datos de configuración	D.A, D.I, D.C, D.DS	1/10	1	1	1	1	1
[E.7] Deficiencias en la organización	[P] Personal	PS.AT	1				1	
[E.8] Difusión de software dañino	[S] Software – Aplicaciones informáticas	D.A, D.I, D.C, D.DS	1/10	1	1	1	1	1
[E.9] Errores de re encaminamiento	[S] Servicios	S.www	1/10	1	1	1	1	1
	[S] Software – Aplicaciones informáticas	SW.SC	1/10	1	1	1	1	1
	[COM] Redes de comunicaciones	SW.CM, COM.A	1/10	1	1	1	1	1

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
[E.10] Errores de secuencia	[S] Servicios	S.A, S.SC	1/10		1			
	[S] Software – Aplicaciones informáticas	SW.A, SW.SC	1/10		1			
	[COM] Redes de comunicaciones	COM.SC, COM.A	1		1			
[E.15] Alteración accidental de la información	[D] Datos/Información	D.A	1/100	1	1	1	1	1
	[S] Servicios	S.A	1/100	1	1	1	1	1
	[S] Software – Aplicaciones informáticas	SW.A, SW.SC	1/100	1	1	1	1	1
	[COM] Redes de comunicaciones	COM.SC, COM.A	1/100	1	1	1	1	1
	[Media] soportes de información	D.A, D.I, D.C	1/10	1	1	1	1	1
	[L] instalaciones	L.design, L.AC	1/100	1	1	1	1	1
[E.18] Destrucción de la información	[D] Datos/Información	D.A	1/100				1	
	[S] Servicios	S.A, S.SC	1/100				1	

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
	[S] Software – Aplicaciones informáticas	SW.A, SW.SC	1/100				1	
	[COM] Redes de comunicaciones	COM.SC, COM.A	1/100				1	
	[Media] soportes de información	D.A, D.I, D.C	1/100				1	
	[L] instalaciones	L.design, L.AC	1/100				1	
[E.19] Fugas de información	[D] Datos/Información	D.A, D.C	1/100		1			
	[S] Servicios	S.A, S.SC	1/100		1			
	[S] Software – Aplicaciones informáticas	SW.A, SW.SC	1/100		1			
	[COM] Redes de comunicaciones	COM.SC, COM.A	1/100		1			
	[Media] soportes de información	D.A, D.I, D.C	1/100		1			
	[L] instalaciones	L.design, L.AC	1/100		1			
	[P] personal	PS.AT	1/100		1			

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
[E.20] Vulnerabilidades de los programas (software)	[S] Software – Aplicaciones informáticas	SW.A, SW.SC	1/100	1	1	1	1	1
[E.21] Errores de mantenimiento / actualización de programas (software)	[S] Software – Aplicaciones informáticas	SW.A, SW.SC	1	1	1	1	1	1
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[HW] equipos informáticos	HW.SC, HW.A	1	1	1	1	1	1
	[Media] soportes de información	D.A, D.I, D.C	1	1	1	1	1	1
	[AUX] equipamiento auxiliar	AUX.A, AUX.power AUX.wires	1	1	1	1	3	1
[E.24] Caída del sistema por agotamiento de recursos	[S] Servicios	S.SC	1	1	1	1	1	1
	[HW] equipos informáticos	HW.SC, HW.A	1	1	1	1	1	1
	[COM] Redes de comunicaciones	COM.SC, COM.A	1	1	1	1	1	1

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
[E.25] Pérdida de equipos Robo	[HW] equipos informáticos	HW.SC, HW.A	1/100	1			1	
	[Media] soportes de información	D.A, D.I, D.C	1/100	1			1	
	[AUX] equipamiento auxiliar	AUX.A, AUX.power AUX.wires	1/100	1			1	
[E.28] Indisponibilidad del personal	[P] Personal	PS.AT	1/100				1	
[A.3] Manipulación de los registros de actividad (log)	[D] Datos/Información [Log] registros de actividad	D.A, D.C	1/100	1		1		
[A.4] Manipulación de la configuración	[D] Datos/Información [Log] registros de actividad	D.A, D.C	1/100	1	1	1	1	1

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
[A.5] Suplantación de la identidad del usuario	[D] Datos/Información	D.A, D.C	1/100	1	1	1		1
	[S] Servicios	S.SC	1/100	1	1	1		1
	[S] Software – Aplicaciones informáticas	SW.A, SW.SC	1/100	1	1	1		1
	[COM] Redes de comunicaciones	COM.SC, COM.A	1/100	1	1	1		1
[A.6] Abuso de privilegios de acceso	[D] Datos/Información	D.A, D.C	1/100	1	1	1		1
	[S] Servicios	S.A, S.SC	1/100	1	1	1		1
	[S] Software – Aplicaciones informáticas	SW.A, SW.SC	1/100	1	1	1		1
	[HW] equipos informáticos	HW.SC, HW.A	1/10	1	1	1		1
	[COM] Redes de comunicaciones	COM.SC, COM.A	1/100	1	1	1		1
[A.7] Uso no previsto	[S] Servicios	S.A, S.SC	1/100	1	1	1	1	
	[S] Software – Aplicaciones informáticas	SW.A, SW.SC	1/100	1	1	1	1	
	[HW] equipos informáticos	HW.SC, HW.A	1/100	1	1	1	1	

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
	[COM] Redes de comunicaciones	COM.SC, COM.A	1/100	1	1	1	1	
	[Media] soportes de información	D.A, D.I, D.C	1/100	1	1	1	1	
	[AUX] equipamiento auxiliar	AUX.A	1/100	1	1	1	1	
	[L] instalaciones	L.design	1/100	1	1	1	1	
[A.8] Difusión de software dañino	[S] Software – Aplicaciones informáticas	SW.A, SW.SC	1/100	1	1	1	1	1
[A.9] [Re-] encaminamiento de mensajes	[S] Servicios	S.A, S.SC	1/100	1	1	1		1
	[S] Software – Aplicaciones informáticas	SW.A, SW.SC, SW.CM	1/100	1	1	1		1
	[COM] Redes de comunicaciones	COM.SC, COM.A, COM.wifi	1/100	1	1	1		1
[A.11] Acceso no autorizado	[S] Software – Aplicaciones informáticas	SW.A, SW.SC, SW.CM	1/100	1	1	1	1	1
	[HW] equipos informáticos	HW.SC, HW.A	1/100	1	1	1	1	1

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
	[COM] Redes de comunicaciones	COM.SC, COM.A, COM.wifi	1/100	1	1	1	1	1
	[Media] soportes de información	D.A, D.I, D.C	1/100	1	1	1	1	1
	[AUX] equipamiento auxiliar	AUX.A AUX.power, AUX.AC	1/100	1	1	1	1	1
	[L] instalaciones	L.design	1/100	1	1	1	1	1
[A.12] Análisis de tráfico	[COM] Redes de comunicaciones	COM.SC, COM.A, COM.wifi	1/100	1	1			
[A.14] Interceptación de información (escucha)	[COM] Redes de comunicaciones	COM.SC, COM.A, COM.wifi, COM.mobil	1/100	1	1			
[A.15] Modificación deliberada de la información	[D] Datos/Información	D.A, D.C	1/100	1	1	1	1	1
	[S] Servicios	S.A, S.SC	1/100	1	1	1	1	1
	[S] Software – Aplicaciones informáticas	SW.A, SW.SC, SW.CM	1/100	1	1	1	1	1

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
	[COM] Redes de comunicaciones	COM.SC, COM.A, COM.wifi, COM.mobil	1/100	1	1	1	1	1
	[Media] soportes de información	D.A, D.I, D.C	1/100	1	1	1	1	1
	[L] instalaciones	L.design	1/100	1	1	1	1	1
[A.18] Destrucción de información	[D] Datos/Información	D.A, D.C	1/100	1	1	1	1	1
	[S] Servicios	S.A, S.SC	1/100	1	1	1	1	1
	[S] Software – Aplicaciones informáticas	SW.A, SW.SC, SW.CM	1/100	1	1	1	1	1
	[Media] soportes de información	D.A, D.I, D.C	1/100	1	1	1	1	1
	[L] instalaciones	L.design	1/100	1	1	1	1	1
[A.19] Divulgación de información 34 – Copia ilegal de software	[D] Datos/Información	D.A, D.C	1/100	1	1	1		1
	[S] Servicios	S.A, S.SC	1/100	1	1	1		1
	[S] Software – Aplicaciones informáticas	SW.A, SW.SC, SW.CM	1/100	1	1	1		1
	[COM] Redes de comunicaciones	COM.SC, COM.A, COM.wifi, COM.mobil	1/100	1	1	1		1
	[Media] soportes de información	D.A, D.I, D.C	1/100	1	1	1		1
	[L] instalaciones	L.design	1/100	1	1	1		1

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
[A.22] Manipulación de programas	[S] Software – Aplicaciones informáticas	SW.A, SW.SC, SW.CM	1/100	1	1	1	1	1
[A.23] Manipulación de los equipos	[HW] equipos informáticos	HW.SC, HW.A	1/100	1	1	1	1	1
	[Media] soportes de información	D.A, D.I, D.C	1/100	1	1	1	1	1
	[AUX] equipamiento auxiliar	AUX.A AUX.power, AUX.AC	1/100	1	1	1	1	1
[A.24] Denegación de servicio	[S] Servicios	S.A, S.SC	1/100	1	1	1	1	1
	[HW] equipos informáticos	HW.SC, HW.A	1/100	1	1	1	1	1
	[COM] Redes de comunicaciones	COM.SC, COM.A, COM.wifi, COM.mobil	1/100	1	1	1	1	1
[A.25] Robo 20 - Robo de soporte o documentos	[HW] equipos informáticos	HW.SC, HW.A	1/100	1	1			
	[Media] soportes de información.	D.A, D.I, D.C	1/100	1	1			
	[AUX] equipamiento auxiliar	AUX.A AUX.power, AUX.AC	1/100	1	1			

Fuente: El autor

Cuadro 22. Relación Amenazas – Activos - Salvaguardas (Continuación)

Amenazas por activo aplicando las salvaguardas								
[A.29] Extorsión	[P] Personal interno	PS PS.AT	1/100	1	1			
[A.30] Ingeniería social	[P] Personal interno	PS PS.AT	1/100	1	1	1		

Fuente: El autor

9. PRUEBAS PARA LA DETECCIÓN DE VULNERABILIDADES, AMENAZAS Y RIESGOS DE SEGURIDAD DEL SISTEMA DE PEDIDOS WEB DE LA EMPRESA E.B SOFTWARE LTDA.

Para la realización de las pruebas de detección de vulnerabilidades, amenazas y riesgos del sistema de pedidos web de la empresa E.B. Software Ltda., se ha utilizado Kali Linux, la cual es una distribución basada en el sistema operativo Debian GNU/Linux, y es una herramienta que permite la realización de auditorías y seguridad de la información mediante test o pruebas de intrusión o más conocidos como *Pentesting*.

Para la realización de las pruebas se ha tomado como modelo a seguir las fases iniciales para los *test* de intrusión propuesto en el libro *Pentesting* con Kali, Pablo Gonzales Pérez, Germán Garcés y Jose Miguel Soriano de la Cámara, 2013. Y en la cual se especifican las siguientes fases:

- Reglas de juego: alcance y términos del test de intrusión.
- Recolección de información.
- Análisis de vulnerabilidades.
- Explotación de las vulnerabilidades.
- Postexplotación del sistema.
- Generación de informe.

A continuación, se describen las fases iniciales para la realización de las pruebas de detección de vulnerabilidades, amenazas y riesgos de la aplicación web.

9.1 FASE 1: REGLAS DE JUEGO: ALCANCE Y TÉRMINOS DE *TEST* DE INTRUSIÓN

El presente documento tiene un carácter única y exclusivamente académico, y se desarrolla como parte de los requisitos como proyecto de grado para el programa de la Especialización en Seguridad Informática de la Universidad Abierta y a Distancia – UNAD.

El objetivo principal de esta actividad se limita a determinar, mediante pruebas, usando herramientas como la distribución Kali Linux u otras herramientas, que en el siguiente seccionas se irán implementando que se consideren necesarias, en la detección de las vulnerabilidades, amenazas y riesgos de seguridad para el sistema de pedidos web de la empresa E.B. Software Ltda.

No está permitido el uso de este documento con fines malintencionados que busquen la afectación del sistema de pedidos web de la empresa E.B. Software Ltda., ni de cualquier otro sistema, por consiguiente, está totalmente prohibido su uso para tal fin.

9.2 FASE 2: RECOLECCIÓN DE INFORMACIÓN

Esta fase consiste en la recolección de toda de la información relacionada con el sistema de pedidos web, que permita detectar fallas de seguridad en el sistema y de esta forma determinar que herramientas se pueden implementar, y así realizar las pruebas de penetración requeridas.

Cuando no se tiene mucha información, una de las técnicas más populares es llevar a cabo la técnica conocida como google *haking*, la cual no es más que la simple búsqueda mediante este reconocido y útil motor de búsqueda.

Una búsqueda inicial se puede ver en la figura 2. El primer resultado de la búsqueda arroja la URL de la ubicación del sistema de pedidos web, mediante esta URL se dará inicio al proceso de recolección de información a nivel más

Figura 2. Búsqueda inicial del sistema de pedidos web mediante el buscador de Google

Fuente: El autor.

Descripción Figura 2:

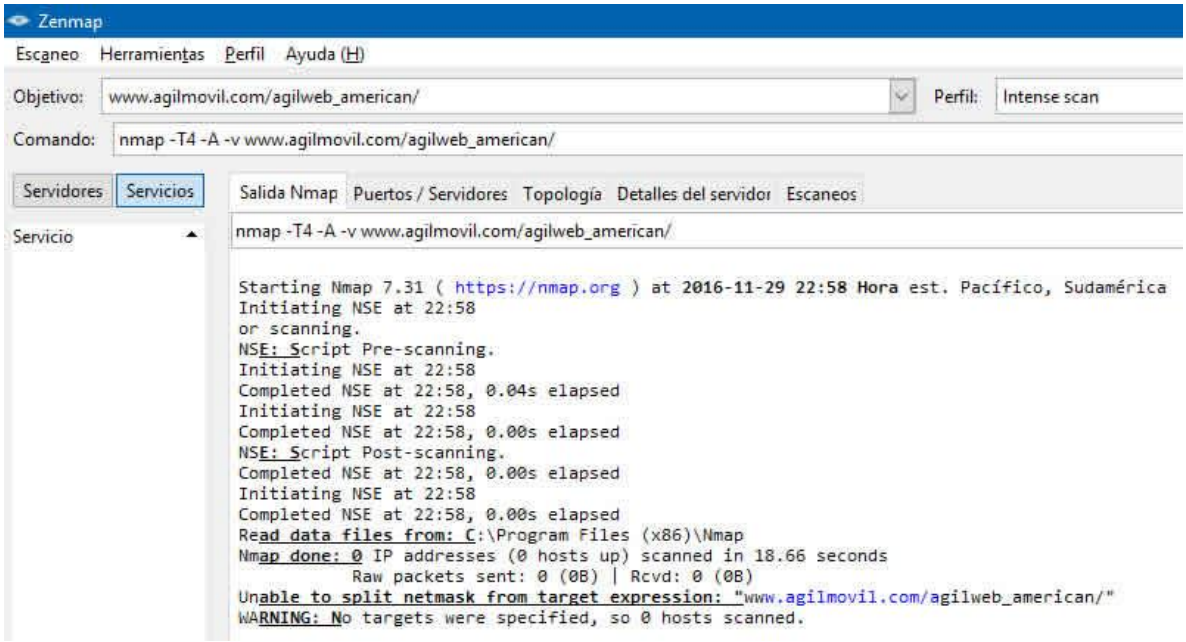
Búsqueda mediante el buscador Google:
Palabras a buscar: agilmovil.com pedidos web

Resultados Figura 2:

El motor de búsqueda genera el resultado de la URL de la aplicación de pedidos web

9.2.1 Recolección de información mediante Nmap. En la figura 3, se puede ver la ejecución del programa Nmap.

Figura 3. Recolección de información Nmap



Fuente: El autor.

Descripción Figura 3:

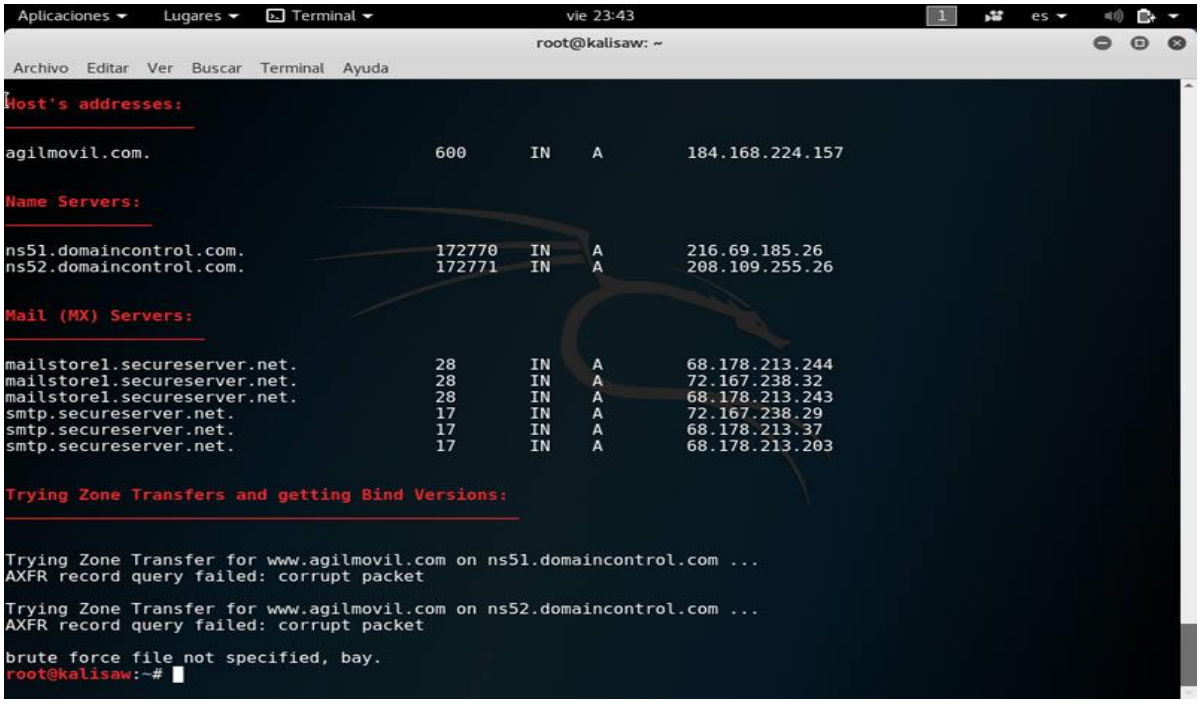
Ejecución de la aplicación nmap con el comando:
Nmap -T4 -VA -v www.agilmovil.com

Resultados Figura 3:

El resultado no arroja información relevante.

9.2.2 Trasferencia de zona. Este proceso puede realizar mediante la aplicación dnsenum, en la Figura 4, se puede ver el resultado de la ejecución del comando.

Figura 4. Recolección de información mediante dnsenum



Fuente: El autor.

Descripción Figura 4:

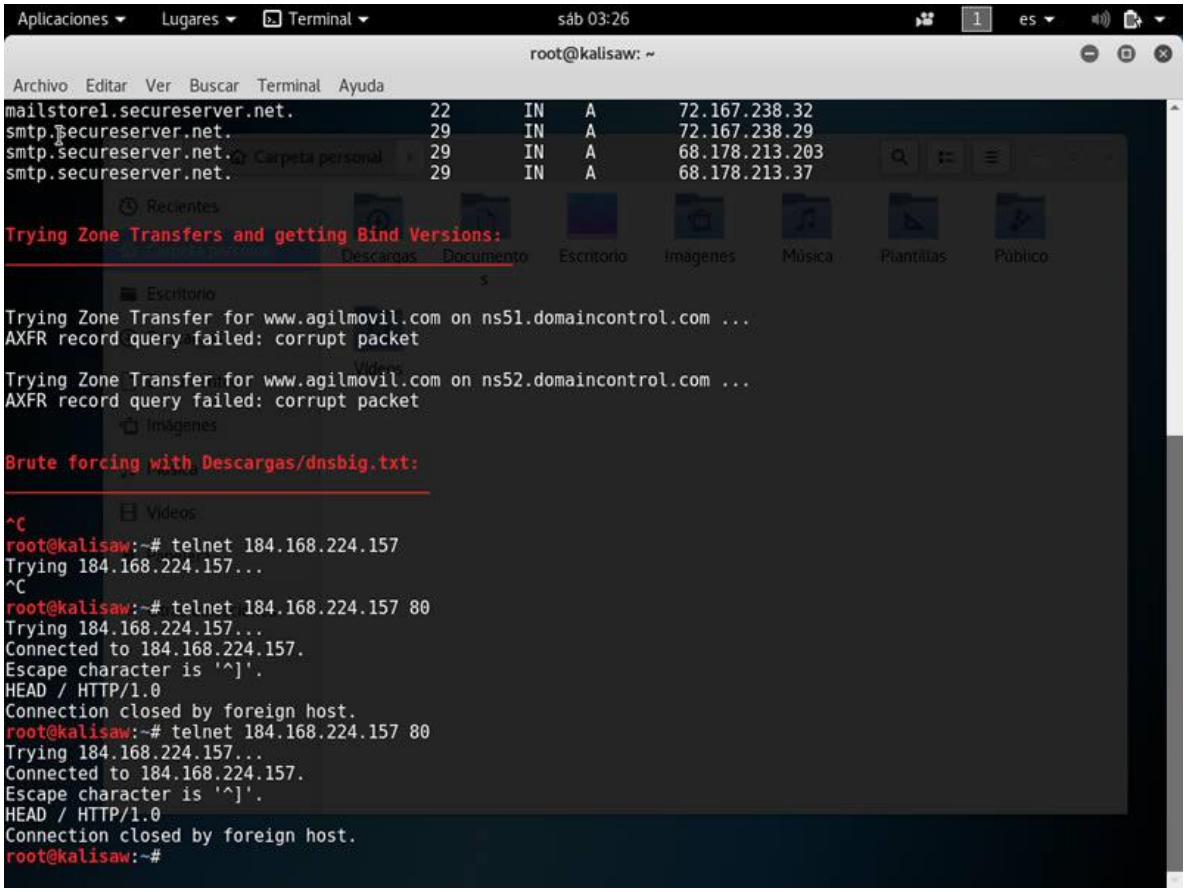
Ejecución de la aplicación dnsenum mediante el comando:
Perl dnsenum.pl --dnsserver www.agilmovil.com

Resultados Figura 4:

Se obtiene que el dominio agilmovil.com direcciona a la IP 184.168.224.157 y sus respectivos servidores DNS.

9.2.3 Fingerprinting web - Banner Grabbing. Una de las estrategias y más sencillas utilizadas es el uso de comando Telnet, La Figura 5, muestra la ejecución de dicho comando.

Figura 5. Recolección de información mediante telnet



Fuente: El autor.

Descripción Figura 5:

Ejecución de comando telnet:
telnet 184.168.224.157

Resultados Figura 5:

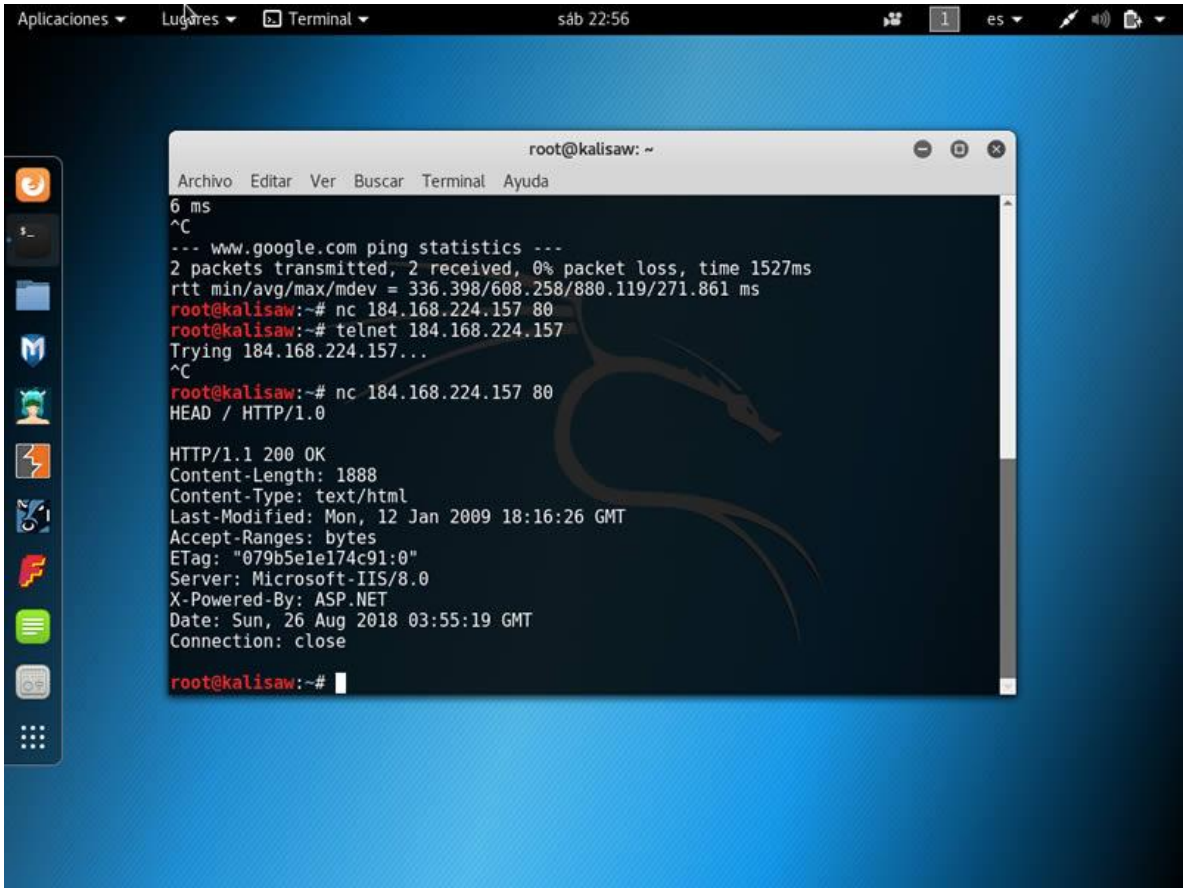
No se obtiene cabeceras de información del tipo de servidor.

Otra de las herramientas utilizadas en Netcat, la cual permite el envío de un mensaje sin contenido al servidor para conseguir información de servicios en cada puerto especifico, la Figura 6, muestra la ejecución de este comando.

Se pueden detectar los siguientes servicios:

- Finger, protocolo para obtener usuarios de una máquina
- Gopher, servicio que permite el acceso a información mediante menus
- Bootpc, Cliente bootstrap (BOOTP); también usado por el protocolo de configuración dinámica de host (DHCP)
- Bootps, Servicios del Protocolo Bootstrap o de inicio (BOOTP); también usado por los servicios del protocolo de configuración dinámica de host (DHCP).
- Tacacs-ds, es un protocolo cliente/servidor que proporciona la Seguridad centralizada para los usuarios que intentan tener el Acceso de administración a un router o a un servidor de acceso a la red
- domain Servicios de nombres de dominio
- re-mail-ck, Protocolo de verificación de correo remoto
- Whois
- Nameserver, Servicio de nombres de Internet
- time Protocolo de hora (Time Protocol)
- smtp Protocolo simple de transferencia de correo (SMTP)
- terlent
- ssh, Servicio de shell seguro (SSH)
- ftp, Puerto del Protocolo de transferencia de archivos (FTP); algunas veces utilizado por el Protocolo de servicio de archivos (FSP).

Figura 6. Información del servidor que aloja la aplicación web mediante netcat



Fuente: El autor.

Descripción Figura 6:

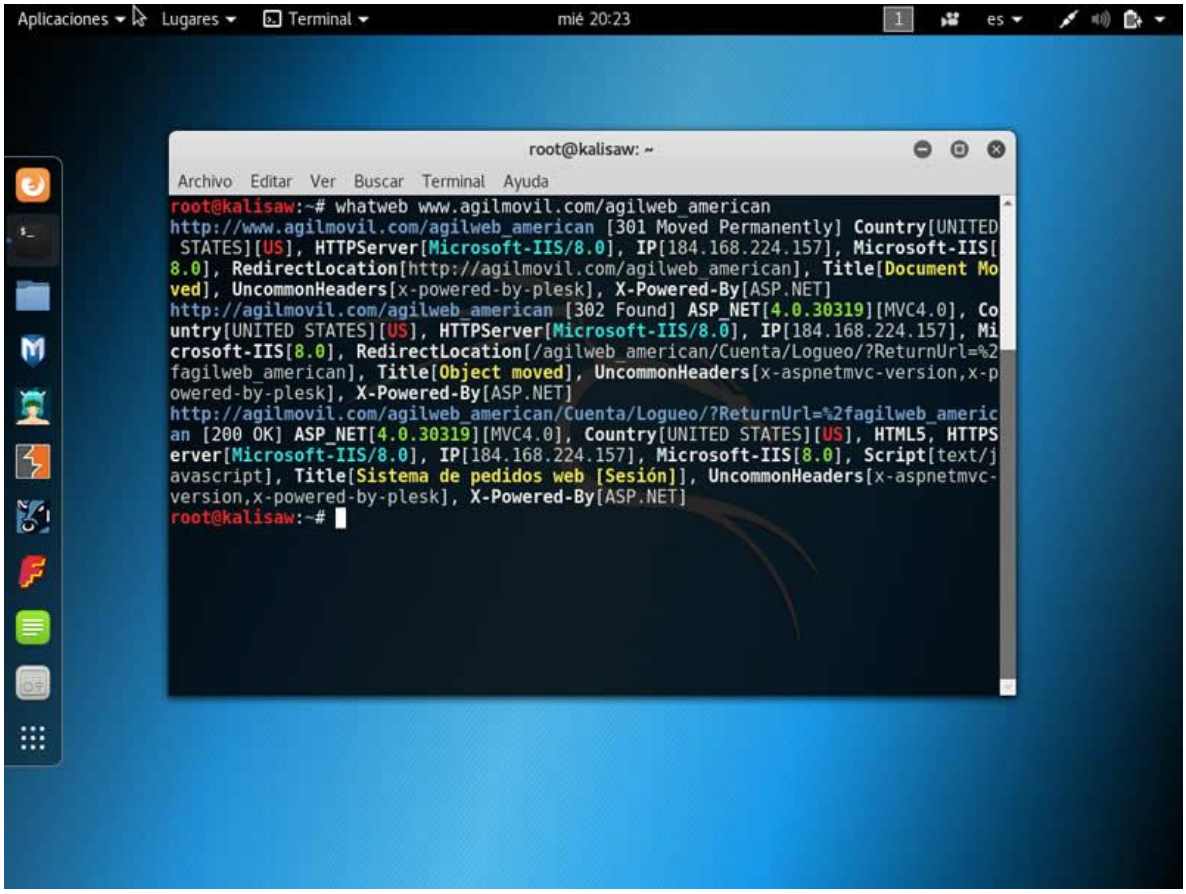
Ejecución de la aplicación netcat con el comando:
nc 184.168.224.157 80

Resultados Figura 6:

Se obtiene cabeceras de información del tipo de servidor Microsft-IIS/8.0.

9.2.4 WhatWeb. Desde una consola de comando se inició la aplicación WhatWeb, y desde esta se pudo recuperar información sensible, como lo muestran las figuras 7 a 13.

Figura 7. Información del sistema de pedidos web mediante WhatWeb



Fuente: El autor.

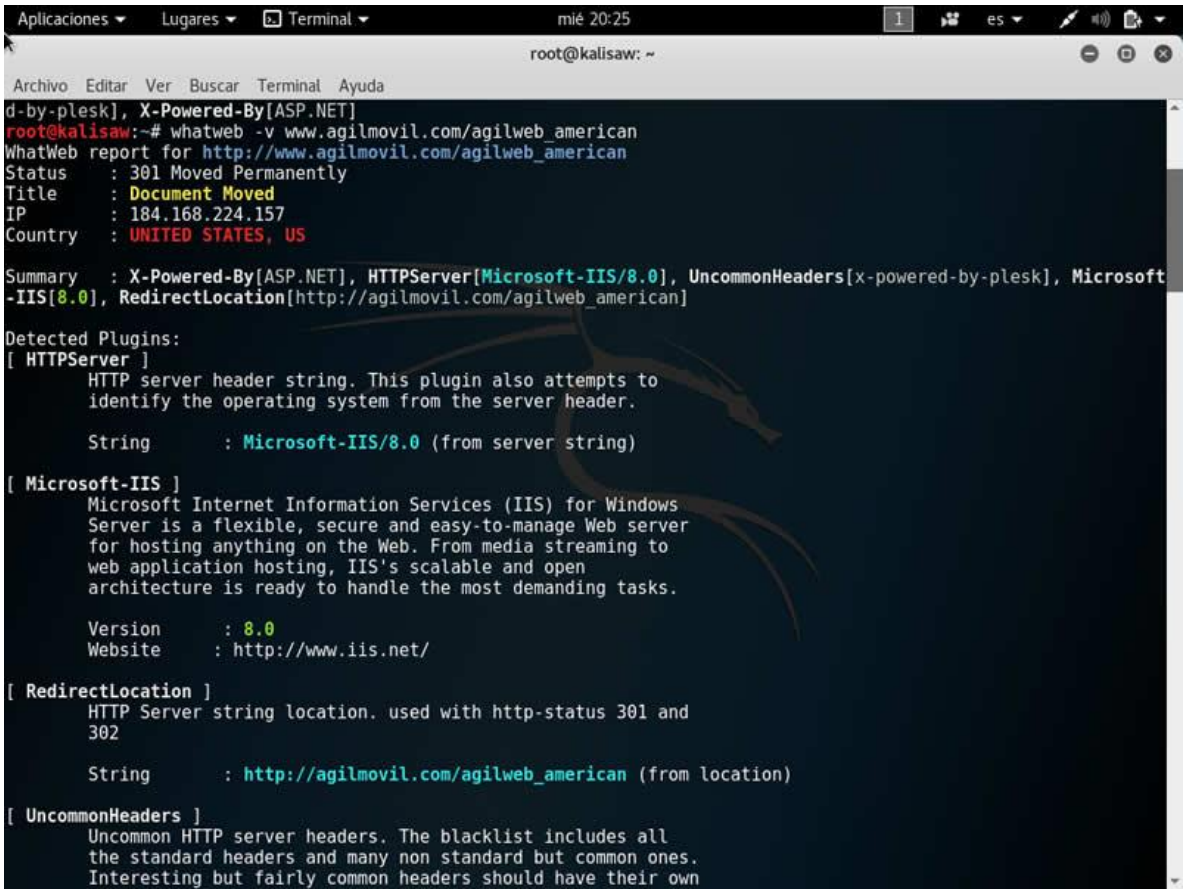
Descripción Figura 7:

Se ejecuta el comando:
WhatWeb www.agilmovil.com/agilweb_american

Resultados Figura 7:

Se identifica la IP del servidor: 184.168.224.157, así como el tipo de servidor: Microsoft IIS 8.0, la versión de ASP: 4.0.30319 y la versión de MVC. .Net: 4.0

Figura 8. Identificación de información del aplicativo web - 1



Fuente: el autor.

Descripción Figura 8:

Se ejecuta el comando:

WhatWeb -v www.agilmovil.com/agilweb_american

Resultados Figura 8:

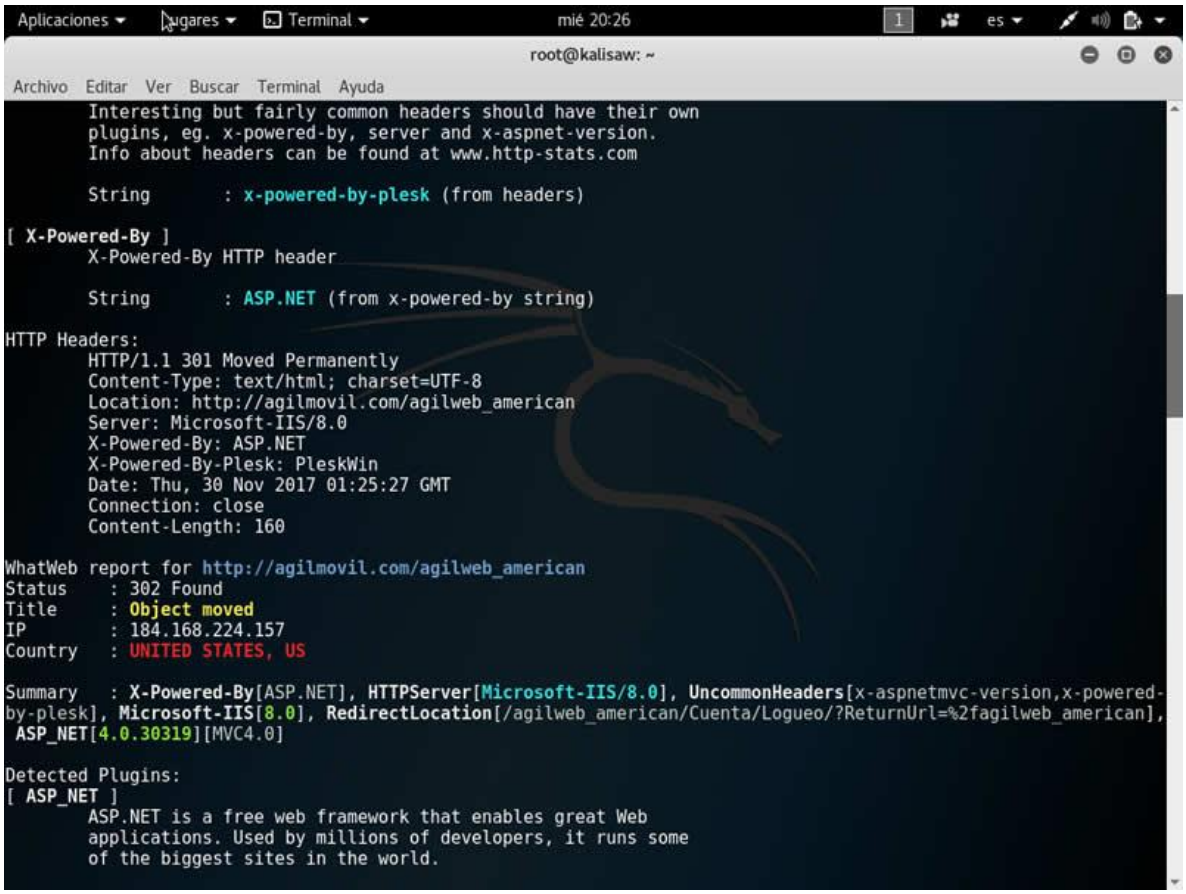
El servidor da como código de respuesta HTTP: 301 *Moved Permanently*, dado que estos estados del tipo 3xx, se refieren a redirecciones, significa que el navegador o el software debe ejecutar una consecuente acción para que la solicitud sea completada, para el estado 301 la solicitud actual y las nuevas solicitudes realizadas se deben dirigir al URI dada.

Se obtiene la dirección IP: 184.168.224.157

País: Estados unidos

En el resumen se muestra que la versión del servidor es IIS 8.0 de Microsoft

Figura 9. Identificación de información del aplicativo web - 2



Fuente: el autor.

Descripción Figura 9:

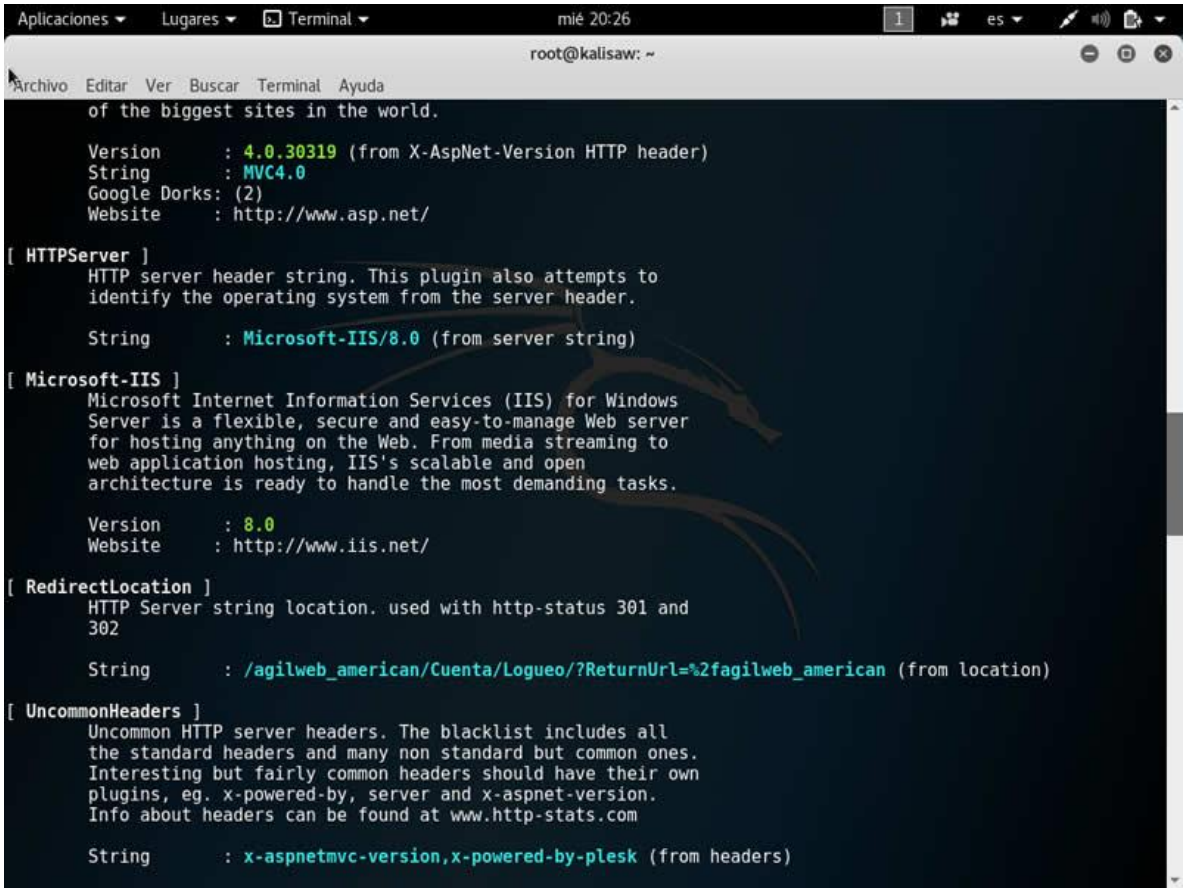
Se ejecuta el comando (continuación Fig. 7.):
WhatWeb -v www.agilmovil.com/agilweb_american

Resultados Figura 9:

Se detecta que el servidor usa el panel de control Plesk herramienta que permite la administración del servidor, tanto la gestión de archivos, las cuentas de correo y las bases de datos.

Se muestra la respuesta de la cabecera HTTP así como la versión de MVC utilizada para ASP_NET, la 4.0.

Figura 10. Identificación de información del aplicativo web - 3



Fuente: el autor.

Descripción Figura 10:

Se ejecuta el comando (continuación Fig. 7.):

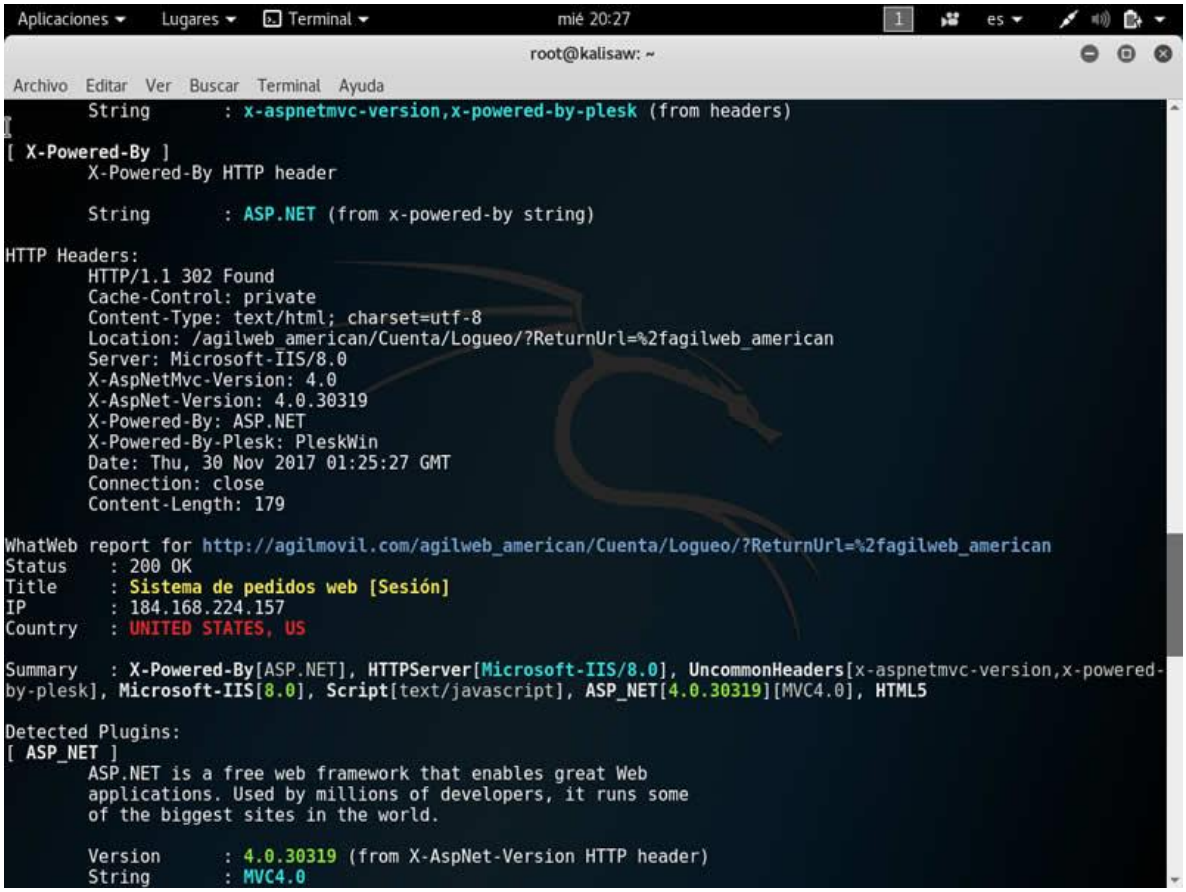
WhatWeb -v www.agilmovil.com/agilweb_american

Resultados Figura 10:

Se muestra en detalle la versión MVC 4.0.30319 así como la versión del ISS 8.0

También se muestra la URI de redirección /agilweb_american/Cuenta/Logueo….

Figura 11. Identificación de información del aplicativo web - 4



Fuente: el autor.

Descripción Figura 11:

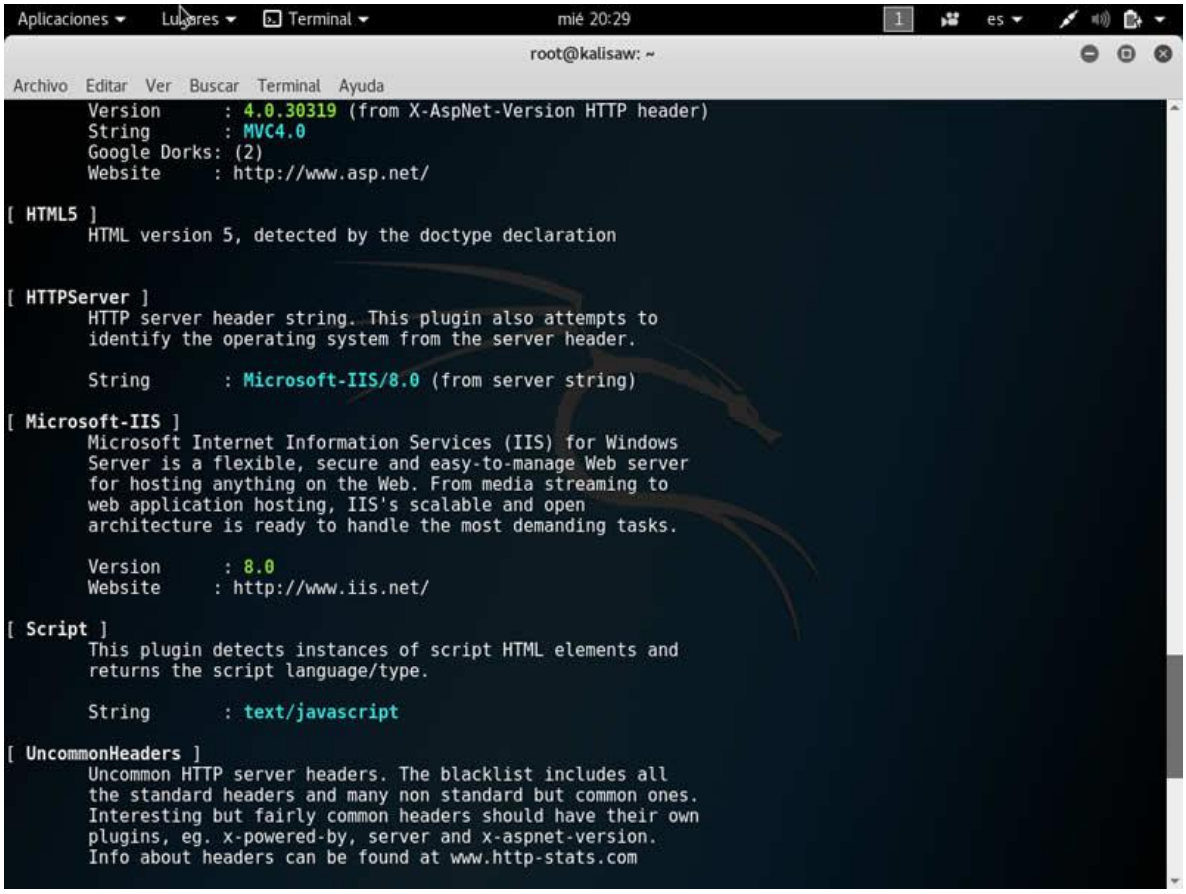
Se ejecuta el comando (continuación Fig. 7.):
WhatWeb -v www.agilmovil.com/agilweb_american

Resultados Figura 11:

Se muestra la respuesta de cabecera HTTP, así como el código de respuesta 200 correspondiente a una petición correcta, en la que se identifica el título de la aplicación web: “Sistema de pedidos web [Sesión]”, la IP: 184.165.244.157 y el País Estados Unidos

En resumen, se identifica la aplicación se está ejecutando en servidor con ISS 8.0, desarrollada en MVC 4.0, con JavaScript y HTML5

Figura 12. Identificación de información del aplicativo web - 5



Fuente: el autor.

Descripción Figura 12:

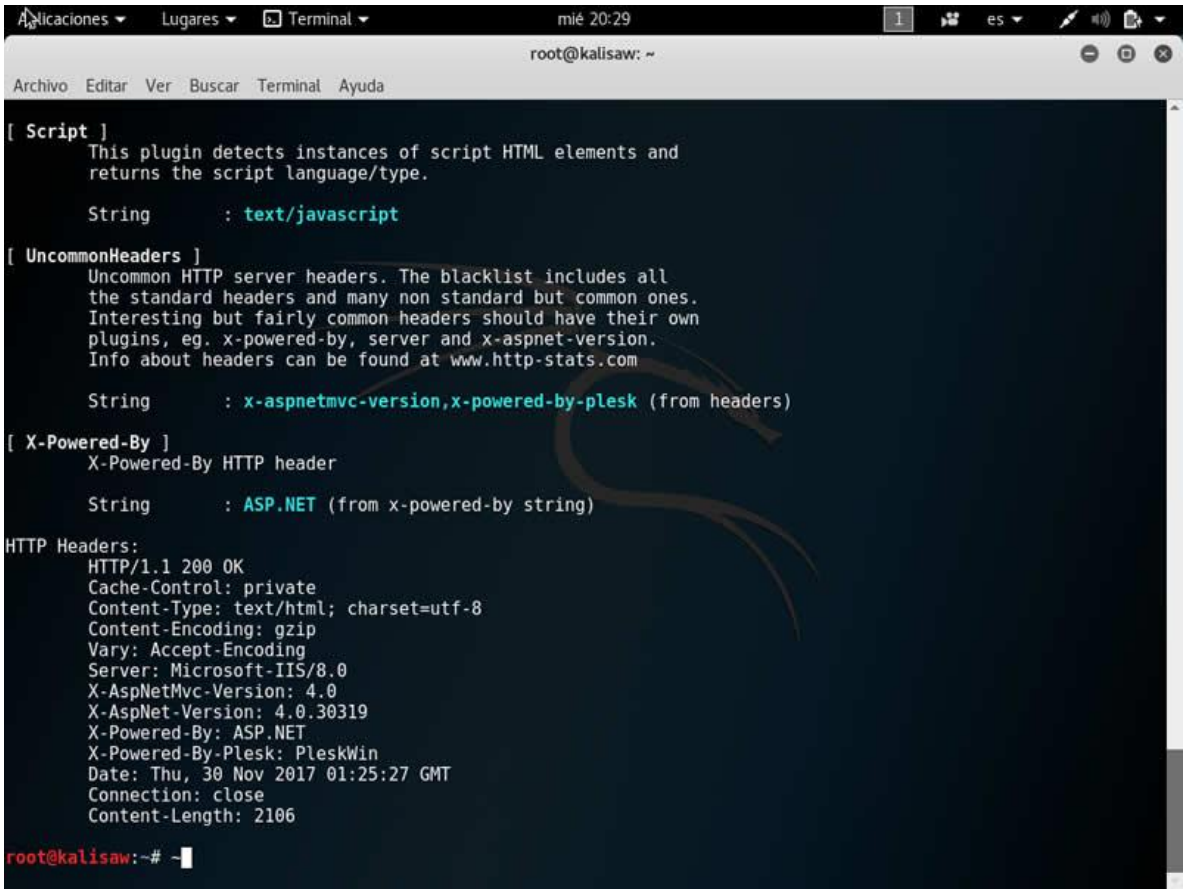
Se ejecuta el comando (continuación Fig. 7.):

WhatWeb -v www.agilmovil.com/agilweb_american

Resultados Figura 12:

Se muestra en detalle la versión de MVC 4.0.30319 y que se han implementados 2 combinaciones de operadores de búsqueda denominados Google dorks, que el servidor es IIS 8.0 y se ha identificado que implementa el lenguaje Javascript.

Figura 13. Identificación de información del aplicativo web - 6



Fuente: el autor.

Descripción Figura 13:

Se ejecuta el comando (final resultado Fig. 7.):
WhatWeb -v www.agilmovil.com/agilweb_american

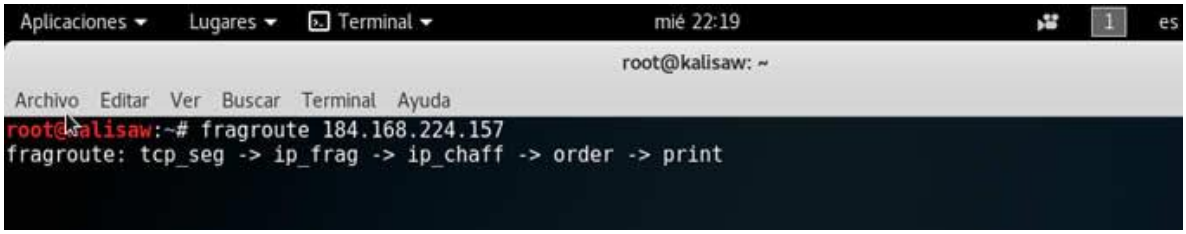
Resultados Figura 13:

Se identifica que el servidor usa el panel de control Plesk, identificado anteriormente, que la aplicación está desarrollada bajo ASP.NET de Microsoft, y se muestra la respuesta del servidor en la cabecera HTTP.

9.3 FASE 3: EXPLOTACIÓN DE LAS VULNERABILIDADES

9.3.1 IDS/IPS - Fragroute. La Figura 14 muestra la ejecución de la aplicación fragroute desde la consola de comando de Kali Linux para evadir los IDS/IPS posibles.

Figura 14. Fragroute al sistema de pedidos web



Fuente: el autor

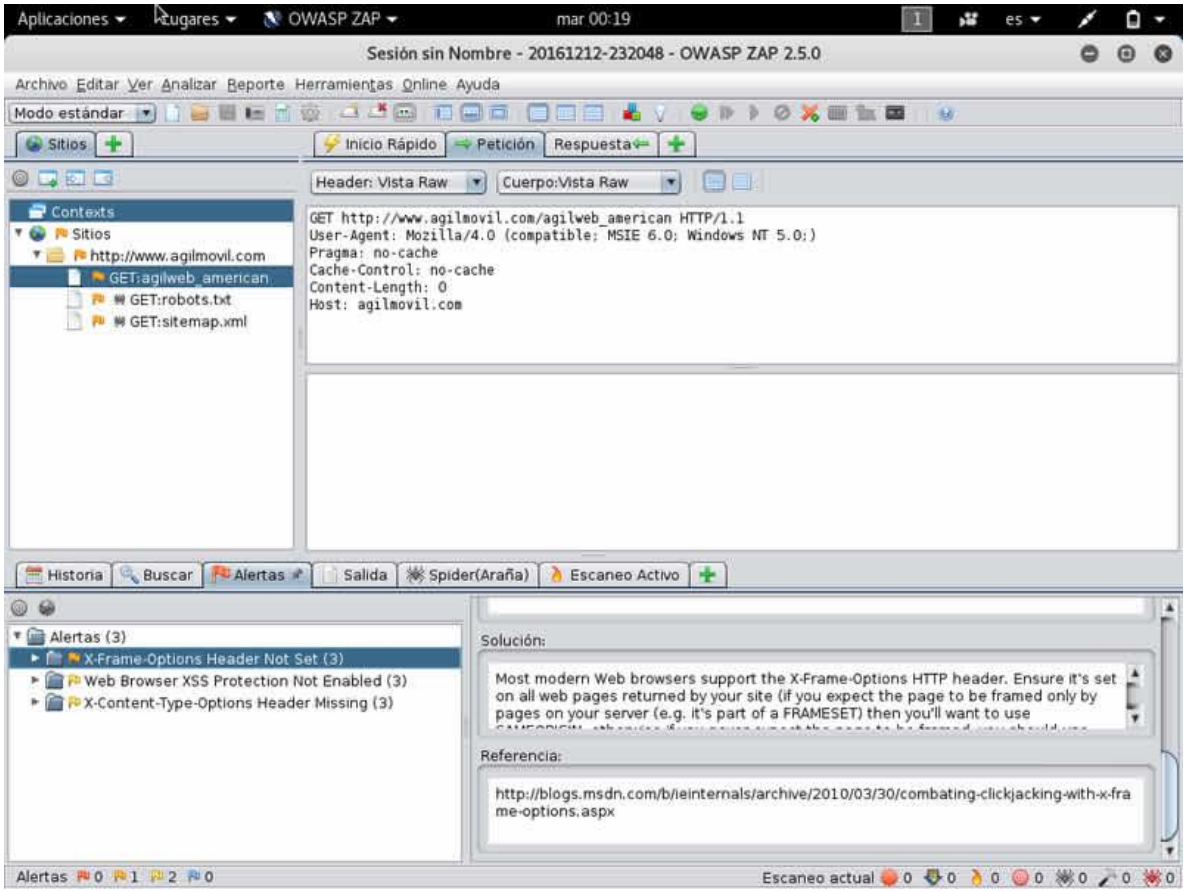
Descripción Figura 14:

Se ejecuta el comando:
fragroute 184.168.224.157

Resultados Figura 14:
El proceso demora en ejecución y no arroja información.

9.3.2 *Pentesting* mediante OWASP ZAP. La Figura 15, muestra la ejecución de la aplicación OWASP ZAP desde el entorno de sistema operativo Kali Linux

Figura 15. Ejecución de *pentesting* mediante OWASP ZAP



Fuente: el autor.

Descripción Figura 14:

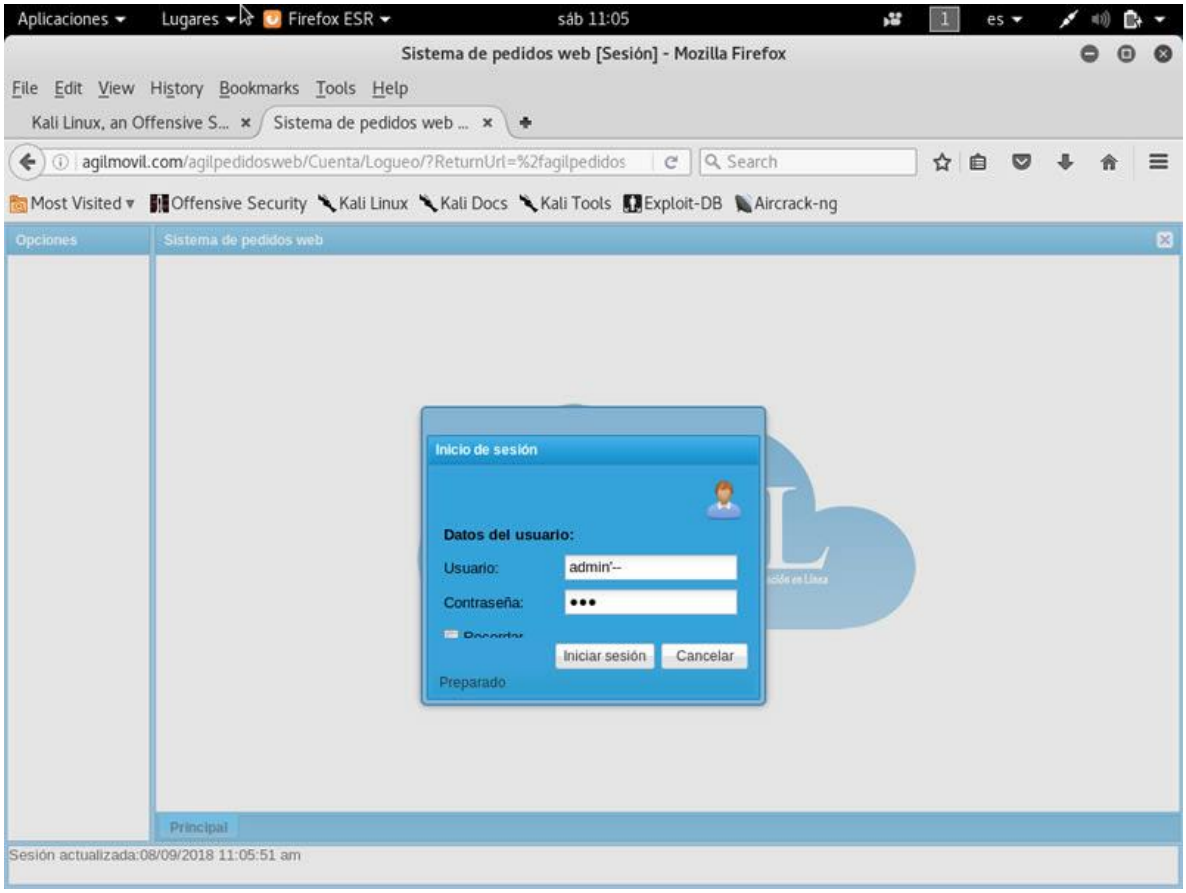
Se ejecuta aplicación OWAS ZAP

Resultados Figura 14:

Se retorna información de parámetros no establecidos para mejorar la seguridad de la aplicación web.

9.3.3 SQL *Injection*. En las Figuras 16 a 30, se muestra intentos de inyección SQL mediante el formulario de loguin de usuarios.

Figura 16. SQL *Injection* – 1



Fuente: el autor.

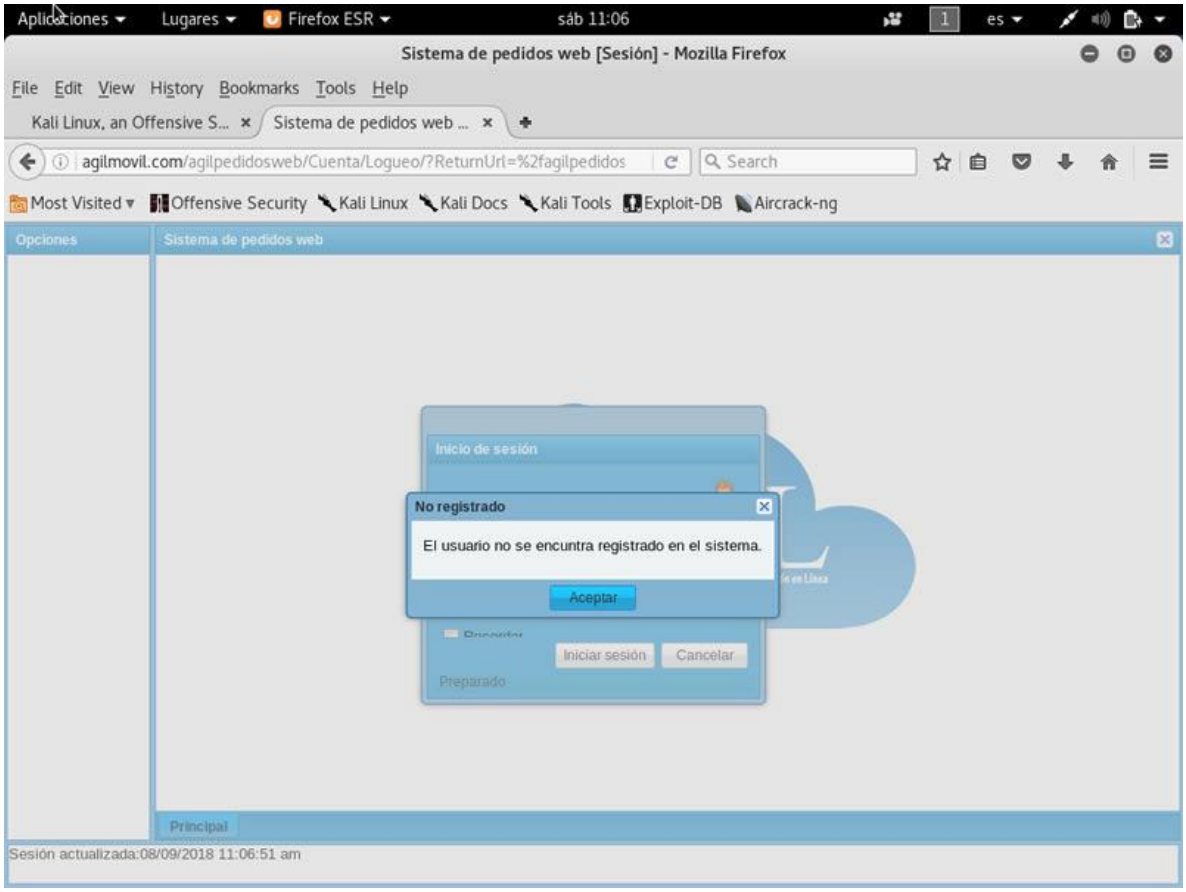
Descripción Figura 16:

Inyección admin’ --

Resultados Figura 16:

Se ingresa el tipo de inyección con el objetivo de evadir la contraseña.

Figura 17. SQL *Injection* – 2



Fuente: el autor.

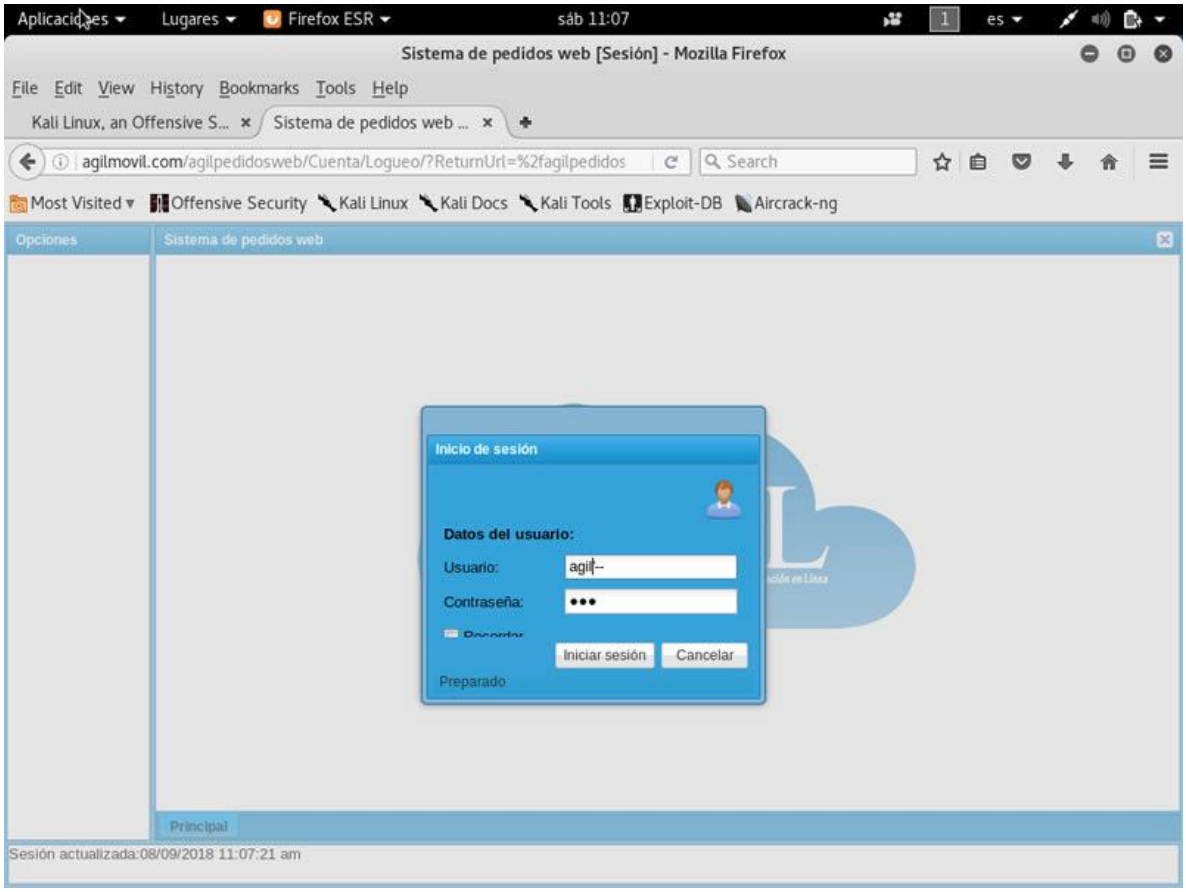
Descripción Figura 17:

Inyección admin’ --

Resultados Figura 17:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado.

Figura 18. SQL *Injection* – 3



Fuente: el autor.

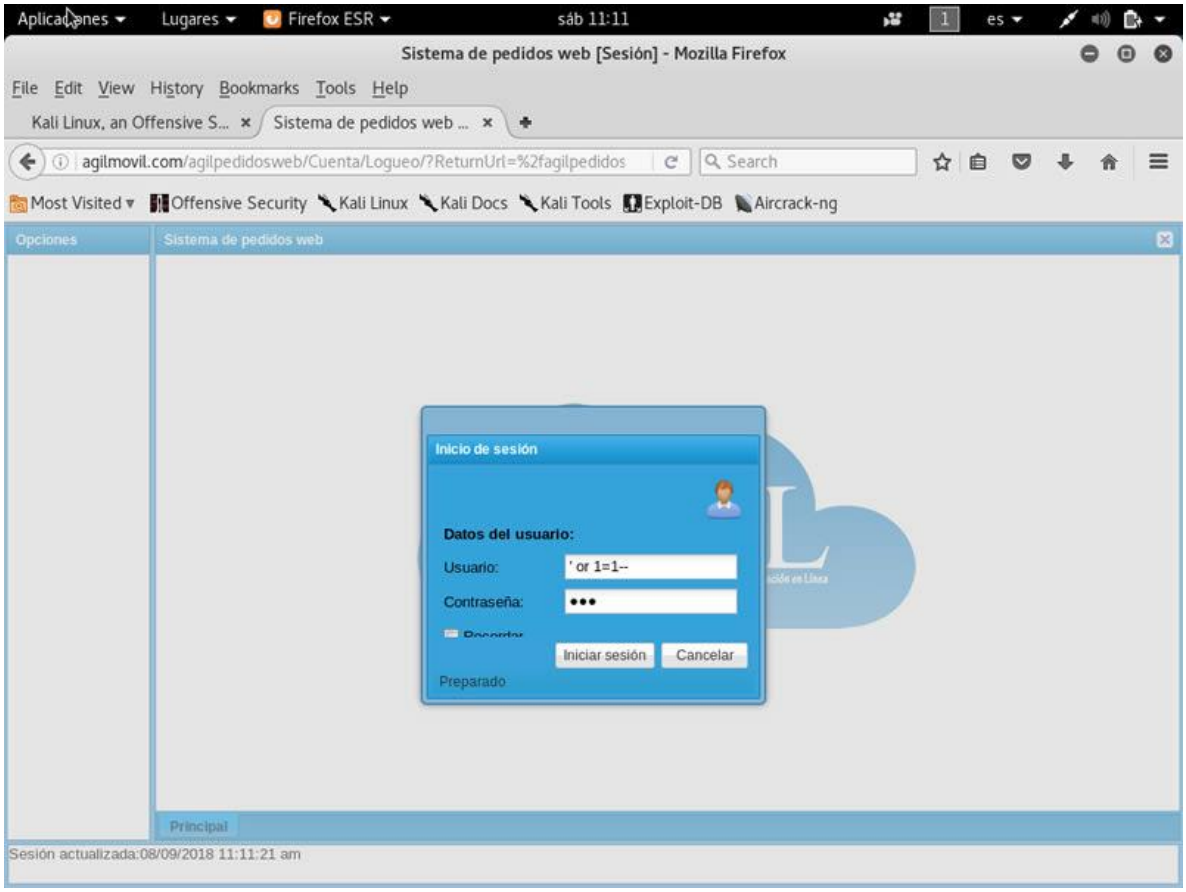
Descripción Figura 18:

Inyección agil’ --

Resultados Figura 18:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 19. SQL *Injection* – 4



Fuente: el autor.

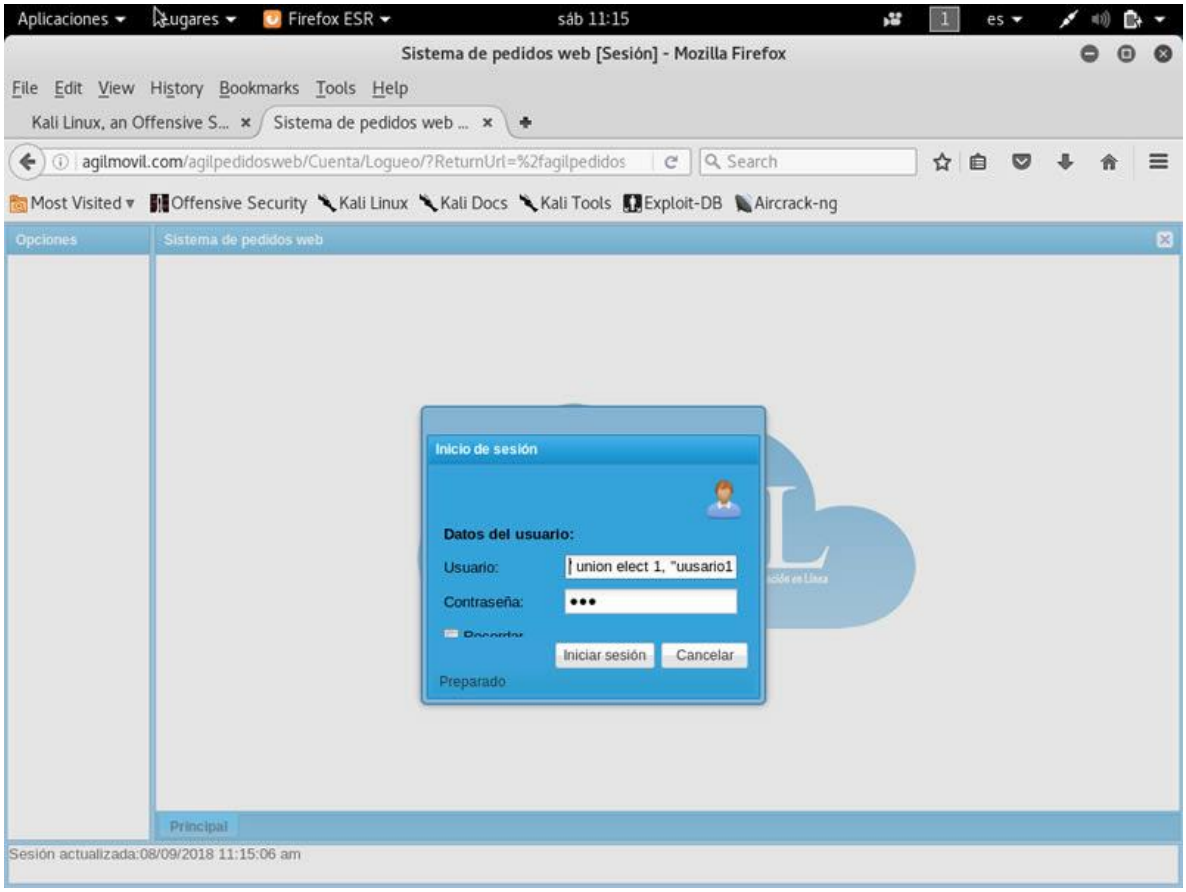
Descripción Figura 19:

Inyección ‘ or 1=1--

Resultados Figura 19:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 20. SQL *Injection* – 5



Fuente: el autor.

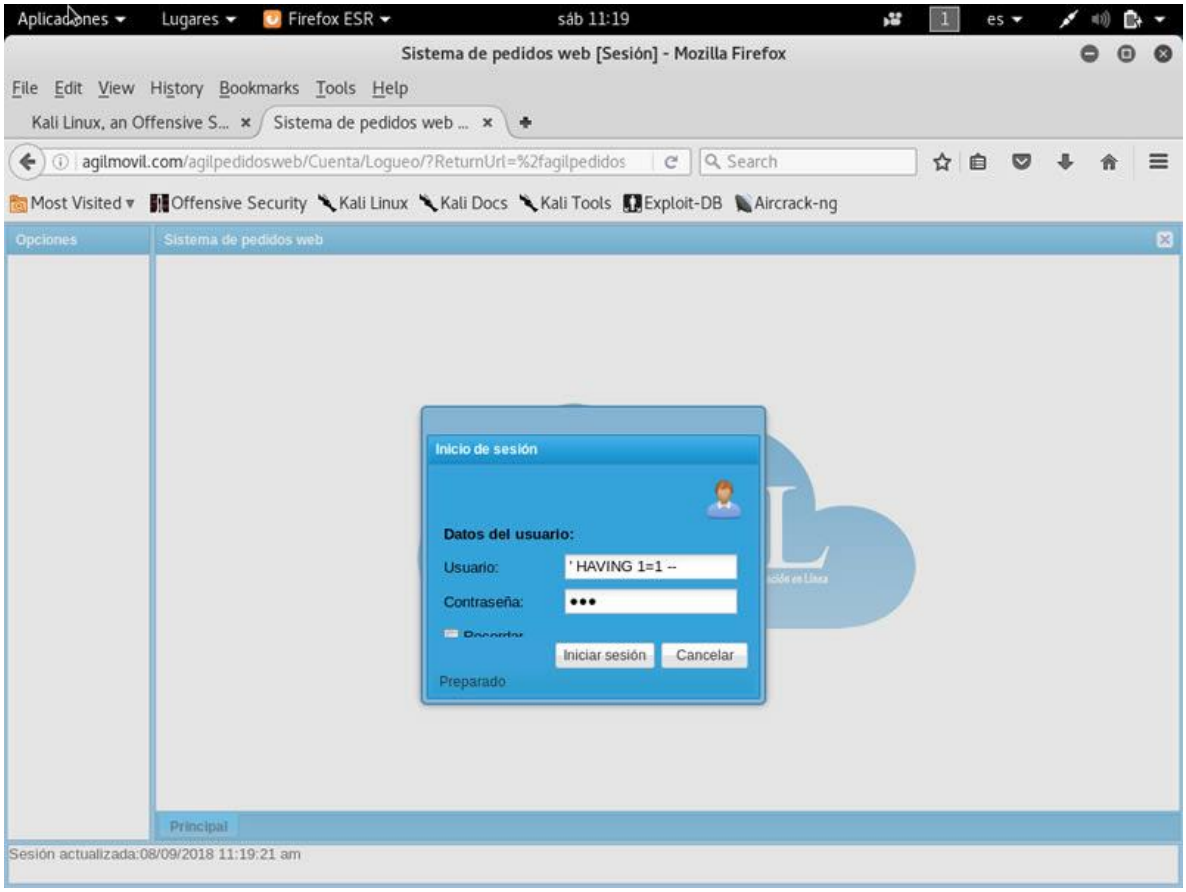
Descripción Figura 20:

Inyección ‘ unión select 1,”usuario1”,”clave1”, 1--

Resultados Figura 20:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 21. SQL *Injection* – 6



Fuente: el autor.

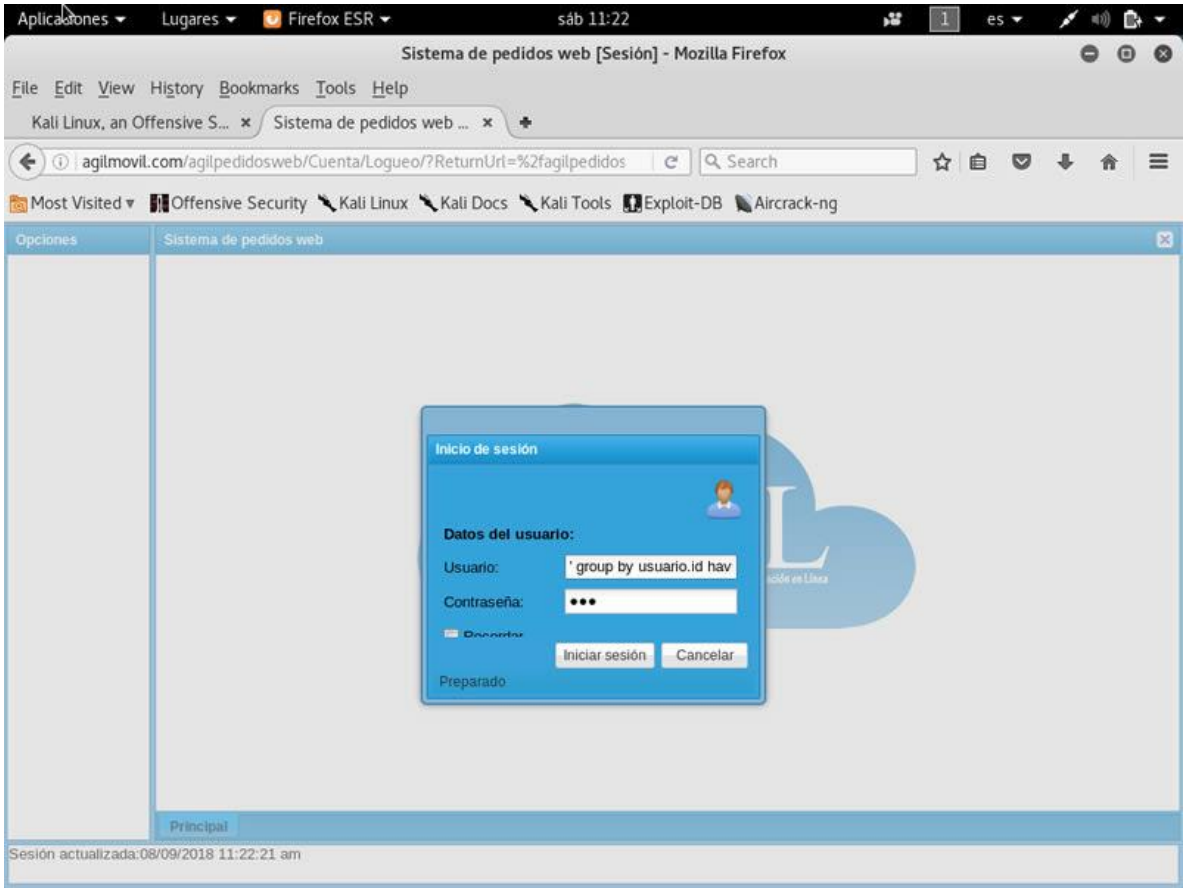
Descripción Figura 21:

Inyección ‘ HAVING 1=1 --

Resultados Figura 21:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 22. SQL *Injection* – 7



Fuente: el autor.

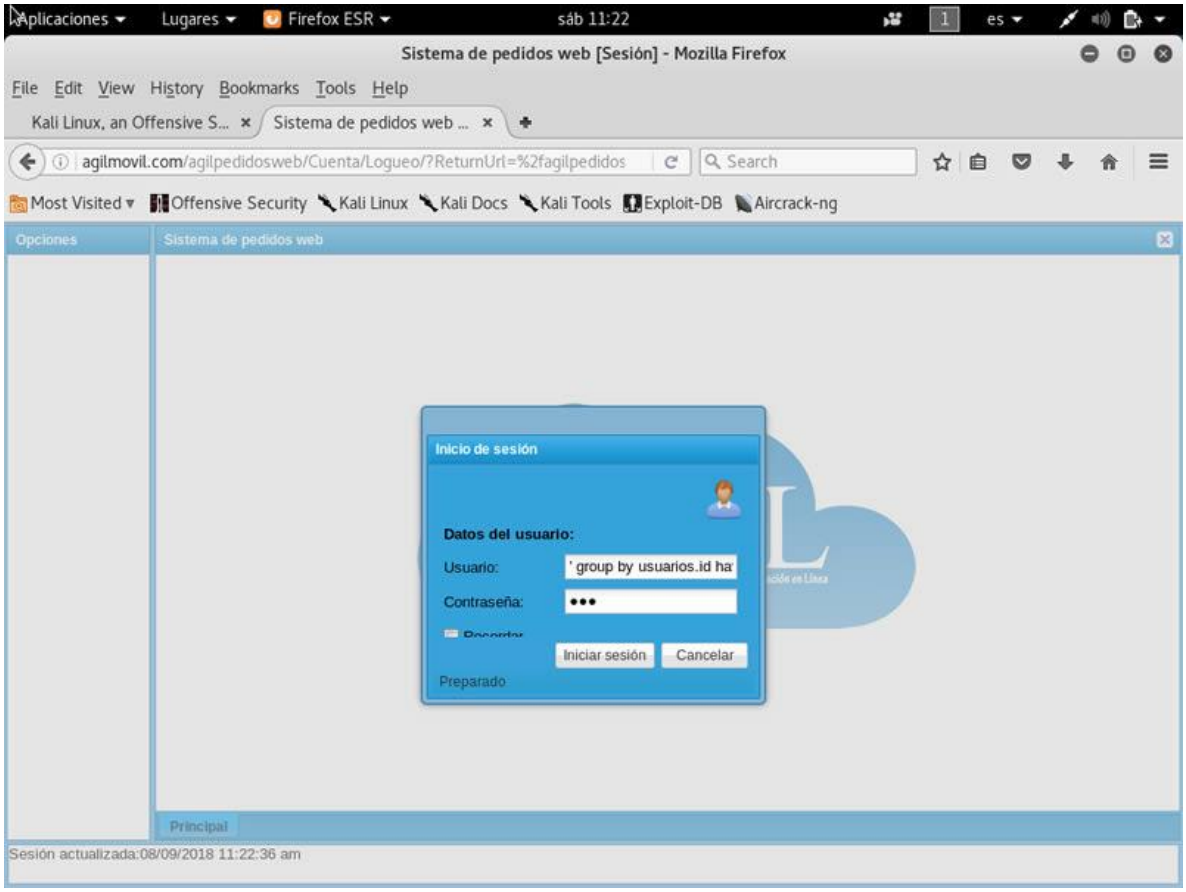
Descripción Figura 22:

Inyección ‘ group by usuario.id, usuario.nombre having 1=1 --

Resultados Figura 22:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 23. SQL *Injection* – 8



Fuente: el autor.

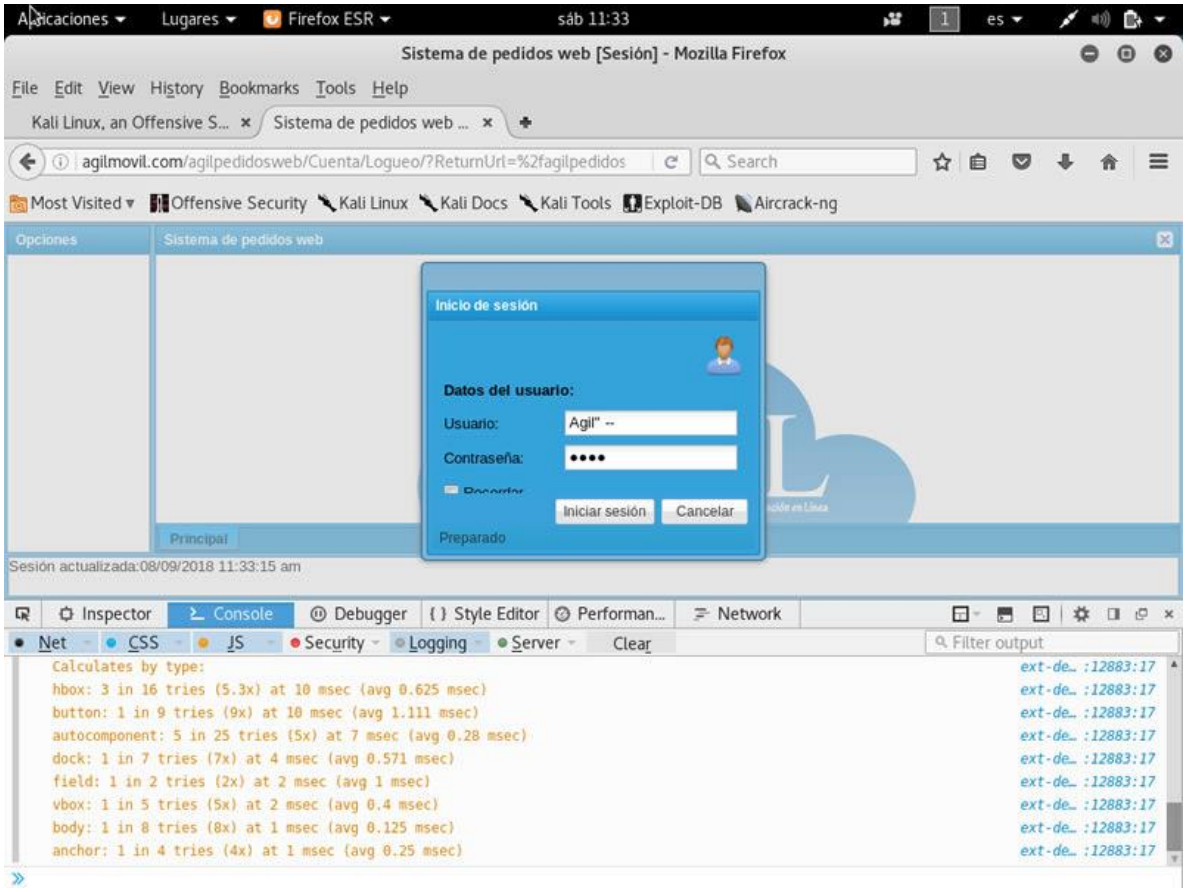
Descripción Figura 23:

Inyección ‘ group by usuario.id, usuario.nombre, usuario.clave having 1=1 --

Resultados Figura 23:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 24. SQL *Injection* – 9



Fuente: el autor.

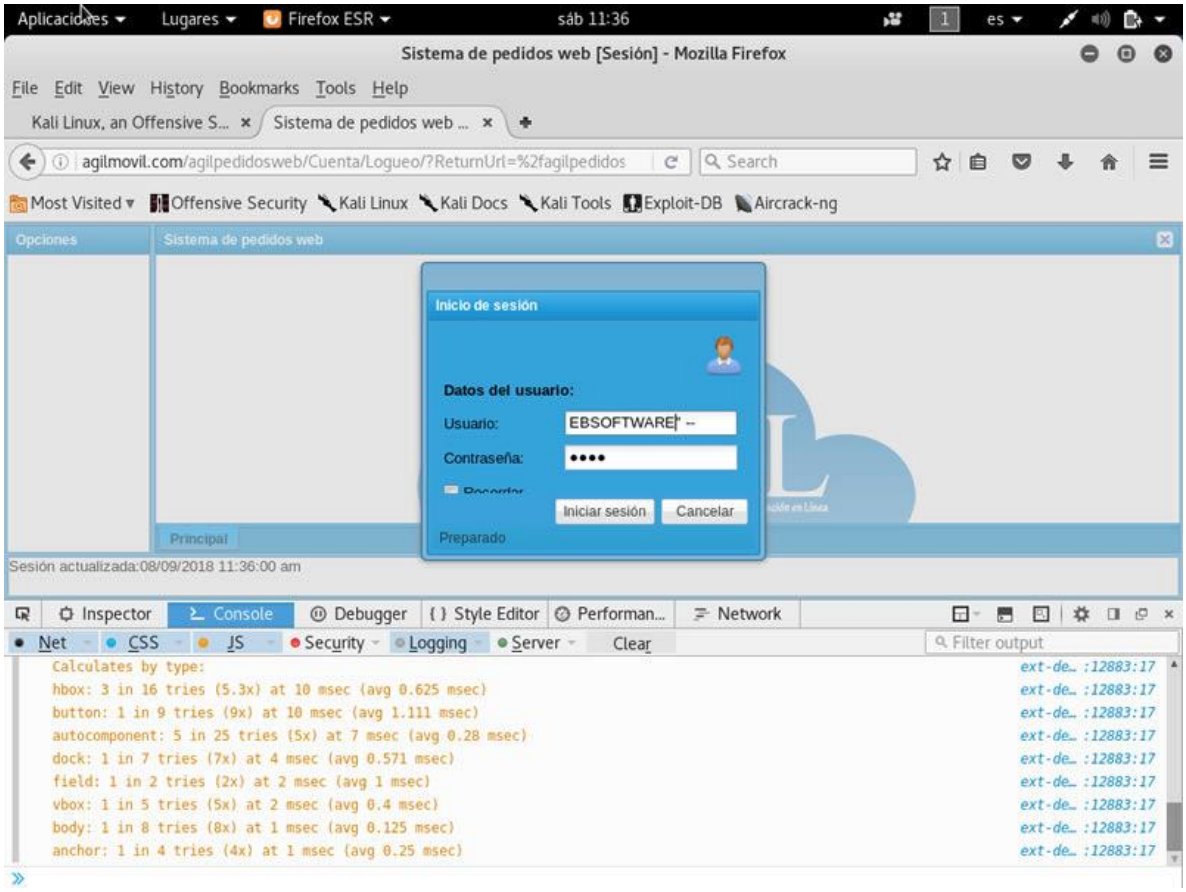
Descripción Figura 24:

Inyección Agil” --

Resultados Figura 24:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 25. SQL *Injection* – 10



Fuente: el autor.

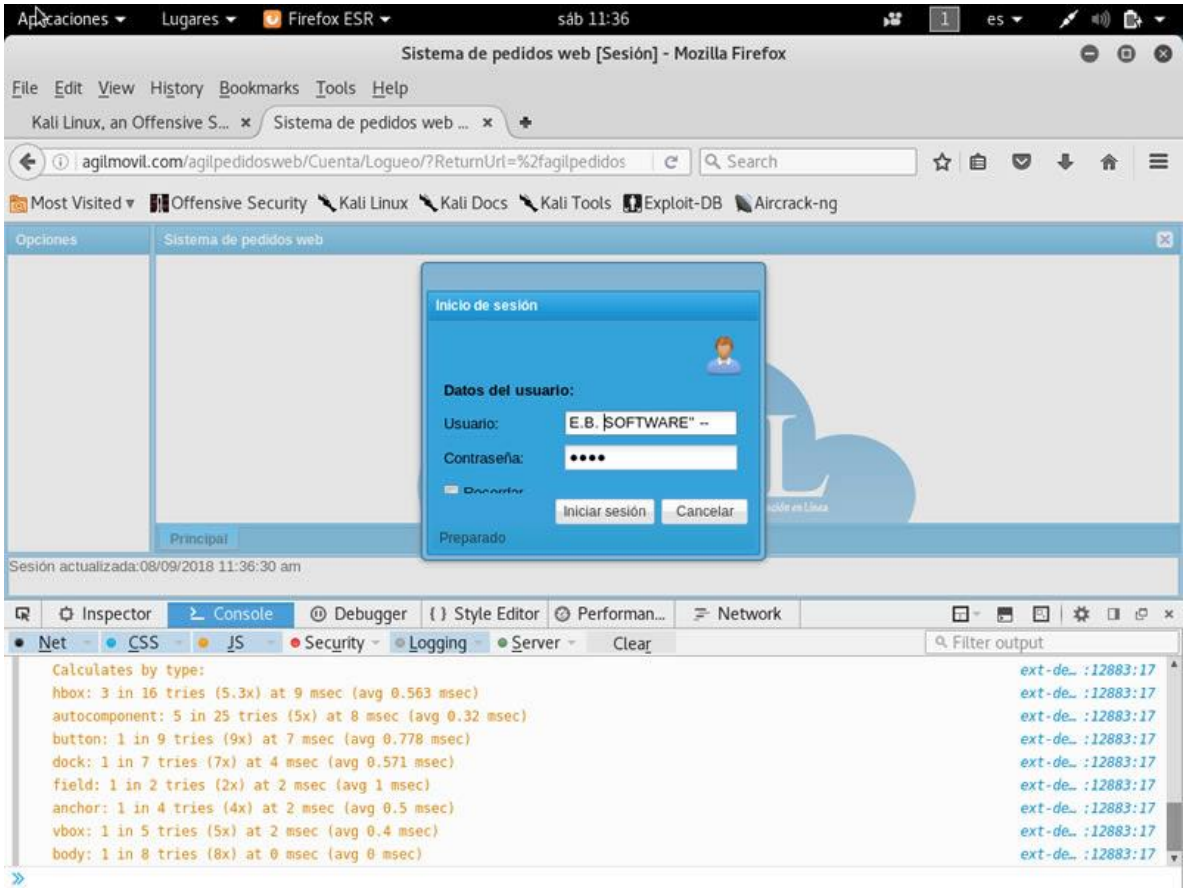
Descripción Figura 25:

Inyección EBSOFTWARE” --

Resultados Figura 25:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 26. SQL *Injection* – 11



Fuente: el autor.

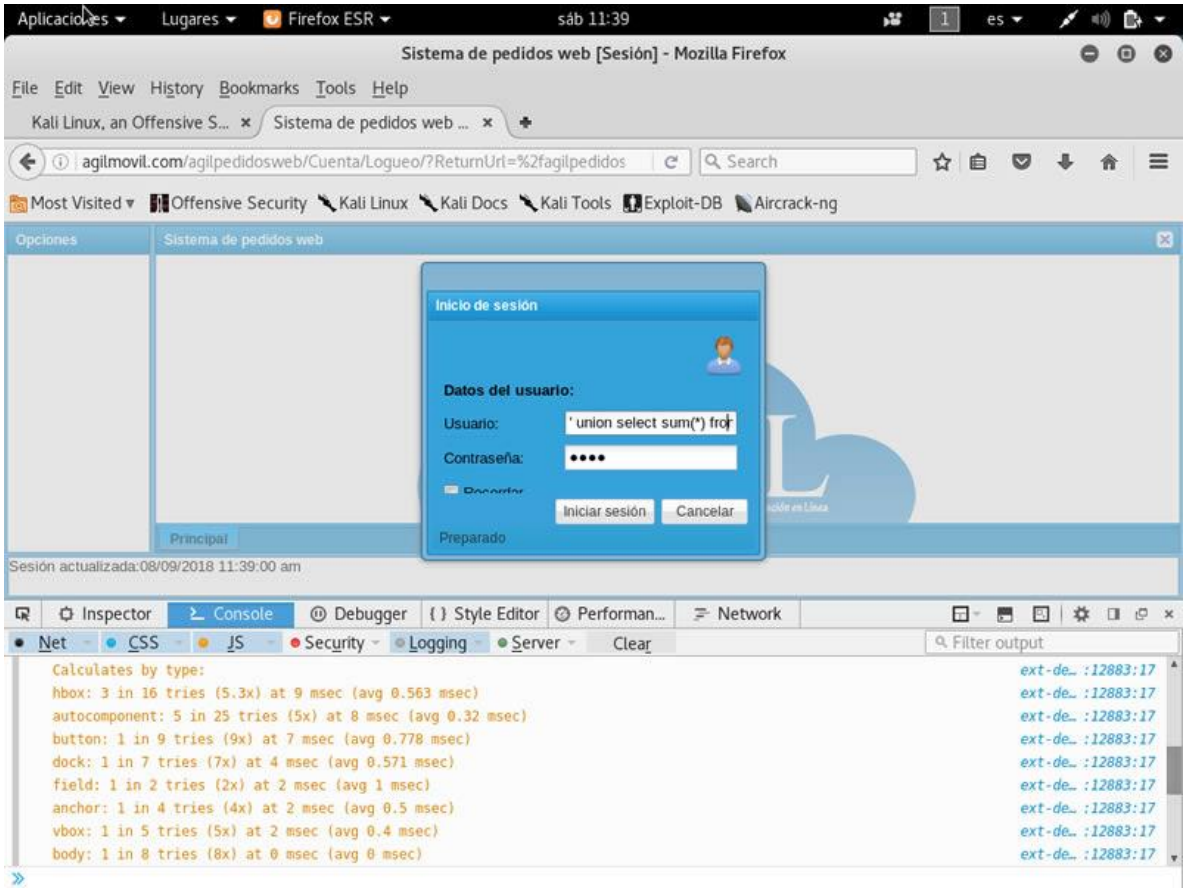
Descripción Figura 26:

Inyección E.B. SOFTWARE" --

Resultados Figura 26:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 27. SQL *Injection* – 12



Fuente: el autor.

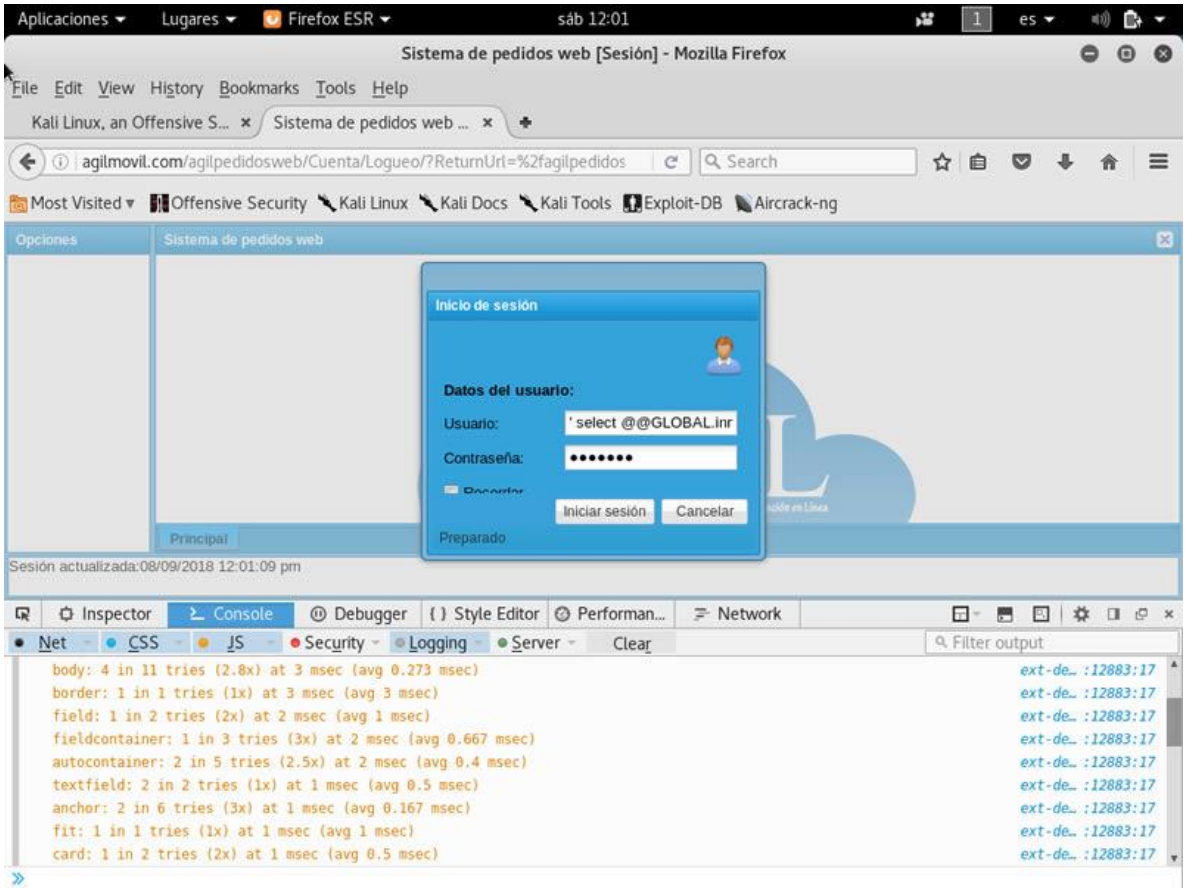
Descripción Figura 27:

Inyección ‘union select sum(*) from users

Resultados Figura 27:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 28. SQL *Injection* – 13



Fuente: el autor.

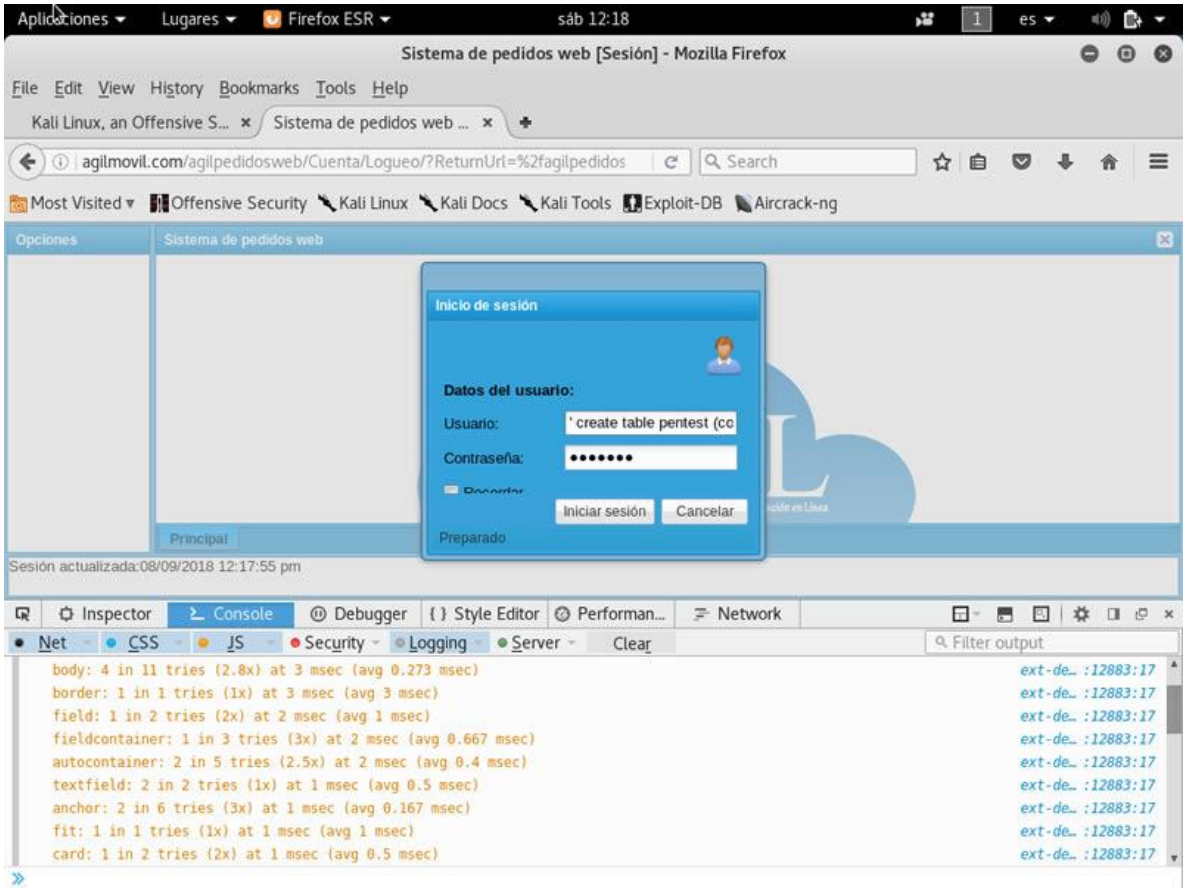
Descripción Figura 28:

Inyección ‘ select @@GLOBAL.innodb_data_file_path; --

Resultados Figura 28:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 29. SQL *Injection* – 14



Fuente: el autor.

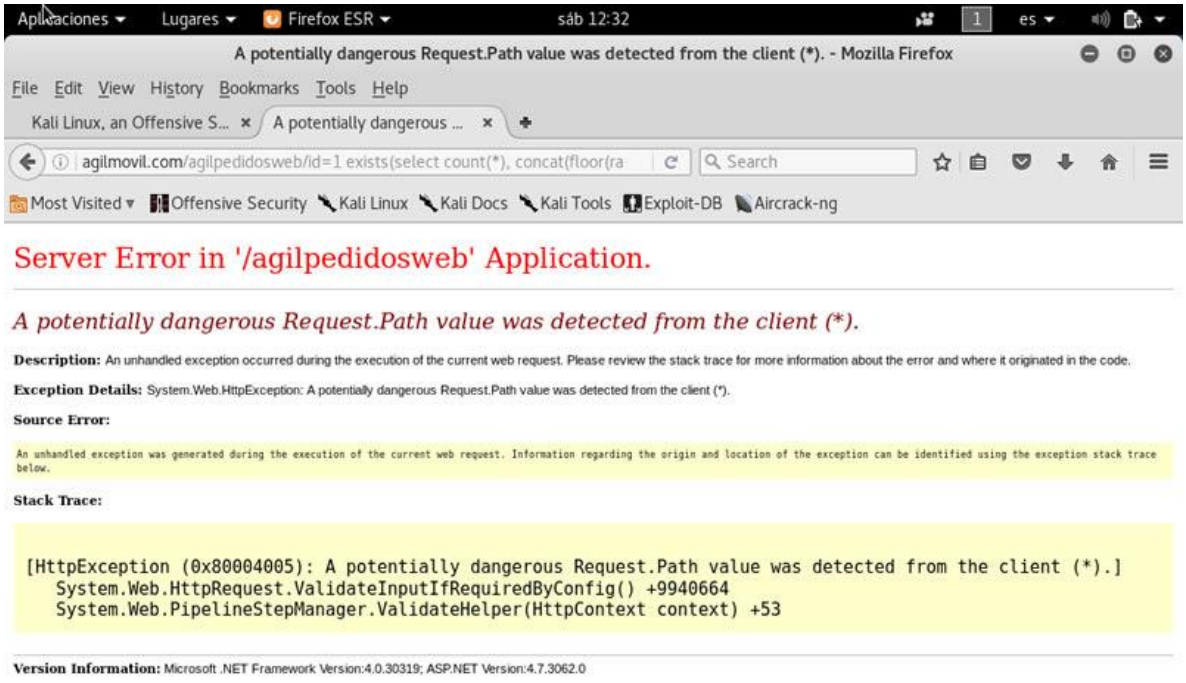
Descripción Figura 29:

Inyección ‘ create table pentest (columnatest varchar(45)); --

Resultados Figura 29:

Sin resultados al tipo de inyección, el aplicativo reporta que el usuario no se encuentra registrado, como se indicó en la Figura 17.

Figura 30. SQL *Injection* – 15



Fuente: el autor.

Descripción Figura 30:

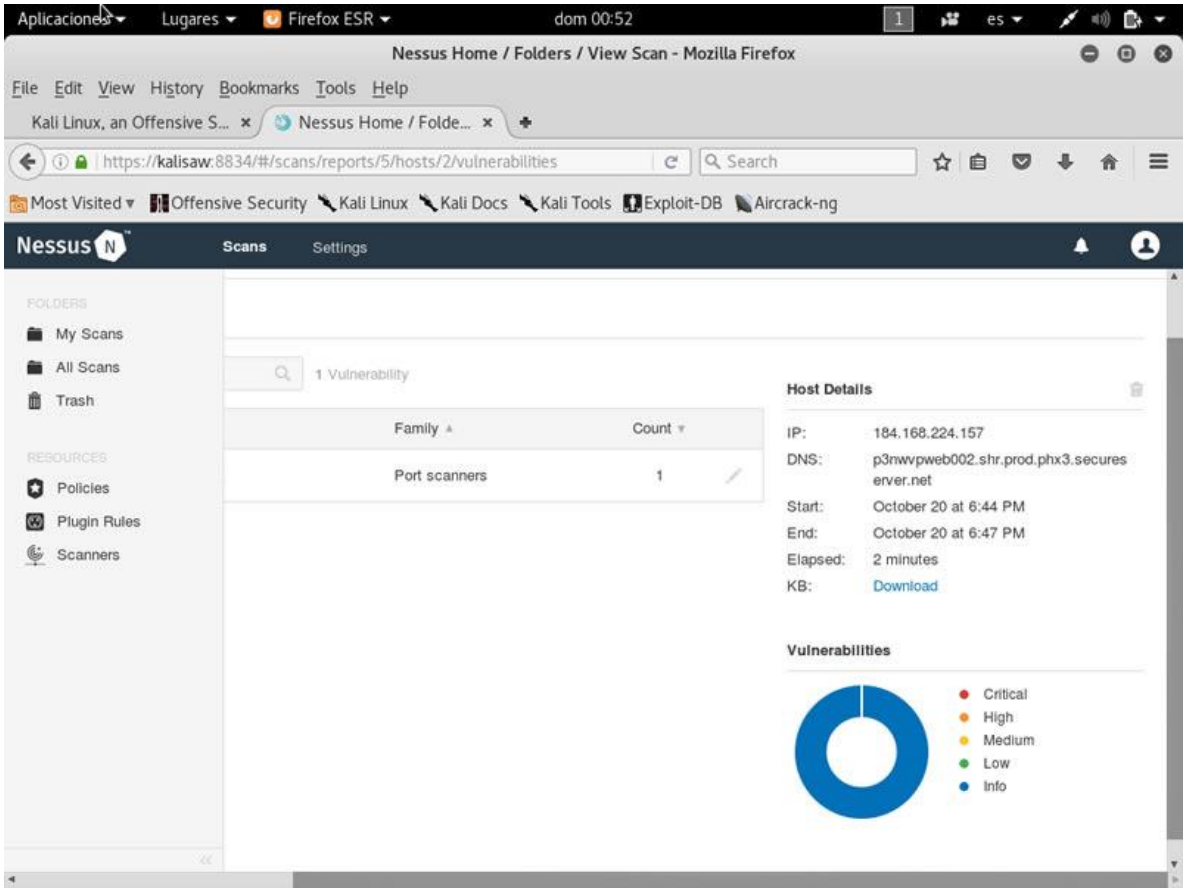
Inyección id=1 and exists(select count(*), concat(floor(rand(0)*2), '->', usuarios()) from (select 1 union selec 2 union select 3) t group by 2)#

Resultados Figura 30:

Sin resultados al tipo de inyección, el aplicativo error advirtiendo de una solicitud de ruta peligrosa.

9.3.4 Vulnerabilidad de Microsoft-IIS/8.0. Verificación de la vulnerabilidad del archivo /uncpatch/ que puede permitir *cross site scripting*, Figura 31.

Figura 31. Vulnerabilidad de Microsoft-IIS/8.0



Fuente: el autor.

Descripción Figura 31:

Verificación de vulnerabilidad cross site scripting mediante Nessus.

Resultados Figura 31:

Sin resultados pata el tipo de vulnerabilidad en el servidor de la aplicación de pedidos web.

10. RESULTADOS Y DISCUSIÓN

Inicialmente se realizó un proceso de recolección de información, mediante distintas técnicas de tal forma que se pudiera capturar la mayor cantidad de información del aplicativo web, teniendo en cuenta que esta está disponible en Internet, y que cualquier usuario de la red tiene acceso a la misma.

Se inició con datos básicos como el nombre de la empresa desarrolladora y el texto general “pedidos web”, mediante le navegador web más utilizado, Google.com, desde el cual se puedo conocer el enlace principal para acceder a la interfaz principal de la aplicación web.

Una vez obtenido la URL principal del aplicativo web se recuperó la dirección IP del mismo, para luego obtener información más detalla, como el tipo servidor, el tipo de tecnología utilizada

10.1 RECOMENDACIONES

Las herramientas WAF, son los cortafuegos para aplicaciones web, existen implementaciones tanto a nivel hardware como de software, establece una protección centralizada para las vulnerabilidades más comunes y ataques a las aplicaciones web. Estos están basados en Conjunto de reglas básicas ModSecurity de OWASP (CRS) y están diseñados para analizan el tráfico de red entrante al servidor web.

Un cortafuegos tradicional trabaja sobre la capa de red y la capa de trasporte del Modelo OSI y una de las ventajas de las WAF es que trabajan a nivel de capa de aplicación.

Los cortafuegos de aplicaciones web proteger de ataques de tipo inyección SQL, XSS, inclusión local o remota de archivos entre otros.

Pueden ser configurado de tal forma que deniegue cualquier tipo de transacción y que acepta las que se consideren como seguras y válidas, a esto se lo conoce como modelo de seguridad positiva, y del contrario se puede configurar para aceptar cualquier transacción y denegar las que sean consideradas amenaza o de riesgo a lo cual se le conoce como modelo de seguridad negativa.

Una correcta implementación de los cortafuegos de aplicaciones web mejora la seguridad de las aplicaciones web, sin embargo, se puede afectar la velocidad de respuesta en las transacciones y se requiere de esfuerzo para su adaptación y configuración eficaz.

El Top 10 de OWASP, es un proyecto que busca la sensibilización en las empresas sobre la seguridad de las aplicaciones y pretende identificar algunos altos riesgos afrontados por estas. Este proyecto es usado por diferentes instituciones, normas y hasta en libros, como referencia en materia de seguridad informática, de ahí la importancia. Y aunque abarca muchos aspectos a tener en cuenta para mantener buenas prácticas se seguridad en las aplicaciones, esta recomienda que se debe ir más allá del TOP 10, ya que existes una variedad de problemas directamente

relacionadas con las aplicaciones WEB, por lo cual se debe mantener una cultura regular orientada a mantener la seguridad de las aplicaciones web.
Dentro de los riesgos que se numeran en el TOP 10 de OWASP, se encuentra:

Exposición de datos sensible (*Sensitive Data Exposure*)
Existen datos sensibles dentro las aplicaciones web, como pueden ser los datos de sesión (usuario y contraseña) o números de identificación personal o datos de las tarjetas usadas en las transacciones bancarias, que deben ser protegidos, y a los cuales no se les presta la debida importancia para mantener su integridad y seguridad. Estos datos pueden ser aprovechados por los delincuentes informáticos no solo para causar fraudes, robos de identidad, sino, que, además pueden ser utilizados en otros delitos. Por esto es importante brindar en las aplicaciones web, mecanismos que permitan ocultar estos datos sensibles, mediante el uso estrategias como el encriptado o cifrado de datos y adicionalmente usar todas las precauciones necesarias en el intercambio de datos entre el cliente y el servidor, principalmente prestando atención al navegador web utilizado.

Para prestar atención a este de tipo riesgo se recomienda tener en cuenta los siguientes factores:

Agente de amenaza: En este factor, se tiene en cuanta la posibilidad de quién puede tener acceso a los datos de carácter sensible para el usuario, desde datos localizados o guardados de forma local, como aquellos que viajan entre el cliente y el servidor.

Vectores de ataques: Se debe tener en cuenta que los datos pueden ser tomados por los delincuentes informáticos, antes de que estos sean cifrados o encriptados,

y por ende son legibles, los cuales pueden ser tomados en el viaje desde el cliente al servidor.

Debilidades de seguridad: La principal debilidad de los datos, está relacionada con el bajo nivel de encriptación o la ausencia de este, el manejo de claves débiles y algoritmos poco seguros.

Impactos técnicos: En las aplicaciones web, existen datos como los de registro de usuario, inicio de sesión, números de tarjetas de crédito, entre otros, que por sentido común debería tener un grado alto de protección, pero por la ausencia de esta protección, podrían llegar a estar comprometidos, lo que causaría un impacto técnico.

Impacto de negocio: En este aspecto es importante determinar cómo afectaría la reputación de una organización la posible pérdida de datos, y en que implicaciones legales tendría.

Para identificar si una aplicación web es vulnerable en cuanto a este riesgo se debe, identificar cada uno de los datos sensibles, como contraseñas, números de tarjetas y similares. Por esto es importante identificar como son almacenados, como son transmitidos, qué mecanismos de criptografía se emplean, qué tan débiles con las contraseñas y qué directivas de seguridad del navegador son empeladas.

Para proteger una aplicación web de este riego, se recomienda, usar certificados de seguridad, almacenar los datos sensibles de forma cifrada, no almacenar datos

sensibles que puedan ser innecesarios, utilizar algoritmos de cifrado fuerte y claves fuertes, no usar los mecanismos de autocompletado de los formularios que sean sensibles, así prevenir la memoria temporal de los navegadores que puedan almacenar estos datos.

Herramientas a usar:

Certificado SSL: por sus siglas: *Secure Socket Layer*, este es un protocolo de seguridad que permite que la información o datos que van desde el cliente o navegador al servidor web, o viceversa, fluyan de tal forma que no sea legible si estos son interceptados, ya que usa cifrado o encriptación. Para esto el servidor web debe soportar este tipo de certificado. Las aplicaciones web o portales que usan certificados digitales se identifican por que la url está formada de la siguiente forma: https://sitioweb

Ausencia de Control de Acceso a Funciones (*Missing Function Level Access Control*)

Las aplicaciones web deben validar a qué funciones se tiene acceso antes de hacer la interfaz de usuario, tanto a nivel de la aplicación como a nivel del servidor, ya que la ausencia de esta validación podría ser aprovechada por los delincuentes informáticos.

Agente de amenaza: en este aspecto se debe validar qué privilegios tienen los usuarios para acceder a las funciones de las aplicaciones, ya si se está conectado

a la red un usuario anónimo o un usuario normal podría enviar cualquier tipo de petición que debe ser validada para conocer si posee los permisos requeridos.

Vectores de ataques: Un usuario de una aplicación web, podría ser cualquier usuario legítimo, como un atacante, este último podría realizar cambios en la URL para intentar acceder a una función a la cual usuarios con privilegios tienen acceso. Es importante determinar si existen funciones de uso privado que no han sido protegidas y puedan accedidas por usuarios anónimos.

Debilidades de seguridad: el mayor riesgo se presenta por la poca atención en la configuración que deben tener las funcionalidades de las aplicaciones web, ya que pueden estar mal configuradas, por descuidos de los programadores los cuales dejan de realizar las verificaciones adecuadas al código. La tarea de detectar que funcionalidades pueden ser objeto de ataque.

Impactos técnicos: el mayor riesgo está en la posibilidad de que un delincuente informático pueda acceder a las funciones propias del sistema y funciones de carácter administrativo lo cual podría ser un desastre total.

Impacto de negocio: Determinar el grado de importancia para la organización, si un ataque de este tipo podría llegar a concretarse, como podría afectar e buen nombre de la misma.

Para identificar si una aplicación web es vulnerable en cuanto a este riesgo se debe realizar una revisión de cada una de las funcionalidades para determinar los

privilegios de acceso para cada tipo de usuario, para ello se requiere verificar si la interfaz de usuario permite acceso a funciones no restringidas sin previa autorización, determinar si existes autenticación del lado del servidor, validar si el servidor no brinda información que pueda ser aprovechada por los delincuentes informáticos.

Para validar lo vulnerable, frente a este ataque, que puede ser una aplicación web, se puede realizar pruebas mediante un Proxy, de tal forma que se puedan explorar todas las funcionalidades de la aplicación web con distintos usuarios y privilegios, para determinar los comportamientos entre distintos niveles de acceso para cada usuario. También se debe revisar el código, mediante la realización de pruebas unitarias para determinar los patrones seguidos en cada solicitud de acuerdo a los privilegios de usuarios.

Para proteger una aplicación web de este riego, se debería implementar un módulo de acceso, que pueda ser invocado desde cualquier funcionalidad de la aplicación web, este debe ser configurable, donde la configuración por defecto niegue cualquier acceso no configurado.

Herramientas a usar:

Se puede utilizar la lista de acceso o ACL, creando roles y perfiles de usuarios para determinar los permisos a cada funcionalidad.

ASP.NET's *Membership*, este es un servicio incluido en Framework para desarrollo de aplicaciones web con .Net, el cual permite la gestión de las credenciales de usuarios.

A8 - Falsificación de peticiones en sitios cruzados (*Cross-Site Request Forgery*)

Cuando un usuario legitimo (victima) ha iniciado sesión en una aplicación web, que podría ser de un portal bancario, y con alguna estrategia o artimaña un atacante induce a este usuario a ingresar a un determinado enlace dentro de otro portal, distinto al portal en el que el usuario se encuentra logueado, donde el atacante previamente ha creado algún código malintencionado para que el enlace modificado o falsificado realice alguna acción determinada, la cual podría ser una petición sobre el sitio web del usuario, sin que el usuario lo note, realizando por ejemplo, transacciones que el usuario no ha autorizado; este es el caso de un ataque de tipo Falsificación de peticiones en sitios cruzados.

Agente de Amenaza: En este aspecto se debe considerar que cualquier usuario puede realizar la carga de sitios web desde los cuales se pueden hacer solicitudes a un sitio web especifico.

Vectores de ataques: Una de las estrategias más utilizadas en este tipo de ataque es el envío de enlaces que están asociados a una imagen, los cuales han sido falsificados para aprovechar si el usuario ha iniciado sesión en algún portal, buscando la ingenuidad del usuario para que este siga dicho enlace, o cualquier enlace que ejecute algún tipo de script o código.

Debilidades de seguridad: Los navegadores web envían los datos de credenciales, cookies de sesión de forma automática, lo cual puede ser aprovechada por los delincuentes informáticos para falsificar las peticiones, desde sitios web distintos sobre sitios web en los que el usuario ha iniciado una sesión. Toda aplicación web está diseñada para realizar acciones que los usuarios ejecutan con regularidad, eso facilita la labor del atacante a la hora de diseñar su estrategia. Es importante realizar pruebas de penetración sobre los sitios web para identificar la falsificación de peticiones en sitios cruzados.

Impactos técnicos: Con el éxito de un ataque de tipo falsificación de peticiones en sitios cruzados, el delincuente informático podría realizar acciones legitimas de un usuario autenticado sin que le usuario lo note, desde realizar cambio de estado, acceder a zonas privilegiadas y hasta cerrar sesiones.

Impacto de negocio: No poder garantizar si el usuario posee la seguridad de realizar acciones o realizó acciones que no ha autorizado, generaría un alto impacto en la reputación del negocio que implemente aplicaciones web vulnerables a este tipo de ataques, por ende es un aspecto que debe ser tenido en cuanta y valorado.

Se puede determinar si una aplicación web es vulnerable al tipo de ataque falsificación de peticiones en sitios cruzados, identificando si usa tokens de sesión que pueden ser fácilmente predecibles.

La forma de proteger las aplicaciones web de este tipo de riesgo es el uso de re autenticación, para confirmar si el usuario realmente desea ejecutar alguna

operación, o mediante el uso de las CAPCHA, para confirmar si es un usuario real. Es importante que los desarrolladores realicen verificaciones a las funcione que ejecutan cambios de estado para protegerlas adecuadamente, también se deben realizar pruebas de testeo o penetración para mejorar la seguridad.

Herramientas a usar

La generación de tokens por sesión y usuario que sean únicos y se deben enviar en la solicitud HTTP como un campo oculto.

Uso de las CAPCHA, las cuales son medidas de seguridad que permiten distinguir si una operación fue realizada por un ser humano o por un proceso automatizado.

Las aplicaciones ASP MVC, utilizan un archivo de configuración que se denomina web.config, desde este archivo se puede eliminar cabeceras informativas que puede ser utilizadas por los atacantes informáticos, por consiguiente, se recomienda eliminar las cabeceras X-Powered-By, X-AspNetMvc-Version mediante la siguiente configuración:

```
<system.webServer>
  <httpProtocol>
    <customHeaders>
      <clear />
    </customHeaders>
  </httpProtocol>
  <security>
```

```
    <requestFiltering removeServerHeader="true"/>
  </security>
</system.webServer>
<system.web>
  <httpRuntime enableVersionHeader="false" />
</system.web>
```

BIBLIOGRAFÍA

[Anónimo]. Pentesting con OWASP Zed Attack Proxy. Disponible en http://www.tic.udc.es/~nino/blog/psi/2012/pentestingZAP2.pdf

ALONSO, Chema. UN INFORMÁTICO EN EL LADO DEL MAL. Atacar un sitio web usando sus estadísticas: Pentesting, Hacking & doxing, [en línea], 20 diciembre de 2014, [revisado 29 noviembre 2017]. Disponible en http://www.elladodelmal.com/2014/12/atacar-un-sitio-web-usando-sus.html.

BORTNIK, Sebastián. Pruebas de penetración para principiantes: 5 herramientas para empezar [en línea], 6 julio 2013, [revisado 29 noviembre 2017]. Disponible en: http://revista.seguridad.unam.mx/numero-18/pruebas-de-penetraci%C3%B3n-para-principiantes-5-herramientas-para-empezar.

BUCKER Caleb. Penetration Testing - Hacking Etico Análisis Web - Evaluación de Vulnerabilidades – Explotacion [en línea], 19 octubre 2012, [revisado 29 noviembre 2017]. Disponible en: http://calebbucker.blogspot.com.co/2012/10/penetration-testing-hacking-etico.html.

BUCKER Caleb. Seguridad Informática [en línea], 2012, [revisado 19 noviembre 2017]. Disponible en https://www.exploit-db.com/docs/22954.pdf.

MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid, octubre 2012. 127 p.

MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p.

MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III – Guía de Técnicas. Madrid, octubre 2012. 42 p.

SEGURIDAD Y ETICA. 5 Herramientas útiles en Penetration Testing para Aplicaciones Web [en línea], 11 abril 2012 [revisado 29 noviembre 2017]. Disponible en https://seguridadetica.wordpress.com/2012/04/11/5-heramientas-utiles-en-penetration-testing-para-aplicaciones-web/.

The Internet Society. Hypertext Transfer Protocol -- HTTP/1.1. [1999]. Disponible en: https://www.w3.org/Protocols/rfc2616/rfc2616.html

ANEXOS

Anexo A. Resumen analítico especializado.

TEMA	Pentesting Web
TÍTULO	ANALISIS DE SEGURIDAD DEL SISTEMA DE PEDIDOS WEB DE LA EMPRESA E.B. SOFTWARE LTDA. MEDIANTE PENTESTING
AUTORES	Ciro Alfonso Pacheco
FUENTES BIBLIOGRÁFICAS	BUCKER Caleb. Penetration Testing - Hacking Etico Análisis Web - Evaluación de Vulnerabilidades – Explotacion [en línea], 19 octubre 2012, [revisado 29 noviembre 2017]. Disponible en: http://calebbucker.blogspot.com.co/2012/10/penetration-testing-hacking-etico.html. BUCKER Caleb. Seguridad Informática [en línea], 2012, [revisado 19 noviembre 2017]. Disponible en https://www.exploit-db.com/docs/22954.pdf. MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid, octubre 2012. 127 p. MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Madrid, octubre 2012. 75 p. MINISTERIO DE AMINISTRACIÓN PÚBLICA, GOBIERNO DE ESPAÑA, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III – Guía de Técnicas. Madrid, octubre 2012. 42 p.

AÑO	2018
RESUMEN	Mediante la realización de pruebas de pentesting web, este proyecto pretende determinar la seguridad del aplicativo de pedidos web de la empresa E.B. Software Ltda.
PALABRAS CLAVES	Pentesting, Pruebas de penetración, Gestión de riesgos, Análisis de seguridad, Seguridad Web, Seguridad Informática.
CONTENIDOS	INTRODUCCIÓN 1. PROBLEMA 1.2 PLANTEAMIENTO DEL PROBLEMA 2. OBJETIVOS 2.1 OBJETIVO GENERAL 2.2 OBJETIVOS ESPECÍFICOS 3. JUSTIFICACIÓN 4. ALCANCES Y DELMITACIÓN DEL PROYECTO 5. MARCO REFERENCIAL 5.1 ANTECEDENTES 5.2 MARCO TEÓRICO 5.3 Ataques a los sistemas de información 5.4 MARCO CONCEPTUAL 5.5 MARCO LEGAL 6. MARCO METODOLÓGICO 6.1 POBLACIÓN Y MUESTRA 6.2 METODOLOGÍA DE INVESTIGACIÓN 6.3 METODOLOGÍA DE DESARROLLO 7. PRODUCTO RESULTANTE A ENTREGAR 8. ANÁLISIS DE RIESGOS 8.1 IDENTIFICACIÓN DE ACTIVOS 8.2 AMENAZAS

	8.3 SALVAGUARDAS 8.4 IMPACTO Y RIESGO RESIDUAL 9.PRUEBAS PARA LA DETECCIÓN DE VULNERABILIDADES, AMENAZAS Y RIESGOS DE SEGURIDAD DEL SISTEMA DE PEDIDOS WEB DE LA EMPRESA E.B SOFTWARE LTDA. 9.1 FASE 1: REGLAS DE JUEGO: ALCANCE Y TÉRMINOS 9.2 FASE 2: RECOLECCIÓN DE INFORMACIÓN 9.3FASE 3: EXPLOTACIÓN DE LAS VULNERABILIDADES 10 RESULTADOS Y DISCUSIÓN
DESCRIPCION DEL PROBLEMA	La empresa E.B. Software Ltda., actualmente no se puede definir con certeza la seguridad con la que cuenta, las posibles vulnerabilidades que presenta.
OBJETIVOS	General: Analizar la seguridad de la aplicación web de pedidos de la empresa E.B. Software Ltda. mediante pruebas de penetración. Específicos: Analizar los riesgos y las vulnerabilidades del aplicativo de pedidos web de la empresa E.B Software Ltda. Realizar pruebas de penetración o Pentesting, a la aplicación de pedidos web la empresa E.B Software Ltda. mediante herramientas de código abierto. Generar informe de las posibles amenazas encontradas a la aplicación de pedidos web la empresa E.B Software Ltda. Brindar información de los controles necesario para mejorar la seguridad del aplicativo de pedidos web de la empresa E.B. Software Ltda.
METODOLOGÍA	Se implementa un enfoque de investigación cualitativa. Este proyecto implementa la metodología Magerit, que propone las siguientes etapas: 1. Planificación del proyecto de

	riesgos. 2. Análisis de riesgos 3. Gestión de riesgos 4. Selección de salvaguardas.
PRINCIPALES REFERENTES TEÓRICOS	Aplicación web, codificación y desarrollo de una aplicación web, seguridad en aplicaciones web basado, la confidencialidad, la integridad y disponibilidad, proyecto OWASP, vulnerabilidades en la web, métodos de análisis de aplicaciones web. Normas, estándares y metodologías norma ISO 27000, COBIT, MAGERIT, ataques a los sistemas de información.
PRINCIPALES REFERENTES CONCEPTUALES	La seguridad de la información, La seguridad de los sistemas informáticos, la metodología Magerit, buenas prácticas a la hora de desarrollar aplicaciones web en la empresa E.B Software Ltda.
RESULTADOS	El proyecto recopila formación documental como información que permitió llevar a cabo el proceso de pruebas de pentesting web al aplicativo de pedidos.
CONCLUSIONES	Implementación de herramientas WAF. Usar certificados de seguridad, almacenar los datos sensibles de forma cifrada. Las aplicaciones web deben validar a qué funciones se tiene acceso antes de hacer la interfaz de usuario, tanto a nivel de la aplicación como a nivel del servidor. Se debería implementar un módulo de acceso, que pueda ser invocado desde cualquier funcionalidad de la aplicación web, este debe ser configurable, donde la configuración por defecto niegue cualquier acceso no configurado. Es fundamental el uso de las CAPCHA. Eliminar cabeceras informativas del archivo web.config.