IDENTIFICAR VULNERABILIDAD Y DISEÑAR POLÍTICAS DE SEGURIDAD PARA LA APLICACIÓN WEB SISTEMA INTEGRAL DE REGISTRO EDUCACIÓN PERMANENTE (SIREP) DE LA UNAD CCAV CARTAGENA

ALEXANDRA MILENA GONZÁLEZ POMBO
ORLANDO GÓMEZ BARBOZA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD-
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CARTAGENA
2015

IDENTIFICAR VULNERABILIDAD Y DISEÑAR POLÍTICAS DE SEGURIDAD PARA LA APLICACIÓN WEB SISTEMA INTEGRAL DE REGISTRO EDUCACIÓN PERMANENTE (SIREP) DE LA UNAD CCAV CARTAGENA

ALEXANDRA MILENA GONZÁLEZ POMBO
ORLANDO GÓMEZ BARBOZA

Monografía para obtener el título de
Especialista en Seguridad Informática

Asesor
Esp. Freddy Enrique Acosta

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD-
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CARTAGENA
2015

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Cartagena de Indias, 28 de octubre de 2015

DEDICATORIA

A Dios por darme la vida, la capacidad de aprender, por ser mi horizonte y por permitirme alcanzar este logro.

A mis ángeles por su guía.

A mi mamá por ser la razón de mi vida.

A mi abuela por ser mí ser de luz.

Alexandra M. González Pombo

A Dios, porque por su inmenso amor y misericordia me dio la sabiduría, paciencia y todos los medios para realizar cada una de las etapas de este proyecto.

A mi familia, porque fueron un apoyo incondicional en todo momento.

Orlando Gómez Barboza

AGRADECIMIENTOS

Alexandra Milena González Pombo y Orlando Gómez Barboza expresan sus agradecimientos a:

Dios, por brindarnos su sabiduría, por permitirnos no desmayar y siempre mandar una luz que nos motivara para seguir adelante y terminar el proyecto.

A nuestros seres queridos que permanentemente nos dieron sus respaldo y comprensión para cumplir nuestra meta.

A la señora Nelvys Rodriguez, funcionaria de la Oficina de Registro y Control del CCAV de la ciudad de Cartagena, por su apoyo e interés para la realización del proyecto.

Al Ingeniero Freddy Enrique Acosta, por su importante orientación metodológica en el desarrollo de este proyecto; donde destacamos su disponibilidad, conocimiento, y confianza, cualidades que sin duda alguna han enriquecido nuestro trabajo realizado.

A todos MUCHÍSIMAS GRACIAS.

CONTENIDO

pág.

pág.

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

pág.

LISTA DE ANEXOS

pág.

GLOSARIO DE TERMINOS

AMENAZA: Elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información[1].

APLICACIÓN: Tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos[2].

ATAQUE INFORMÁTICO: Consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización[3].

BASE DE DATOS: Una base de datos es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite. Una base de datos es un sistema de archivos electrónico.

CONFIDENCIALIDAD: Los recursos del sistema solo pueden ser accedidos por los elementos autorizados[4].

CONTROL: Cualquier acción o proceso que se utiliza para mitigar el riesgo[5].

CONTROL DE ACCESO: es el mecanismo dispositivo o sistema que neutraliza el acceso no autorizado a los sistemas informático[6].

CRACKER: Delincuente informático, persona que utiliza sus conocimientos para invadir sistemas, descifrar claves, robar datos personales con la intención de utilizar la información robada para su propio beneficio o para cometer ilícitos informáticos a favor de otros.

---

[1] UNIVERSIDAD NACIONAL DE LUJÁN. Amenazas a la Seguridad de la Información. Departamento de seguridad Informática. Disponible en internet http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

[2] Aplicación informática. WIKIPEDIA. Octubre 25, Disponible en internet https://es.wikipedia.org/wiki/Aplicaci%C3%B3n_inform%C3%A1tica

[3] MIERES, Jorge. Ataques informáticos Debilidades de seguridad comúnmente explotadas. Evil Filgers Disponible en internet https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

[4] UNIVERSIDAD NACIONAL ABIERTA YA DISTANCIA. Seguridad de la Información. Gerencia de Innovación y Desarrollo Tecnológico Disponible en internet http://gidt.unad.edu.co/seguridad

[5] Seguridad de la información. WIKIPEDIA. Octubre 26 Disponible en internet https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

[6] ALEGRE RAMOS, María del Pilar y GARCIA-CERVIGÓN HURTADO, Alfonso (2011). Seguridad. Madrid: Paraninfo 11.

DISPONIBILIDAD: Los recursos del sistema deben permanecer accesibles a los elementos autorizados[7].

HACKER: Persona con elevados conocimientos informáticos independientemente de la finalidad con que los use.

IMPACTO: Resultado y consecuencia de que se materialice un riesgo[8].

INTEGRIDAD: Los recursos del sistema solo pueden ser modificados o alterados por los elementos autorizados[9].

MySQL: Gestor de bases de datos SQL (Structured Query Language), es una implementación Cliente-Servidor que consta de un servidor y diferentes clientes (programas/librerías). Se puede agregar, acceder y procesar datos grabados en una base de datos. Actualmente el gestor de base de datos juega un rol central en la informática, como única utilidad, o como parte de otra aplicación.

NEWBIE: Hacker novato que está empezando una carrera.

NORMA: Establecer los límites permisibles de acciones y procesos para cumplir con las políticas[10].

PHP: Lenguaje de script interpretado en el lado del servidor utilizado para la generación de páginas Web dinámicas, embebido en páginas HTML y ejecutado en el servidor. La mayor parte de su sintaxis ha sido tomada de C, Java y Perl con algunas características específicas de sí mismo. La meta del lenguaje es permitir rápidamente a los desarrolladores la generación dinámica de páginas. No es un lenguaje de marcas como podría ser HTML, XML o WML. Está más cercano a JavaScript o a C.

POLÍTICAS DE SEGURIDAD: es el conjunto de leyes, normas y procedimientos que permiten regular la seguridad de un sistema informático[11].

PRUEBA DE PENETRACIÓN (PEN TEST): Las pruebas de penetración (también llamadas “pen testing”) son una práctica para poner a prueba un sistema

---

[7] UNIVERSIDAD NACIONAL ABIERTA YA DISTANCIA. Seguridad de la Información. Gerencia de Innovación y Desarrollo Tecnológico Disponible en internet http://gidt.unad.edu.co/seguridad

[8] Seguridad de la información. WIKIPEDIA. Octubre 26 Disponible en internet https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

[9] Ibid., p.1

[10] Seguridad de la información. WIKIPEDIA. Octubre 26 Disponible en internet https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

[11] UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Políticas de Seguridad. Laboratorio de Redes y Seguridad. UNAM Disponible en internet http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php

informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar**.**

RIESGO: Es la posibilidad de que una amenaza aproveche una vulnerabilidad y dañe un activo de información[12].

SISTEMAS INFORMÁTICOS: Conjunto de elementos hardware, software y recursos humanos utilizados para manipular, almacenar y procesar datos[13].

SQL (Structured Query Language): Tipo de lenguaje vinculado con la gestión de bases de datos de carácter relacional que permite la especificación de distintas clases de operaciones entre éstas. Gracias a la utilización del álgebra y de cálculos relacionales, el SQL brinda la posibilidad de realizar consultas con el objetivo de recuperar información de las bases de datos de manera sencilla.

TEXTO EN CLARO: Texto sin ningún tipo de cifrado.

VULNERABILIDAD: Debilidad de cualquier tipo que compromete la seguridad del sistema informático[14].

[12] UNIVERSIDAD NACIONAL DE LUJÁN. Amenazas a la Seguridad de la Información. Departamento de seguridad Informática Disponible en internet http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/21

[13] Ibid., p. 1.

[14] MIFSUD, Elvira. MONOGRÁFICO: Introducción a la seguridad informática - Vulnerabilidades de un sistema informático. Observatorio Tecnológico. Disponible en internet http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

RESUMEN

El proyecto "*identificar vulnerabilidad y diseñar políticas de seguridad para la aplicación WEB del sistema integral de registro educación permanente (SIREP) de la UNAD CCAV Cartagena*", el cual se encuentra en funcionamiento en mencionado centro, para llevar los diferentes registros académicos del programa de educación básica y media a distancia para jóvenes y adultos, aplicación que almacena información referente a: datos de los estudiantes, docentes, entrega de módulos y calificaciones.

Para el desarrollo de la identificación de las vulnerabilidades en el aplicativo SIREP, se realizaron pruebas y ataques con los programas de escaneo VEGA y OWASP ZED ATTACK PROXY, con estas herramientas de escaneo, se lograron detectar las vulnerabilidades que posee la aplicación, buscando conocer cuáles son las debilidades de la aplicación WEB, con esto poder mitigar los riesgos que allí se lograron observar tales como: pérdida de información por robo, modificación o eliminación, o el ingreso de usuarios no permitidos.

A través de OWASP (Open Web Aplication Security Project) logramos clasificar las vulnerabilidades encontradas, donde se pudo especificar el alcance de cada una de ellas y lo que sucedería si llegaran a materializarsen, lo que nos lleva a realizar las recomendaciones para que sean implementadas por la Universidad.

Con base en el estándar MAGERIT, se realizó un análisis y evaluación de los posibles riesgos que causarían ataques al aplicativo SIREP, y si llegaran a materializarsen las vulnerabilidades encontradas. En este análisis se tuvo en cuenta la valoración económica de los activos con los que cuenta el CCAV de Cartagena, las amenazas encontradas las cuales pueden ser de origen natural o por causa humana, lo que nos lleva a evaluar la confidencialidad, integridad y disponibilidad de la Información en el aplicativo SIREP, de igual manera el impacto potencial de estas amenazas y la relación de costos por perdida de información.

Las vulnerabilidades encontradas demostraron que la información que es manipulada a través del aplicativo SIREP está en riesgo de ser atacada por ciberdelicuentes si no se toman los respectivos correctivos basados en las recomendaciones dadas.

Finalmente se crearon las Políticas de Seguridad que se deben implementar en todo el CCAV para los usuarios que tienen acceso al SIREP.

Palabras Claves

SIREP, Aplicación, Seguridad, Penetración, Ataques Informáticos, Políticas de Seguridad, Vulnerabilidad, Amenazas.

INTRODUCCIÓN

Preservar la información y la integridad de un sistema informático es muy importante para una empresa, por lo que en pérdidas económicas y de tiempo podría suponer, sin olvidar el peligro que podía acarrear el acceso a un sistema de un usuario no autorizado. Por este motivo se considera muy importante la seguridad informática, la cual es un conjunto de procedimientos, dispositivos y herramientas encargadas de garantizar la integridad, disponibilidad y autenticidad de la información de un sistema informático e intentar reducir las amenazas que puedan afectar al mismo[15].

La información es un conjunto de datos organizados que pueden ser interpretados como un mensaje. En muchos casos la información que es procesada a través de una Aplicación Web tiene carácter confidencial ya que es parte fundamental del negocio. Una propiedad de la información es que ésta adquiere diferentes valores según el interés de diferentes personas o entidades[16]. Lo que para unos puede parecer insignificante para otros es realmente valioso. Por eso se debe hacer todo lo posible para resguardarla ya que es el activo más valioso con el que cuenta una organización.

En el siguiente escrito encontrará un proyecto que pretende identificar las debilidades de la aplicación web SIREP (Sistema Integral Registro y Control Permanente), el cual fue diseñado y desarrollado como tesis de grado por un estudiante de la Universidad Nacional Abierta y a Distancia UNAD.

Para conseguir, identificar las vulnerabilidades se aplicarán herramientas de escáner de vulnerabilidad que permitan conocer los agujeros que pueden ser aprovechados por los hackers para causar daños al sistema y por ende a la Universidad, se evaluará algunos de los riesgos revelados por el proyecto OWASP (Open Web Aplication Security Project), se tendrá en cuenta la norma ISO 27001 para revisar y mejorar el Sistema de Gestión de la Seguridad de la Información, en donde se recogerán documentos que permitan evidenciar el buen funcionamiento de la aplicación, en caso contrario se pueden aplicar acciones correctivas y preventivas basadas en la evaluación continua del programa y por último se aplicará el estándar MAGERIT, para probar e identificar los requisitos de la seguridad e identificar los riesgos que puede soportar la aplicación.

[15] ALEGRE RAMOS, María del Pilar y GARCIA-CERVIGON HURTADO, Alfonso. Seguridad Informática. 1 ed. Madrid, España: Paranifo SA, 2011. p 2.

[16] HERMOSO METAUTE, Adrian. Seguridad en Aplicativos Web. Barcelona (España): Universidad de Barcelona, dic. 2013. Disponible en internet http://diposit.ub.edu/dspace/bitstream/2445/49106/1/AdrianHermoso_memoria.pdf

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Las aplicaciones web vienen acompañadas con una nueva variedad de vulnerabilidades de seguridad. Muchos de los ataques que se pueden dar resultan impensables al momento de desarrollar la aplicación y con la rápida evolución de la tecnología se han desarrollado nuevas posibilidades de explotación. Es indiscutible que en la actualidad la seguridad en las aplicaciones web es el principal campo de batalla entre atacantes y aquéllos que administran recursos y datos que se deben defender, y es probable que siga así en el futuro mediato[17].

Una vulnerabilidad es la probabilidad que existe de una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Por ejemplo los datos son vulnerables a la acción de los hackers, mientras que una instalación eléctrica es vulnerable a un corto circuito. Se hace necesario identificar las vulnerabilidades de una aplicación web ya que si se identifican claramente las vulnerabilidades, las amenazas no se pueden materializar y por lo tanto los riesgos disminuirían notablemente. Las consecuencias del aprovechamiento de una vulnerabilidad se miden en el impacto que puede tener el daño causado. Los impactos pueden ser cuantitativos, si los perjuicios pueden cuantificarse económicamente y cualitativos, si suponen daños no cuantificables[18].

Por la anterior y teniendo en cuenta que el sistema integral de registro educación permanente (SIREP) de la UNAD CCAV Cartagena es un aplicativo WEB, el cual se encuentra instalado en un computador con acceso a INTERNET para realizar diferente tipos de consultas, el cual no cuenta con las medidas de seguridad necesarias que permita proteger la información del registro académico del programa de educación básica y media a distancia para jóvenes y adultos, al no existir ningún tipo de control hace vulnerable a nuestra aplicación caso de estudio, aplicación que puede ser atacada por ciberdelincuentes a través de la INTERNET, lo que puede llegar a ocasionar perdida de información, modificación de notas, modificación de datos de estudiantes, eliminación de información, entre otros, logrando con esto perder la integridad de la información.

---

[17] ROMANIZ, Susana. Seguridad de Aplicaciones WEB: vulnerabilidades en los controles de acceso. Grupo de Investigación en Seguridad de las Tecnologías de Información y Comunicaciones. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/21581/1927+-+Seguridad+de+aplicaciones+web+vulnerabilidades+en+los+controles+de+acceso.pdf;jsessionid=8D08E03C5F98771CCFB6FE3A79732C42?sequence=1G

[18] AGUILERA LOPEZ, Purificación. Seguridad Informática. Editex. 2010. 240 p.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo identificar las vulnerabilidades en el manejo de la información y qué mecanismos implementar para garantizar la seguridad de los datos contenidos en el aplicativo SIREP de la UNAD CCAV Cartagena?

1.3 JUSTIFICACIÓN

En la Seguridad Informática no es posible evitar la inseguridad, por lo que se hace necesario explorar en profundidad dicha propiedad, es decir, entre más se comprenda la realidad de la inseguridad, mejor se podrá comprender la seguridad informática, en otras palabras entre más se conoce la inseguridad informática más se comprenden las acciones y resultados de la seguridad, por tanto, al identificar la vulnerabilidades que tiene una aplicación web, se pueden tomar medidas de seguridad que permitan no solo mayores niveles de confiabilidad, sino también de evaluar el nivel de dificultad requerido por los atacantes para ingresar y vulnerar los medios de protección de la aplicación.

Desde el inicio de las tecnologías de la información y la comunicación se han presentado fallos y errores, generando que varios sean poco fiables y no funcionales, lo que lleva a las necesidades o requerimientos sean cada vez mayor.

Uno de los elementos que afectan las aplicaciones son las vulnerabilidades de seguridad y confiabilidad, debido a que al momento de realizar el análisis, diseño, desarrollo e implementación, no se contemplan todas las posibilidades de proveer seguridad a las tecnologías y se crean las puertas traseras de acceso o agujeros (espacios que permiten el acceso no deseado), que son aprovechados por hackers o personas mal intencionadas con el fin de acabar con la integridad, confiabilidad y disponibilidad de las aplicaciones.

Hoy en día muchas empresas han sido víctima de ataques de Hackers, por el robo, modificación e incluso eliminación de la información, por lo que es recomendable evaluar los niveles de seguridad de las aplicaciones que manipulan dichos datos, con el fin de identificar cada una de la vulnerabilidades e impartir recomendaciones y políticas de seguridad que permitan garantizar una mayor confiabilidad de la información manejados por el software.

Cada día que pasa, las vulnerabilidades de los sistemas de información aumentan exageradamente sobrepasando las medidas de seguridad que se establecen para ellas mismas, los ataques informáticos están presentes en los trabajos cotidianos de cada usuario, por lo que un estudio de vulnerabilidad traerá como beneficio, la identificación de cada uno de los agujeros con que un hacker, cracker o newbie

pueda penetrar la aplicación y manipular la información a su antojo, además permite tomar decisiones a la hora de diseñar un sistema de políticas de seguridad con el fin de garantizar un mejor servicio a los clientes y garantizar la CIA de la SIREP.

Con la identificación de las vulnerabilidades del SIREP, se busca minimizar los riesgos de pérdida de información en el CCAV Cartagena. Si la aplicación SIREP presentará vulnerabilidades y por esas vulnerabilidades se concretaran amenazas se perdería toda la información referente a las calificaciones de los estudiantes registrados en el aplicativo. Se perderían el registro de entrega de módulos a los estudiantes, así como el registro de Proyecto Social y los datos almacenados de los estudiantes de bachillerato.

1.4 ALCANCE Y LIMITACIONES

1.4.1 Alcance. Este proyecto se encuentra ubicado en la línea de gestión de sistemas del área de la ciencia de la computación y busca realizar una identificación de vulnerabilidades para el Sistema Integrado de Registro de Educación Permanente SIREP, con las herramientas VEGAS y OWASP ZEP ATTACK PROXY. Además de la realización de Políticas de Seguridad para el CCAV de la UNAD de la ciudad de Cartagena.

1.4.2 Limitaciones. El desarrollo del presente proyecto no enmarcará temas como los que se definen a continuación:

- Implementación de las recomendaciones al aplicativo SIREP.
- Verificación de las vulnerabilidades del Sistema Operativo donde se encuentra alojado el aplicativo SIREP.
- Verificación de las vulnerabilidades de los equipos red que cuenta el CCAV de la UNAD de la Ciudad de Cartagena
- Capacitación de los usuarios del aplicativo SIREP.
- Verificación de la integridad de la información del aplicativo SIREP.
- No se evaluaran las demás aplicaciones que se tienen instaladas en el CCAV.

1.5 OBJETIVOS

1.5.1 Objetivos General

Identificar las vulnerabilidades en el manejo de la información y formular las políticas de Gobierno de Tecnología para el manejo seguro de la aplicación SIREP del CCAV Cartagena.

1.5.2 Objetivos Específicos

- Realizar análisis de vulnerabilidades al aplicativo SIREP (sistema integral de registro educación permanente) del CCAV Cartagena, a través de VEGA de Subgrap, y OWASP ZAP 2.4.0.

- Verificar las vulnerabilidades obtenidas del aplicativo SIREP mediante el uso de las herramientas de análisis VEGA y OWASP ZAP 2.4.0, y proponer posibles correctivos para mitigar el riesgo.

- Analizar los riegos que se obtuvieron en el aplicativo SIREP, mediante la utilización del estándar MAGERIT.

- Diseñar políticas de seguridad para el aplicativo SIREP, bajo modelos abiertos de seguridad basados en la Norma ISO 27001.

2. MARCO REFERENCIAL

2.1 ANTECEDENTE INVESTIGATIVO

A lo largo de la historia moderna, se han logrado grandes avances tecnológicos en lo referente a la Seguridad de las Aplicaciones específicamente en las Aplicaciones Web. Un factor clave ha sido la posibilidad de identificar los riesgos y las vulnerabilidades en los Sistemas de Información, esto ha sido posible gracias al desarrollo de herramientas que amenazan la seguridad de la información de las empresas y a la realización de investigaciones y estudios realizados por personas cuyo propósito es dar a conocer cómo prevenir los riesgos y detectar vulnerabilidades.

En el trabajo investigativo para la realización de la presente monografía, traemos a colación los resultados de investigaciones y tesis de grados que trabajaron sobre identificación de vulnerabilidades.

A nivel internacional en los años 80 un integrante de las Fuerzas Armadas de los Estados Unidos de nombre James Anderson, publica un manual llamado "Computer Security Threat Monitoring and Surveillance" en donde da a conocer la forma como se detectan intrusos en los computadores utilizando y consultando los fichero log y define palabra como ataques y vulnerabilidad, este manual es reconocido como "*el antecedente para la instauración y posterior celebración del Día Internacional de la Seguridad Informática*"[19].

De los trabajos investigativos realizados en la Universidad Nacional Abierta y a Distancia UNAD, destacamos las siguientes investigaciones:

Trabajo de monografía de grado "***ANALISIS Y DIAGNOSTICO DE LA SEGURIDAD INFORMATICA DE INDEPORTES BOYACA[20]",*** el propósito principal del trabajo fue determinar cuál es el nivel de Seguridad Informática en Indeportes Boyacá, el trabajo está desarrollado a nivel de hardware, software y redes. El resultado final fue un documento con las vulnerabilidades encontradas y las recomendaciones para aumentar la seguridad en Indeportes Boyacá.

En el año 2014 se desarrolló proyecto de grado que lleva por título ***"Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria***

[19] 25 años celebrando el Día Internacional de la Seguridad Informática. Nov 2013. Disponible en internet en http://www.confirmasistemas.es/es/contenidos/canal-basics/25-anos-celebrando-el-dia-internacional-de-la-seguridad-informatica.

[20] RODRÍGUEZ CARRILLO, Ana María. Tesis de Especialización Seguridad Informática. Tunja, Boyacá.: Universidad Nacional Abierta y a Distancia. Escuela de Ingenierías y Ciencias Básicas. 2014.

***Colegio Mayor Del Cauca*”** en la que tuvieron como objetivo evaluar los riesgos mediante la metodología de Magerit con el fin de identificar las vulnerabilidades y amenazas de la seguridad, sugerir mecanismos de control y gestión que minimicen las vulnerabilidades en el colegio Mayor, dejando como recomendaciones la implementación del Sistema de gestión de Seguridad de la Información para proteger el activo más valioso “*La información*”[21] debido a las vulnerabilidades encontradas durante el estudio.

Centrándonos en nuestra sitio de estudio, en la Universidad Nacional Abierta y a Distancia CCAV Cartagena, sus funcionarios desconocen si se han realizado estudios previos de seguridad a las aplicaciones sin embargo aseguran que reciben correos internos con publicaciones sobre políticas de seguridad de información así como también de algunas amenazas y virus que se estén propagando en la red.

Es por eso que se hace necesario realizar el Diagnostico de la Aplicación Web SIREP, ya que la contribución que se hace con este trabajo es sumamente importante, porque será el primero de este tipo que se hace sobre seguridad específicamente en una Aplicación Web.

A lo largo del uso de las aplicaciones web han sido mucho los ataques que se han realizado, los cuales aprovechan las vulnerabilidades de las aplicaciones, que han tenido éxitos de penetración algunas de estas, las más recientes fueron:

En mayo de 2014 la página web de pagos online de eBay y PayPal fue hackeada y permitió acceso a los ciberdelincuentes a la red interna y a la base de datos obteniendo manipulación sobre los nombres de usuarios, teléfonos, direcciones de correo electrónico y contraseñas de los usuarios.

Otro ataque fue el robo de 5.000.000 millones de contraseñas de acceso de usuarios del correo electrónico Gmail, pero según el buscador Google las validaciones realizadas a dichas cuentas eran cuentas inactivas o sus propietarios no accedían.

El 13 de enero de 2015 se produjo un nuevo ataque a la página web del equipo de fútbol profesional colombiano Millonarios, en los primeros dejaron un mensaje de burla y dejaron claro que los ataques no solo se aplican a empresas y gente famosa, además que el ataque lo había realizado con la intención de demostrar a la persona encargada las fallas que presentaba la aplicación, cosas que con este ataque queda claro que aún no han logrado corregir.

[21] PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMBA, Mildred. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Tesis de Especialización Seguridad Informática. Popayán, Cauca.: Universidad Nacional Abierta y a Distancia. Escuela de Ingenierías y Ciencias Básicas. 2014.

Hoy en día las bases de datos son el objetivo principal de ataque para un hacker con el fin de obtener la información que la empresa guarda en ellas. Desde hace varios años el proyecto OWASP (Open Web Aplication Security Project) busca crear conciencia sobre la seguridad en aplicaciones mediante la revelación de algunos riesgos[22].

OWASP, da a conocer un listado de los 10 riesgos más críticos sobre la seguridad en aplicación, describe la probabilidad general y los factores de consecuencia utilizadas para clasificar la amenaza de cada riesgo, con el fin educar a desarrolladores sobre las consecuencias de las vulnerabilidades más relevantes que existen en la web, dentro de los cuales menciona los siguientes:

- A1 – Inyección: Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete en ejecutar comandos no intencionados o acceder datos no autorizados.

- A2 – Pérdida de Autenticación y Gestión de Sesiones: Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, llaves, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios.

- A3 – Secuencia de Comandos en Sitios Cruzados (XSS – Cross-site scripting): Las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la víctima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.

- A4 - Referencia Directa Insegura a Objetos: Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.

- A5 – Configuración de Seguridad Incorrecta: Una buena seguridad requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base

[22] CREATIVE COMMONS ATTRIBUTION SHARE-ALIKE. OWASP, The Open Web Application Security Project. OWASP Top 10. Los diez riesgos más criticos en Aplicaciones Web. 2013.

de datos, y plataforma. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto. Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación.

- A6 – Exposición de Datos Sensibles: Muchas aplicaciones web no protegen adecuadamente datos sensibles tales como números de tarjetas de crédito o credenciales de autenticación. Los atacantes pueden robar o modificar tales datos para llevar a cabo fraudes, robos de identidad u otros delitos. Los datos sensibles requieren de métodos de protección adicionales tales como el cifrado de datos, así como también de precauciones especiales en un intercambio de datos con el navegador.

- A7 – Ausencia de Control de Acceso a Funciones: La mayoría de aplicaciones web verifican los privilegios de acceso a nivel de función antes de hacer visible en la misma interfaz de usuario. A pesar de esto, las aplicaciones necesitan verificar el control de acceso en el servidor cuando se accede a cada función. Si las solicitudes de acceso no se verifican, los atacantes podrán realizar peticiones sin la autorización apropiada.

- A8 - Falsificación de Peticiones en Sitios Cruzados (CSRF): Un ataque CSRF obliga al navegador de una víctima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la víctima para generar pedidos que la aplicación vulnerable piensa son peticiones legítimas provenientes de la víctima.

- A9 –Utilización de componentes con vulnerabilidades conocidas: Algunos componentes tales como librerías, los frameworks y otros módulos de software casi siempre funcionan con todos los privilegios. Si se ataca a un componente vulnerable esto podría facilitar la intrusión en el servidor o una perdida seria de datos. Las aplicaciones que utilicen componentes con vulnerabilidades conocidas debilitan las defensas de la aplicación y permiten ampliar el rango de posibles ataques e impactos.

- A10 –Redirecciones y reenvíos no validados: Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing o malware, o utilizar reenvíos para acceder páginas no autorizadas.

2.2 MARCO CONCEPTUAL

Actualmente, los datos de las empresas, instituciones, y organizaciones son unos de los activos más valiosos con los que cuentan cada una de ellas, por lo que es de vital importancia que dichas entidades tengan acceso a la información en cualquier momento de una manera confiable, en la que se garantice la integridad y confidencialidad de la misma.

Para garantizar la Autenticidad, Integridad y Confidencialidad de la información, se debe lograr que el desarrollo de una aplicación Web, cuente con los soportes de seguridad adecuados, que ayuden a evitar, bloquear y reducir los riesgos y amenazas que pueden acabar con estos tres pilares, por tal motivo mediante este proyecto se busca evaluar los niveles de seguridad que tiene la aplicación SIREP.

Por tanto, se requiere tener bases teóricas y un conocimiento previo de fundamentos de Seguridad Informática como los referenciados a continuación:

2.2.1 Acceso a una Base de Datos. Tal y como da a conocer Adobe en su página, "*un servidor de aplicaciones le permite trabajar con recursos del lado del servidor, como las bases de datos. Por ejemplo, una página dinámica puede indicar al servidor de aplicaciones que extraiga datos de una base de datos y los inserte en el código HTML de la página. La instrucción para extraer datos de una base de datos recibe el nombre de consulta de base de datos. Una consulta consta de criterios de búsqueda expresados en un lenguaje de base de datos denominado SQL (Structured Query Language, lenguaje de consulta estructurado). La consulta SQL se escribe en los scripts o etiquetas del lado del servidor de la página*".

2.2.2 Brecha de Seguridad. Falta de algún recurso que pone en riesgo los servicios de información o expone los datos de sí misma, sea o no protegida por reserva legal.

2.2.3 Criptografía de Datos. Técnica utilizada para proteger los datos, se puede utilizar como recurso de seguridad ya que al momento de enviar los datos al sitio de almacenamiento o trasmitido por la red, este sea enviado en modo de bits ilegibles por aquellos que intenten obtenerla de manera ilegal. Con la criptografía busca contribuir en la seguridad de las bases de datos, buscando como objetivo garantizar la confidencialidad, integridad y autenticación.

2.2.4 Delitos Informáticos. Acciones llevadas a cabo, antijurídicas y culpables, cometidas por vías informáticas con el objetivo de espiar, destruir, robar, dañar, chantajear, falsificar la información de una persona u organización.

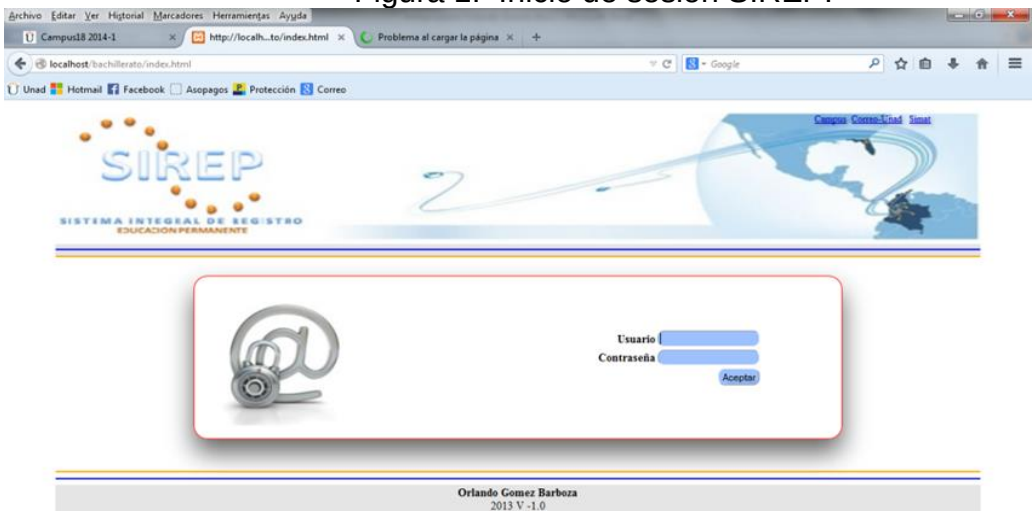
2.2.5 Ettercap. Interceptor/sniffer/registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle (Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing[23].

2.2.6 Exploits o Programas intrusos. Técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

2.2.7 Malware. Códigos maliciosos, que tienen como objetivo entorpecer o dañar una computadora o sistema de información sin la aprobación de su propietario. Los malware incluyen virus, gusanos, troyanos y puertas traseras, y para su propagación utiliza recursos de comunicaciones populares, medios magnéticos extraíbles, los sitios de descargas y ataques a las vulnerabilidades de seguridad en el software, con el fin de robar información personal que pueda ser utilizada por los atacantes para cometer fechorías e incluso entorpecer el sistema informático**.**

2.2.8 Sistema Integral de Registro Educación Permanente (SIREP). Aplicación en entorno web, utilizada por la Universidad Nacional Abierta y a Distancia CCAV Cartagena para llevar a cabo el registro de estudiantes, registro entrega de módulos, registro de calificaciones, generación de certificados y reportes**.** En la siguiente figura se muestra el Inicio de Sesión del Aplicativo SIREP.

Figura 1. Inicio de sesión SIREP.



Fuente. Aplicativo SIREP, Inicio de Sesión.

[23] Ettercap. Marzo, 2013. Disponible en internet en http://es.wikipedia.org/wiki/Ettercap

Esta aplicación fue desarrollada en 2012, como solución al registro de matrícula de los estudiantes del programa de bachillerato del CCAV, el cual se realizaban en archivos Excel, obligando a los funcionarios trabajar en archivos compartidos, los cuales después de tener un número considerable de registros, el documento se volvía muy pesado y por estar compartido lo hacía muy lento causando con esto pérdida de tiempo en los proceso, mala calidad en la atención a los estudiantes, constantes bloqueos del archivo y en algunos casos perdidas de información registradas.

Teniendo en cuenta la información manipulada, la importancia en que la que se ha convertido el uso de esta herramienta dentro del CCAV y los riesgos y amenazas a los que están expuestos la misma, es conveniente realizar un análisis que permita identificar las vulnerabilidades que presenta la aplicación para establecer políticas y medidas correctivas que garantice la disponibilidad, integridad y la autenticidad de la información.

2.3 MARCO TEÓRICO

2.3.1 Como trabajan las aplicaciones web[24]**.** El uso de aplicaciones web es tan común como tan masificado hoy en día por todo tipo de usuarios, empresas e instituciones. Su uso va desde la simple acción de leer un correo electrónico hasta realizar una compra en línea o una transacción bancaria sin importar el cubrimiento de estas aplicaciones, el tamaño, diseño, código en que estén realizadas, plataformas y arquitecturas en las que estén montadas.

Algo en común de estas aplicaciones es que la mayoría son interactivas, agradables para el usuario, con datos en línea que se comparten y que ponen a disposición del usuario. Muchas de ellas soportadas por grandes bases de datos y que usan como canal de distribución Internet.

La forma como una aplicación web trabaja, a simple vista es sencilla y práctica. Tal vez por ello y sin ser una afirmación, es que son vulnerables. Po lo general consisten en una base de datos que por decirlo así, está ubicada detrás del sitio web alojado en un servidor y que está escrita en un lenguaje de programación que es capaz de extraer información específica de esa base de datos por solicitudes y peticiones de los usuarios remotos o locales mediante interacciones dinámicas con esos usuarios o clientes.

Cuando se usan bases de datos para la gestión de los mismos en aplicaciones web, es común que estas aplicaciones estén compuestas por tres niveles:

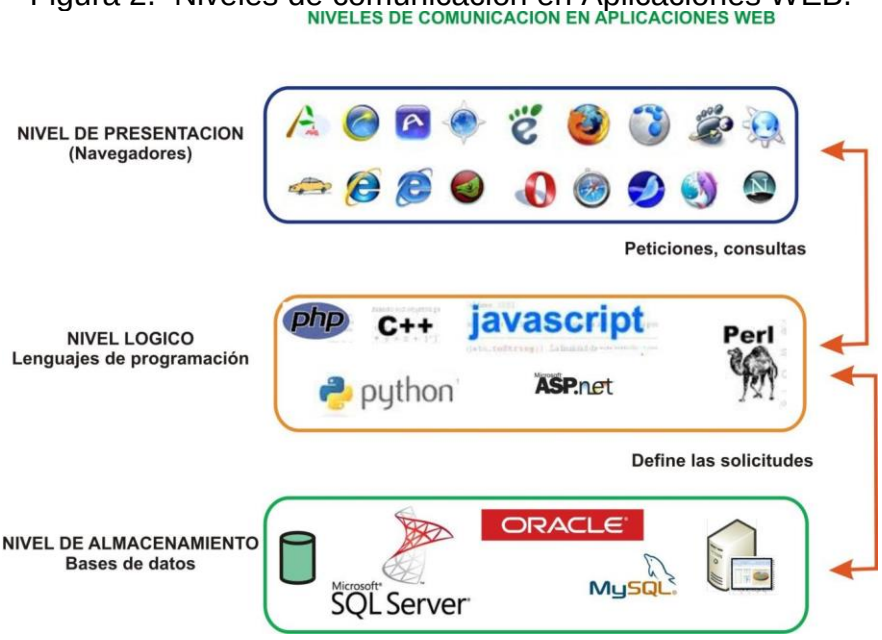
[24] AMAYA, Carlos. Como trabajan las Aplicaciones WEB. En: Módulo Curso Seguridad en Aplicaciones WEB. UNAD. Boyacá. 2013. p. 22-23.

Un nivel de presentación (un navegador web o motor de búsqueda).

Un nivel lógico (un lenguaje de programación, como C #, ASP, NET, PHP, JSP, etc.).

Y un nivel de almacenamiento (base de datos como Microsoft SQL Server, MySQL, Oracle, etc.)

Figura 2. Niveles de comunicación en Aplicaciones WEB.



Fuente. AMAYA, Carlos. A. Módulo Curso Seguridad en Aplicaciones WEB. UNAD. Boyacá. 2013. p. 23.

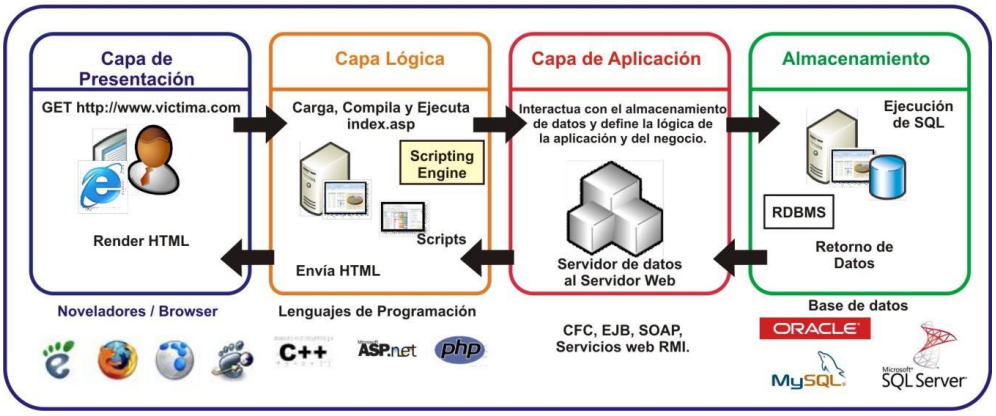
En la figura anterior se identifica la secuencia de peticiones y operación de los tres niveles en donde si el navegador Web (el nivel de presentación, por ejemplo, Internet Explorer, Safari, Firefox, etc.) envía peticiones a la capa media (la capa de lógica), que define los servicios, las solicitudes, consultas y actualizaciones de la base de datos (el nivel de almacenamiento).

2.3.2 Una arquitectura más compleja[25]**.** En los últimos años, el modelo de tres niveles fue reevaluado y un nuevo concepto basado en la escalabilidad y mantenimiento fue creado. Surge una solución de cuatro niveles que implica el uso de una pieza de middleware, típicamente llamado un servidor de aplicaciones, entre el servidor Web y el servidor de aplicaciones de base de datos.

[25] Ibid., p. 23-24.

Esta nueva capa de abstracción, consta de un servidor que aloja una interfaz de programación de aplicaciones (API) para exponer la lógica de negocio y procesos de negocio para uso de los servidores Web. Además, el servidor de aplicaciones puede hablar con varias fuentes de datos, incluyendo bases de datos, mainframes u otros sistemas de legado.

Figura 3. Arquitectura de cuatro capas en aplicaciones web.



Fuente. AMAYA, Carlos. Módulo Curso Seguridad en Aplicaciones WEB. UNAD. Boyacá. 2013. p. 23.

En la Figura anterior, el navegador Web (presentación) envía peticiones a la capa intermedia (lógica), que a su vez llama a la API expuesta del servidor de aplicaciones que residen en la capa de aplicación y es el que realiza las consultas y actualizaciones de la base de datos (almacenamiento).

El usuario ejecuta en el navegador de Internet una consulta y se conecta a http://www.victima.com. El servidor web que reside en la capa de lógica carga una secuencia de comandos del sistema de archivos y se lo pasa a través de su motor de scripting en el que se analiza y se ejecuta El script llama a una API expuesta desde el servidor de aplicación que reside en la capa de aplicación. El servidor de aplicación abre una conexión con el nivel de almacenamiento usando un conector de base de datos y ejecuta una instrucción SQL en la base de datos.

Se devuelven los datos al conector de la base de datos y al servidor de aplicaciones que implementa las reglas de la lógica de aplicación o negocio antes de devolver los datos al servidor Web que aplica un retoque de (lógica final) antes de la presentación de los datos en formato HTML en el navegador Web del usuario. La presentación de la web se hace mediante HTML que le muestra al usuario una representación gráfica de la código Esto sucede de manera instantánea y es transparente para el usuario.

¿Pero por qué se dividen las tareas en capas o niveles?: El concepto básico de una arquitectura estratificada implica dividir una aplicación en trozos lógicos, o niveles, cada uno de los cuales se le asignan roles. Las capas se pueden localizar

(implementar) en diferentes máquinas o en la misma máquina de forma virtualizada o separados el uno del otro.

Ventajas: Cuando se dividen las responsabilidades de una aplicación en múltiples capas hace que sea más fácil de escalar la aplicación, permite una mejor distribución de las tareas de desarrollo entre los desarrolladores, y hace una aplicación más fácil de leer dándole incluso enfoque de rehúso y de adaptabilidad a otras aplicaciones existentes o nuevas.

Le da características de robustez a las aplicaciones permitiendo eliminar puntos de fallos críticos y únicos que se puedan presentar si la aplicación sufre una caída total o irreparable.

Por ejemplo, la decisión de cambiar de proveedor de bases de datos debe requerir nada más que algunos cambios en las porciones aplicables de la capa de aplicación, la presentación y los niveles lógicos.

2.3.3 Amenazas y tipos de amenazas. Las amenazas son todas las posibles ocurrencias, circunstancias, eventos o acciones que tiene el potencial de causar daño sobre los elementos de un sistema de información, las cuales se puede clasificar en:

- Amenazas de software. Tipos de amenazas que están conformadas por todo tipo de software que tengan objetivos maliciosos. Dentro de estos tipos de software encontramos los virus, espías, troyanos, gusanos, phishing, spamming, entre otros.

- Amenazas físicas. Dentro de esta clasificación encontramos todas aquellas amenazas que puedan dañar al sistema informático en forma física y natural, por ejemplo incendio (fortuito o provocado), catástrofes naturales e incluso robos del hardware entre otros.

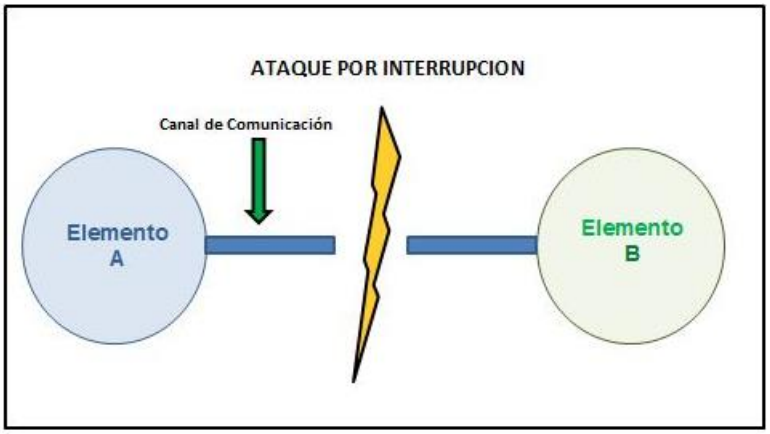
- Amenazas humanas. Las amenazas humanas pueden ser de dos tipos:

a. Por intrusos informáticos, hacker, piratas informáticos, que penetran o ingresan al sistemas en forma remota.
b. Fallos humanos del usuario del sistema de información.

2.3.4 Los ataques informáticos y su clasificación[26]. Los ataques informáticos son los métodos y técnicas utilizados por personas mal intencionadas para violar, control, sabotear, desestabilizar o dañar la seguridad de un sistema informático. Actualmente los ataques se clasifican en tres grandes grupos que son: interrupción, interceptación y modificación**.**

- Ataques de tipo interrupción. Como se puede apreciar en la figura 4, este tipo de ataque ocurre cuando los recursos del sistemas se vuelven en no disponibles, entre otras palabra este tipo de ataques estas destinados a acabar con la disponibilidad del sistema informático.

Figura 4. Ataque por Interrupción.

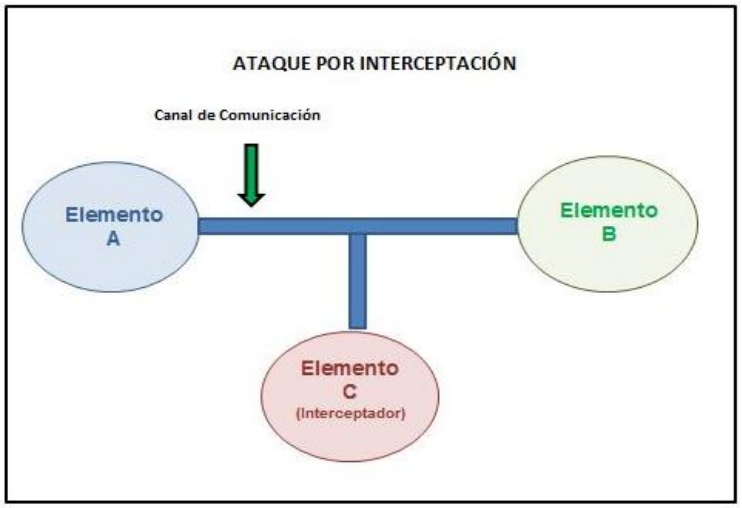


Fuente. GONZALEZ SABABRIA, Yulied y CASTAÑO GALVIS, Wilson. Modulo Curso Fundamentos de Seguridad Informática UNAD. Bucaramanga. 2012. p. 54.

- Ataques de tipo intercepción. En la figura siguiente se puede apreciar que este tipo de ataques se dan cuando una persona mal intencionada consigue acceso a recursos del sistema informático (servidor, dispositivo de comunicación, base de datos, aplicación, entre otros), estos tipos de ataque estas destinado a acabar y entorpecer la confiabilidad del sistemas de información.

[26] GONZALEZ SABABRIA, Yulied y CASTAÑO GALVIS, Wilson. Modulo Curso Fundamentos de Seguridad Informática UNAD. Bucaramanga. 2012. p. 54-56

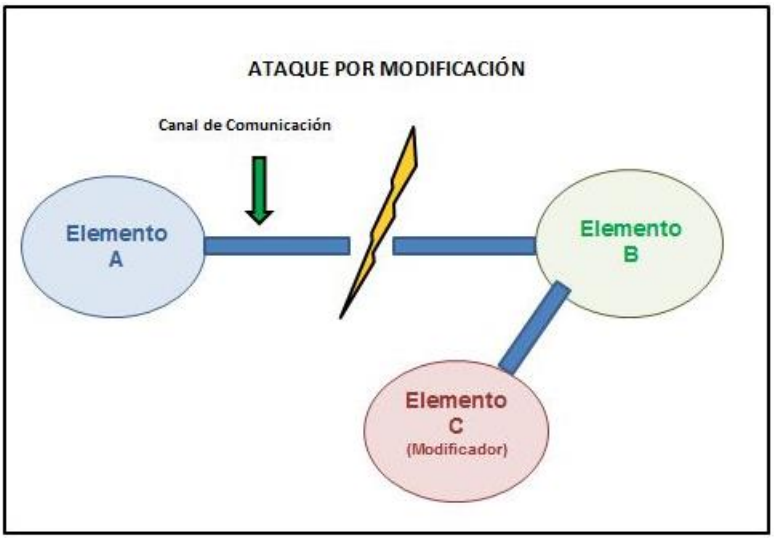
Figura 5. Ataque por Interceptación.



Fuente. GONZALEZ SABABRIA, Yulied y CASTAÑO GALVIS, Wilson. Modulo Curso Fundamentos de Seguridad Informática UNAD. Bucaramanga. 2012. p. 55.

- Ataques de tipo modificación. Este tipo de ataque se da cuando la persona mal intencionada no solo consigue el acceso al sistema de información si no que modifica y manipula los datos e información que en ella se encuentra, como se muestra en la figura siguiente. Este tipo de ataque se da contra la integridad del sistema de información.

Figura 6. Ataque por Modificación.



Fuente. GONZALEZ SABABRIA, Yulied y CASTAÑO GALVIS, Wilson. Modulo Curso Fundamentos de Seguridad Informática UNAD. Bucaramanga. 2012. p. 56.

2.3.5 Tipos de ataques informáticos. En la actualidad existen varios tipos de ataques, dentro de los cuales tenemos:

- **Ingeniería Social**: Este tipo de ataque busca manipular las acciones de las personas con el fin de que ejecuten acciones para que estas revelen los datos necesarios para superar las barreras de seguridad de un sistema de información. Esta es una de las técnicas más utilizadas actualmente para obtener usuarios y claves.

- **Ingeniería Social Inversa:** Consiste en la generación, por parte de los intrusos, de una situación inversa a la originada en la Ingeniería Social.

- En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios y estos lo llaman ante algún imprevisto. El intruso aprovechara esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el suyo propio (la forma de acceso al sistema)[27].

- **Trashing (Cartoneo):** este tipo de ataque ocurre cuando el usuario del sistema anota usuario y clave en un papel o archivo electrónico y este es desechado, teniendo la posibilidad la persona mal intencionada obtener las credenciales de acceso del sistema de información. El Trashing puede ser físico (como el ejemplo anterior) o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc.

- **Ataques de Monitorización:** De este tipo de ataques existen varios, entre los cuales tenemos:

    a. **Shoulder Surfing**: Consiste en espiar físicamente a los usuarios para obtener el usuario y su clave correspondiente, este ataque aprovecha el error de los usuarios de dejar su usuario y contraseña anotados cerca de la computadora.

    b. **Decoy:** Este ataque simula o clona la interfaz gráfica de una página de acceso de una aplicación, en donde se imita la solicitud de un ingreso.

    c. **Scanning:** Este ataque escanea los puertos de escucha como sea posible, con el fin de identificar aquellos canales sucesibles de ser explotados.

[27] Ibid., p. 60

d. **Eavesdropping-Packet Sniffing:** este tipo de ataque busca interceptar el tráfico o los paquetes de una red.

e. **Sniffers:** consiste en colocar la tarjeta de red en un modo llamado promiscuo, el cual desactiva el filtro de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa[28].

- **Ataques de Autenticación:** dentro de esta categoría de ataque se encuentran los siguiente:

  a. **Spoofing-Looping:** Este tipo de ataque consiste en hacerse pasar por otro, algunas de las formas en la que se realiza este tipo de ataque es conseguir el nombre y contraseña de un usuario legitimo para, una vez ingresado al sistema, tomar acciones sobre él, o el envíos de falsos correos electrónicos en donde en nombre de otra persona se envía correo falsos con cualquier motivo y objetivo.

  b. **Spoofing**: Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing[29].

  c. **Web Spoofing:** El caso Web Spoofing el atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta las contraseñas, números de tarjeta de crédito, etc[30].

  d. **IP Splicing-Hijacking:** Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la víctima se identifique ante el sistema y tras ellos se suplanta como usuario autorizado[31].

- **Denial of Service (DoS):** ocurre cuando un servicio que debe estar disponible no lo está.

[28] Ibid., p. 61
[29] Ibid., p. 62
[30] Ibid., p. 63
[31] Ibid., p. 63

- **Ataques de Modificación – Daño:** En este tipo de ataque se encuentra Tampering o Data Diddling, el cual consiste en la modificación desautorizada de los datos o el software instalado en el sistema víctima, incluyendo borrado de archivos.

2.3.6 Riesgos informáticos. Es la probabilidad de ocurrencia de un evento que puede ocasionar un daño potencial a servicios, recursos o sistemas de una empresa. El Análisis de riesgo informático es un proceso busca identificar cada uno de los activos del sistema informático, así como también cada una de las vulnerabilidades y amenazas a los que se encuentran expuestos y la probabilidad de ocurrencia y el impacto que estos causaría en caso que se materialice, con el fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

2.3.7 Técnicas y Procedimientos para la Seguridad de los Datos Las técnicas de protección de datos deben englobar las tres fases del proceso de producción de datos estadísticos: la recogida, el procesamiento o análisis y la difusión. Sin embargo, las más extendidas y desarrolladas se aplican en la última fase del proceso por lo que se denominan Técnicas de Control de la Divulgación Estadística, las cuales se clasifican de una manera casi natural, según el formato en el que los datos son publicados o difundidos. Comúnmente, existen tres principales formas de difundir los datos estadísticos:

- Mediante archivos de registros individuales.
- Mediante Tablas de magnitud o frecuencias.
- Mediante consultas secuenciales en Bases de Datos[32].

2.3.8 Vega. Es una plataforma de software libre, diseñada para realizar y ejecutar pruebas sobre la Seguridad de las páginas WEB. Es una herramienta escrita en JAVA, que puede ser instalada en sistemas operativos como Windows, MAC OS X y Linux. VEGA genera un examen recursivo, controlado y configurable sobre la estructura del sitio. Proporciona información sobre el árbol de directorios y archivos con parámetros POST o GET. Permite realizar escaneos automáticos de sitios web a través de una interfaz gráfica. Para auditorias informáticas puede encontrar y/o detectar vulnerabilidades y realizar pruebas de validación sobre las técnicas de ataque más comunes en entornos WEB. La herramienta se organiza por módulos de ataque, que incluye los ataques consignados en OWASP.

Entre las principales características se encuentran:

[32] VEGA, Jesús Emiro. Modulo Curso Seguridad en Bases de Datos UNAD. Ocaña, Norte de Santander. 2013. p. 43

- Capacidad de realización de Análisis de Vulnerabilidades
- Análisis del Contenido
- Mensajes de notificación personalizables
- Función de manipulación manual de paquetes HTTP mediante interceptación mediante Proxy
- Modelo de datos propio
- API en Javascript personalizable para el desarrollo de complementos y extensiones personalizadas.

2.3.9 Owasp zep attack proxy(ZAP). Es una herramienta de código libre escrita en Java proveniente del Proyecto OWASP. Esta plataforma está especialmente diseñada para monitorizar la seguridad de las aplicaciones web.

Características:

- **Proxy de interceptación:** Configurado de la manera correcta permite ver todo el tráfico entre el navegador y el servidor web, dejando ver las cabeceras y cuerpo de los mensajes HTTP sin importar el método usado (HEAD, GET, POST, etc.) .
- **Spider:** Ayuda a descubrir nuevas URL's en el sitio auditado. Para esto analiza el código HTML de la página para descubrir etiquetas <*a*> y seguir sus atributos *href*.
- **Forced Browsing:** Permite descubrir directorios y archivos no indexados en el sitio como pueden ser páginas de inicio de sesión.
- **Active Scan:** Genera de manera automatizada diferentes ataques web contra el sitio como CSRF,XSS, inyección SQL entre otros.
- Herramienta gratuita y de código abierto.
- **Multiplataforma:** Posibilidad de comprobar todas las peticiones y respuestas entre cliente y servidor.
- **Análisis pasivos:** Capacidad para utilizar certificados SSL dinámicos.
- Análisis de sistemas de autenticación.

2.4 MARCO LEGAL

2.4.1 Ley 1273 de 2009 (Enero 05)[33]**.** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA DECRETA:

Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

Capitulo. I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena

[33] BOGOTA. CONGRESO DE LA REPUBLICA. Ley 1273. (5, enero, 2009) "Por Medio De La Cual Se Modifica El Código Penal, Se Crea Un Nuevo Bien Jurídico Tutelado - Denominado "De La Protección De La Información Y De Los Datos"· Y Se Preservan Integralmente Los Sistemas Que Utilicen Las Tecnologías De La Información Y Las Comunicaciones, Entre Otras Disposiciones. Diario Oficial. 2009. 1-3 p

de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Capitulo. II De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. Circunstancias de mayor punibilidad. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: (...)

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Artículo 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. De los Jueces Municipales. Los jueces penales municipales conocen: (...)

6. De los delitos contenidos en el título VII Bis.

Artículo 4°. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.

2.4.2 Constitución Política de Colombia[34].

Protección a la propiedad intelectual

Artículo 61. El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

2.4.3 Decisión Andina.

DECISIÓN ANDINA 351 DE 1993 RÉGIMEN COMÚN SOBRE DERECHO DE AUTOR Y DERECHOS CONEXOS[35]

Capítulo I Del Alcance De La Protección

Artículo 1. Las disposiciones de la presente Decisión tienen por finalidad reconocer una adecuada y efectiva protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino.

Capítulo II Del Objeto De La Protección

[34] COLOMBIA. . CONSTITUCION POLITICA DE COLOMBIA. Bogota. D.C. 1991
[35] BOLIVIA, COLOMBIA, ECUADOR, PERU. COMUNIDAD ANDINA. Régimen común sobre Derecho de Autor y Derechos conexos. (5, diciembre,1993) Lima. Perú. 1993

Artículo 4. La protección reconocida por la presente Decisión recae sobre todas las obras literarias, artísticas y científicas que puedan reproducirse o divulgarse por cualquier forma o medio conocido o por conocer, y que incluye, entre otras, las siguientes:

a) Las obras expresadas por escrito, es decir, los libros, folletos y cualquier otro tipo de obra expresada mediante letras, signos o marcas convencionales;
b) Las conferencias, alocuciones, sermones y otras obras de la misma naturaleza;
c) Las composiciones musicales con letra o sin ella;
d) Las obras dramáticas y dramático-musicales;
e) las obras coreográficas y las pantomimas;
f) Las obras cinematográficas y demás obras audiovisuales expresadas por cualquier procedimiento;
g) Las obras de bellas artes, incluidos los dibujos, pinturas, esculturas, grabados y litografías;
h) Las obras de arquitectura;
i) Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía;
j) Las obras de arte aplicado;
k) Las ilustraciones, mapas, croquis, planos, bosquejos y las obras plásticas relativas a la geografía, la topografía, la arquitectura o las ciencias;
l) Los programas de ordenador;
ll) Las antologías o compilaciones de obras diversas y las bases de datos, que por la selección o disposición de las materias constituyan creaciones personales.

Artículo 5. Sin perjuicio de los derechos del autor de la obra preexistente y de su previa autorización, son obras del ingenio distintas de la original, las traducciones, adaptaciones, transformaciones o arreglos de otras obras.

Artículo 6. Los derechos reconocidos por la presente Decisión son independientes de la propiedad del objeto material en el cual esté incorporada la obra
.
Artículo 7. Queda protegida exclusivamente la forma mediante la cual las ideas del autor son descritas, explicadas, ilustradas o incorporadas a las obras.

No son objeto de protección las ideas contenidas en las obras literarias y artísticas, o el contenido ideológico o técnico de las obras científicas, ni su aprovechamiento industrial o comercial.

Capítulo III. De Los Titulares De Derechos

Artículo 8. Se presume autor, salvo prueba en contrario, la persona cuyo nombre, seudónimo u otro signo que la identifique, aparezca indicado en la obra.

Artículo 9. Una persona natural o jurídica, distinta del autor, podrá ostentar la titularidad de los derechos patrimoniales sobre la obra de conformidad con lo dispuesto por las legislaciones internas de los Países Miembros.

Capítulo VIII De Los Programas De Ordenador Y Bases De Datos

Artículo 23. Los programas de ordenador se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o código objeto.

En estos casos, será de aplicación lo dispuesto en el artículo 6 bis del Convenio de Berna para la Protección de las Obras Literarias y Artísticas, referente a los derechos morales.

Sin perjuicio de ello, los autores o titulares de los programas de ordenador podrán autorizar las modificaciones necesarias para la correcta utilización de los programas.

Artículo 24. El propietario de un ejemplar del programa de ordenador de circulación lícita podrá realizar una copia o una adaptación de dicho programa siempre y cuando:

a) Sea indispensable para la utilización del programa; o,
b) Sea con fines de archivo, es decir, destinada exclusivamente a sustituir la copia legítimamente adquirida, cuando ésta ya no pueda utilizarse por daño o pérdida.

Artículo 25. La reproducción de un programa de ordenador, incluso para uso personal, exigirá la autorización del titular de los derechos, con excepción de la copia de seguridad.

Artículo 26. No constituye reproducción ilegal de un programa de ordenador, la introducción del mismo en la memoria interna del respectivo aparato, para efectos de su exclusivo uso personal.

No será lícito, en consecuencia, el aprovechamiento del programa por varias personas, mediante la instalación de redes, estaciones de trabajo u otro procedimiento análogo, sin el consentimiento del titular de los derechos.

Artículo 27 No constituye transformación, a los efectos previstos en la presente Decisión, la adaptación de un programa realizada por el usuario para su exclusiva utilización.

Artículo 28. Las bases de datos son protegidas siempre que la selección o disposición de las materias constituyan una creación intelectual. La protección concedida no se hará extensiva a los datos o información compilados, pero no afectará los derechos que pudieran subsistir sobre las obras o materiales que la conforman.

2.4.4 Ley No. 23 de 1982 (enero 28) [36].

Sobre derechos de autor, el Congreso de Colombia decreta:

Capítulo III De Las Limitaciones Y Excepciones Al Derecho De Autor

Artículo 31. Es permitido citar a un autor transcribiendo los pasajes necesarios, siempre que éstos no sean tantos y seguidos que razonablemente puedan considerarse como una reproducción simulada y sustancial, que redunde en perjuicio del autor de la obra de donde se toman. En cada cita deberá mencionarse el nombre del autor de la obra citada y el título de dicha obra.

Cuando la inclusión de obras ajenas constituya la parte principal de la nueva obra, a petición de parte interesada, los tribunales fijarán equitativamente y en juicio verbal la cantidad proporcional que corresponda a cada uno de los titulares de las obras incluidas.

2.4.5 Políticas de Seguridad de la Universidad Nacional Abierta y a Distancia UNAD [37]. La Universidad Nacional Abierta y a Distancia (UNAD) es un ente universitario autónomo del orden nacional, con régimen especial, cuyo objeto principal es la educación abierta y a distancia, vinculado al Ministerio de Educación Nacional.

La Universidad mediante Resolución 004256 del 3 de marzo de 2015, define las políticas en cuanto a Seguridad de la Información.

RESOLUCION 004256 DEL 3 DE MARZO DE 2015

Por la cual se define las políticas del Marco de Referencias del SGSI.

[36] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley No. 23. (28, enero, 1982). Sobre Derechos de autor. Diario Oficial. Bogota, D.C., 1982. p. 12.
[37] UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD. Resolución 004256. (3, marzo, 2015). Por la cual se define las políticas del Marco de Referencias del SGSI. Bogotá. 2015

EL RECTOR DE LA UNIVERSIDAD NACIONAL

ABIERTA Y A DISTANCIA-UNAD

En uso de sus atribuciones legales y estatutarias y,

CONSIDERANDO:

Que la Universidad Nacional Abierta y a Distancia (UNAD), creada por la ley 52 de 1981, transformada por la ley 396 de 1997 y Decreto 2770 del 16 de agosto de 2006, es un ente universitario autónomo del orden nacional, con régimen especial, personería jurídica, autónoma académica, administrativa y financiera, patrimonio independiente y capacidad para gobernarse, vinculado al Ministerio de Educación Nacional en los temimos definidos en la ley 30 de 1992

Que el Articulo 28, de la ley 30 de 1992, establece que: "*La autonomía universitaria consagrada en la Constitución Política de Colombia y de conformidad con la presente ley, reconoce a las universidades el derecho a darse y modificar sus estatutos, designar sus autoridades académicas y administrativas, crear, organizar y desarrollar sus programas académicos, definir y organizar sus labores formativas, académicas, docentes, científicas y culturales, otorgar los títulos correspondientes, seleccionar a sus profesores, administrar a sus alumnos y adoptar sus correspondientes regímenes y establecer, arbitrar y aplicar sus recursos para el cumplimiento de su misión social y de su función institucional* ".

Que la UNAD tiene como misión contribuir a la educación para todo a través de la modalidad abierta y a distancia, mediante la investigación pedagógica, la proyección social y las innovaciones metodológicas didácticas, con la utilización de las tecnológicas de la información y de las comunicaciones para fomentar y acompañar el aprendizaje autónomo, generador de cultura y espíritu emprendedor, que en el marco de la sociedad global y del conocimiento propicie el desarrollo económico, social y humano sostenible de las comunidades locales, regionales y globales con calidad, eficiencia y equidad social.

Que mediante Resolución No. 004815 del 27 de agosto de 2012, derogada por la Resolución No. 6018 del 5 de diciembre de 2012, se establecieron las políticas de clasificación y el manejo de la información confidencial en la UNAD.

Que mediante Resolución No. 0047793 del 22 de agosto de 2013, se establecieron las políticas de seguridad de la información en la UNAD.

Que mediante Resolución No. 7966 del 16 de Octubre de 2014, modificatoria de la Resolución No. 006858 del 22 de Agosto de 2014 la UNAD, se conformó el sistema Integrado de Gestión, y en el mismo se constituyeron el Componente de Gestión de la Seguridad de la Información y el Componente de gestión de Servicios de Infraestructura Tecnológica.

Que la UNAD para satisfacer su creciente demanda educativa, ha aumentado su inventario tecnológico tanto en hardware, software e información, por lo que se hace necesario crear una Política de Seguridad de la Información, basada en las normas ISO 27001:2013, desde la cual se asegure el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejoras de Sistemas de Gestión de la Seguridad de la Información (SGSI).
En mérito de lo expuesto,

RESUELVE:

CAPÍTULO VI
POLÍTICA DE DESARROLLO SEGURO

Artículo 35. Las solicitudes de desarrollos nuevos o modificación de las aplicaciones actualmente instaladas que se encuentran en producción, deben ser elevadas por líder de cada unidad ante la GIDT durante los primeros quince días de cada trimestre (es decir los meses enero, abril, julio y octubre). Las solicitudes realizadas en el tiempo estipulado, serán sometidas a un proceso de verificación y posterior aprobación o rechazo de la solicitud. La decisión tomada, será corroborada por el Gerente de Innovación y Desarrollo Tecnológico, quien comunicara al solicitante para que realice las acciones pertinentes.
Parágrafo. En caso que la solicitud sea extemporánea, será incluida en las solicitudes del siguiente periodo de recepción.

Artículo 36. La GIDT es la única unidad encargada de la realización de desarrollos dentro de la Universidad y dará cumplimiento a los lineamientos de construcción de aplicaciones seguras adoptados por la Universidad a través de esta gerencia.
Parágrafo. La UNAD apoyará la debida aplicación de los lineamientos de desarrollo mediante la facilitación de elementos y ambientes de trabajo adecuados para el equipo de desarrollo de la UNAD.

Artículo 37. Queda prohibido el acceso y/o uso de los recursos físicos y/o tecnológicos a personal no autorizado y en general, a los recursos asignados al grupo de desarrollo de la GIDT. El intento de uso total o parcial de código fuente de aplicaciones administradas y/o adquiridas por parte de personal no autorizado queda expresamente prohibido.

Artículo 38. Con el fin de garantizar la seguridad, estabilidad y usabilidad de las soluciones, todos los desarrollos nuevos o modificaciones a desarrollo existentes, se deben realizar de conformidad con el “Instructivo de Prueba de Software de la GIDT”.
Parágrafo. Las áreas solicitantes de desarrollos nuevos o modificaciones a desarrollos ya existentes, deben asignar a funcionarios idóneos para colaborar en la realización y aprobación de los resultados de dichas pruebas.

Artículo 39. Las solicitudes de desarrollo o modificaciones de aplicaciones que no pueden ser atendidas por la oficina GIDT, se regirán por el procedimiento de “Contratación de bienes y servicios” vigente en la UNAD.

CAPÍTULO IX
POLÍTICA DE VERSIONES

Artículo 48. La GIDT es la responsabilidad de gestionar la implementación, prueba y despliegue de versiones y de versiones emergencia, así como de realizar la entrega de nuevas funcionalidades, cambios o servicios nuevos sin afectar la integridad de los servicios ya existentes.

La gestión debe contemplar que todas las versiones aprobadas e implementadas pueden ser probadas, verificadas, desplegadas en producción (Instaladas) y retiradas (o desinstaladas) cuando sea necesario.

Artículo 49. La GIDT será la responsable de definir los planes de pruebas e implementación de los servicios nuevos o mejorados con cada uno de sus interesados.
Parágrafo 1. El gerente de Innovación y Desarrollo Tecnológico o su delegado será el responsable de aprobar cada uno de estos planes con apoyo del líder de equipo interno de trabajo encargado de realizar el despliegue.
Parágrafo 2. La solicitud de la nueva versión deberá documentarse utilizando los lineamientos definidos en el procedimiento de Gestión de Cambios y Despliegue del Servicio y Despliegue del Servicio y su verificación y aceptación formal estará a cargo del gerente de Innovación y Desarrollo Tecnológico o su delegado, el líder de equipo interno de trabajo encargado de realizar el despliegue y el usuario solicitante del cambio.

Artículo 50. La GIDT se encargará de implementar los repositorios, medios y herramientas seguras, para realizar la gestión y el control de las versiones de manera eficiente y respetando los medios de identificación definidos para su manejo y trazabilidad.

CAPÍTULO XII
APLICABILIDAD

Artículo 80. El contenido de este documento aplica a todos los procesos y procedimientos que conforman el Sistema Integrado de Gestión de la Universidad, así como a todas las actuaciones administrativas que desarrollen las distintas unidades, por intermedio de sus administrativos, contratistas y/o docentes.

Artículo 81. Se sancionará disciplinaria, administrativa, civil y/o penalmente a toda persona que viole las disposiciones del presente documento de conformidad con lo establecido en los reyes colombianas vigentes.

2.4.6 Las leyes SOPA y PIPA[38].

Los proyectos de ley Stop Online Piracy Act y Protect Intelectual Property Act están pendientes de aprobación en el Congreso y el Senado respectivamente y tienen como objetivo terminar con la piratería y el robo de material protegido por derechos de autor.

Apartados clave de la ley SOPA

1. Imponen a los proveedores de internet ejercer de "*vigilantes*" para detectar las páginas que compartan contenido ilegal y les otorga inmunidad a los proveedores de internet si bloquean portales de usuarios que no hayan cometido delito.

2. El Gobierno podrá cerrar páginas alojadas en EE UU y que permitan las descargas de contenido protegido por derechos de autor, violando por tanto la propiedad intelectual, aunque sus dueños residan en el extranjero.

3. El Departamento de Justicia podrá cerrar páginas web sin orden judicial así como impedir que cobren beneficios de anunciantes, bloquear dominios de internet y hacer que buscadores como Google eliminen esas páginas de los resultados de búsqueda.

4. El Gobierno de EE UU podrá impedir el uso de las herramientas empleadas por ciudadanos de China o Irán para burlar la censura.

¿Qué significaría en la práctica?

[38] PEREDA, Cristina. Las Claves de las leyes SOPA y PIPA. Periódico El País. Oct 2012. Tecnología. Disponible en internet en http://tecnologia.elpais.com/tecnologia/2012/01/19/actualidad/1326967261_850215.html

La ley responsabilizaría a aquellos buscadores, portales y páginas que publiquen links a contenido protegido y otras webs de descargas. Mediante una orden judicial, cualquier productora de cine que descubra que una página ofrece copias ilegales de sus películas, podría obligar a Google a eliminarla de los resultados del buscador.

Sitios como Facebook, YouTube o Flickr deberían responder por el contenido que recomienden los usuarios en cuanto haya sospecha de que viola la propiedad intelectual. Los usuarios, por tanto, serían responsabilizados al compartir-en páginas personales, redes sociales y correos electrónicos- links a webs que alojen copias ilegales, aunque no las hayan hecho ellos mismos ni se beneficien económicamente de su distribución.
A favor y en contra

2.4.7 Ley 599 de 2000[39]

EL CONGRESO DE COLOMBIA

Por la cual se expide el Código Penal

EL CONGRESO DE COLOMBIA

DECRETA:

ARTICULO 270. (Modificado por el artículo 14 de la Ley 890 de 2004). VIOLACIÓN A LOS DERECHOS MORALES DE AUTOR. Incurrirá en prisión de treinta y dos (32) a noventa (90) meses y multa de veinte seis punto sesenta y seis (26.66) a trescientos (300) salarios mínimos legales mensuales vigentes quien:

1. Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.

2. Inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

[39] COLOMBIA. CONGRESO DE COLOMBIA. Ley 599 (24, julio, 2000). Por la cual se expide el Código Penal. Diario Oficial. Bogotá, D.C.

3. Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

PARAGRAFO. Si en el soporte material, carátula o presentación de una obra de carácter literario, artístico, científico, fonograma, videograma, programa de ordenador o soporte lógico, u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho, en los casos de cambio, supresión, alteración, modificación o mutilación del título o del texto de la obra, las penas anteriores se aumentarán hasta en la mitad.

ARTICULO 271. (Modificado por el artículo 2 de la Ley 1032 de 2006).VIOLACIÓN A LOS DERECHOS PATRIMONIALES DE AUTOR Y DERECHOS CONEXOS. Incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26.66) a mil (1.000) salarios mínimos legales mensuales vigentes quien, salvo las excepciones previstas en la ley, sin autorización previa y expresa del titular de los derechos correspondientes:

1. Por cualquier medio o procedimiento, reproduzca una obra de carácter literario, científico, artístico o cinematográfico, fonograma, videograma, soporte lógico o programa de ordenador, o, quien transporte, almacene, conserve, distribuya, importe, venda, ofrezca, adquiera para la venta o distribución, o suministre a cualquier título dichas reproducciones.

2. Represente, ejecute o exhiba públicamente obras teatrales, musicales, fonogramas, videogramas, obras cinematográficas, o cualquier otra obra de carácter literario o artístico.

3. Alquile o, de cualquier otro modo, comercialice fonogramas, videogramas, programas de ordenador o soportes lógicos u obras cinematográficas.

4. Fije, reproduzca o comercialice las representaciones públicas de obras teatrales o musicales.

5. Disponga, realice o utilice, por cualquier medio o procedimiento, la comunicación, fijación, ejecución, exhibición, comercialización, difusión o distribución y representación de una obra de las protegidas en este título.

6. Retransmita, fije, reproduzca o, por cualquier medio sonoro o audiovisual, divulgue las emisiones de los organismos de radiodifusión.

7. Recepcione, difunda o distribuya por cualquier medio las emisiones de la televisión por suscripción

ARTICULO 272. (Modificado por el artículo 3 de la Ley 1032 de 2006). VIOLACIÓN A LOS MECANISMOS DE PROTECCIÓN DE DERECHO DE AUTOR Y DERECHOS CONEXOS, Y OTRAS DEFRAUDACIONES

.

Incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26.66) a mil (1.000) salarios mínimos legales mensuales vigentes, quien:

1. Supere o eluda las medidas tecnológicas adoptadas para restringir los usos no autorizados.

2. Suprima o altere la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada.

3. Fabrique, importe, venda, arriende o de cualquier forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal; o, de cualquier forma, eluda, evada, inutilice o suprima un dispositivo o sistema, que permita a los titulares del derecho controlar la utilización de sus obras o fonogramas, o les posibilite impedir o restringir cualquier uso no autorizado de estos.

4. Presente declaraciones o informaciones destinadas directa o indirectamente al pago, recaudación, liquidación o distribución de derechos económicos de autor o derechos conexos, alterando o falseando, por cualquier medio o procedimiento, los datos necesarios para estos efectos

Decreto 1070 de 2008 “Por el cual se reglamenta el artículo 26 de la Ley 98 de 1993”.	Se mantiene el contenido
Decreto 4540 de 2006 Por medio del cual se adoptan controles en aduana, para proteger la Propiedad Intelectual.	Se mantiene el contenido
Decreto 2041 de 1991 “Por el cual se crea la Dirección Nacional del Derecho de Autor como Unidad Administrativa Especial, se establece su estructura orgánica y se determinan sus funciones”.	Se mantiene el contenido
Decreto 1278 de 1996 “Por el cual se fija la estructura interna de la Dirección Nacional de Derecho de Autor y se establecen sus funciones”.	Se mantiene el contenido
Decreto 1360 de 1989 “Por el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor” .	Se mantiene el contenido
Decreto 162 de 1996 “Por el cual se reglamenta la Decisión Andina 351 de 1993 y la Ley 44 de 1993, en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos”.	Se mantiene el contenido
Decreto 460 de 1995 “Por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal”.	Se mantiene el contenido

3. METODOLOGÍA

2.5 LÍNEA DE INVESTIGACIÓN[40]

Teniendo en cuenta las líneas de investigación ofrecidas por la escuela ECBTI (Escuela de Ciencias Básica, Tecnología e Ingenierías), para el desarrollo de este proyecto se aplicara la línea de gestión de sistemas del área de la ciencia de la computación, el cual según Salazar (1999), está orientada a integrar, planificar y controlar los aspectos técnicos, humanos, organizativos, comerciales y sociales del proceso completo, empezando con el análisis del dominio del problema, continuando con el diseño de alternativas de solución y finalizando con la operatividad de un sistema. La idea de esta línea es partir conceptualización se pueda evaluar la situación actual y las perspectivas de los procesos para hacerlos más eficientes y dinámicos, a partir de la investigación aplicada, impulsada por la investigación inductiva y participativa.

Esta metodología plantea instrumentos de recolección de información acordes a las interconexiones de las diferentes categorías de análisis y se definirán las fuentes primarias y secundarias que conducen a la apropiación del conocimiento de los diversos ámbitos de indagación de la región. Dentro de este contexto y con la implementación de los observatorios regionales, con el apoyo de los grupos de investigación, se generaran diversos productos para optimización de procesos a través de proyectos investigativos específicos. La investigación aplicada en sinergia con la investigación participativa e inductiva, permitirá a la línea realizar proyectos que podrán ser demostrados en la práctica.

2.6 MODELOS DE SEGURIDAD INFORMÁTICA[41]

2.6.1 ISO 27001. Es la norma principal de la serie ISO/EIC 27000 y se puede aplicar a cualquier tipo de organización, sin importar su tamaño o su actividad comercial. La norma contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información, documentado dentro del contexto global de los riesgos de negocio de la organización.

La norma ISO 27001, recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los registros que permiten evidenciar el

[40] GÓMEZ, Margarita, *et al.* LA INVESTIGACIÓN CIENCIAS EN LA ESCUELA DE BÁSICAS, TECNOLOGÍA E INGENIERÍA. Bogotá. 2011

[41] RAMÍREZ VILLEGAS, Gabriel y CONSTAIN MORENO, Gustavo. Módulo Curso MODELOS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA UNAD. Palmira. 2012

buen funcionamiento del sistema. Asimismo, especifica los requisitos para implantar controles y medidas de seguridad adaptados a las necesidades de cada organización. Esta además, es la norma con la que se certifican los Sistemas de Gestión de Seguridad de la Información de las organizaciones que lo deseen.

El objetivo de esta norma es el mejoramiento continuo del sistema de gestión de seguridad de la información a través de la adopción del modelo Plan-Do-CheckAct (PDCAO Ciclo de Deming) para todos los procesos de la organización. Estas siglas obedecen a las siguientes fases:

Fase de Planificación (Plan) [Establecer el SGSI]: Establecer la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo y mejorar la seguridad de la información de la organización para ofrecer resultados de acuerdo con las políticas y objetivos generales de la organización.

Fase de Ejecución (Do) [Implementar y gestionar el SGSI]: Implementar y gestionar el SGSI de acuerdo a su política, controles, procesos y procedimientos.
Fase de Seguimiento (Check) [Monitorizar y revisar el SGSI]: Medir y revisar las prestaciones de los procesos del SGSI.

Fase de Mejora (Act) [Mantener y mejorar el SGSI]: Adoptar acciones correctivas y preventivas basadas en auditorías y revisiones internas o en otra información relevante a fin de alcanzar la mejora continua del SGSI.

Justificación del modelo: El proyecto ASEGURA, está plasmado sobre la teoría por lo tanto este modelo de seguridad anteriormente detallado permite enmarcar todo el proceso que se requiere en este proyecto comenzando por la etapa de planeación, en donde se encuentra actualmente, permitirá seguir con la ejecución, el seguimiento y la fase de retroalimentación con acción brindando las mejoras que vayan siendo requeridas, en el caso planteado se contempla la posibilidad de desarrollar la implementación del proyecto por etapas, este modelo brinda la opción de estar complementando y mejorando constantemente el sistema de seguridad desarrollado.

2.7 ESTÁNDARES DE SEGURIDAD INFORMÁTICA[42]

Un estándar es la radicación y aprobación de normas, con el fin de garantizar la calidad y la seguridad de funcionamiento. Por tal fin para este proyecto se emplearan el estándar Common Criteria CC, que permite identificar y definir los requisitos de seguridad, además de crear y desarrollar dos tipos de documentos que son el Perfil de protección (Protection Profile o PP) y Objetivo de seguridad

[42] Ibid, p 40-45

(Security Target o ST), después de identificados los requisitos de seguridad se aplica el estándar OSSTMM ("Open Source Testing Methodology"), el cual es una metodología abierta para pruebas de seguridad, enfocada específicamente en los detalles técnicos a comprobar, qué vigilar durante el proceso de comprobación desde la preparación hasta la evaluación post comprobación y, sobre todo, en cómo deben ser medidos y evaluados los resultados.

OSSTMM se puede integrar con ISMS (Del Inglés Information Security Management System, Sistema de Administración de Seguridad de la Información) y permitir implementar una gestión de riesgos más confiable y un análisis de compatibilidad mejor y más rentable.

2.8 METODOLOGÍAS DE ANÁLISIS DE SEGURIDAD WEB

Las aplicaciones web pueden ser analizadas utilizando distintos enfoques, para el caso en estudio se realizará bajo el enfoque Black box, en el cual, el analista de seguridad posee únicamente acceso a la aplicación. Tiene como ventajas la simplicidad, menor tiempo de testing y provee un enfoque real, ya que se posee el mismo nivel de conocimiento sobre la aplicación que un potencial intruso.

Como desventajas están: Vulnerabilidades trivialmente detectables con white box testing, no pueden ser detectadas con este enfoque.
(if user == 'tester002' and password == 'backdoor__')
No se aprovecha el código fuente de la aplicación a favor de la seguridad de la misma.

2.9 MAGERIT

Estándar utilizado para el análisis de riesgos informáticos, que estudia los riesgos que soporta un sistema de información y el entorno asociado a él, por lo que busca evaluar el impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados. Los resultados del proceso de análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios[43].

Como se ha venido diciendo, existen muchas personas mal intencionadas que desean obtener, estropear, eliminar, modificar y dañar la información de una

[43] BENAVIDES RUANO, Mirian y SOLARTE SOLARTE, Francisco. Módulo Curso Modelo riesgos y control informático. Pasto. 2012.

empresa, para evitar estos, las empresas utilizan varias estrategias que le permitan asegurar sus elementos más precisado y dentro de esto está la información, los equipos que los contiene y por donde se transportan. Una de las técnicas utilizadas por las empresas es la de utilizar e implementar Sistemas de Gestión de Seguridad Informática que garanticen y preserven la confidencialidad, integridad, disponibilidad y autenticidad de los datos, para ello realizan análisis de riesgos que permitan identificar las causas de las posibles amenazas y eventos no deseados que se pueden materializar, identificando las vulnerabilidades de los activos de información y las posibles herramientas que puedan explotar dichas vulnerabilidades. No está demás aclarar que una vez identificadas las vulnerabilidades y amenazas se podrán realizar acciones preventivas y correctivas que garanticen mayores niveles de seguridad en su información, y que con una gestión bien aplicada e implementada se puedan mitigar los riesgos a niveles permisibles.

Para determinar cuáles son los riesgos, potenciales que se pueden materializar por la utilización del SIREP, se implementará un procesos de análisis y pruebas a los sistemas y demás activos de información, procurando identificar todas las actividades que permitan obtener información clara y oportuna del manejo en la seguridad que se le da a los activos ya mencionados, y los agujero encontrados con las pruebas y análisis realizados.

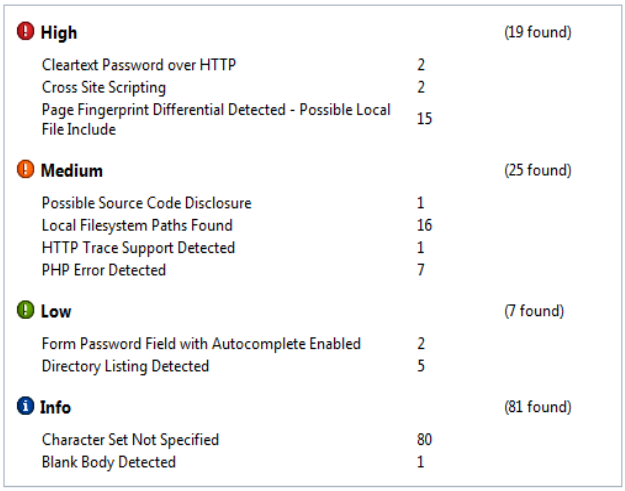
4. ANALISIS DE VULNERABILIDAD EN EL APLICATIVO SIREP, MEDIANTE EL USO DE LAS HERRAMIENAS VEGA DE SUBGRAP Y OWASP ZAP 2.4.0

Para la identificación de las vulnerabilidades del Aplicativo SIREP (Sistema Integral de Registro de Educación Permanente), se basó en las herramientas de escaneo VEGA y ZAP OWASP ATTACK, las cuales permiten realizar un análisis detallado de cada una de las páginas que conforman la aplicación, teniendo en cuenta el lenguaje en que está desarrollada la aplicación y el código fuente de la misma.

4.1 VULNERABILIDADES DEL SIREP IDENTIFICADAS CON LA APLICACIÓN VEGA

Una vez se ha configurado la aplicación VEGA y realizado el proceso de escaneo de las páginas de la Aplicación SIREP (Ver Anexo A), se muestran las vulnerabilidades encontradas, clasificadas según su nivel de riesgo, como se muestra en la siguiente figura.

Figura 7. Resultado de escáner con Vega.



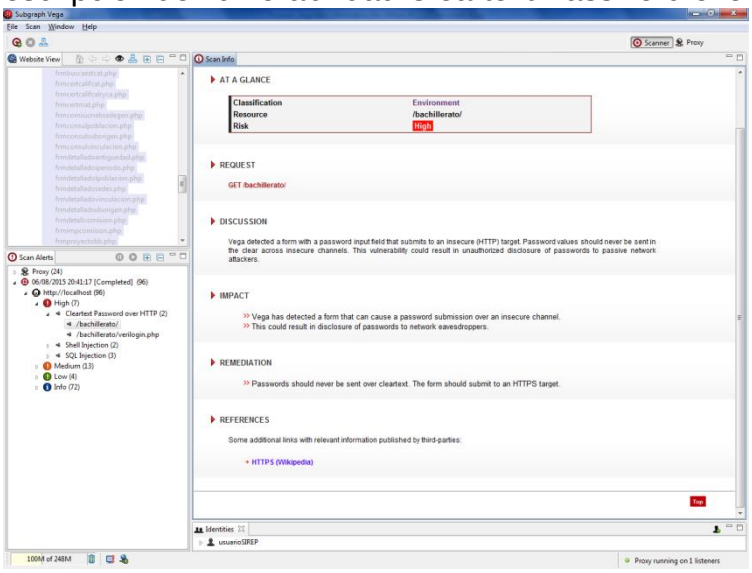
Fuente. Propiedad de los autores.

4.1.1 Cleartext Password over HTTP. (Contraseñas sin cifrado en HTTP).

Descripción: La aplicación detectó que en dos formularios que solicitan introducir una contraseña para poder entrar, estos dos campos son objetivos HTTP inseguros. Las contraseñas nunca deben ser enviadas en texto en claro a través

de canales inseguros. Esta vulnerabilidad podría dar lugar a la divulgación no autorizada de las contraseñas a los atacantes de red pasivos. Ver figura 8.

Figura 8. Descripción de vulnerabilidad Cleartext Password over HTTP.



Fuente. Propiedad de los autores

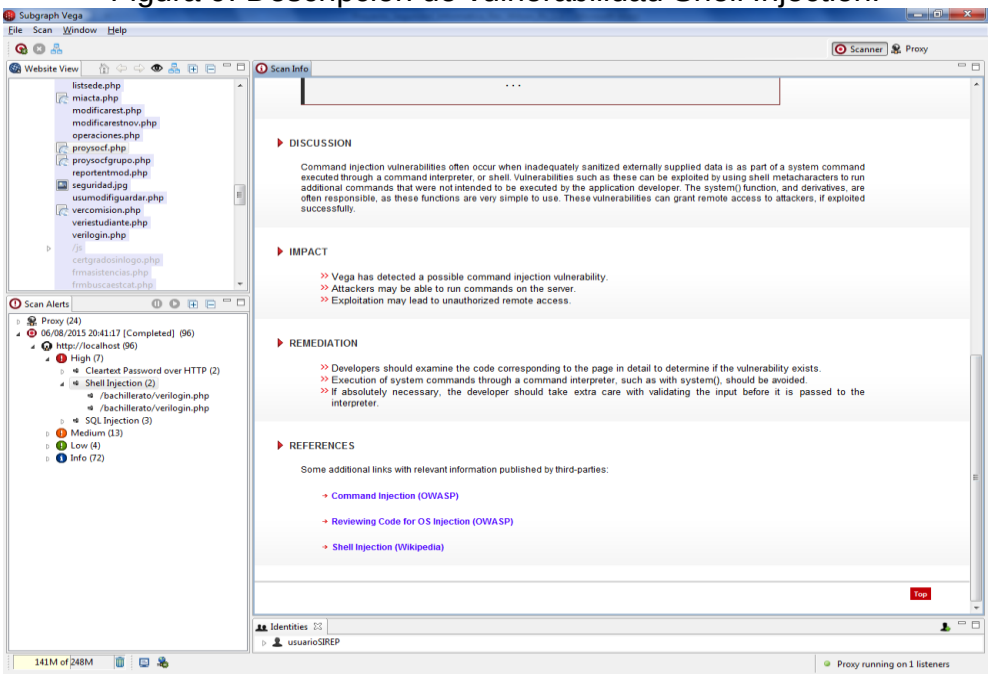
Páginas que presentan la vulnerabilidad:

- /bachillerato/
- /bachillerato/verilogin.php

4.1.2 Shell Injection. (Inyecciones de intérprete de comandos)

Descripción: Las vulnerabilidades Command injection (Inyección de Comandos) a menudo ocurren cuando se desinfectan inadecuadamente datos externos que hacen parte de un sistema de comandos que son ejecutados a través de un intérprete de comandos o Shell, como se aprecia en la figura 9. Las vulnerabilidades de este tipo pueden ser explotadas usando meta caracteres del Shell para correr comandos adicionales los cuales no estaban destinados para ser ejecutados por la aplicación. La función system() y sus derivaciones, son a menudo las responsables de que esto ocurra ya que son funciones muy fáciles de usar.

Figura 9. Descripción de vulnerabilidad Shell Injection.



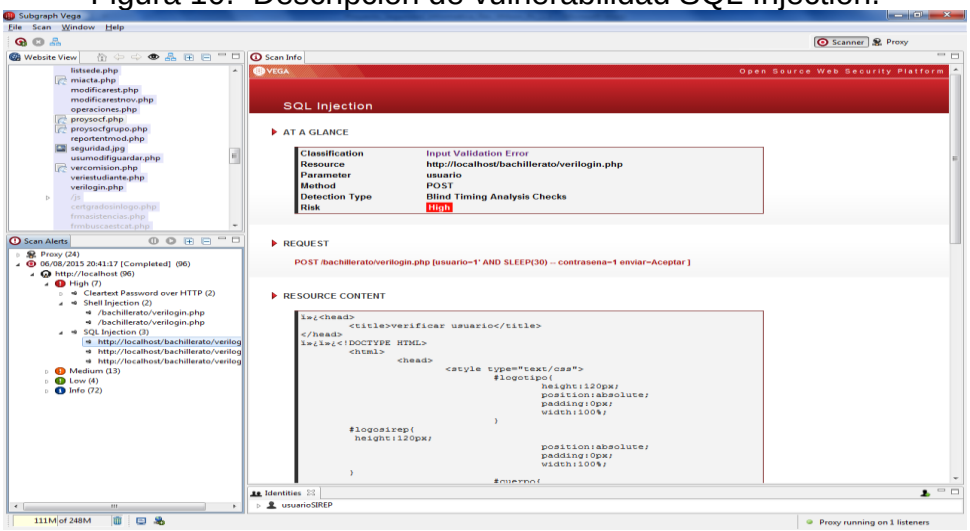
Fuente. Propiedad de los autores

Páginas que presentan la vulnerabilidad:

- /bachillerato/verilogin.php

4.1.3 SQL Injection. (Inyección SQL)

Figura 10. Descripción de vulnerabilidad SQL Injection.



Fuente. Propiedad de los autores

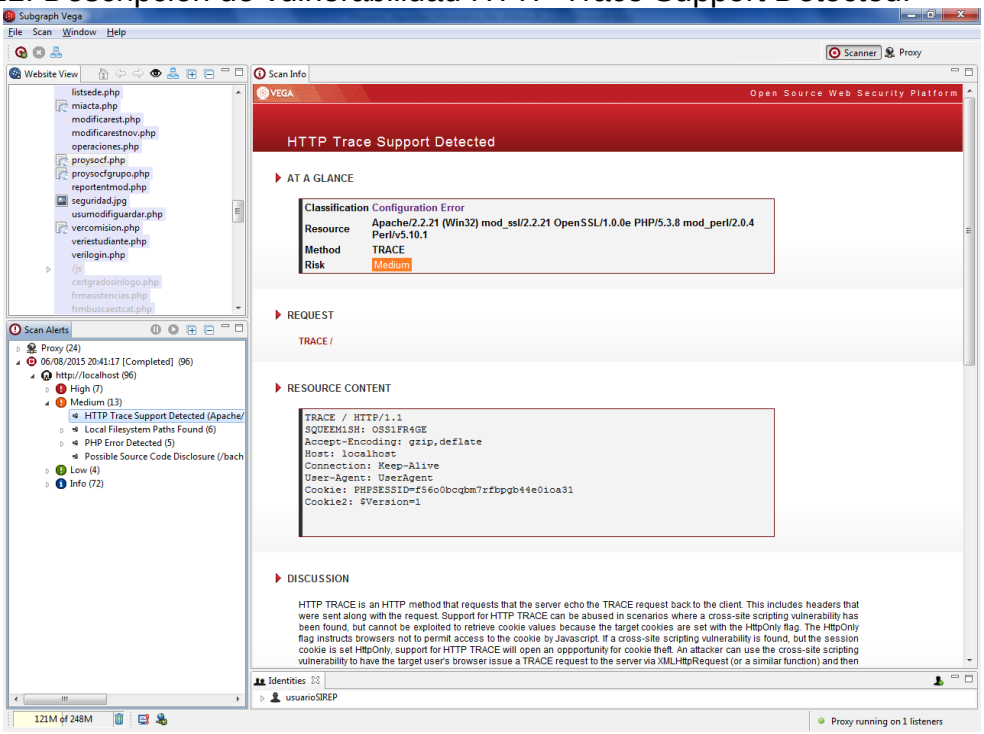
Descripción: Este tipo de vulnerabilidad se presenta cuando se utilizan parámetros externos para construir una sentencia SQL. Si no se toman precauciones los parámetros externos de entrada (con cabeceras GET o POST) pueden modificar una consulta, con lo cual pueden obtener acciones mal intencionadas, tales como permisos no autorizados de escritura o lectura sobre la base de datos o modificar la lógica de la aplicación. Ver figura anterior.

Páginas que presentan la vulnerabilidad:

- http://localhost/bachillerato/verilog.php.

4.1.4 HTTP Trace Support. (Soporte de rastreo HTTP)

Figura 11. Descripción de vulnerabilidad HTTP Trace Support Detected.



Fuente. Propiedad de los Autores

Descripción: El método HTTP TRACE es un método HTTP que devuelve al cliente las peticiones realizadas al servidor. Esto incluye también a las cabeceras. Se puede abusar del soporte para HTTP TRACE en escenarios donde existan vulnerabilidades Cross-site scripting, pero no puede ser explotada para obtener los valores de las cookies, puesto que las cookies objetivo se establecen con la bandera HttpOnly. La bandera HttpOnly en los navegadores no permite el acceso

a una cookie mediante Javascript. Si una vulnerabilidad Cross-site Scripting es encontrada, pero la cookie de una sesión está establecida con HttpOnly, el soporte para HTTP TRACE abrirá una oportunidad para robo de la cookie. Un atacante puede usar la vulnerabilidad Cross-site Scripting para poder en el navegador de un usuario-objetivo emitir una petición TRACE al servidor a través de XMLHttpRequest (o cualquier función similar) y luego recuperar la cookie de la respuesta, la cual contiene la petición que fue enviada por el navegador incluyendo las cookies. Esto se puede apreciar en la figura anterior.

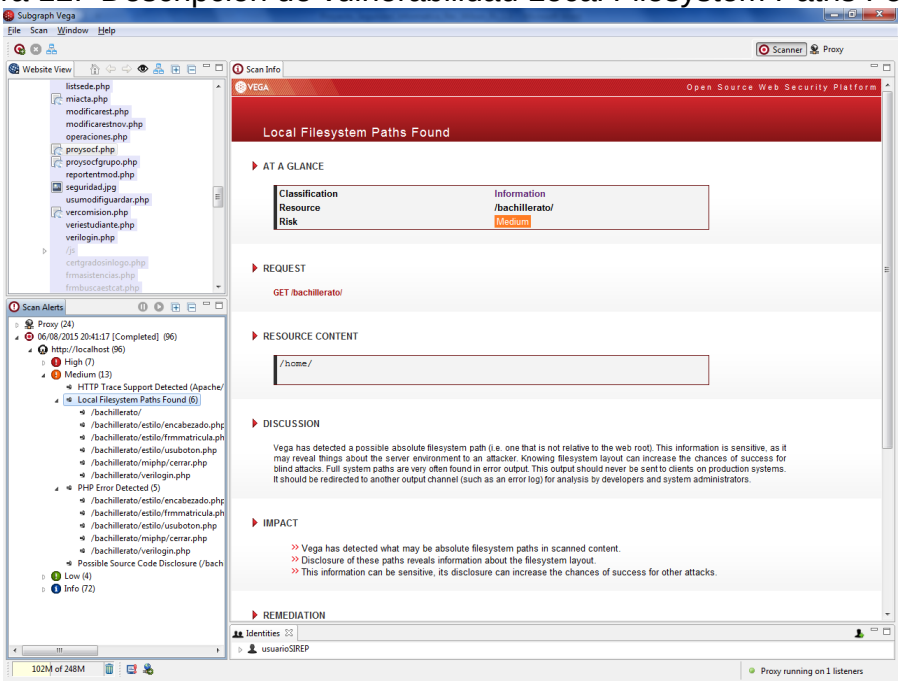
4.1.5 Local Filesystem Paths Found. (Rutas del Sistema de archivos encontradas)

Descripción: La aplicación ha detectado una posible ruta de sistema de archivos absoluta (es decir, una que no es relativa a la ruta raíz de la página web). Esta información es sensible, ya que puede revelar aspectos sobre el entorno de servidor a un atacante. Conocer la disposición del sistema de archivos puede aumentar las posibilidades de éxito para ataques a ciegas. Cuando se producen mensajes de error en la aplicación, aparece la ruta completa de los archivos del sistema. Esta información no debe ser enviada a los clientes de las aplicaciones. En vez de esto, deben ser redirigidas a otros canales de salidas (por ejemplo, un registro de errores) para su análisis por los desarrolladores y administradores de sistemas. Ver figura 12.

Páginas que presentan la vulnerabilidad:

/bachillerato/califeval.php
/bachillerato/estilo/encabezado.php
/bachillerato/estilo/frmmatricula.php
/bachillerato/estilo/usuboton.php
/bachillerato/export_excel/exportexceantiguedad.php
/bachillerato/export_excel/exportexcelperiodo.php
/bachillerato/export_excel/exportexcelsedes.php
/bachillerato/export_excel/exportexcesuborigen.php
/bachillerato/export_excel/exportexcetipopob.php
/bachillerato/export_excel/exportexcetipovin.php
/bachillerato/export_excel/exportexcevinculacion.php
/bachillerato/export_excel/expotexcelcomision.php
/bachillerato/miphp/cerrar.php
/bachillerato/proysoc.php
/bachillerato/verilogin.php

Figura 12. Descripción de vulnerabilidad Local Filesystem Paths Found.



Fuente. Propiedad de los Autores.

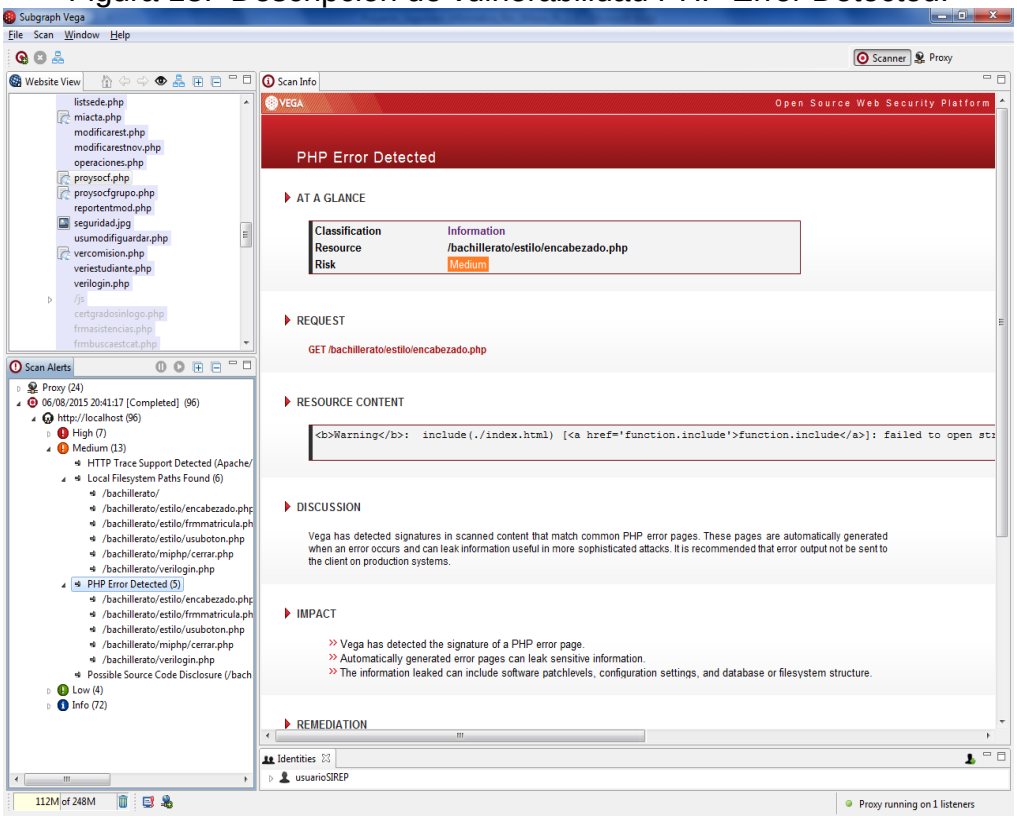
4.1.6 PHP Error Detected. (Detección de Errores PHP)

Descripción: Se han encontrado firmas en el contenido escaneado, que corresponden a páginas de errores de PHP. Estas páginas se generan automáticamente cuando se produce un error y puede filtrar información útil en ataques más sofisticados. Se recomienda que la salida de error no se envíe al cliente en sistemas de producción. Ver figura 13.

Páginas que presentan la vulnerabilidad:

/bachillerato/estilo/encabezado.php
/bachillerato/estilo/frmmatricula.php
/bachillerato/estilo/usuboton.php
/bachillerato/miphp/cerrar.php
/bachillerato/proysoc.php
/bachillerato/verilogin.php

Figura 13. Descripción de vulnerabilidad PHP Error Detected.

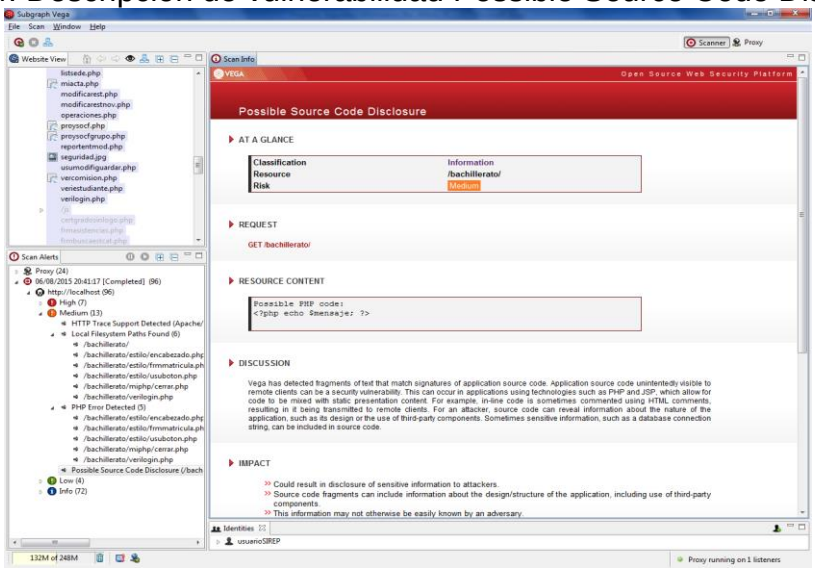


Fuente. Propiedad de los Autores

4.1.7 Possible Source Code Disclosure. (Divulgación de Código Fuente)

Descripción: Se ha detectado fragmentos de texto que concuerda con sentencias del código fuente de la aplicación. El código fuente de la aplicación es visualizado de forma no intencional a los clientes remotos puede convertirse en una vulnerabilidad de seguridad. Esto puede ocurrir en aplicaciones que usan tecnologías tanto de PHP como JSP, las cuales permiten ser mezcladas con contenido de presentación estático. Por ejemplo, las líneas de código son comentadas algunas veces usando comentarios HTML, los cuales son enviados a clientes remotos. Para una atacante, el código fuente puede revelar información acerca de la naturaleza de las aplicaciones, su diseño o el uso de componentes de terceros. En algunas ocasiones, información sensible, como la cadena de conexión de la base de datos, puede ser incluida en el código fuente. Ver figura 14.

Figura 14. Descripción de vulnerabilidad Possible Source Code Disclosure.



Fuente. Propiedad de los Autores

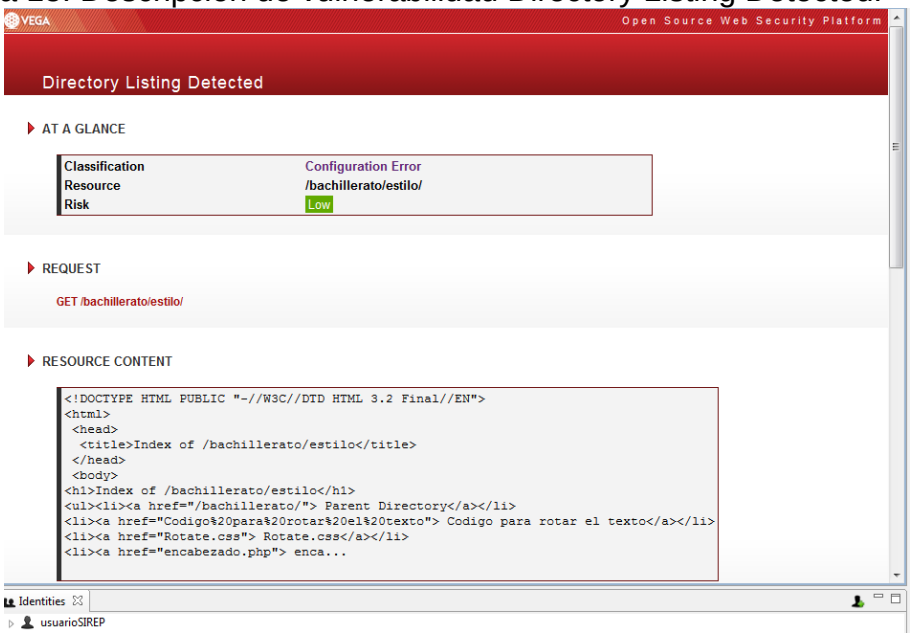
4.1.8 Directory Listing Detected (Lista del Directorio Detectada).

Descripción: Visualizar la lista de directorio cuando no hay ningún archivo índice es práctica común de una mala configuración. El contenido del directorio pueden proporcionar información útil para un atacante, especialmente si hay archivos que no están destinados a ser accesibles, como el código fuente o copias de seguridad. El listado del directorio también puede proporcionar información útil sobre los hábitos de la administración del servidor y / o desarrolladores web, como la denominación de archivos, que podrían utilizarse para aumentar el éxito probable de fuerza bruta o de otros ataques. Ver figura 15.

Páginas donde se presentan los riesgos:

- /bachillerato/estilo/
- /bachillerato/export_excel/
- /bachillerato/js/
- /bachillerato/js./
- /bachillerato/miphp/

Figura 15. Descripción de vulnerabilidad Directory Listing Detected.



Fuente. Propiedad de los Autores

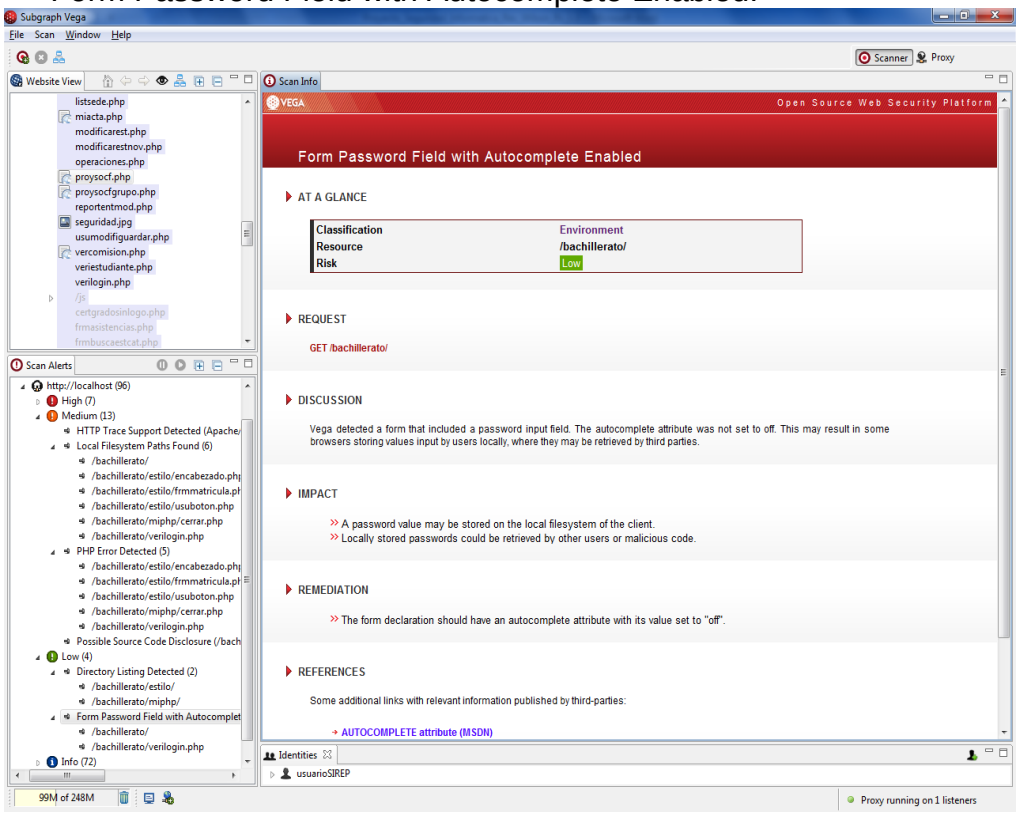
4.1.9 Form Password Field with Autocomplete Enabled (Campos de Contraseña con Autocompletar habilitado)

Descripción: Se ha detectado un formulario que incluye un campo de introducción de contraseña. El atributo autocomplete (autocompletar) no fue desactivado. Esto puede resultar en algunos navegadores que queden almacenados valores de entrada de los usuarios a nivel local, en los que pueden ser recuperados por terceros. Ver figura 16.

Páginas donde se presenta la vulnerabilidad:

- /bachillerato/
- /bachillerato/verilogin.php

Form Password Field with Autocomplete Enabled.

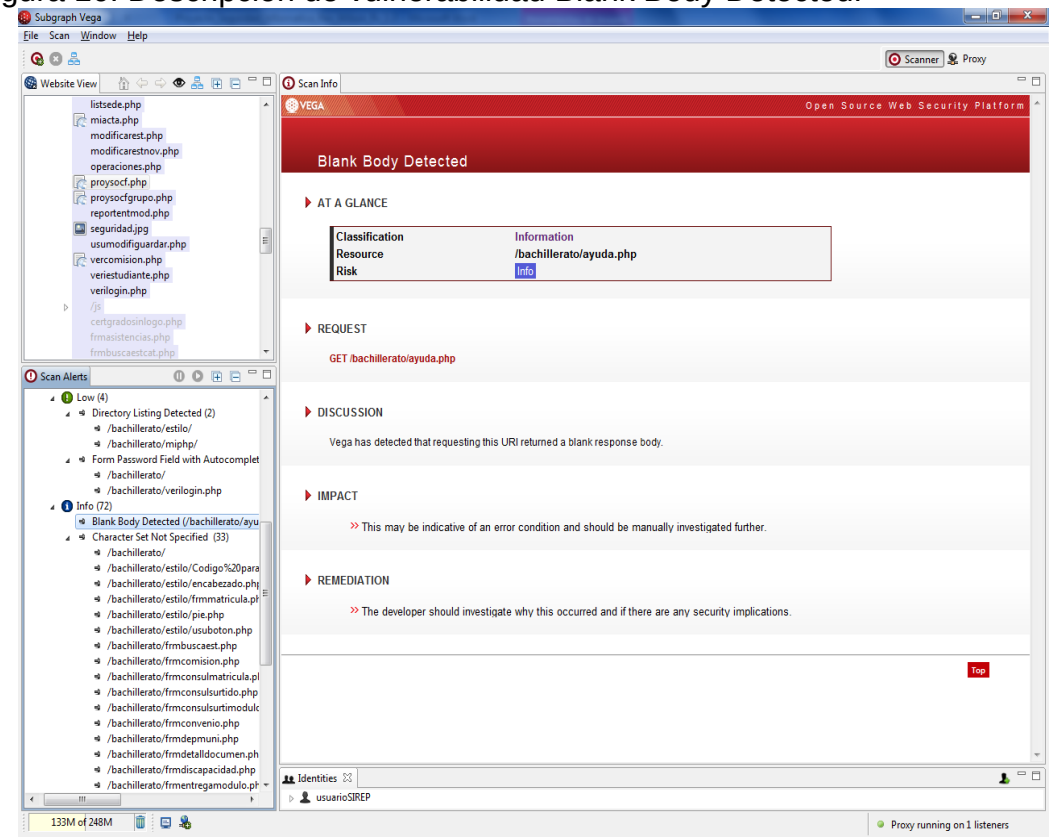


Fuente. Propiedad de los Autores

4.1.10 Blank Body Detected.

Descripción: Se ha detectado que en el momento de solicitar la página "/bachillerato/ayuda.php, la respuesta es una página en blanco. Ver figura 17.

Figura 16. Descripción de vulnerabilidad Blank Body Detected.

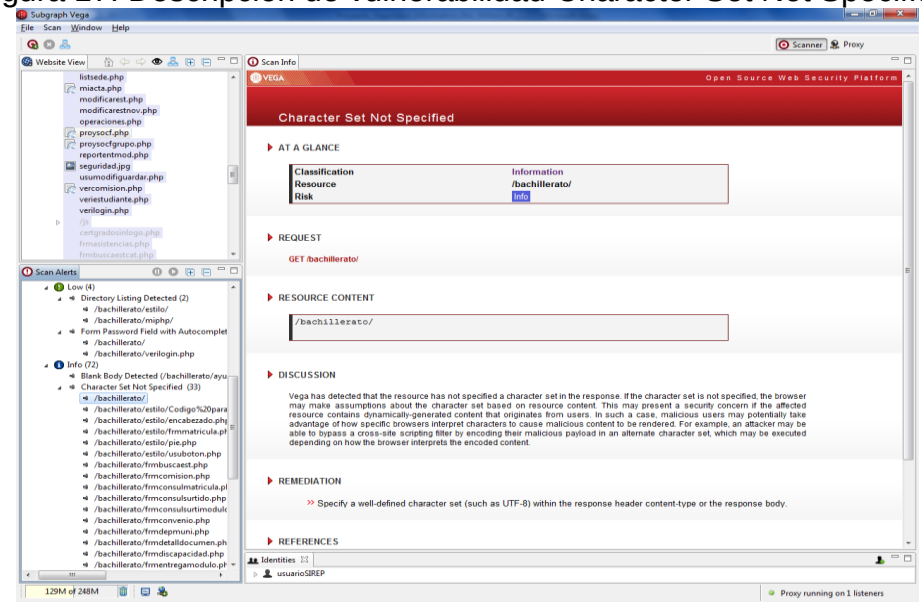


Fuente. Propiedad de los Autores

4.1.11 Character Set Not Specified (Juego de Caracteres no especificado).

Descripción: Se ha detectado que no se ha especificado un conjunto de caracteres en las respuestas de la aplicación. Si no se especifica el conjunto de caracteres, el navegador puede hacer suposiciones sobre el conjunto de caracteres basado en el contenido de los recursos. Esto puede representar un problema de seguridad si el recurso afectado contiene contenido generado dinámicamente que se origina en los usuarios. Ver figura 18.

Figura 17. Descripción de vulnerabilidad Character Set Not Specified.

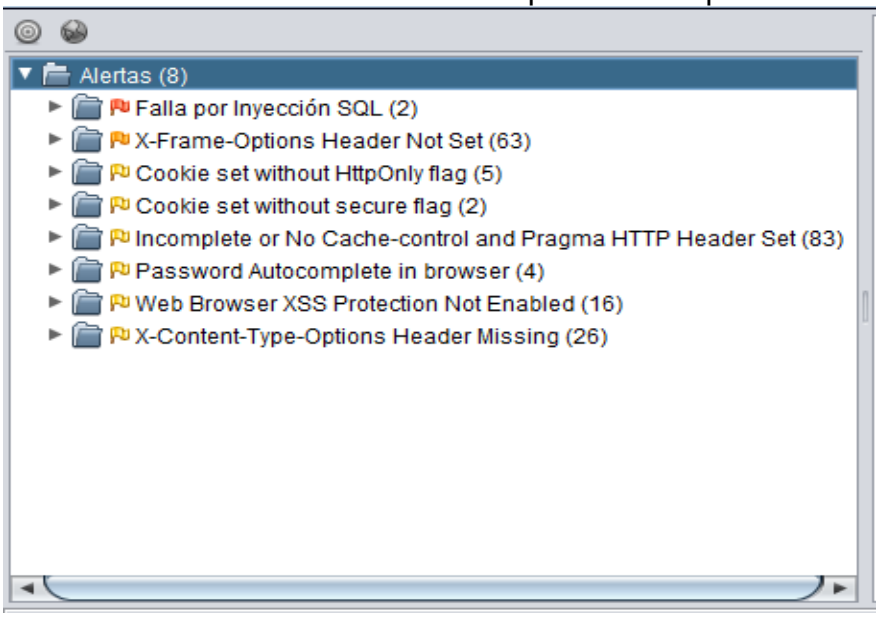


Fuente. Propiedad de los Autores.

4.2 VULNERABILIDADES DEL SIREP IDENTIFICADAS CON ZAP

Cuando se haya terminado de instalar y configurar el software de escaneo ZAP, se procede a realizar el escaneo de todas las páginas del aplicativo SIREP (Ver Anexo B). La figura siguiente muestras las vulnerabilidades encontradas por ZAP.

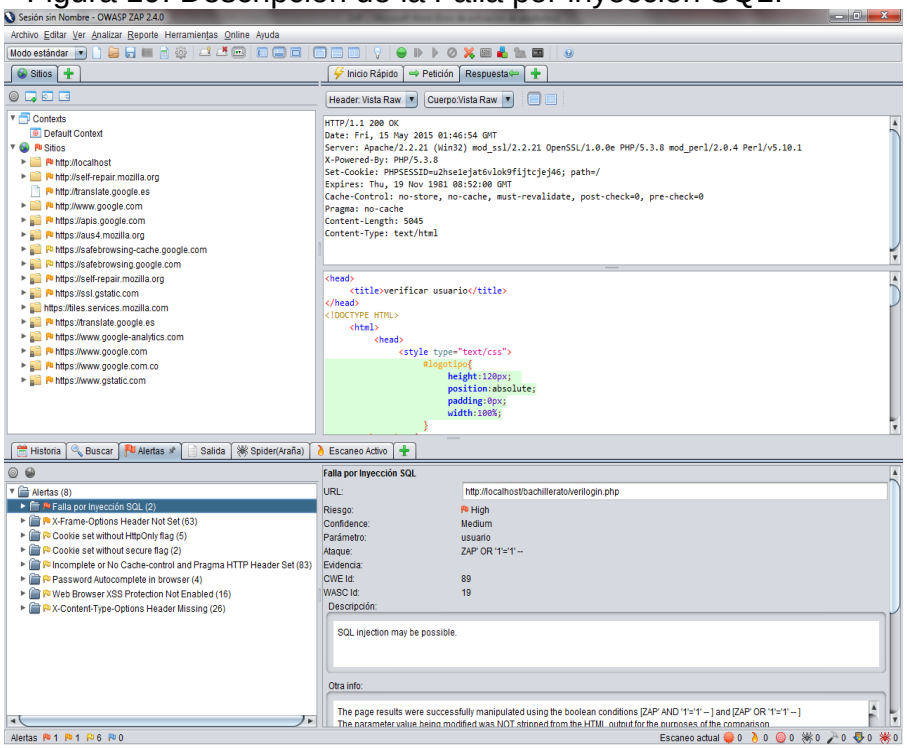
Figura 18. Vulnerabilidades encontradas por ZAP al aplicativo SIREP.



Fuente. Propiedad de los Autores.

4.2.1 Falla por Inyección SQL.

Figura 19. Descripción de la Falla por inyección SQL.



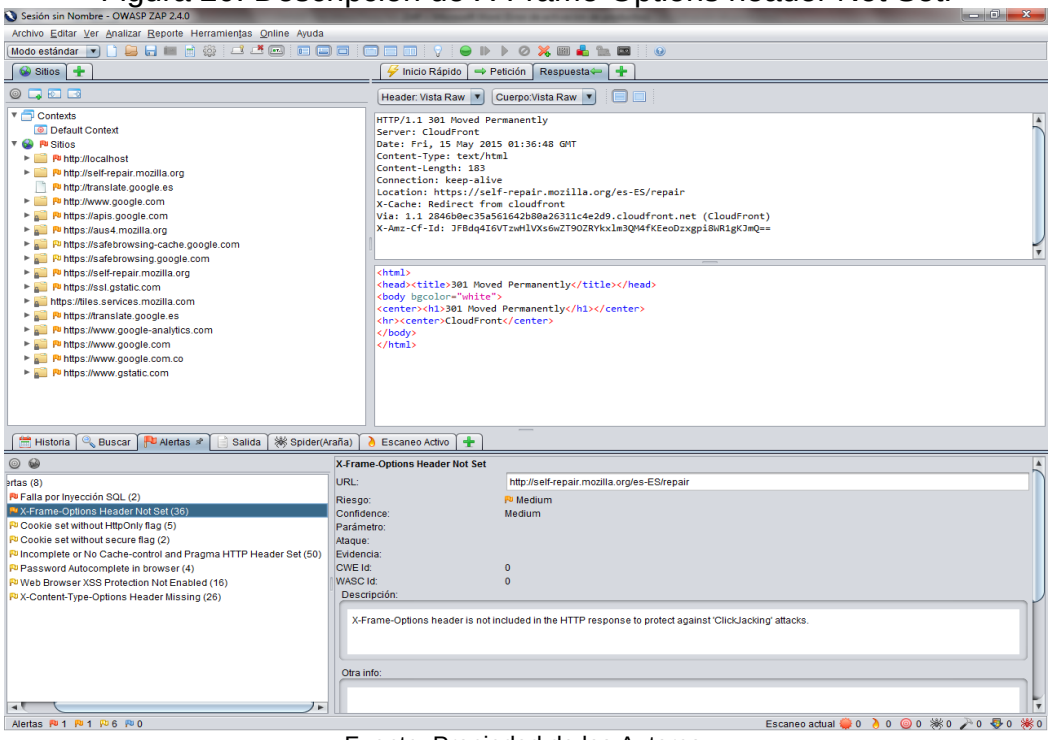
Fuente. Propiedad de los Autores.

Descripción: La figura anterior muestra la realización de un ataque booleano con la sentencia [ZAP' AND 1 '=' 1 '-] y [ZAP' OR '1' = '1' -], dando como resultado que la aplicación es vulnerable por Inyección SQL. La vulnerabilidad se detectó mediante la recuperación con éxito de más datos que los devueltos originalmente, mediante la manipulación del parámetro

4.2.2 X-Frame-Options header Not Set.

- **Descripción:** La cabecera X-Frame-Options no está incluida en las respuestas HTTP, lo que protege de los ataques 'ClickJacking'. Ver figura 20.

Figura 20. Descripción de X-Frame-Options header Not Set.

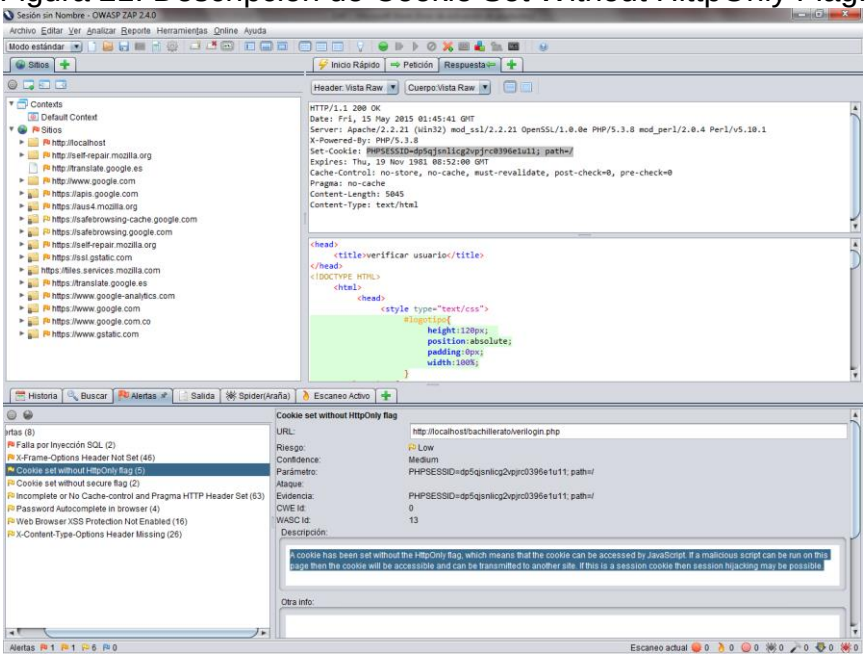


Fuente. Propiedad de los Autores.

4.2.3 Cookie Set Without HttpOnly Flag.

Descripción: se establecen cookies sin la bandera HttpOnly, lo que permite que desde JavaScript se pueda acceder utilizando código malicioso, lo que permitiría la transferencia a un sitio diferente o si es una cookie de inicio de sesión es posible realizar un secuestro de sesión. Ver figura 21.

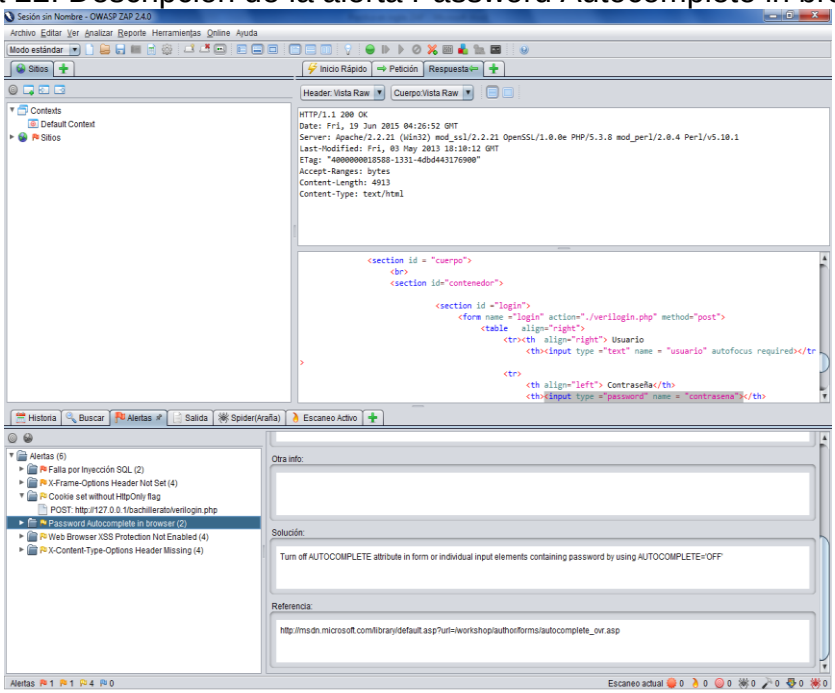
Figura 21. Descripción de Cookie Set Without HttpOnly Flag.



Fuente. Propiedad de los Autores.

4.2.4 Password Autocomplete in browser.

Figura 22. Descripción de la alerta Password Autocomplete in browser.

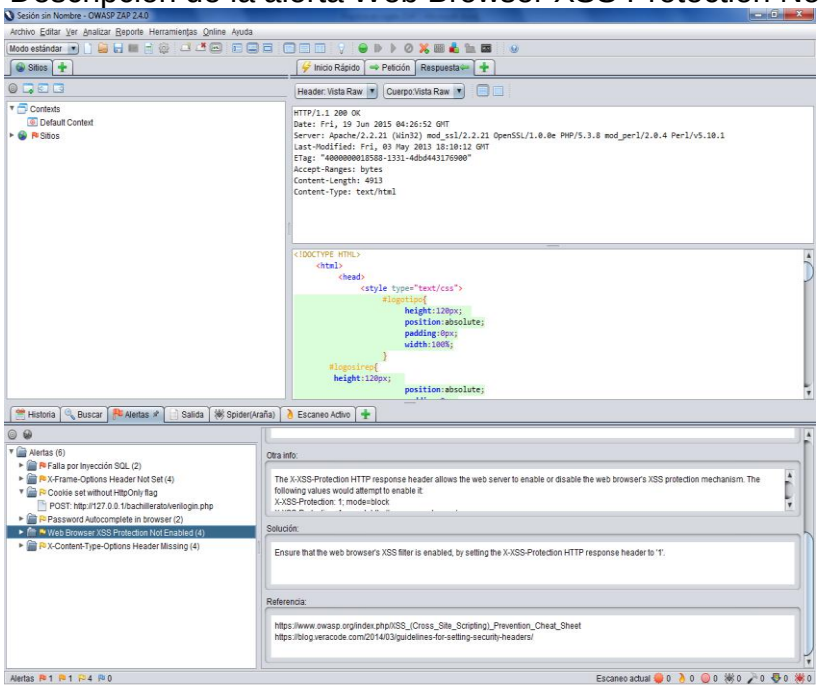


Fuente. Propiedad de los Autores.

- **Descripción:** el atributo AUTOCOMPLETE no está deshabilitado en los elementos HTML FORM/INPUT que contienen entradas donde se solicitan contraseñas. Las contraseñas pueden quedar almacenadas en los navegadores y pueden ser recuperadas. Ver figura 22.

4.2.5 Web Browser XSS Protection Not Enabled.

Figura 23. Descripción de la alerta Web Browser XSS Protection Not Enabled.



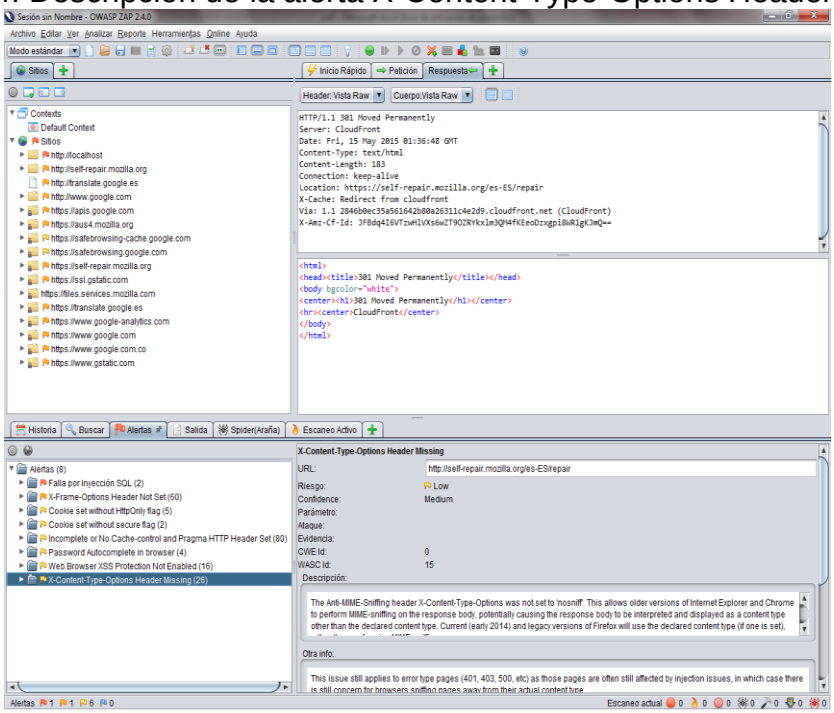
Fuente. Propiedad de los Autores.

Descripción: La protección XSS en los navegadores Web no está habilitada, o está deshabilitada por la configuración de 'X-XSS-Protection' en la cabecera de respuesta HTTP en el servidor Web. Ver figura anterior.

X-XSS-Protection de la cabecera de respuesta HTTP permite a los servidores web habilitar o deshabilitar el mecanismo de protección XSS de los servidores web.

4.2.6 X-Content-Type-Options Header Missing.

Figura 24. Descripción de la alerta X-Content-Type-Options Header Missing.



Fuente. Propiedad de los autores.

Descripción: La opción X-Content-Type de la cabecera Anti-MIME-Sniffing no está en 'nosniff'. Esto permite a las versiones antiguas de Internet Explorer y Chrome realizar MIME-sniffing en la respuesta, causando que la respuesta se interprete y se muestre con un tipo de contenido que no haya sido declarado. Ver figura anterior.

4.3 ATAQUES INYECCIÓN SQL AL APLICATIVO SIREP

La inyección SQL es uno de los ataques más fácil de realizar, el cual ocurre por errores de validación en la entrada de datos, siendo esto por despiste del programador o desconocimiento. Este tipo de ataque consiste en introducir consulta SQL desde el computador cliente por medio de los datos de entradas, permitiendo leer, modificar y eliminar registros.

Unos aspectos a tener en cuenta son:

- **Al materializarse este tipo de ataque los atacantes podrán suplantar identidad, alterar datos existentes, causar problemas de repudio, acceder a todos los datos, modificar y/o eliminar los datos, etc.**

- **Estos tipos de ataques son muy comunes en aplicaciones PHP.**

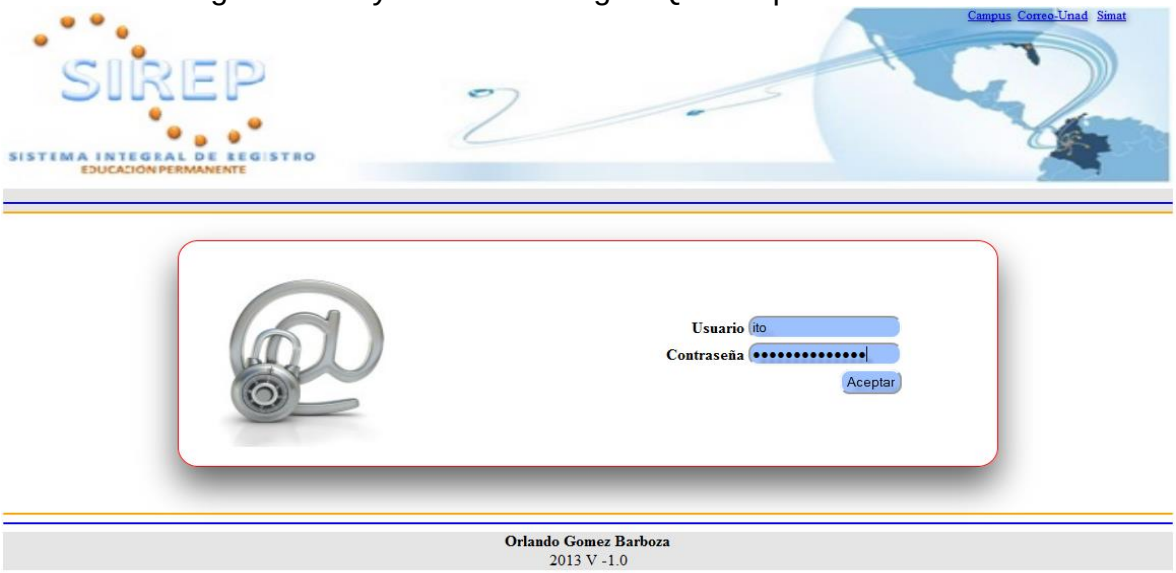
Identificar si una aplicación es vulnerable a este tipo de ataques es medianamente fácil, para tal fin se utiliza el método de ensayo de error, lo que muchas vece puede ser muy engorroso; por esta razón muchos utilizan herramientas que permitan identificar este tipo de vulnerabilidades, un ejemplo puede ser la herramienta SQLmap, el cual realiza múltiples combinaciones para encontrar un error válido que permita realizar la inyección Sql.

SQLmap es una herramienta que permite realizar acciones como descargar la base de datos o consultas SQL, a continuación se procede a realizar la prueba.

4.3.1 Ataque por inyección de código SQL al aplicativo SIREP.

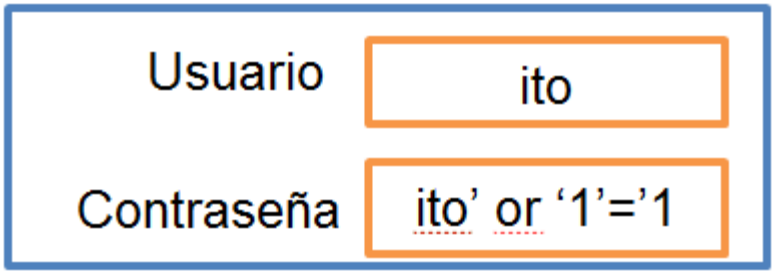
Una vez ubicado en la página de inicio de la aplicación, en el campo de usuario y contraseña se escribe la siguiente información:
Usuario: cualquier usuario para el caso se escribirá ito.
Contraseña: en esta parte si es necesario escribir el mismo usuario seguido de ‘ or ‘1’=’1, como se muestra en las figuras 25 y 26.
ito‘ or ‘1’=’1

Figura 25. Inyección de código SQL en aplicativo SIREP



Fuente. Aplicación SIREP, realizando prueba de inyección SQL.

Figura 26. Ataque con código de inyección SQL.



Fuente. Propiedad de los autores.

Al presionar aceptar se logra ingresar con un usuario legítimo de la aplicación tal como se evidencia en la siguiente figura:

Figura 27. Inicio de Sesion SIREP: ataque exitoso con la inyección SQL.

Fuente. Propiedad de los Autores.

Figura 28. Código fuente aplicativo SIREP, inicio de sesión.

```
<head>
    <title>verificar usuario</title>
</head>
<?php
$Sql= mysql_query("select * from usuario where usuario = '$usuario' and contrasena = '$contrasena'",$
    $numsql= mysql_num_rows($Sql);
    if ($numsql>0){
        //ingreso permitido
    }else{
        //ingreso no permitido
```

Fuente. Propiedad de los autores.

Como se puede notar en la figura anterior los datos enviados desde el formulario van dirigidos a una consulta SQL, aprovechando esto y la forma como el programador desarrollo el código, se inyecta el código antes descrito con el fin de concatenar este y el existente (programado por el desarrollador, teniendo en cuenta que las comillas son utilizadas para terminar la cadena 'ito', lo demás (or '1'=1) es interpretado como sentencia SQL, y es esto último que permite que la consulta realizada dé como resultado siempre un valor verdadero. En la siguiente figura se observa el código fuente con los datos de la inyección SQL

Figura 29. Código fuente Aplicativo SIREP después de la inyección SQL.

```
<head>
    <title>verificar usuario</title>
</head>
<?php
$Sql= mysql_query("select * from usuario where usuario = 'ito' and contrasena = 'ito' or '1'='1'",$
    $numsql= mysql_num_rows($Sql);
    if ($numsql>0){
        //ingreso permitido
    }else{
        //ingreso no permitido
```

Fuente. Propiedad de los autores.

4.4 VULNERABILIDADAES DE PHP

Vulnerabilidad CGI o interfaz de entrada común (CVE-2012-1823) [44]. Esta vulnerabilidad admite la inyección de argumentos debido a que los mismos no son debidamente controlados y permiten acceder al código fuente de una página PHP o incluso la ejecución de comandos de forma remota.

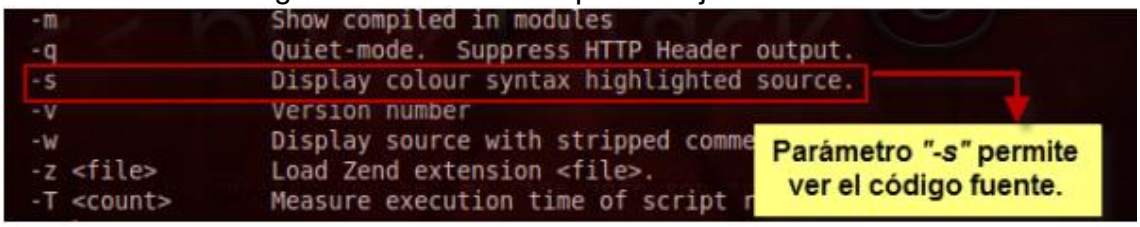
CGI es una tecnología permite la comunicación entre el cliente y el servidor mediante el programa web, por cada petición que recibe el servidor crea un nuevo proceso para atender la misma, y en el caso de PHP crea un proceso del intérprete PHP por cada petición.

La vulnerabilidad reside en la falta de controles en el pasaje de parámetros.

Existen diferentes parámetros para la ejecución de CGI tal como se ve en la siguiente figura:

[44] CATOIRA, Fernando. Grave vulnerabilidad en PHP-CGI. May 2012. Disponible en internet en http://www.welivesecurity.com/la-es/2012/05/09/grave-vulnerabilidad-php-cgi-parte-i/

Figura 30. Parametros para la ejecución CGI.



Fuente: CATOIRA, Fernando. Grave vulnerabilidad en PHP-CGI. May 2012. Disponible en internet en http://www.welivesecurity.com/la-es/2012/05/09/grave-vulnerabilidad-php-cgi-parte-i/

Puntualmente el parámetro "-s" permite ver el código fuente de aquella aplicación que se esté ejecutando mediante CGI. Esto puede revelar información muy sensible si alguien, por ejemplo, inserta mediante un navegador este parámetro en el contexto de un archivo PHP. En otras palabras, permitirá ver el código fuente de cualquier archivo que se ejecute mediante la interfaz CGI. Si esto se lo proyecta en archivos de configuración, se puede acceder a información muy sensible, como por ejemplo, contraseñas de bases de datos, entre otros.

Hay que tener presente que apache cuenta con módulos que soportan PHP nativo que utilizan procesos hijos e hilo para la comunicación entre el servidor y el cliente, lo que hace que la configuración sea muy utilizada ya que brinda un buen rendimiento a la hora de atender múltiples peticiones.

4.5 VULNERABILIDADES DE MYSQL

Vulnerabilidad CVE-2012-2122. Es una vulnerabilidad crítica, que afecta a la función memcmp() del archivo sql/password.c del componente Password Authentication. Mediante la manipulación de un input desconocido que causa la vulnerabilidad de clase autenticación débil lo que repercute sobre la confidencialidad, integridad y disponibilidad[45]. Esta vulnerabilidad solo explotada si MySQL está basado en un sistema en el que la función memcmp () puede devolver valores fuera del rango -128 a 127; que sería el caso de los sistemas Linux que utilizan una librería GNU C SSE. Así lo explica Sergei Golubchik, coordinador de seguridad de MariaDB[46].

[45] GOLUBCHIK, Sergei. VulDB: Oracle MySQL hasta 5.6.5 Password Authentication sql/password.c memcmp() autenticación débil. JUN 2012. Disponible en internet en http://www.scip.ch/es/?vuldb.5503

[46] ARROYO, Rosalia. Una vulnerabilidad en MySQL permite superar la verificación de contraseñas. JUN 2012. Disponible en internet en http://www.channelbiz.es/2012/06/13/vulnerabilidad-mysql-permite-superar-verificacion-contrasenas/

Vulnerabilidad CVE-2015-3152[47]. Esta vulnerabilidad permitía que una tercera persona se ubicara entre el servidor y el cliente, provocando que las comunicaciones entre el usuario y este no fuesen seguras, y sin embargo entre el ciberdelincuente y el servidor sí que se utilizará cifrado. Esta vulnerabilidad reside en una carencia a la hora de configurar los clientes que se conectan a la base de datos, ya que el servidor sí posee la función de forzar la utilización de una conexión cifrada, algo que en el otro extremo no sucede.

Vulnerabilidad CVE-2015-4864. La vulnerabilidad fue publicada el 2015-10-20 con identificación Oracle Critical Patch Update Advisory – October 2015 con un advisory (Website) (confirmado). La vulnerabilidad se debe a una función desconocida del componente Privileges el cual es afectado por esta vulnerabilidad. Esto tiene repercusión sobre la integridad. El ataque se puede hacer desde la red. Para explotarla se requiere una autentificación. No se conoce los detalles técnicos ni hay ningún exploit disponible. Para eliminar esta vulnerabilidad se debe actualizar.

4.6 VULNERABILIDADES DE XAMPP

Teniendo en cuenta que la aplicación SIREP se encuentra montada en el servidor XAMPP 1.7.7, a continuación se nombran las vulnerabilidades que este presenta:

Vulnerabilidades XSS (Cross-site scripting). Conocida en español como Secuencias de órdenes en sitios cruzados es un tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones Web, que permite a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar (ej: VBScript), evitando medidas de control como la Política del mismo origen[48].

Ejemplo[49]:

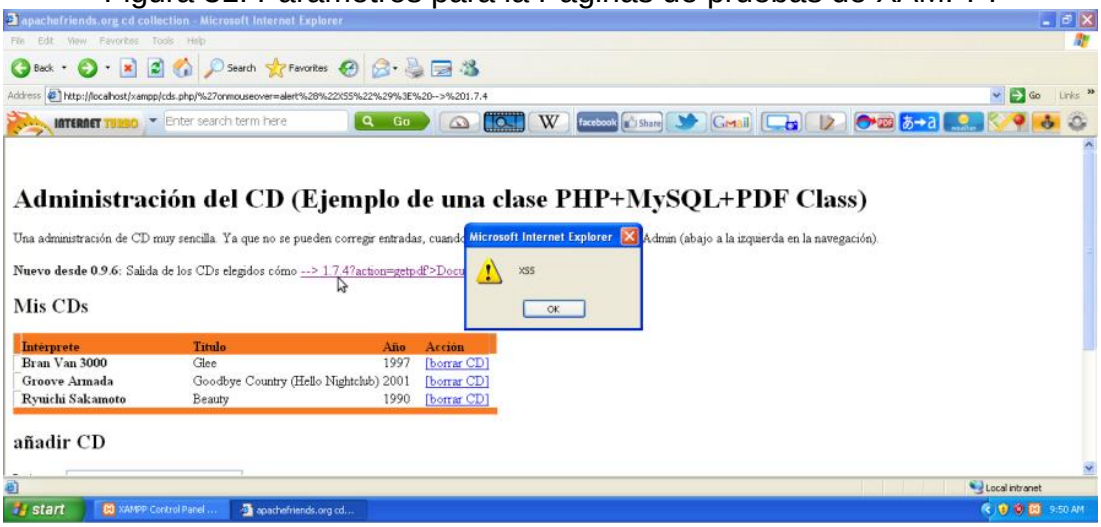
XAMPP contienen páginas de pruebas con ejemplos de aplicaciones típicas con conexiones a bases de datos y scripts en PHP o Perl, algunas veces por error, estas páginas se no se eliminan en un entorno productivo y dado que no son precisamente “seguras” pueden ser utilizadas por un atacante, tal como lo enseña la siguiente figura:

[47] CRESPO, Adrian. (2015, Mayo 2). Una vulnerabilidad en MySQL permite al usuario enviar datos sin cifrar. MAY, 2015. Disponible en internet en http://www.redeszone.net/2015/05/02/mysql-vulnerabilidad-enviar-datos-sin-cifrar/

[48] Cross-site scripting. WIKIPEDIA. Octubre 25. Disponible en internet en https://es.wikipedia.org/wiki/Cross-site_scripting

[49] WEB HACKING – Vulnerabilidades en XAMPP (Continuación) – Parte XXIII. MAR, 2012. Disponible en internet en http://thehackerway.com/2013/03/12/web-hacking-vulnerabilidades-en-xampp-continuacion-parte-xxiii/

Figura 31. Parámetros para la Paginas de pruebas de XAMPP.



WEB HACKING – Vulnerabilidades en XAMPP (Continuación) – Parte XXIII. MAR, 2012. Disponible en internet en http://thehackerway.com/2013/03/12/web-hacking-vulnerabilidades-en-xampp-continuacion-parte-xxiii/

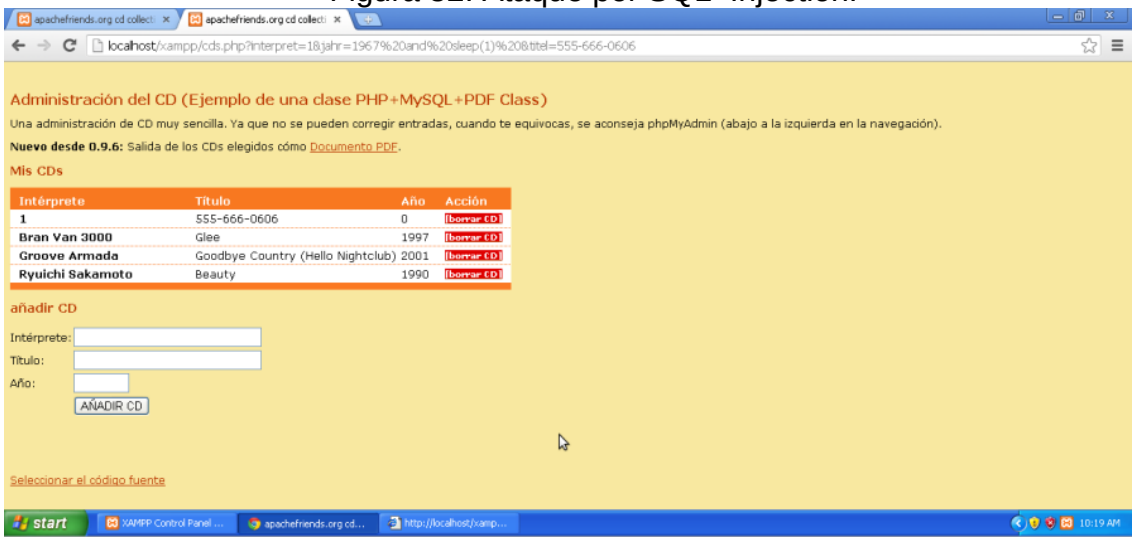
La petición que se ha realizado en la figura anterior ha sido: http://localhost/xampp/cds.php/%27onmouseover=alert%28%22XSS%22%29%3E%20–>%201.7.4

Se reproduce simplemente con activar el evento onMouseOver sobre el enlace que se ha inyectado en la página.

SQL Injection[50]. En esta parte encontramos la vulnerabilidad Blind SQLi, el cual para explorarla o aprovecharla es necesario solamente, manipular los parámetros que se envían en el formulario de inserción de CD's. En este caso concreto no se puede apreciar ningún resultado "obvio" en apariencia visual, sin embargo, esta vulnerabilidad permite a un atacante extraer información de la base de datos e incluso del sistema de ficheros conformando correctamente las peticiones SQL. Esto se puede apreciar en la siguiente figura:

[50] WEB HACKING – Vulnerabilidades en XAMPP (Continuación) – Parte XXIII. MAR, 2012. Disponible en internet en: http://thehackerway.com/2013/03/12/web-hacking-vulnerabilidades-en-xampp-continuacion-parte-xxiii/

Figura 32. Ataque por SQL Injection.



WEB HACKING – Vulnerabilidades en XAMPP (Continuación) – Parte XXIII. MAR, 2012. Disponible en internet en: http://thehackerway.com/2013/03/12/web-hacking-vulnerabilidades-en-xampp-continuacion-parte-xxiii

La petición que se realizó ha sido esta: http://localhost/xampp/cds.php?interpret=1&jahr=1967 and sleep(1) &titel=555-666-0606

Como se puede apreciar, justo después de indicar el valor del parámetro “jahr” se ha ingresado una función SQL, este es el punto de ataque. Aquí se recomienda leer el libro de Chema Alonso sobre Hacking de Aplicaciones Web SQL Injection: http://www.informatica64.com/libros.aspx?id=hwsql

5. VERIFICACIÓN DE VULNERABILIDADES OBTENIDAS EN EL ANALISIS AL APLICATIVO SIREP, Y PROPUESTA PARA LA MITIGACION DE LAS VULNERABILIDADES

5.1 IMPACTO Y CORRECTIVOS POR NIVEL DE RIESGO

De acuerdo a la identificación realizada de las vulnerabilidades encontradas en el aplicativo SIREP se procede a verificar el impacto que tienen las vulnerabilidades y a dar las recomendaciones necesarias para mitigar el impacto de estas vulnerabilidades. En las Tablas 1, 2 y 3 se consolidan los impactos y las recomendaciones clasificadas de acuerdo al nivel de riesgo.

Tabla 1. Impacto y Recomendación de las vulnerabilidades NIVEL ALTO

Vulnerabilidad	Impacto	Recomendaciones	
		VEGA	ZAP
Riesgo de Nivel Alto			
Cleartext Password ver HTTP. (Contraseñas sin cifrado en HTTP).	Las contraseñas viajan a través de canales inseguros. Las contraseñas pueden ser divulgadas a intrusos de la red.	Las contraseñas no deben ser enviadas a través de texto en claro. Las formas de la aplicación deben presentarse como objetivos HTTPS HyperText Transfer Protocolo Secure (en español Protocolo Seguro de Transferencia de Hipertexto). .Encriptar los datos transferidos.	
Shell Injection. (Inyecciones de intérprete de comandos)	Atacantes pueden ser capaces de correr comandos del lado del servidor. La explotación de esta vulnerabilidad puede provocar el acceso remoto no autorizado.	Los desarrolladores deben examinar el código fuente de las páginas web al detalle, para determinar si existen vulnerabilidades. Se debe evitar ejecutar comandos de sistemas con la función system() a través de un intérprete de comandos. Es absolutamente necesario que los desarrolladores destinen tiempo extra a validad las entradas antes de ser pasadas por un intérprete.	
SQL Injection. (Inyección SQL)	Estas vulnerabilidades pueden ser explotadas por atacantes remotos para obtener acceso no autorizado para escribir o leer sobre la base de datos. La explotación de una vulnerabilidad de Inyección SQL permite ataques en contra de la lógica de la aplicación. Los atacantes pueden ser capaces de obtener acceso no autorizado al servidor	El desarrollador deben revisar las solicitudes y respuestas en el código de la base de datos para verificar manualmente si la vulnerabilidad existe o no. La mejor defensa en contra de las vulnerabilidades SQL es el uso de consultas parametrizadas. Se deben validar las entradas de los usuarios. Las variables tipo cadena (String) deben estar filtradas de caracteres de escape, y los tipos numéricos deben validarse que son caracteres válidos. El uso de procedimientos almacenados puede simplificar consultas complejas y permitir ajustes en el control de acceso más estrictos.	No hay que confiar en las entradas del lado del cliente, incluso si la validación se realiza del lado del cliente. En general, se debe comprobar todos los datos en el lado del servidor. Si la aplicación utiliza JDBC, se debe utilizar PreparedStatement o CallableStatement, con parámetros pasados con '?'. Si la aplicación utiliza ASP, se debe utilizar ADO Command Objects con una fuerte comprobación de tipos y consultas parametrizadas. Si se pueden usar bases de datos con procedimientos almacenados, úselas. No concatenar cadenas en las consultas en los procedimientos almacenados, o usar 'exec', 'exec immediate', o la función equivalente.

Vulnerabilidad	Impacto	Recomendaciones	
		VEGA	ZAP
	donde se encuentra la base de datos. ●	Configurar los controles de acceso de la base de datos pueden limitar el impacto de explotar esta vulnerabilidad. Esta estrategia puede emplearse en entornos en los que no se puede modificar el código.	No crear consultas SQL dinámicas utilizando concatenación de cadenas sencillas. Aplicar una 'lista blanca' de caracteres permitidos, o una "lista negra" de los caracteres no permitidos en la entrada del usuario. Aplicar el mínimo de privilegios posibles mediante el uso de bases de datos de usuario. En particular, evitar el uso de los usuarios de base de datos 'sa' o 'db-owner'. Esto no elimina la inyección de SQL, pero minimiza su impacto. Conceder el mínimo acceso a la base de datos que es necesario para la aplicación.

Fuente. Propiedad de los Autores

Tabla 2. Impacto y Recomendación de las vulnerabilidades NIVEL MEDIO

Vulnerabilidad	Impacto	Recomendaciones	
		VEGA	ZAP
Riesgo de Nivel Medio			
HTTP Trace Support. (Soporte de rastreo HTTP)	Permitir HTTP TRACE puede permitir un rastreo cross-site. Los atacantes pueden ser capaces de utilizar Cross-site tracing (Cross-site de rastreo) con Cross-Site scripting para recuperar el valor de HttpOnly de las cookies.	Para los servidores basados e Apache, la directiva TraceEnable se puede utilizar para desactivar el soporte para HTTP TRACE. Para los servidores basados en IIS, el registro EnableTraceMethod ajusta el soporte para HTTP TRACE.	
Local Filesystem Paths Found. (Rutas del Sistema de archivos encontradas)	Esta información puede ser sensible, su divulgación puede aumentar las posibilidades de éxito para otros ataques	Las rutas absolutas a menudo se encuentran en los mensajes de salida de errores. Tanto los administradores de sistemas y desarrolladores deben ser cuidadosos, ya que el problema puede deberse a un error de aplicación o mala configuración del servidor. Las salidas de errores que contienen información confidencial, como las rutas del sistema absolutos, no debe ser enviado a los clientes remotos en servidores de producción. Estos mensajes de salida deben ser enviados a través de otros canales de salida, como un registro de errores.	
PHP Error Detected. (Detección de Errores PHP)	Se ha detectado firmas que corresponden a páginas de errores de PHP. Las páginas de error, las cuales se generan automáticamente, pueden filtrar información sensible. La información filtrada puede incluir parches para el software, ajustes de configuración y la base de datos o la estructura del sistema de ficheros.	El manual de PHP recomienda deshabilitar "display_errors" en servidores con salida a Internet. Para PHP 5.2.4 y superior, los ajustes en "display_errors" en el archivo de configuración "php.ini" se debe establecer en "stderr" (flujo de salida de error), en lugar de "stdout" (flujo de salida enviado a los clientes). Para versiones anteriores, "display_errors" es un tipo booleano, y se pueden configurar en "False" para desactivar. El ajuste también se puede desactivar en tiempo de ejecución usando ini_set () desde un script PHP.	

Possible Source Code Disclosure. (Divulgación de Código Fuente)	Podría dar lugar a la revelación de información sensible a los atacantes. Fragmentos de código fuente pueden incluir información sobre el diseño / estructura de la aplicación, incluyendo el uso de componentes de terceros. Esta información puede ser de otra forma no fácilmente conocida por un adversario. A veces el código fuente también contiene información altamente sensible, como contraseñas (cadenas de conexión de base de datos).	Los desarrolladores deben verificar que las salidas detectadas por Vega son efecto código fuente de la aplicación. La causa debe ser determinada, y el material eliminado o prevenir su salida	
X-Frame-Options header Not Set.		Atacantes pueden ser capaces de correr comandos del lado del servidor. Se pueden dar accesos remotos no autorizados.	Los navegadores Web más modernos soportan la cabecera HTTP X-Frame-Options HTTP. Se debe asegurar que todas las páginas web que conformar la aplicación este establecido

Fuente. Propiedad de los Autores

Tabla 3. Impacto y Recomendación de las vulnerabilidades NIVEL BAJO

Vulnerabilidad	Impacto	Recomendaciones	
		VEGA	ZAP
Riesgo de Nivel Bajo			
Cookie Set Without HttpOnly Flag	Se establecen cookies sin la bandera HttpOnly, lo que permite que desde JavaScript se pueda acceder utilizando código malicioso, lo que permitiría la transferencia a un sitio diferente o si es una cookie de inicio de sesión es posible realizar un secuestro de sesión.	Para Apache, se debe realizar una de las siguientes opciones: añadir "IndexIgnore *" al archivo .htaccess del directorio, o bien eliminar "Índexes" de la línea "Options All Indexes FollowSymLinks MultiViews" en su archivo de configuración de Apache. Para lighttpd, cambie "dir-listing.activate = "enable"" to "dir-listing.activate = "disable"" en el archivo de configuración lighttpd	Se debe establecer la bandera HttpOnly para todas las cookies.
Directory Listing Detected (Lista del Directorio Detectada)	El servidor está emitiendo el contenido de los directorios. Esto podría exponer archivos no destinados a la recuperación de usuario (archivos .htaccess antiguos, copias de seguridad, código fuente). El listado del directorio puede proporcionar, además información útil sobre el diseño y las características del sistema, como las convenciones de nomenclatura utilizadas por los desarrolladores y administradores. Esta información puede aumentar la probabilidad de éxito para ataques a ciegas y la fuerza bruta para adivinar.	El atributo autocompletar de los campos donde se ingresan contraseñas debe estar deshabilitado.	
Form Password Field with Autocomplete Enabled	Un valor de la contraseña puede ser almacenada en el sistema de archivos local del cliente. Localmente contraseñas almacenadas podrían ser recuperados por otros	El atributo autocompletar de los campos donde se ingresan contraseñas debe estar deshabilitado.	Esta vulnerabilidad es conocida en ZAP como Password Autocomplete in browser y recomienda Desactivar el atributo

(Campos de Contraseña con Autocompletar habilitado)	usuarios o código malicioso.		AUTOCOMPLETE en las formas o de manera individual en cada uno de los elementos que solicitan entradas de contraseñas usando la sentencia AUTOCOMPLETE='OFF'.
Web Browser XSS Protection Not Enabled	La protección XSS en los navegadores Web no está habilitada, o está deshabilitada por la configuración de 'X-XSS-Protection' en la cabecera de respuesta HTTP en el servidor Web. X-XSS-Protection de la cabecera de respuesta HTTP response permite a los servidores web habilitar o deshabilitar el mecanismo de protección XSS de los servidores web.	Se debe asegurar que el filtro XSS de los servidores web se encuentre habilitado.	
X-Content-Type-Options Header Missing.	Descripción: La opción X-Content-Type de la cabecera Anti-MIME-Sniffing no está en 'nosniff'. Esto permite a las versiones antiguas de Internet Explorer y Chrome realizar MIME-sniffing en la respuesta, causando que la respuesta se interprete y se muestre con un tipo de contenido que no haya sido declarado.	Se debe asegurar que el servidor de aplicaciones o servidor web se halla establecido la cabecera Content-Type apropiadamente, y que este la cabecera X-Content-Type-Opciones de 'NOSNIFF', establecida para todas las páginas web.	Los navegadores Web más modernos soportan la cabecera HTTP X-Frame-Options HTTP. Se debe asegurar que todas las páginas web que conformar la aplicación este establecido

Fuente. Propiedad de los Autores

A nivel de Riesgo información se analizan los impactos causados por las vulnerabilidades encontradas y se dan las acciones correctivas necesarias, las cuales quedan recopiladas en la tabla siguiente:

Tabla 4. Impacto y Recomendación de las vulnerabilidades NIVEL INFORMACIÓN

Vulnerabilidad	Impacto	Recomendaciones	
		VEGA	ZAP
Riesgo de Nivel Información			
Blank Body Detected	• Indicativo de una condición de error y debe ser investigado manualmente. •	El desarrollador debe investigar por qué ocurrió esto y si hay alguna implicación de seguridad.	
Character Set Not Specified (Juego de Caracteres no especificado)	Usuarios maliciosos potencialmente pueden tomar ventaja de la forma específica navegadores interpretan personajes para causar el contenido malicioso que se prestarán. Por ejemplo, un atacante puede ser capaz de pasar por alto un filtro de cross-site scripting mediante la codificación de su carga maliciosa en un juego de caracteres alternativo, que puede ser ejecutado en función de cómo el navegador interpreta el contenido codificado.	Especificar un conjunto de caracteres bien definidos (como UTF-8) en la cabecera de la respuesta de tipo de contenido o en el cuerpo de la respuesta.	

Fuente. Propiedad de los Autores

5.2 MITIGACIÓN DEL RIESGO POR ATAQUES POR INYECCIÓN SQL [51]

- En el archivo de configuración de php “php.ini”, en la variable magic_quotes colocar el valor **On**, con esto se conseguirá a todas las entradas por la barra invertida delante de la comilla simple. Ejemplos:

  a. Comillas mágicas para datos de tiempo de ejecución generados, por ejemplo, datos de SQL, exec (), etc ; http://php.net/magic-quotes-runtime
  magic_quotes_runtime = On

  b. comillas al estilo Sybase mágicos (de escape 'con'' en lugar de \'). ; http://php.net/magic-quotes-sybase
  magic_quotes_sybase = On

- Evitar todos los caracteres especiales, para el caso se puede utilizar Mysql_real_scape_string($cadena), que coloca barra a los caracteres que se señalen en la sentencia.

- Siempre verificar los datos que son ingresados al formulario, por ejemplo Si se espera recibir un entero, verifique con is_int(), que los datos ingresados sean correctos; lo mismo si es un long con is_long(), char, varchar, o cualquier tipo con gettype().

- Comprueba la longitud de las cadenas, para esto puede utilizar strlen() o su formato con strpos(), lo que le permitirá evitar posibles técnicas de inyección SQL avanzadas.

- Implementación del paquete DB del grupo PEAR va más allá de la seguridad. Es una capa de abstracción para bases de datos, con la cual no tendrás que preocuparte más por nada de lo que has visto en este curso. El inconveniente es que tendrás que depender siempre de sus paquetes. Pero la ventaja es la despreocupación52.

[51] PHP.ini
[52] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. (2014, Abril 11). Sistema Gestión de calidad. Retrieved Abril 11, 2014, from Sistema Gestión de calidad: http://calidad.unad.edu.co/evaluacion-seguimiento-y-medicion/balance-de-gestion-y-rendicion-de-cuentas

5.3 CORRECTIVOS PARA VULNERABILIDADES MSQL

5.3.1 Vulnerabilidad CGI o interfaz de entrada común (CVE-2012-1823)[53]

Existen algunas alternativas para solucionar esta vulnerabilidad. Es posible realizar algunas modificaciones ya sea mediante el código fuente, es decir, descargándolo nuevamente con las modificaciones para que esto no ocurra, así como también es posible modificar uno de los módulos del servidor de Apache.

Si no es posible actualizar, es recomendable que se modifique el módulo *mod rewrite* de Apache. Para ello se debe agregar la siguiente regla:

RewriteCond %{QUERY_STRING} ^(%2d|-)[^=]+$ [NC]

RewriteRule ^(.) $1? [L]*

De esta manera se controlan los parámetros que se insertan en las URL y como consecuencia el servidor ya no será vulnerable a este tipo de ataques.

Es más que notorio que la seguridad no puede ser tomada a la ligera. A veces una simple falla o vulnerabilidad que parece sencilla puede tener un gran impacto a nivel de la seguridad de un sistema si se lo utiliza en conjunción con otras técnicas. Es por eso que la seguridad debe ser gestionada para lograr la protección adecuada ante estos eventos y en caso de que un incidente ocurra, reponerse del mismo de la mejor forma posible.

5.3.2 Vulnerabilidad CVE-2012-2122[54].

Para mitigar la vulnerabilidad se sugiere aplicar un parche es posible eliminar el problema. El parche puede ser descargado de bazaar.launchpad.net. Poniendo el filtro tcp/3306 (mysql) en el firewall, es posible mitigar el efecto del problema. El mejor modo sugerido para mitigar el problema es aplicar el parche al componente. Una solución posible ha sido publicada antes y no simplemente después de la publicación de la vulnerabilidad.

---

53 CATOIRA, Fernando. Grave vulnerabilidad en PHP-CGI. May 2012. Disponible en internet en http://www.welivesecurity.com/la-es/2012/05/09/grave-vulnerabilidad-php-cgi-parte-i/

54 GOLUBCHIK, Sergei. VulDB: Oracle MySQL hasta 5.6.5 Password Authentication sql/password.c memcmp() autenticación débil. JUN 2012. Disponible en internet en http://www.scip.ch/es/?vuldb.5503

5.3.3 Vulnerabilidad CVE-2015-3152[55].

Para mitigar la vulnerabilidad se debe configurar en el lado del cliente el parámetro REQUIRE X509 option, obligando que las comunicaciones entre ambos extremos deban utilizar de forma obligada SSL/TLS.

5.3.4 Vulnerabilidad CVE-2015-4864.

Para mitigar esta vulnerabilidad solo es necesario actualizar la aplicación.

[55] CRESPO, Adrian. (2015, Mayo 2). Una vulnerabilidad en MySQL permite al usuario enviar datos sin cifrar. MAY, 2015. Disponible en internet en http://www.redeszone.net/2015/05/02/mysql-vulnerabilidad-enviar-datos-sin-cifrar/

6. ANALISIS, EVALUACIÓN Y GESTÓN DEL RIESGO, BASADOS EN EL ESTANDAR MAGERIT

Los riesgos son un factor implícito en cualquier actividad, tarea, proceso o procedimiento que se realice en la vida cotidiana o en el entorno de una organización, unos son de mayor impacto, otros son más permisibles y tolerables, pero siempre habrá riesgos.

Gestionar los riesgos significa analizar e implementar metodologías, estándares, normas y buenas prácticas, buscando llevarlos a un nivel aceptable para la organización, y ejercer en ellos un control constante para evitar que las amenazas y vulnerabilidades ligadas a estos se materialicen y generen impactos negativos en los activos de información.

Por este motivo la implementación de una metodología con la aplicación de estándares para la gestión de los riesgos a los que están sometidos los activos de información SIREP utilizado en CCAV Cartagena, permitirá dar a los riesgos un tratamiento adecuado y un resultado que posiblemente mejorará la competitividad de la organización en el medio y la credibilidad de los clientes en la manera en que esta hace gestión de la seguridad de la información y los activos que intervienen con esta.

Ahora teniendo en cuenta que el servidor en donde se encuentra alojado el aplicativo SIREP, está ubicado en la oficina de registro y control se evaluará y analizará los activos de dicha zona.

6.1 ANÁLISIS DETALLADO DE LOS ACTIVOS RELEVANTE DE SEGURIDAD PARA EL CCAV CARTAGENA EN LA OFICINA DE REGISTRO Y CONTROL ACADÉMICO

La oficina de registro y control académico del CCAV Cartagena, se cuentan con los activos mostrados en la Tabla 5:

Tabla 5. Activos de la oficina de registro y control académico de la UNAD CCAV Cartagena

Inventarios de Activos	
Tipos de Activos	**Nombre de Activos CCAV Cartagena**
Activo de Información	Datos del estudiantes (Archivos en Excel)
	Base de datos Sistema Integral de Registro Educación Permanente SIREP (Aplicativo local donde se registra información de los estudiantes de bachillerato).
	Documentos Físicos
Software o aplicación	Edunat
	Sirep
	Sistemas de Turnos
Hardware	PC1 Computador All-in-one Compaq. Computadora con permisos en el servidor, usado por el líder de RYCA en el CCAV.
	PC2 Computador All-in-one Compaq. Obtiene alojado el aplicativo SIREP, tiene acceso al servidor.
	PC3 Computadora cliente utilizada para la atención de los estudiantes del programa bachillerato y pregrado, tiene acceso al servidor y no manipula ningún tipo de información importante para la empresa en su disco local.
	PC4. Computadora que donde se aloja la aplicación de turno.
	PC5. Portátil (Archivo Pregrado), tiene acceso al servidor del CCAV, y manipula la información sobre los documentos entregados por los estudiantes así como sus datos más básicos.
	PC6 Computadora de escritorio (Archivo Bachillerato), tiene acceso al servidor del CCAV, y manipula la información sobre los documentos entregados por los estudiantes así como sus datos más básicos.
	PC7 Computadora de escritorio (Archivo Bachillerato), tiene acceso al servidor del CCAV, y manipula la información sobre los documentos entregados por los estudiantes así como sus datos más básicos.
	Impresora Laser
Red	Switch
Equipamiento auxiliar	Sistema de alimentación ininterrumpida (UPS)
Instalación	Cables UTP, Cables para el fluido eléctrico
Servicios	Conectividad a internet
Personal	Usuarios finales del aplicativo Edunat, Sirep, Aplicativo de turno
	Desarrollador del aplicativo SIREP y Aplicativo de turno
	Usuarios que manipulan la información de los documentos de Bachillerato y Pregrado

Fuente. Propiedad de los Autores

6.1.1 Valoración de los activos. A continuación se realizará la valoración y dimensión de los pilares de seguridad de los activos teniendo en cuenta las s tablas valorativas 6 y 7:

Tabla 6. Escala de valoración para activos

Valoración Cualitativa	Escala de Valor Cuantitativo	Valor Cuantitativo
Muy Alto (MA)	> $ 15.000.001	$ 16.000.000
Alto (A)	$ 15.000.000 hasta $ 6.000.001	$ 7.500.000
Medio (M)	$ 6.000.000 hasta $ 1.000.001	$ 3.000.000
Bajo (B)	$ 1.000.000 hasta $ 100.001	$ 500.000
Muy bajo (MB)	$ 100.000 hasta $ 30.000	$ 50.000

Fuente. Propiedad de los Autores

Tabla 7. Criterio de Valoración de activos

•	• C
10	Muy Grave
9-7	Grave
6-4	Importante
3-1	Menor
0	Irrelevante

Fuente. Propiedad de los Autores

Teniendo definidos los criterios y las valoraciones expuestas en las tablas anteriores se procede con la realización de la tabla de valoración 9 de cada uno de los activos de la oficina de registro y control del CCAV Cartagena.

Tabla 8. Valoración de activos de acuerdo a la dimensiones de seguridad y criterios para activos

		DIMENSIONES				
Tipo	Nombre de Activo	Confidencialidad ¿Qué daño causaría que lo conociera quien no debe?	Integridad ¿Qué perjuicio causaría que estuviera dañado o corrupto?	Disponibilidad ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?	Autenticidad ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?	Trazabilidad ¿Qué daño causaría no saber a quién se le presta tal servicio?
Activo de información	Datos del estudiantes	[3][MB]	[8][A]	[9][MA]	[8][A]	
	Base de datos Sistema Integral de Registro Educación Permanente SIREP	[9][A]	[10][MA]	[10][MA]	[10][M]	
	Documentos Físicos	[10][MA]	[1][MB]	[1][MB]		
Software o aplicación	Edunat	[10][MA]	[10][MA]	[10][MA]	[10][MA]	[7]
	Sirep	[10][MA]	[10][MA]	[10][MA]	[10][MA]	[7]
	Sistemas de Turnos	[7]	[3]	[8]	[1]	
Hardware	PC1	[7]	[3][M]	[5]	[3]	
	PC2(Alojado Sirep)	[9]	[10] [MA]	[10][M]	[7]	
	PC3	[7]	[3] [M]	[5]	[3]	
	PC4(Alojado Sistema de turno)	[7]	[3] [M]	[9]	[1]	
	PC5	[10]	[7] [M]	[5]	[3]	
	PC6	[10]	[7] [M]	[5]	[3]	
	PC7	[10]	[7] [M]	[5]	[3]	
	Impresora laser		[M]	[7]		
Red	Switch			[10][MA]	[10][MA]	
Equipamiento auxiliar	UPS			[3][B]		
Instalación	Cables UTP			[7]		
	Cables del fluido eléctrico			[7]		

		DIMENSIONES				
Tipo	Nombre de Activo	Confidencialidad ¿Qué daño causaría que lo conociera quien no debe?	Integridad ¿Qué perjuicio causaría que estuviera dañado o corrupto?	Disponibilidad ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?	Autenticidad ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?	Trazabilidad ¿Qué daño causaría no saber a quién se le presta tal servicio?
Personal	Usuarios finales del aplicativo Edunat, Sirep, Aplicativo de turno			[9]		
	Desarrollador del aplicativo SIREP y Aplicativo de turno			[10]		
	Usuarios que manipulan la información de los documentos de Bachillerato y Pregrado			[7]		

Fuente. Propiedad de los Autores

6.1.2 Amenazas a la que se encuentran expuestos el aplicativo SIREP. Una vez identificado cada uno de los activos de la oficina de registro y control académico del CCAV Cartagena, se identifican las amenazas que pueden acabar con su integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad, dentro de las cuales se recopilaron en las tablas 9, 10, 11, 12 y 13.

Tabla 9. Dimensiones de valoración del impacto

Cod	Dimensiones De Valoración
[D]	Disponibilidad
[I]	Integridad de los datos
[C]	Confidencialidad de la información
[A]	Autenticidad
[T]	Trazabilidad

Fuente. Propiedad de los Autores

Tabla 10. Amenazas

[N] DESASTRES NATURALES		
COD	**AMENAZAS**	**IMPACTO**
[N.1]	Incendio	[D][I]
[N.2]	Inundación	[D][I]
[I] DE ORIGEN INDUSTRIAL		
COD	**AMENAZAS**	**IMPACTO**
[I.5]	Avería de origen físico o lógico	[D]
[I.7]	Condiciones inadecuadas de temperatura o humedad	[D]
[I.9]	Interrupción de otros servicios o suministros esenciales	[D]
[E] ERRORES Y FALLOS NO INTENCIONADOS		
COD	**AMENAZAS**	**IMPACTO**
[E.1]	Errores de los usuarios	[D][I][C]
[E.16]	Introducción de falsa información	[I]
[E.20]	Vulnerabilidades de los programas (software)	[D][I][C][A][T]
[E.28]	Indisponibilidad del personal	[D]

Tabla 10. (Continuación)

[A] ATAQUES DELIBERADOS		
COD	AMENAZAS	IMPACTO
[A.11]	Acceso no autorizado	[D][I][C][A][T]
[A.15]	Modificación deliberada de la información	[I]
[A.16]	Introducción de falsa información	[I]
[A.18]	Destrucción de la información	[D][I]
[A.22]	Manipulación de programas	[D][I][C][A]
[A.24]	Denegación de servicio	[D]
[A.25]	Robo de equipos	[D][I][C][A][T]
[A.30]	Ingeniería social (picaresca)	[D][I][C][A][T]

Fuente. Propiedad de los Autores

Tabla 11 Escala de valoración de rango porcentual de impacto en los activos

Impacto	Valoración del Impacto
Muy Alto (MA)	100%
Alto (A)	75%
Medio (M)	50%
Bajo (B)	25%
Muy bajo (MB)	5%

Fuente. Propiedad de los Autores

Tabla 12 Escala de rango de frecuencia de amenazas

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente. Propiedad de los Autores

Tabla 13. Valoración de las amenazas

[N] Desastres Naturales				
Cod	**Amenazas**	**Frecuencia**	**Impacto**	**Causas**
[N.1]	Incendio		100%	Corto circuitos, sobrecalentamiento de los cables
[N.2]	Inundación	5	50%	Lluvia
[I] De Origen Industrial				
Cod	**Amenazas**	**Frecuencia**	**Impacto**	**Causas**
[I.5]	Avería de origen físico o lógico	5	25%	Corto circuito, mal uso, variación eléctrica, apagado incorrecto
[I.7]	Condiciones inadecuadas de temperatura o humedad	10	25%	Humedad en las paredes
[I.9]	Interrupción de otros servicios o suministros esenciales	50	5%	Interrupción del fluido eléctrico, acceso a internet
[E] Errores Y Fallos No Intencionados				
Cod	**Amenazas**	**Frecuencia**	**Impacto**	**Causas**
[E.1]	Errores de los usuarios	50	5%	Por el poco conocimiento de algunos administrativos
[E.16]	Introducción de falsa información	50	25%	Por permitir que estudiantes de pregrado realicen su proceso de preinscripción y carga de documentos a la base de datos
[E.20]	Vulnerabilidades de los programas (software)	5	25%	Error en el desarrollo de la aplicación.
[E.28]	Indisponibilidad del personal	10	5%	Incapacidad o enfermedad

Tabla 13. (Continuación)

[A] Ataques Deliberados				
Cod	**Amenazas**	**Frecuencia**	**Impacto**	**Causas**
[A.11]	Acceso no autorizado	5	5%	Error en la configuración en autorización de permisos
[A.15]	Modificación deliberada de la información	5	25%	Ataques por personas mal intencionada
[A.16]	Introducción de falsa información	50	25%	Por permitir que estudiantes de pregrado realicen su proceso de preinscripción y carga de documentos a la base de datos
[A.18]	Destrucción de la información	5	25%	Daño de PC, corto del fluido eléctrico
[A.22]	Manipulación de programas	5	5%	Poco personal de vigilancia
[A.24]	Denegación de servicio	5	5%	Falta de conocimiento de algunos funcionarios
[A.25]	Robo de equipos	5	5%	Error en la configuración en autorización de permisos
[A.30]	Ingeniería social (picaresca)	5	5%	Ataques por personas mal intencionada

Fuente. Propiedad de los Autores

Una vez identificada las amenazas y teniendo en cuenta las tablas de valoración y criterios, se relacionan los activos que pueden ser afectados y en qué aspecto o dimensión, todo esto se encuentra recopilado en la siguiente tabla:

Tabla 14. Daños a la que puede afectar las amenazas

		Dimensiones				
Tipo	Nombre De Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
Activo de información	Datos del estudiantes	[A.11]	[A.15]	[A.18] [A.25]	[I.5]	
	Base de datos Sistema Integral de Registro Educación Permanente SIREP	[A.11]	[A.15]	[A.18] [A.25]	[I.5]	
	Documentos Físicos	[E.1]	[N.1] [N.2] [I.7]	[E.28]		
Software o aplicación	Edunat	[A.30]	[E.16]	[A.24]	[A.22]	[A.30]
	Sirep	[E.20]	[E.20]	[A.25] [A.24]	[A.30]	[E.20]
	Sistemas de Turnos			[A.24]		
Hardware			[E.1]	[A.25]		
	PC2(Alojado Sirep)		[E.1]	[A.25]		
			[E.1]	[A.25] [I.9]		
	PC4(Alojado Sistema de turno)		[E.1]	[A.25] [I.9]		
			[E.1]	[A.25] [I.9]		
	PC6		[E.1]	[A.25] [I.9]		
	PC7		[E.1]	[A.25] [I.9]		
	Impresora laser		[E.1]	[A.25] [I.9]		
Red	Switch			[A.25] [I.9] [I.5]		

Tabla 14. (Continuación)

		Dimensiones				
Tipo	Nombre De Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
Equipamiento auxiliar	UPS			[A.25] [I.9] [I.5]		
Instalación	Cables UTP			[I.7] [I.9]		
	Cables del fluido eléctrico			[I.7] [I.9]		
Personal	Usuarios finales del aplicativo Edunat, Sirep, Aplicativo de turno			[A.30]		
	Desarrollador del aplicativo SIREP y Aplicativo de turno			[A.30]		
	Usuarios que manipulan la información de los documentos de Bachillerato y Pregrado			[A.30]		

Fuente. Propiedad de los autores

6.1.3 Evaluación del impacto potencial en caso de materialización de las amenazas.

Tabla 15. Evaluación del impacto potencial

		Dimensiones				
Tipo	**Nombre De Activo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Activo de información	Datos del estudiantes	75%	50%	75%		
	Base de datos Sistema Integral de Registro Educación Permanente SIREP	50%	20%	75%	100%	
	Documentos Físicos	20%	5%	5%		
Software o aplicación	Edunat	5%	20%	100%	5%	
	Sirep	20%	50%	5%	5%	50%
	Sistemas de Turnos			5%		
Hardware	PC1			50%		
	PC2(Alojado Sirep)			100%		
	PC3			20%		
	PC4(Alojado Sistema de turno)			100%		
	PC5			20%		
	PC6			20%		
	PC7			20%		
	Impresora laser			100%		
Red	Switch			50%		
Equipamiento auxiliar	UPS			5%		
Instalación	Cables UTP			20%		
	Cables del fluido eléctrico			75%		
Personal	Usuarios finales del aplicativo Edunat, Sirep, Aplicativo de			5%		

Tipo	Nombre De Activo	Dimensiones				
		Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	turno					
	Desarrollador del aplicativo SIREP y Aplicativo de turno			5%		
	Usuarios que manipulan la información de los documentos de Bachillerato y Pregrado			5%		

Fuente. Propiedad de los autores

Según la tabla anterior en caso que se materialice el robo del PC2, la empresa perdería más del 75% de la información ya que en este se encuentra alojado el aplicativo SIREP, que es un aplicativo utilizado solo en el CCAV para registrar la información académica de los estudiantes de bachillerato. Además cabe anotar que este aplicativo tiene vulnerabilidades que podrían poner en riesgo la seguridad, la integridad y la disponibilidad de la información, es necesario implementar herramientas salvaguardias que permitan garantizar la seguridad de los sistemas informáticos así como los datos que estas tienen.

Hoy en día existen muchas herramientas (Salvaguardias), que sirven para proteger los sistemas de información de una organización, las cuales se ven amenazada ante los diferentes casos y sucesos que puedan dañar su sistemas. Es de tener en cuenta que estas herramientas o medidas de restricción evitan que los daños o causas de los daños sean materializados. En la tabla siguiente se relacionan los salvaguardias que se pueden utilizar para cada activo:

Tabla 16. Listado de salvaguardias para cada activo

Tipo	Nombre De Activo	Salvaguardias
Activo de información	Datos del estudiantes	[D] Protección de la Información [D] Copias de seguridad de los datos (backup) [D] Aseguramiento de la integridad [D] Cifrado de la información
	Base de datos Sistema Integral de Registro Educación Permanente SIREP	[K] Gestión de claves criptográficas [K] Gestión de claves de cifra de información [K] Gestión de claves de firma de información [K] Gestión de certificados
	Documentos Físicos	Carpetas Estantes
Software o aplicación	Edunat	[SW] Protección de las Aplicaciones Informáticas [SW] Copias de seguridad (backup) [SW] Se aplican perfiles de seguridad [SW] Cambios (actualizaciones y mantenimiento) [SW] Aseguramiento de la disponibilidad [SW] Gestión de cambios (mejoras y sustituciones) [SW] Protección de servicios y aplicaciones web 5%
	Sirep	
	Sistemas de Turnos	
Hardware	PC1	[HW] Protección de los Equipos Informát [HW] Se aplican perfiles de seguridad
	PC2(Alojado Sirep)	

Tipo	Nombre De Activo	Salvaguardias
	PC3	[HW] Aseguramiento de la disponibilidad [HW] Cambios (actualizaciones y mantenimiento) [HW] Reproducción de documentos
	PC4(Alojado Sistema de turno)	
	PC5	
	PC6	
	PC7	
	Impresora laser	
Red	Switch	[COM] Protección de las Comunicaciones [COM] Aseguramiento de la disponibilidad [COM] Autenticación del canal [COM] Protección de la integridad de los datos intercambiados [COM] Protección criptográfica de la confidencialidad de los datos intercambiados [COM] Cambios (actualizaciones y mantenimiento) [COM] Internet: uso de ? acceso a [COM] Seguridad Wireless (WiFi)
Equipamiento auxiliar	UPS	[AUX] Elementos Auxiliares [AUX] Aseguramiento de la disponibilidad [AUX] Instalación [AUX] Suministro eléctrico AUX.AC Climatización [AUX] Protección del cableado
Instalación	Cables UTP	Canaletas
	Cables del fluido eléctrico	Ups Reguladores de voltajes Canaletas
Personal	Usuarios finales del aplicativo Edunat, Sirep, Aplicativo de turno	[PS] Gestión del Personal
	Desarrollador del aplicativo SIREP y Aplicativo de turno	[PS] Formación y concienciación
	Usuarios que manipulan la información de los documentos de Bachillerato y Pregrado	[PS] Aseguramiento de la disponibilidad

Fuente. Propiedad de los Autores

6.1.4 Relación de costos en caso que se materialice una amenaza.

Tabla 17. Valoración para activos

Escala de Valoración Cualitativa y Cuantitativa para los Activos		
Valoración Cualitativa	**Escala De Valor Cuantitativo**	**Valor Cuantitativo**
Muy Alto (MA)	> $ 15.000.001	$ 16.000.000
Alto (A)	$ 15.000.001 hasta $ 6.000.001	$ 7.500.000
Medio (M)	$ 6.000.000 hasta $ 1.000.001	$ 3.000.000
Bajo (B)	$ 1.000.000 hasta $ 100.001	$ 500.000
Muy bajo (MB)	$ 100.000 hasta $ 30.000	$ 50.000

Fuente. Propiedad de los Autores

En la tabla anterior se muestra la valoración para los activos que existen en la empresa.

En la tabla 18 se muestran los costos que debe asumir el CCAV en caso de que se materialice una amenaza.

Tabla 18. Costos que la empresa debe asumir en caso que se materialice una amenaza

Tipo	Nombre De Activo	Valoración Cualitativa	Valoración Cuantitativa
Activo de información	Datos del estudiantes	(MA)	$ 16.000.000
	Base de datos Sistema Integral de Registro Educación Permanente SIREP	(MA)	$ 16.000.000
	Documentos Físicos	(A)	$ 10.000.000
Software o aplicación	Edunat	(MA)	$ 16.000.000
	Sirep	(MA)	$ 16.000.000
	Sistemas de Turnos	(MB)	$ 50.000
Hardware	PC1	(M)	$ 3.000.000
	PC2(Alojado Sirep)	(MA)	$ 19.000.000
	PC3	(M)	$ 3.000.000
	PC4(Alojado Sistema de turno)	(M)	$ 4.000.000
	PC5	(M)	$ 3.000.000
	PC6	(M)	$ 3.000.000
	PC7	(M)	$ 3.000.000
	Impresora laser	(M)	$ 3.000.000
Red	Switch	(MB)	$ 100.000
Equipamiento auxiliar	UPS	(B)	$ 500.000
Instalación	Cables UTP	(MB)	$ 100.000
	Cables del fluido eléctrico	(MB)	$ 100.000
Personal	Usuarios finales del aplicativo Edunat, Sirep, Aplicativo de turno	(A)	$ 7.500.000
	Desarrollador del aplicativo SIREP y Aplicativo de turno	(MA)	$ 16.000.000
	Usuarios que manipulan la información de los documentos de Bachillerato y Pregrado	(A)	$ 7.500.000

Fuente. Propiedad de los Autores

7. POLITICAS DE SEGURIDAD PARA EL APLICATIVO SIREP, BASADOS EN LA NORMA ISO 27001

7.1 CAPITULO I: DE LAS FUNCIONES Y OBLIGACIONES DE LOS FUNCIONARIOS

Artículo 1. No enviar sin autorización previa del director del centro información de la empresa por los medios de comunicación.

Artículo 2. Se prohíbe el uso de aplicaciones sin la correspondiente licencia.

Artículo 3. Se le prohíbe los ingresos a redes sociales y el uso de herramientas para evadir los controles de seguridad, que evitan tal ingreso.

Artículo 4. Antes de firmar el contrato el funcionario debe firmar el acuerdo de confidencialidad de la información.

7.2 CAPITULO II: PARA EL CONTROL DE ACCESO FÍSICO

Artículo 5. Solo se permitirá acceso al personal autorizado.

Artículo 6. Si prohíbe manipular, alterar o violar los mecanismos de seguridad implementados para el acceso a la oficina.

Artículo 7. Como en la misma oficina existe personal de varias dependencias, es obligación asegurar la información manipulada en caso de levantarse del puesto.

Artículo 8. Todo usuario debe tener clave de inicio de sesión en sus equipos asignados.

7.3 CAPITULO III: DE LA SALIDA DE INFORMACIÓN.

Artículo 9. Teniendo en cuenta que dentro de la oficina existen funcionarios que desarrollan aplicaciones para apoyo a su gestión estos deben cifrar la información transferidas y guardadas en las bases de datos.

7.4 CAPITULO IV: DEL USO APROPIADO DE LOS RECURSOS.

Artículo 10. Uso de los recursos de la organización en actividades no relacionadas con la finalidad de la oficina.

Artículo 11. Antes de implementar una aplicación desarrollada esta debe ser aprobada por el personal a cargo de la seguridad de la información y por el director del centro.

Artículo 12. Registro en el sistema información ilegal o falsa.

Artículo 13. Instalar voluntariamente programas, virus, spyware o cualquier software malicioso que puedan causar daños a los recursos informáticos de la empresa.

Artículo 14. Desactivar o estropear los programas de protección de los equipos, por ejemplo firewall y antivirus.

Artículo 15. Alterar la información o modificar los datos.

Artículo 16. Falsificar los registros log de los sistemas de información.

Artículo 17. Intentar conseguir las claves de acceso a otros recursos de la empresa a la cual no tiene acceso.

7.5 CAPITULO V: DE LA MANIPULACIÓN SOFTWARE.

Artículo 18. Se debe pedir autorización antes de implementar una aplicación.

Artículo 19. Se prohíbe la instalación, desinstalación, actualización de las aplicaciones en los equipos, debido a que este proceso es realizado solo por el personal autorizado que son los funcionarios pertenecientes a medio y mediaciones.

Artículo 20. En caso de evidenciar errores en los sistemas de información debe comunicarlos a los desarrolladores de los aplicativos (SIREP y TURNOS).

7.6 CAPITULO VI: DEL USO DEL HARDWARE.

Artículo 21. El funcionario solo debe hacer uso de los equipos asignados para desarrollar actividades laborales.

Artículo 22. Se prohíbe al usuario abrir o tratar de abrir físicamente los equipos a su cargo.

Artículo 23. Se prohíbe intentar manipular los mecanismos de seguridad que se implementen a los equipos.

Artículo 24. Nunca sacar los equipos sin autorización.

Artículo 25. En caso de daño o indisponibilidad informar a la oficina de Gerencia de Innovación y Desarrollo Tecnológico (GIDT).

7.7 CAPITULO VII: DEL ACCESO A INTERNET

Artículo 26. Solo se accede a páginas autorizadas y se prohíbe el uso de software o aplicaciones que violen las restricciones establecidas.

Artículo 27. El acceso a la red solo se realizará por medio de la red establecida.

Artículo 28. En caso de tener inconvenientes con el acceso a internet informar a la oficina de Gerencia de Innovación y Desarrollo Tecnológico (GIDT), por tanto se prohíbe en intento de solucionarlo por su cuenta.

7.8 CAPITULO VIII: DEL USO CORRECTO DEL CORREO ELECTRÓNICO.

Artículo 29. Toda información institucional solo puede ser enviada por medio del correo institucional.

Artículo 30. En el correo institucional se prohíbe el envío de información que no tenga que ver con la entidad.

Artículo 31. Se prohíbe alterar los mensajes de correo electrónicos de otros usuarios.

Artículo 32. Se prohíben los envíos de correos masivos con fines publicitarios o comerciales.

Artículo 33. En caso de tener sospecha de correos con intenciones mal intencionado el usuario debe comunicar al personal competente para tal fin.

7.9 CAPITULO IX: DE LAS CONTRASEÑAS

Artículo 34. Todos los usuarios que tengan uso del sistema de información deben tener sus propias credenciales de acceso.

Artículo 35. En caso de retiro o despido del funcionario se debe informar a las personas competentes para deshabilitar de la clave.

Artículo 36. El conocimiento de las claves deben ser enviadas por medio del correo institucional, esta debe ser cambiada por el funcionario al momento de su recepción, dejando claro que el aplicativo generará la clave.

Artículo 37. La contraseña debe ser de un tamaño de longitud de 8 caracteres en la cual se debe tener en cuenta letra mayúscula, símbolos y caracteres especiales.

Artículo 38. La contraseña debe ser cambiada cada 3 meses.

Artículo 39. Se bloqueará bloquear al usuario por quince minutos en casos de más de tres intentos fallidos de acceder al sistema.

7.10 CAPITULO X: DE LAS COPIAS DE SEGURIDAD

Artículo 40. Los funcionarios desarrolladores deben implementar mecanismos o estrategias de copias de seguridad para sus bases de datos y aplicaciones.

Artículo 41. Las copias de seguridad deben ser guardas en un medio diferente al operacional.

Artículo 42. Cada copia de seguridad debe ser rotulada con el nombre de la aplicación seguido de la fecha y hora del proceso de copia de seguridad.

RECOMENDACIONES

La investigación desarrollada para la Identificación de las Vulnerabilidades y el Diseño de Políticas de Seguridad para la Aplicación Web Sistema Integral de Registro Educación Permanente (SIREP) de la UNAD CCAV Cartagena, fue desarrollada siguiendo los pasos metodológicos necesarios para un trabajo de Monografía.

Las siguientes son las recomendaciones de los autores:

1. Desarrollar las Políticas de Seguridad de acuerdo a las necesidades específicas de la empresa.

2. Concientizar al personal en general de la empresa de la importancia de conocer cuáles son las Políticas de Seguridad que están implementadas y de la necesidad de ponerlas en práctica.

3. Los desarrolladores de aplicaciones WEB deben validar cada campo de ingreso de datos esto con el fin de evitar la vulnerabilidad de inyección de datos.

4. Configurar de una forma adecuada el servidor web de acuerdo, con el fin de aumentar la seguridad de la aplicación.

5. Instalar un sistema de operativo para servidores en el servidor web

6. Realizar con los aplicativos VEGA y ZAP escaneo de vulnerabilidades antes de la implementación del Aplicativo WEB, si después del escaneo se identifican vulnerabilidades se deben realizar los respectivas correcciones.

7. Capacitar a las usuarios sobre cada una de las políticas de seguridad establecidas

CONCLUSIONES

De acuerdo a los escaneos realizado a la aplicación SIREP por parte de las aplicaciones VEGA de Subgrap, y OWASP ZAP se puede concluir que es una aplicación actualmente insegura, ya que en ella se encontraron varias vulnerabilidades provenientes desde cómo se ha desarrollado la aplicación y la forma como se tiene configurado el servidor Web.

En el escáner realizado se pudieron identificar vulnerabilidades las cuales según análisis realizado mediante MAGERIT y las mismas aplicaciones fueron consideras de riesgos de alto, medio y bajo nivel debido al impacto que estas pueden causar en caso que una amenaza aproveche dichas debilidades.

Al identificar las vulnerabilidades se plantearon recomendaciones y/o soluciones que permitieran mitigar dicha vulnerabilidad.

Se establecieron políticas de seguridad para el CCAV Cartagena que garantizan la confidencialidad, la disponibilidad y la integridad de la aplicación, por lo que se aconseja sean publicadas por los medios con los que cuenta la Universidad y se socialice con todos los funcionarios que laboran actualmente.

Para futuros desarrollos de aplicaciones, este documento debe ser una consulta necesaria que deben tomar en cuenta los directivos de la Universidad para que los nuevos aplicativos presenten el mínimo de vulnerabilidades.

BIBLIOGRAFÍA

ALAMILLO DOMINGO, I. (2009). Las políticas públicas en materia de seguridad en la sociedad de la información. *IDP: revista de Internet, derecho y política*.

ALEGRE RAMOS, M. D., & GARCIA-CERVIGON HURTADO, A. (2011). *SEGURIDAD INFORMATICA.* Madrid: ED.11 Paraninfo.

AMAYA TARAZONA, C. A. (2013). *Seguridad en aplicaciones WEB.* Boyacá.

BELLO HERNANDEZ, R. O., & ALFONSO SÁNCHEZ, I. R. (2003). Elementos teórico-prácticos útiles para conocer los virus informáticos. *ACIMED*.

BENAVIDES RUANO, M. d., & Solarte Solarte, F. J. (2012). *Modelo riesgos y control informatico.* Pasto.

GÓMEZ DE ILLERA, M., APARICIO RODRÍGUEZ, A., ORTEGA, A. R., CAMACHO OLIVEROS, M., RONDÓN DURÁN, J. E., ROCHA, M. G., Y OTROS. (2011). *La Investigación Ciencias en la Escuela De Básicas, Tecnología E Ingeniería.* Bogotá.

GONZALEZ SABABRIA, Y. A., & CASTAÑO GALVIS, W. (2012). *Fundamentos de Seguridad Informáticas.* Bucaramanga.

INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma Técnica Colombiana para la presentación de tesis, trabajos de grado, y otros trabajos de investigación. Bogotá D.C., ICONTEC, 2008. NTC 1486.

INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma Técnica Colombiana para la Tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información (SGSI), requisitos. Bogotá D.C., ICONTEC, 2006. NTC-ISO/IEC 27001.

INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma Técnica Colombiana para las referencias bibliográficas, contenido, forma y estructura. Bogotá D.C., ICONTEC, 2008. NTC 5613.

INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma Técnica Colombiana para las referencias documentales para fuentes de información electrónicas. Bogotá D.C., ICONTEC, 1998. NTC 4490.

MARRERO TRAVIESO, Y. (2003). La Criptografía como elemento de la seguridad informática. *ACIMED*.

MORALES SALAZAR, J. I. (2013). *Criptografia.* Medellin.

RAMIREZ VILLEGAS, G. M., & CONSTAIN MORENO, G. E. (2012). *Modelos de los Estandares de Seguridad en Informatica.* Zona Centro-Sur Colombia.

ROZO, E. A. (Enero de 2013). PROYECTO DE SEGURIDAD INFORMÁTICA I. La Plata, Huila, Colombia.

VALDIVIA MIRANDA, C. (2014). *Sistemas Informaticos y redes Locales.* Paraninfo, SA.

WEBGRAFÍA

Alcaldia de Bogotá. (23 de Enero de 1996). Recuperado el 12 de Septiembre de 2014, de http://www.sice.oas.org/trade/junac/decisiones/dec351s.asp

Archivo General de la Nación. (18 de Agosto de 1999). Recuperado el 18 de Octubre de 2015, de Archivo General de la Nación: http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf

Asociación Colombiana de Intérpretes. (5 de Febrero de 1993). Recuperado el 18 de Octubre de 2015, de acinpro: http://www.acinpro.org.co/sitio/images/LEY_44_de_1993.pdf

C. a. (27 de noviembre de 2011). *Tutorial como Encriptar archivos de nuestra computadora o usb [TrueCrypt]*. Recuperado el 7 de marzo de 2014, de Tutorial como Encriptar archivos de nuestra computadora o usb [TrueCrypt]: http://www.youtube.com/watch?v=EHtEVfYbjNU

CABEZUELO LÓPEZ, S. (s.f.). *Seguridad en redes*. Recuperado el 10 de Junio de 2014, de http://spi1.nisu.org/recop/al02/sergi/index.html

CANO, J. J., & PH, D. (27 de Enero de 2004). *Inseguridad informática: Un concepto dual en seguridad informática.* Recuperado el 01 de Mayo de 2014, de Inseguridad informática: Un concepto dual en seguridad informática.: http://www.acis.org.co/index.php?id=341

Funk, C., & Garnaeva, M. (10 de Diciembre de 2013). *Virulist*. Recuperado el 14 de Enero de 2015, de Kaspersky Security Bulletin 2013. Estadística principal de 2013: http://www.viruslist.com/sp/analysis?pubid=207271239

INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI. (24 de Julio de 2000). Recuperado el 18 de Octubre de 2015, de LEY 599 DE 2000: http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/Codigo_Penal.pdf

OWASP Top10. (2010). Recuperado el 1 de Diciembre de 2013, de OWASP Top10: http://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CFIQFjAD&url=http%3A%2F%2Fowasptop10.googlecode.com%2Ffiles%2FOWASP%2520Top%252010%2520-%25202013%2520-%2520RC1.pdf&ei=hMWaUsWrJ42pkAfxwYGQDQ&usg=AFQjCNGu9nysl5fTt8L02jm47Ep9hyeaEA&bvm

PALTA VELASCO, E. (2012). *Introduccion en la seguridad en redes.* Popayan.

pereda, C. F. (19 de Enero de 2012). *Tecnologia El país.* Recuperado el 18 de octubre de 2015, de Las claves de las leyes SOPA y PIPA: http://tecnologia.elpais.com/tecnologia/2012/01/19/actualidad/1326967261_850215.html

SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C. (18 de Mayo de 2001). *Política oficial de SeguridadInformática del CICESE.* Recuperado el 30 de Noviembre de 2013, de Política oficial de

SeguridadInformática del CICESE: http://www.slideshare.net/jenyrolfin/ejemplo-politica-de-seguridad

UNIVERSIDAD DE EXTREMADURA. (2 de Abril de 2014). *Inyección de código SQL*. Recuperado el 6 de Junio de 2014, de http://cala.unex.es/cala/epistemowikia/index.php?title=Inyecci%C3%B3n_de_c%C3%B3digo_SQL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. (11 de Abril de 2014). *Sistema Gestion de calidad*. Recuperado el 11 de Abril de 2014, de Sistema Gestion de calidad: http://calidad.unad.edu.co/evaluacion-seguimiento-y-medicion/balance-de-gestion-y-rendicion-de-cuentas

Vega Briceño, E. A. (s.f.). *Introducción*. Recuperado el 21 de Marzo de 2013, de Los sistemas de información y su importancia para las organizaciones y empresas: http://www.monografias.com/trabajos24/tics-empresas/tics-empresas.shtml

wikipedia. (11 de Marzo de 2013). *Ettercap*. Recuperado el 05 de mayo de 2014, de Ettercap: http://es.wikipedia.org/wiki/Ettercap

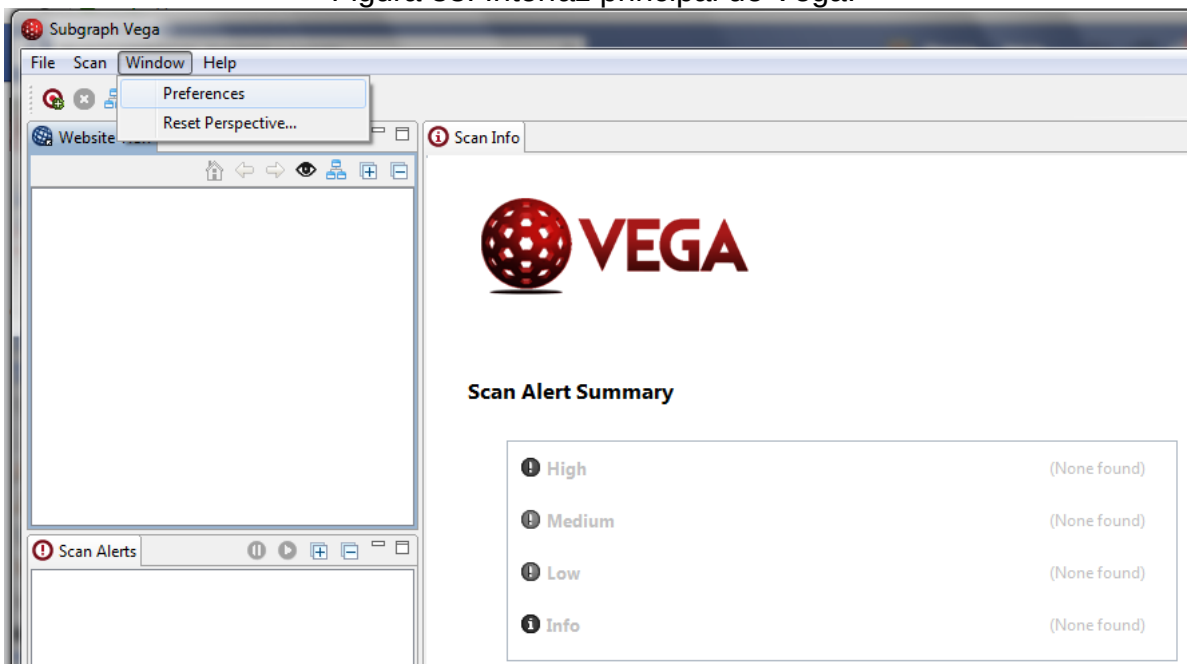
wikipedia. (27 de Abril de 2014). *Seguridad informática*. Recuperado el 05 de Mayo de 2014, de Seguridad informática: http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

ANEXOS

ANEXO A. CONFIGURACIÓN DE VEGA

Una vez instalada la aplicación el siguiente paso es configurarla para su uso, por lo tanto ese será el primer proceso a realizar antes de comenzar; Para configurar el proxy se ingresa al menú principal Windows y se selecciona la opción Preferences, tal como se ve a continuación:

Figura 33. Interfaz principal de Vega.



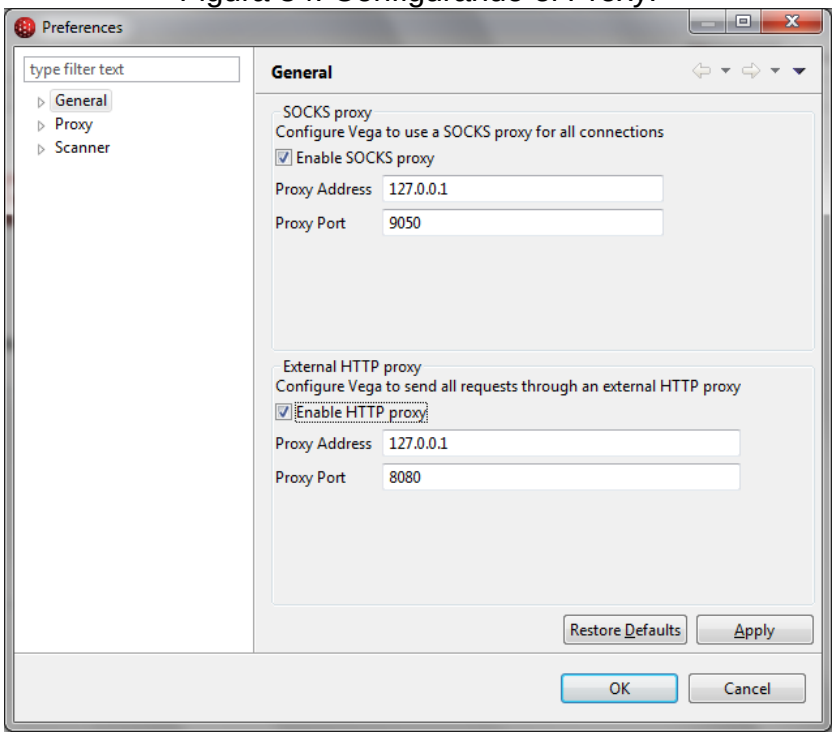
Fuente. Aplicación VEGA, Ubicación de la opción Preference .

Al desplegarse la ventana Preferences y en la pestaña general encontraremos dos opciones que son:

- SOCKS proxy: se configura un socks proxy para usarlo en todas sus conexiones ("").
- External HTTP proxy: Aquí se configura un proxy HTTP externo para enviar todas las *peticiones* DNS ("").

Se selecciona las dos y se presiona el botón Apply

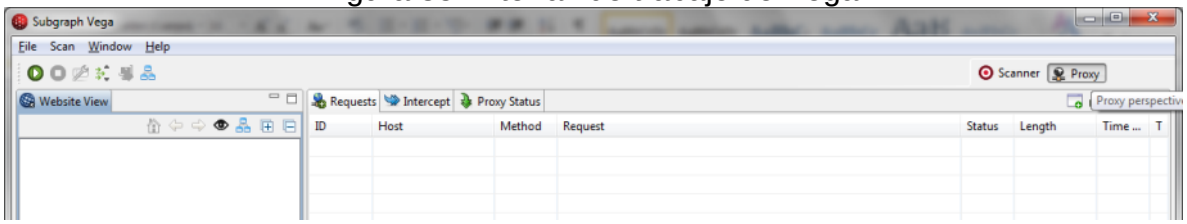
Figura 34. Configurando el Proxy.



Fuente. Aplicación VEGA, Configuración del proxy.

Antes de comenzar con el escáner se debe obtener un valor de cookie usando el proxy, dicho valor se utilizará en la opción de autentificación, para analizar con una sesión autenticada, para tal fin se escoge la opción proxy botón ubicado en parte derecha y luego se presiona el botón Play.

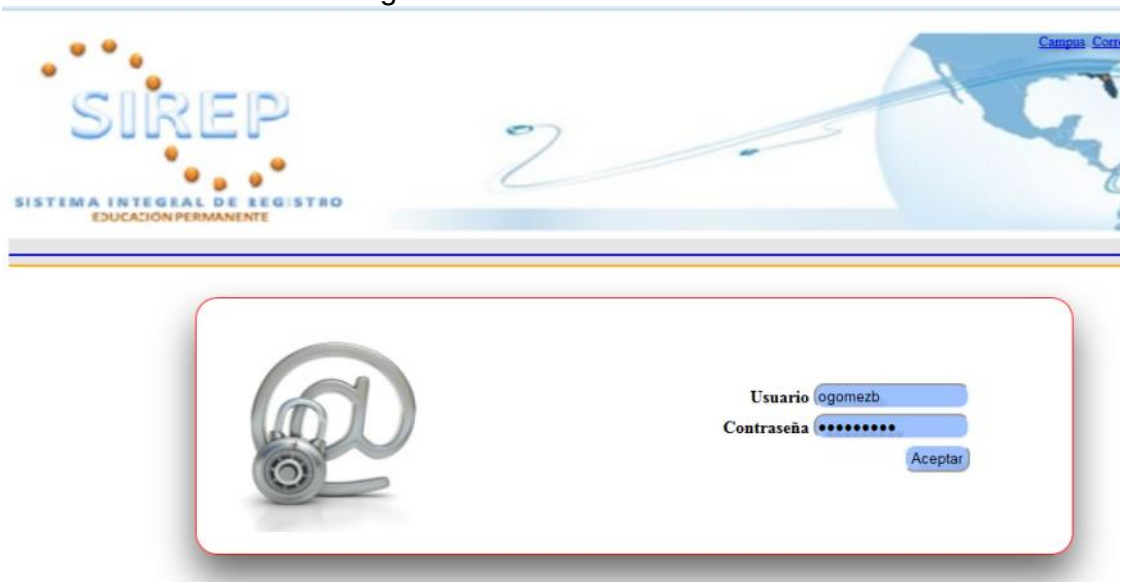
Figura 35. Interfaz de trabajo de Vega.



Fuente. Aplicación Vega, área de trabajo.

Una vez realizado el proceso anterior se ingresa a la aplicación que se desea escanear.

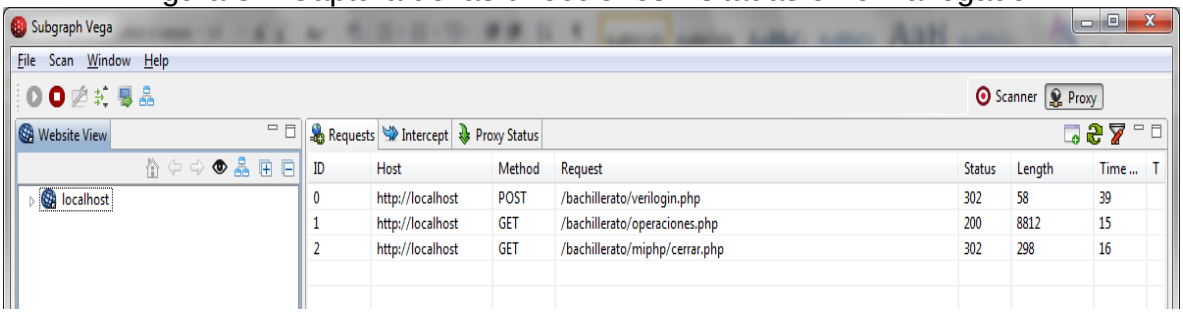
Figura 36. Interfaz de bienvenida.



Fuente. Aplicación SIREP, autenticación de usuario.

Al ingresar al aplicativo abrir nuevamente la aplicación VEGA y en la pestaña Requests se encontrará las páginas a las cuales se ha ingresado:

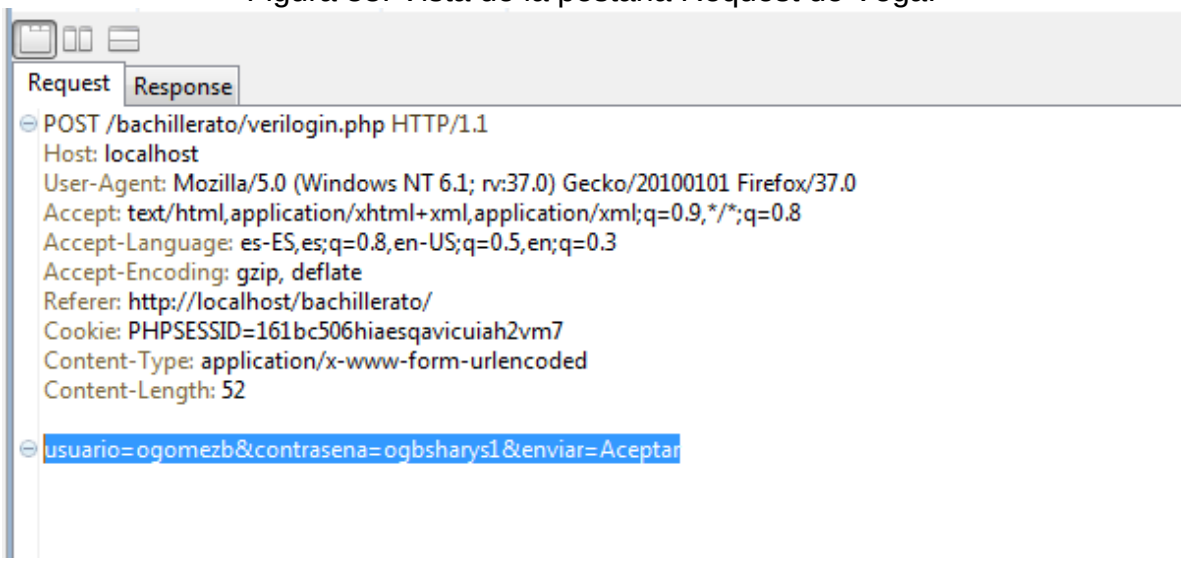
Figura 37. Captura de las direcciones visitadas en el navegador.



Fuente. Aplicación VEGA, captura de direcciones web visitadas.

Al seleccionar la primera página a la que se hace referencia, se encontrará el cookie a utilizar:

Figura 38. Vista de la pestaña Request de Vega.

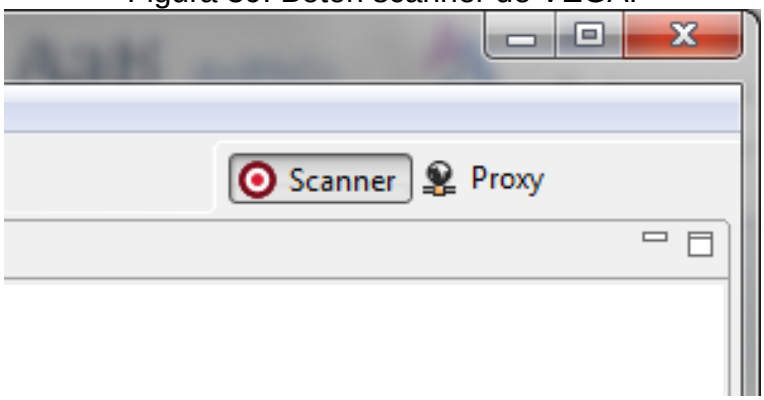


Fuente. Aplicación VEGA, identificación del cookie.

Como se puede apreciar en la imagen anterior SIREP no utiliza ningún tipo de encriptación de datos por lo que en este primer escaneo se obtuvo una clave de acceso sin ningún problema.

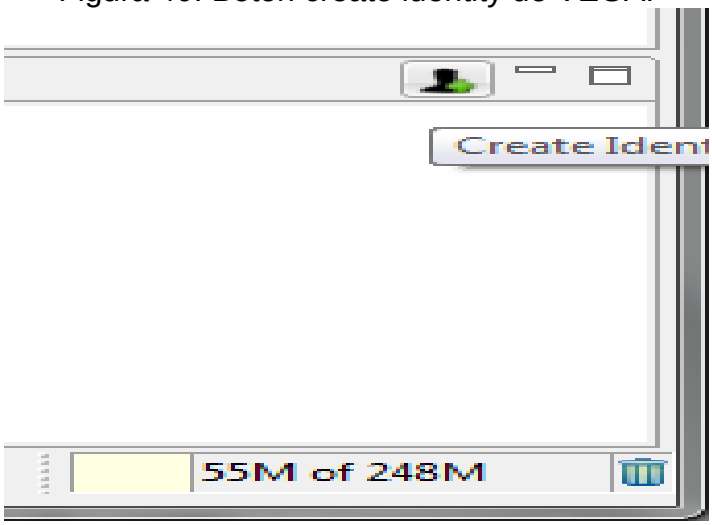
Ahora para automatizar y realizar una exploración autenticada se da clic en el botón Scanner de la herramienta VEGA y se da clic en el botón Create Identity ubicada en la parte inferior de la pantalla:

Figura 39. Botón scanner de VEGA.



Fuente. Aplicación VEGA, identificación del botón Scanner.

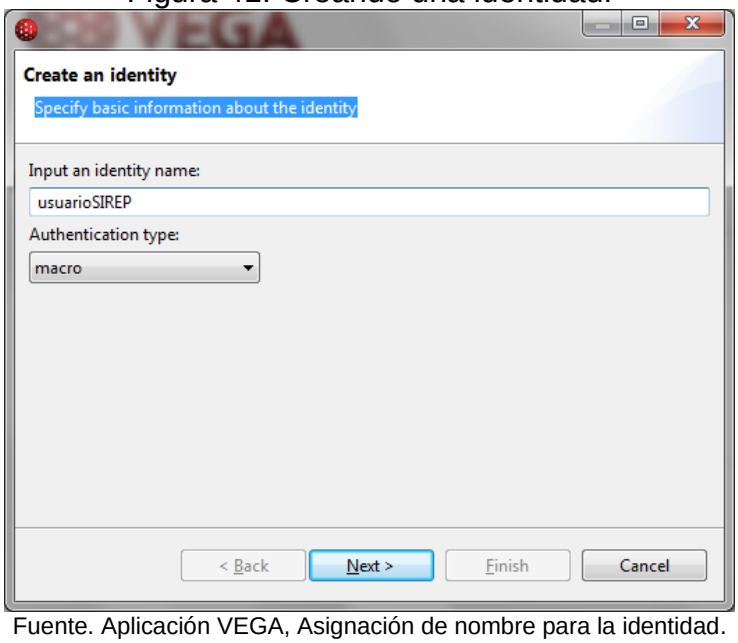
Figura 40. Botón create identity de VEGA.



Fuente. Aplicación VEGA, identificación del botón Create Identity.

Al dar clic en el botón Create Identity, se desplegará una ventana en el cual le pedirá el nombre de la identidad a crear, para el caso lo llamaremos usuarioSIREP y se especifica el tipo de autenticación para el caso se selecciona Macros, el cual permite registrar las solicitudes que se puedan utilizar con la identidad:

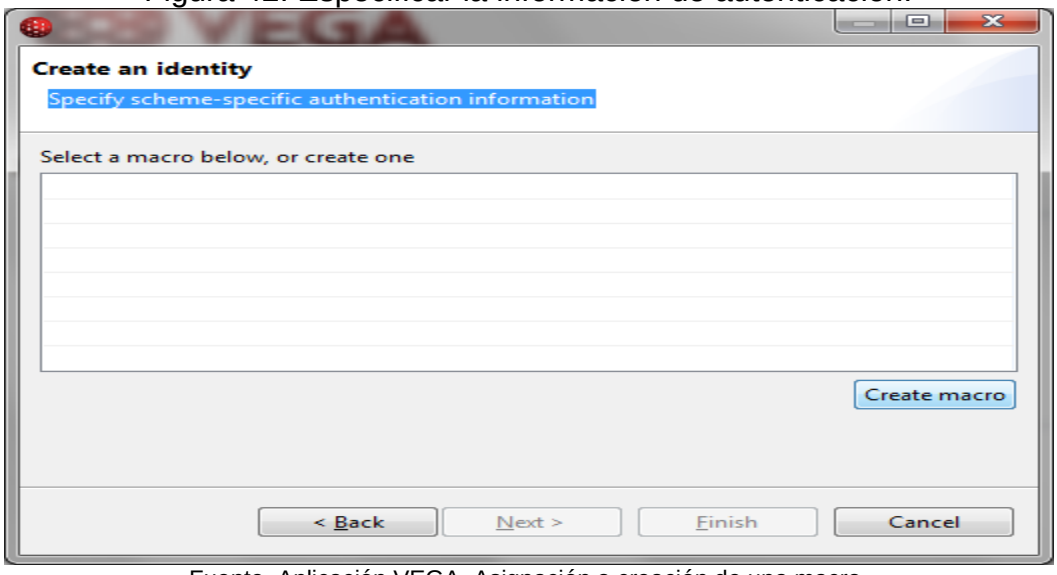
Figura 41. Creando una identidad.



Fuente. Aplicación VEGA, Asignación de nombre para la identidad.

El siguiente paso es especificar la información de autenticación el cual se puede crear o elegir, para el caso se va a crear, por lo que se presiona el botón Create macro.

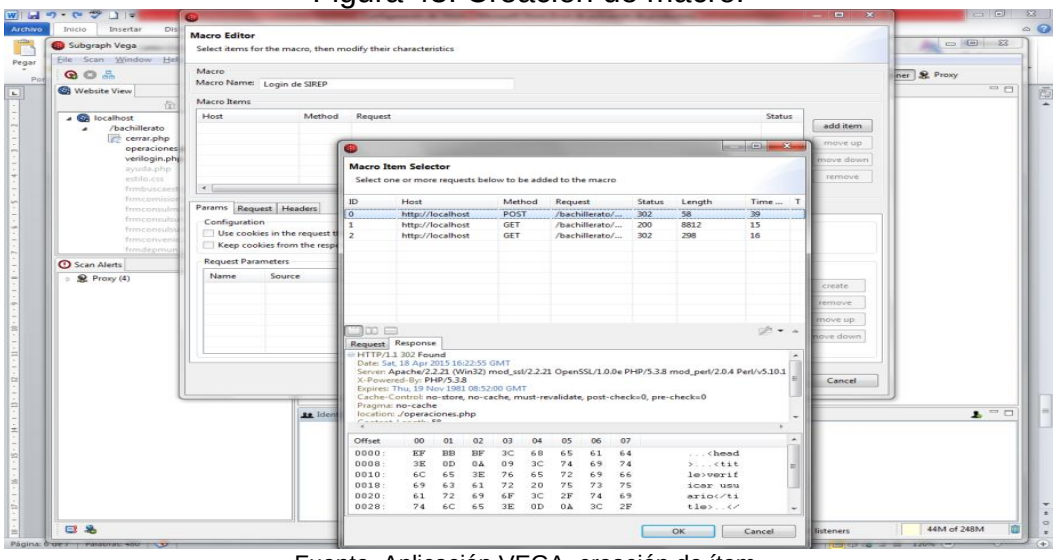
Figura 42. Especificar la información de autenticación.



Fuente. Aplicación VEGA, Asignación o creación de una macro.

Al abrir la nueva ventana se le da el nombre al nuevo macro y se añade lo que abrirá una nueva ventana como se evidencia a continuación:

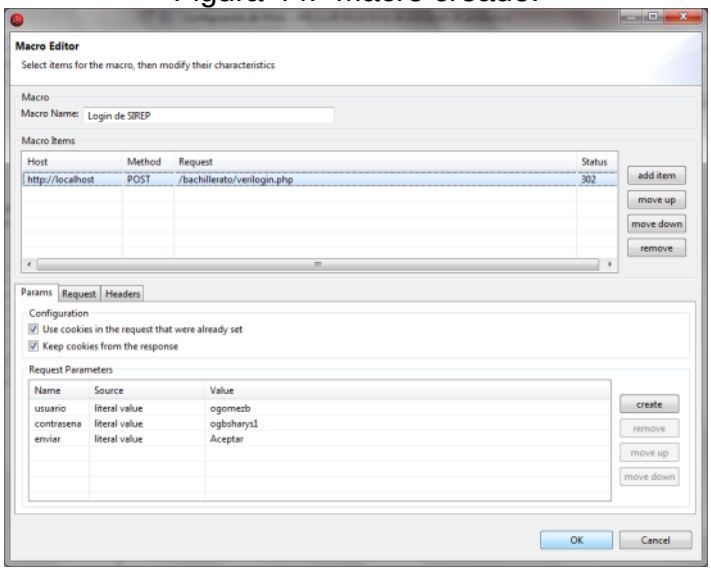
Figura 43. Creación de macro.



Fuente. Aplicación VEGA, creación de ítem.

Se presiona el botón Ok, se selecciona el macro y se presiona Ok

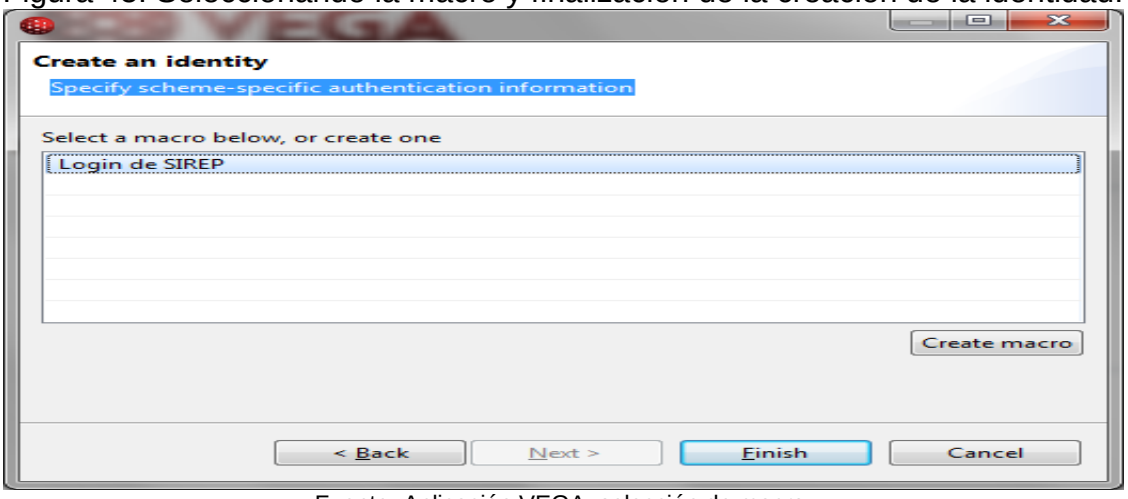
Figura 44. Macro creado.



Fuente. Aplicación VEGA, asignación item de macro.

Por último dar clic en el botón Finish

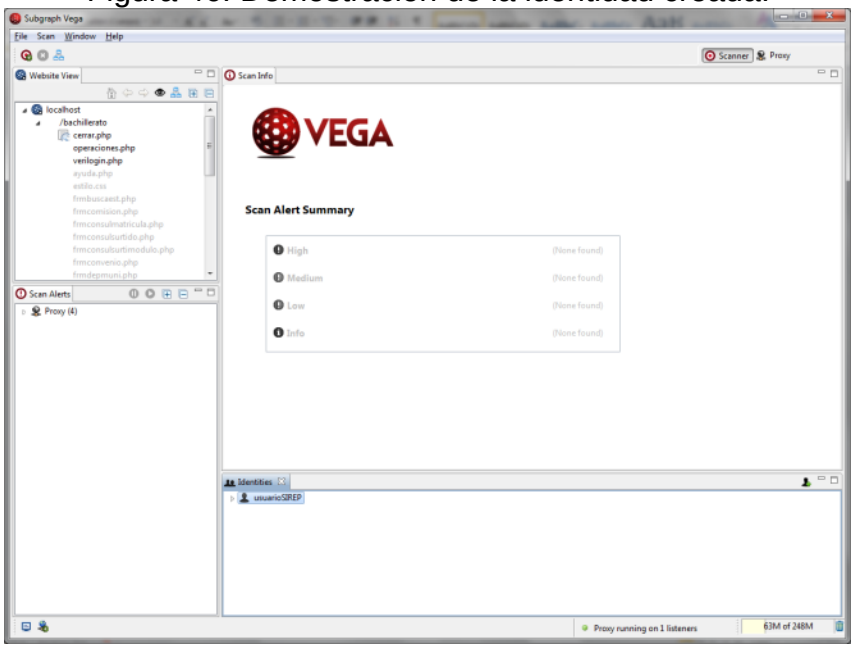
Figura 45. Seleccionando la macro y finalización de la creación de la identidad.



Fuente. Aplicación VEGA, selección de macro.

En la siguiente figura se muestra ya la identidad creada:

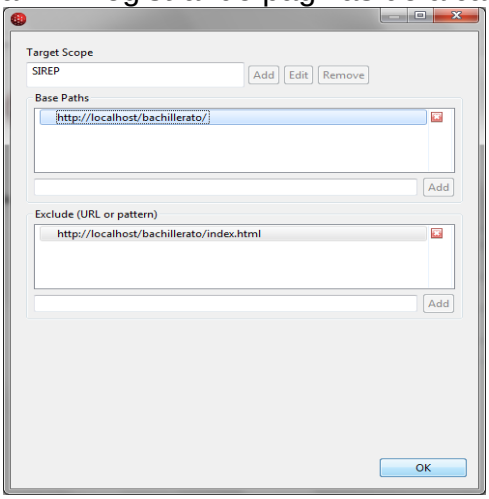
Figura 46. Demostración de la identidad creada.



Fuente. Aplicación VEGA, identidad creada.

El siguiente paso es agregar algunas páginas del SIREP como objetivos de alcances, así como las que se van a excluir para el caso en estudio, se van a agregar todas las páginas, entonces para tal fin se dirige al menú principal Scan y se selecciona la opción Edit Target Scope.

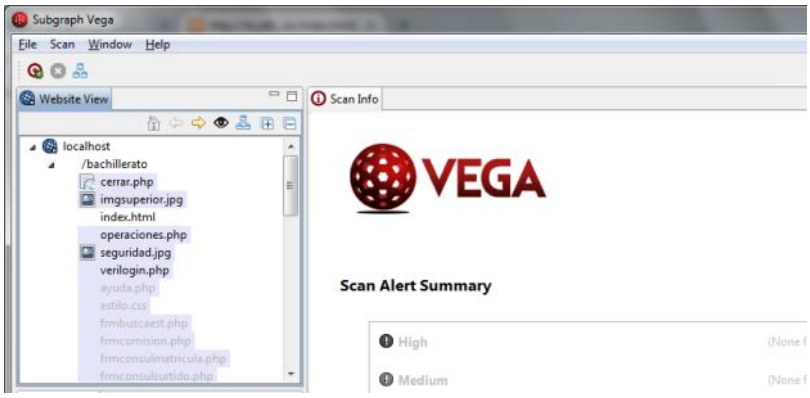
Figura 47. Registrando páginas de alcances.



Fuente. Aplicación VEGA, Asignación de páginas de alcance.

A continuación se resaltan las páginas que se van a escanear, exceptuando la página Index.html.

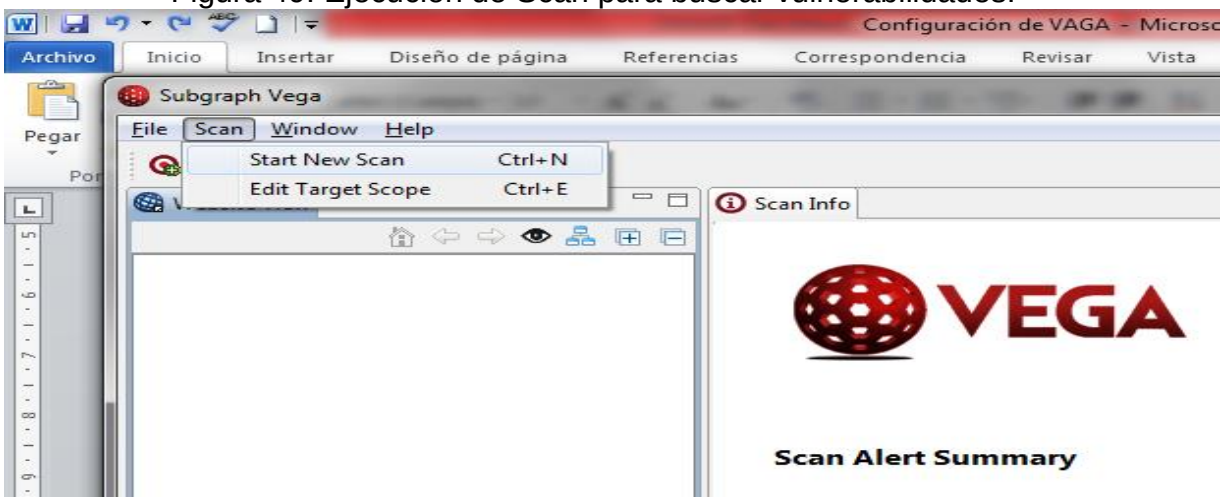
Figura 48. Evidencia de la inclusión y exclusión de las páginas objetivos de alcance.



Fuente. Aplicación VEGA, inclusión de páginas.

Ahora para realizar el escaneo a la aplicación SIREP (el cual está en una red local), con la macro creada, se presiona el botón Start New Scan o Ctrl + N.

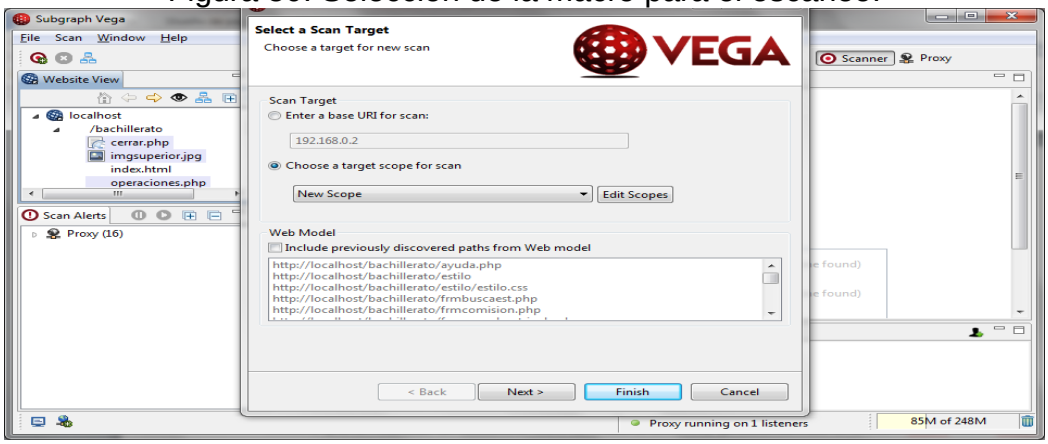
Figura 49. Ejecución de Scan para buscar vulnerabilidades.



Fuente. Aplicación VEGA, botón para inicio de scaner.

Se abrirá una ventana en la que se escogerá la macro el cual se creó con nombre SIREP:

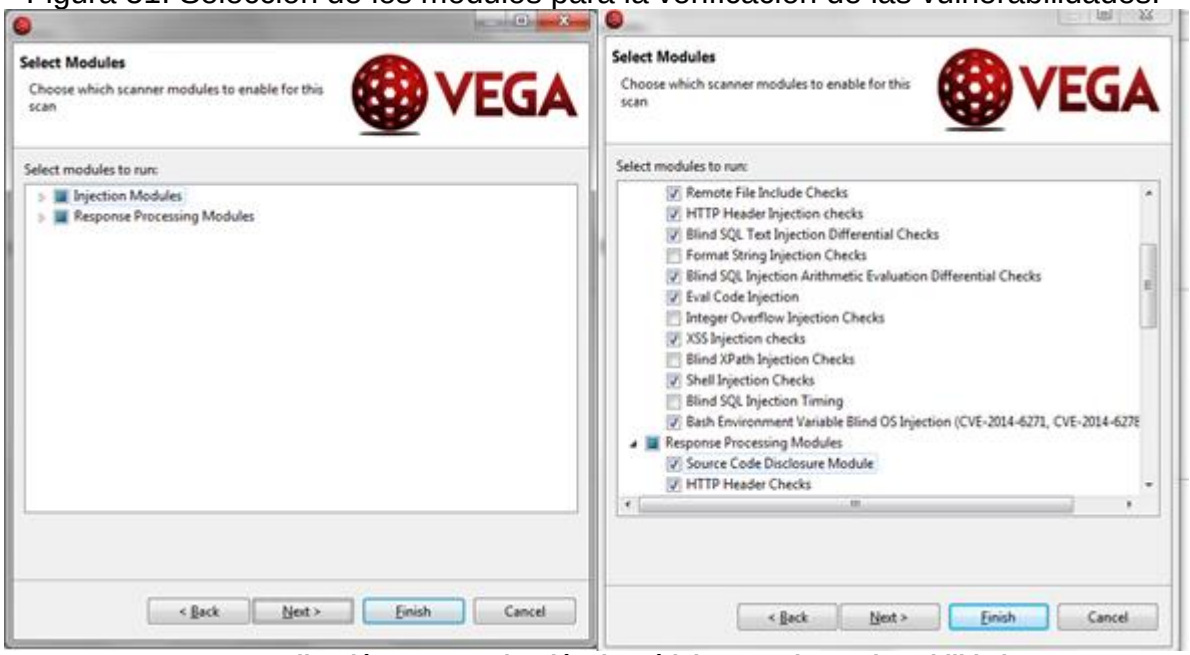
Figura 50. Selección de la macro para el escaneo.



Fuente. Aplicación VEGA, asignación de macro.

Start New Scan desplegará una ventana en la que se le dará la URL a escanear, al dar siguiente se eligen los módulos que se quieren ejecutar los cuales están clasificados en dos grupos que son Inyection Modules y Response Processing Modules tal y como se puede observar en las siguientes imágenes:

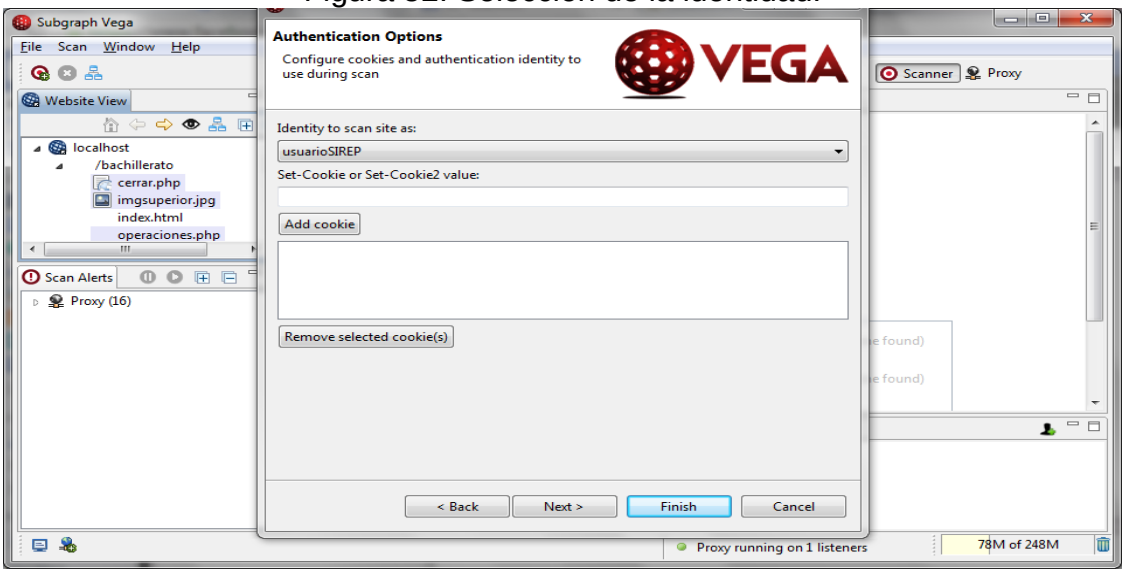
Figura 51. Selección de los módulos para la verificación de las vulnerabilidades.



Fuente. Aplicación VEGA, Selección de módulos a evaluar vulnerabilidad.

Se presiona el botón siguiente para configurar cookies y autenticación de identidad para usar durante la exploración teniendo en cuenta que nuestra identidad creada tiene por nombre usuarioSIREP, se elige y se presiona el botón Next y por ultimo Finish.

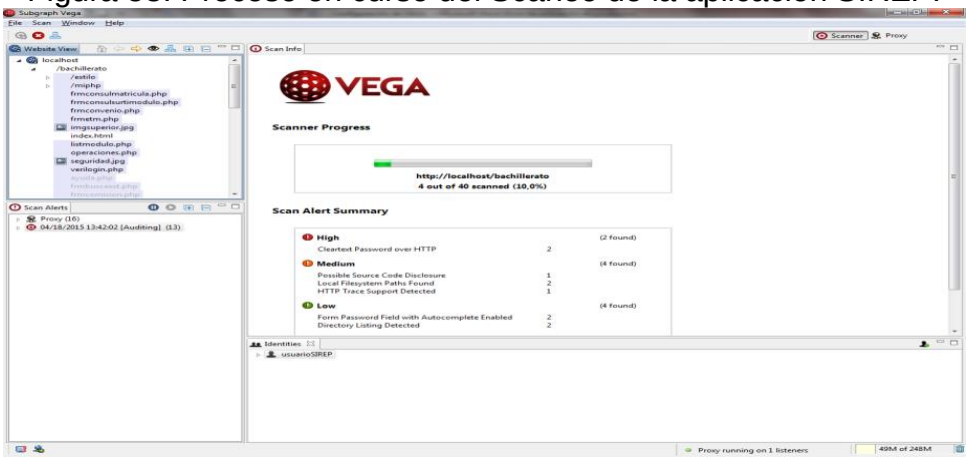
Figura 52. Selección de la identidad.



Fuente. Aplicación VEGA, asignación de identidad.

Al presionar el botón Finish comenzará el proceso de escaneo tal y como se muestra a continuación:

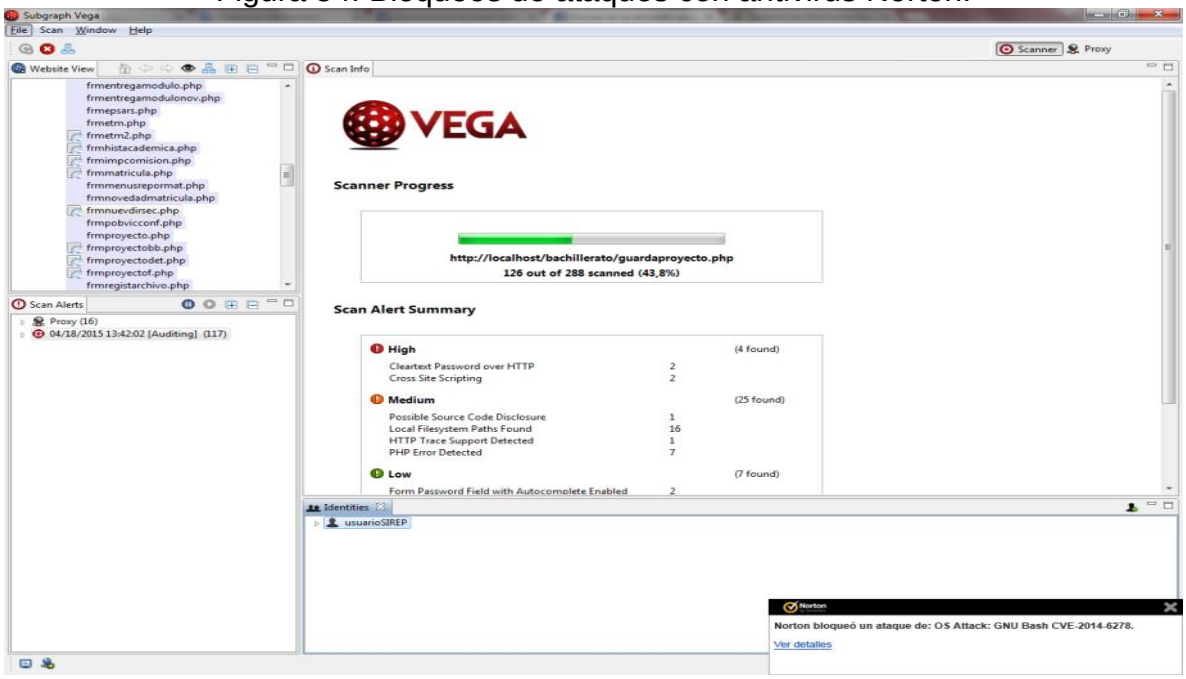
Figura 53. Proceso en curso del Scaneo de la aplicación SIREP.



Fuente. Aplicación VEGA, escáner en proceso.

En la figura 31 se aprecia como el antivirus intenta bloquear los ataques realizados por VEGA, se termina el proceso para ver los resultados:

Figura 54. Bloqueos de ataques con antivirus Norton.



Fuente. Aplicación VEGA y Norton, bloque de ataque por Norton.

Escaneo completo.

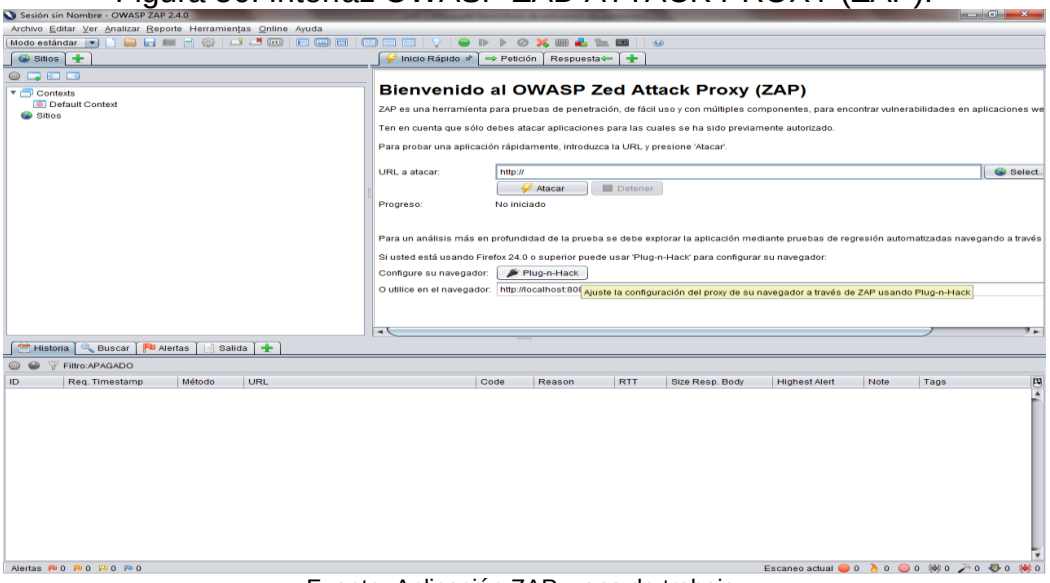
Figura 55. Finalización del escáner.

Fuente. Aplicación VEGA, resultados del escaner.

ANEXO B. CONFIGURACIÓN DE OWASP ZAD ATTACK PROXY (ZAP)

Para configurar ZAP primero hay que tener en cuenta realizar la configuración del navegador antes de realizar los ataques de penetración, para este caso se va a utilizar el navegador Firefox y esta es una versión superior Firefox 24.0 solamente se procederá a presionar el botón “Plug-n-Hack”, tal como se puede apreciar a continuación:

Figura 56. Interfaz OWASP ZAD ATTACK PROXY (ZAP).



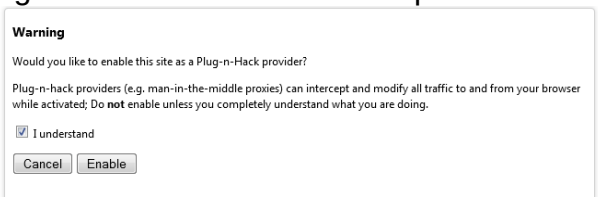
Fuente. Aplicación ZAP, zona de trabajo.

Durante la instalación del complemento Firefox Plug-n-Hack, se preguntará si se desea activar el sitio como un proveedor de Plug-n-Hack. Si se habilita el sitio como Plug-n-Hack este queda activado para que pueda interceptar y modificar todo el tráfico desde y hacia el navegador, siempre y cuando se encuentre activa.

Figura 57. Configuración del navegador Mozilla y ZAP.

Fuente. Navegador Mozilla, configuración de proxy ZAP.

Figura 58. Instalación del complemento ZAP.



Fuente. Navegador Mozilla, instalación de plung-n-Hack provider.

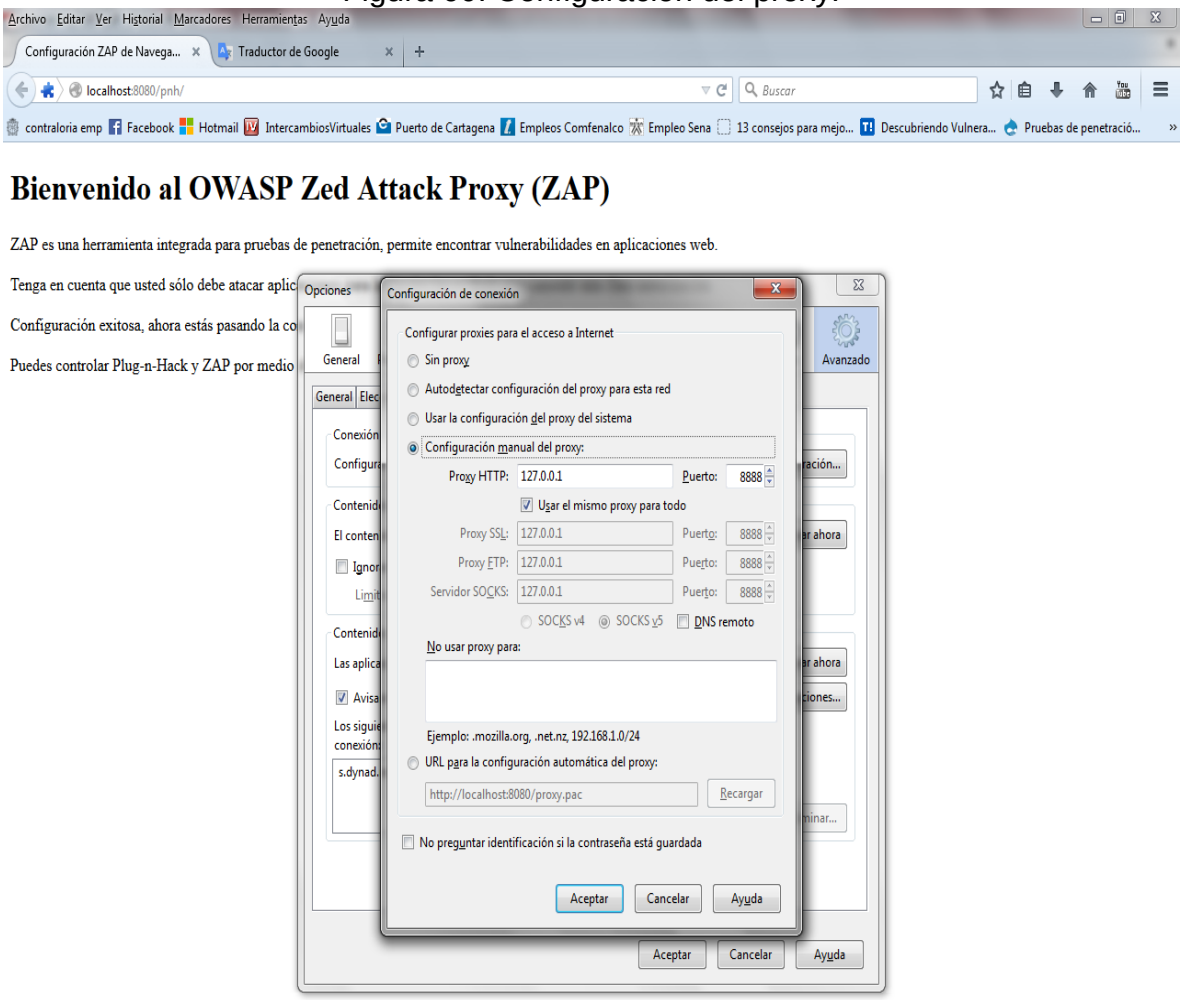
Al terminar la instalación del complemento, dará la bienvenida.

Figura 59. Finalización de la instalación del complemento ZAP.

Fuente. Navegador Mozilla, Instalación exitosa.

Terminada la instalación se procede a configurar los proxies para el acceso a internet del navegador.

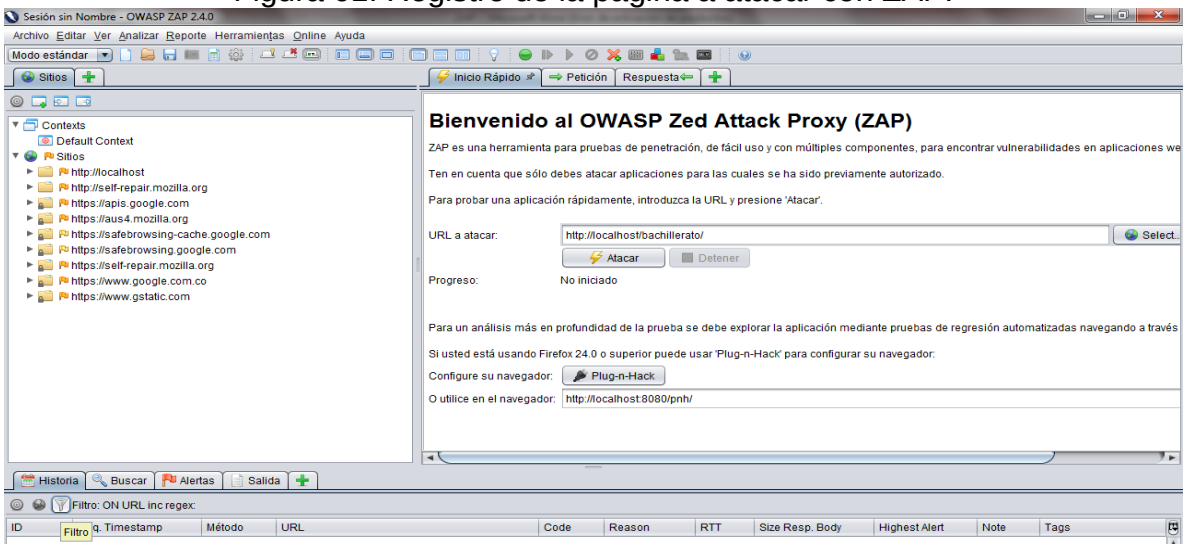
Figura 60. Configuración del proxy.



Fuente. Navegador Mozilla, configuración de proxy con ZAP.

El siguiente paso es crear una sección, se especifica un filtro, si se desea para el caso se registraran tres direcciones web que se desean ignorar, para tal fin se presiona el botón Filtro:

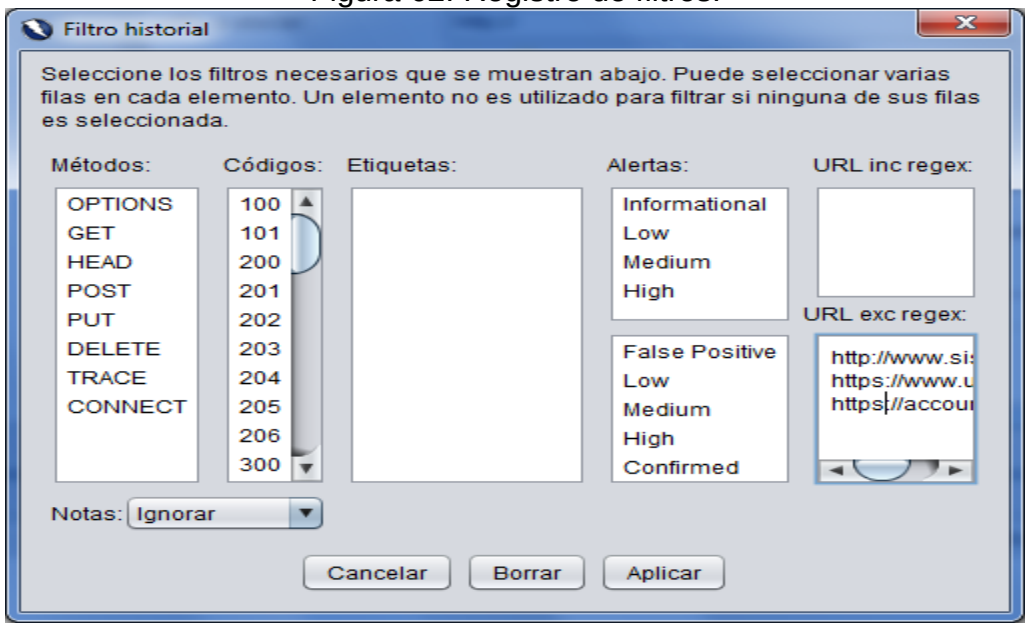
Figura 61. Registro de la página a atacar con ZAP.



Fuente. Aplicación ZAP, registro de objetivo.

AL abrir la ventana de filtro histórico se registran las direcciones que no se desea atacar:

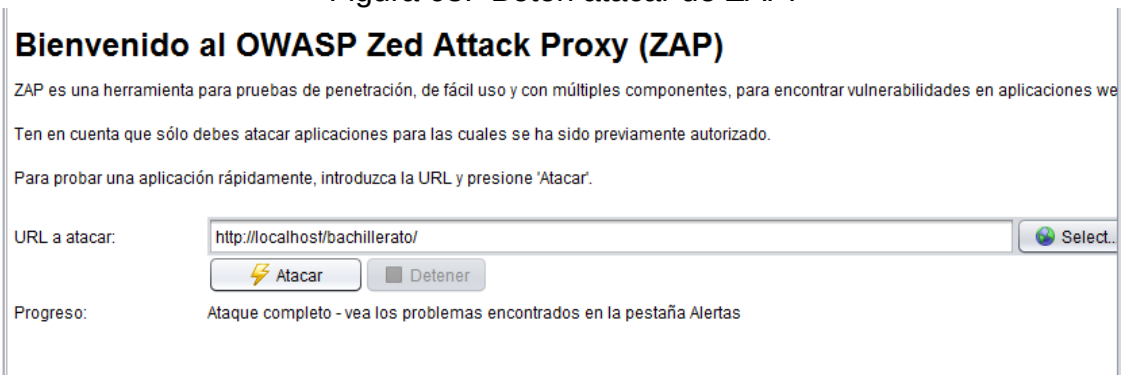
Figura 62. Registro de filtros.



Fuente. Aplicación ZAP, Métodos de filtros.

Se presiona el botón Aplicar. una vez configurada la sección se presiona el botón Atacar.

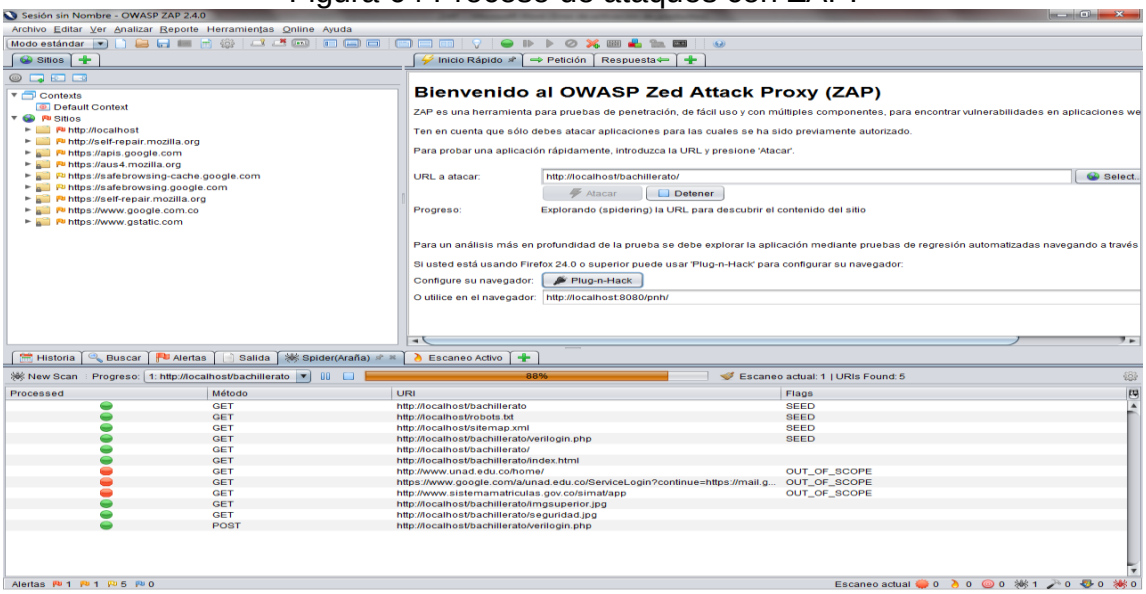
Figura 63. Botón atacar de ZAP.



Fuente. Aplicación ZAP, registro de página a atacar.

En la figura 65 se aprecia los resultados que va arrojando el ataque con ZAP

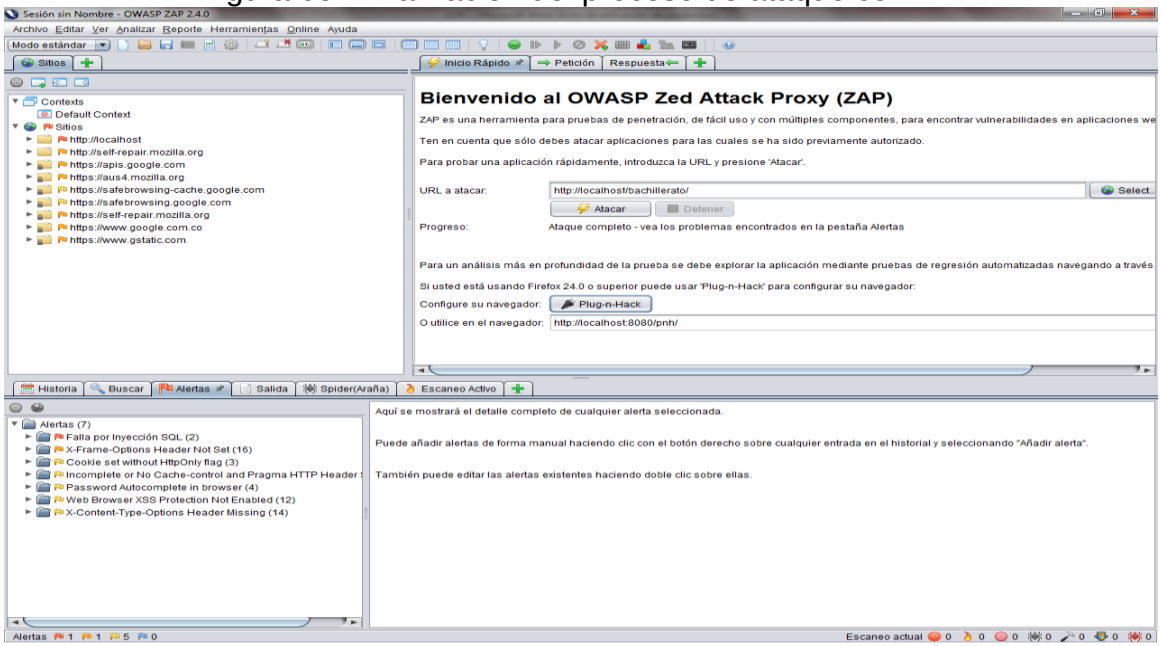
Figura 64 Proceso de ataques con ZAP.



Fuente. Aplicación ZAP, ataque en proceso.

Terminado el proceso se observan los resultados en la parte inferior izquierda, según el siguiente pantallazo obtenido una vez terminado el ataque con ZAP, este ha identificado 8 alertas:

Figura 65. Finalización del proceso de ataque con ZAP.



Fuente. Aplicación ZAP, resultado de ataque.