UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

Análisis de vulnerabilidades y diseño de procesos correctivos de la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato

---

Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

LÍNEA DE INVESTIGACIÓN:

Sistemas Administradores de Recursos

AUTOR: Jorge Alberto Sánchez Freire

TUTOR: Franklin Mayorga

AMBATO - ECUADOR

Abril, 2017

APROBACIÓN DEL TUTOR

En mi calidad de tutor del Trabajo de Investigación sobre el tema: "ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO", del señor Jorge Alberto Sánchez Freire, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato abril, 2017

EL TUTOR

Ing. Mg. Franklin Mayorga

AUTORÍA

El presente Proyecto de Investigación titulado: "ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO", es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato abril, 2017

Jorge Alberto Sánchez Freire

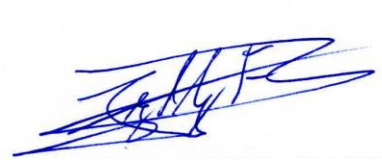
CC: 1804557054

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato abril, 2017



Jorge Alberto Sánchez Freire

CC: 1804557054

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Mg. David Omar Guevara Aulestia e Ing. Ph.D. Félix Oscar Fernández Peña, revisó y aprobó el Informe Final del Proyecto de Investigación titulado "ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO", presentado por el señor Jorge Alberto Sánchez Freire de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. Mg. Elsa Pilar Urrutia Urrutia

PRESIDENTA DEL TRIBUNAL

Ing. David Guevara, M. Sc.	Ing. Félix Fernández, Ph. D.
DOCENTE CALIFICADOR	DOCENTE CALIFICADOR

DEDICATORIA:

El proyecto está dedicado a mis padres Norma y Jorge, cuyo apoyo incondicional a lo largo de mi vida y carrera fue fundamental para mi realización como ser humano y como profesional.

Jorge Alberto Sánchez Freire

AGRADECIMIENTO:

Agradezco en primer lugar a Dios sin el cual no hubiera podido llegar tan lejos.

A mis padres quienes con sus consejos, aliento y apoyo que me fue inculcado desde pequeño, he logrado superar todas las dificultades que se me han presentado a lo largo del camino.

A mis profesores que, con su experiencia, consejos, tiempo, dedicación y principalmente amor a su trabajo me han impartido los conocimientos necesarios para ser un buen profesional con pasión por la tarea que realizo.

A la Universidad Técnica de Ambato, principalmente a la Dirección de Educación a Distancia y Virtual y a su Director, quienes gustosamente abrieron sus puertas y me permitieron desarrollar el presente proyecto.

Finalmente, a mis amigos que han sido mi segunda familia, quienes han estado en los buenos y malos momentos y quienes me han alentado a lo largo de toda mi formación humana y profesional.

Jorge Alberto Sánchez Freire

INDICE

RESUMEN EJECUTIVO

El presente proyecto de investigación está enfocado en la seguridad informática y el análisis de vulnerabilidades de una entidad, siendo en éste caso la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato mediante el uso de la metodología OWASP para el análisis, explotación y corrección de vulnerabilidades informáticas.

La metodología OWASP posee apartados específicos para la realización de test de vulnerabilidades de todos los aspectos de seguridad de una entidad, el proyecto OWASP posee herramientas propias las cuales se utilizan para análisis y explotación de vulnerabilidades, de la misma manera posee apartados específicos de procesos de corrección de vulnerabilidades.

OWASP propone distintos enfoques de ataque hacia una página o aplicación web, en el caso del presente estudio se realiza un análisis de sombrero gris.

ABSTRACT

This investigation project is focused in information security and vulnerabilities analysis of an entity, in this case the “Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato” using the OWASP methodology for the analysis, exploitation and correction of informatics vulnerabilities.

The OWASP methodology has specific statements about vulnerabilities tests of all security aspects of an entity, the OWASP project has own tools which are used for analysis and exploitation of vulnerabilities, it also has corrective processes for every issue.

OWASP propose different focus of web or application attacks, in this projects is used the grey hat focus.

INTRODUCCIÓN

El presente proyecto de investigación se enfoca en el análisis de vulnerabilidades y diseño de procesos correctivos mediante el uso de la metodología OWASP y sus secciones de explotación de vulnerabilidades usando el enfoque de sombrero gris.

Capítulo 1, "El Problema", se presenta el problema desde una contextualización global hasta una institucional y se presenta la necesidad de la realización del presente proyecto.

Capítulo 2, "Marco Teórico", son presentados los antecedentes en los cuales es basada la investigación, mediante el estudio de publicaciones, libros y proyectos anteriormente realizados con temas similares.

Capítulo 3, "Metodología", se describe la manera en la que será realizado el proyecto, justificando el uso de la metodología OWASP y cómo se llevará a cabo.

Capítulo 4, "Desarrollo de la Propuesta", se presenta paso a paso el desarrollo del proyecto mediante las actividades que fueron realizadas utilizando la metodología estudiada en el capítulo 3.

Capítulo 5, "Conclusiones y Recomendaciones", Se describen las conclusiones basadas en los resultados obtenidos y se presentan recomendaciones para la entidad y para quienes realicen análisis de vulnerabilidades similares.

CAPÍTULO 1

EL PROBLEMA

1.1 TEMA:

Análisis de vulnerabilidades y diseño de procesos correctivos de la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato

1.2 PLANTEAMIENTO DEL PROBLEMA

Al hablar de vulnerabilidades de sistemas o páginas web lo primero que se piensa es que se trata de un ataque el cual no puede ser detectado o detenido, es entonces cuando la palabra "hacker" tiene acción, en el presente tema se analizan las formas de ataques más comunes y con mayor énfasis en los métodos de mitigación de vulnerabilidades.

A cada momento se crean nuevas páginas web, ya sean tan grandes como lo es Facebook o simplemente un contacto simple de una tienda pequeña, cada vez se torna más y más necesario el crear una página web para entrar en el mundo de la red.

Es por ésta necesidad que nuevos personajes han aparecido a lo largo de la historia para lograr afectar, dañar o inclusive dar de baja a éstas páginas web, ya sea porque son competencia hacia una empresa rival o por lucrarse con ello, amenazando a los dueños de dichas páginas con no devolverlas o no detener los ataques hasta recibir cierta cantidad de dinero en una cuenta específica [1].

En la actualidad en un estudio realizado por "*Acunetix*", empresa especializada en análisis de vulnerabilidades web, en su reporte del año 2015, demuestra que de 5.500 empresas de las cuales comprenden un total de 15 000 páginas web y 1.9 millones de archivos, cerca de la mitad de los mismos se encuentran con vulnerabilidades graves a varios de los ataques antes mencionados [2] [3].

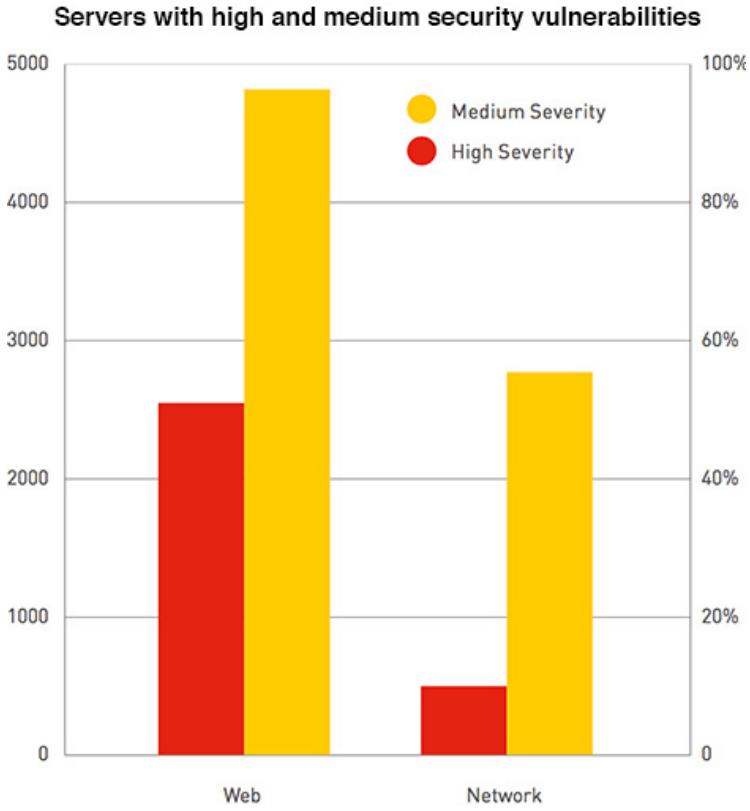


Figura 1. Estudio de Acutenix a vulnerabilidades en seguridad informática dentro de servidores reporte 2015

En el panorama actual del país, con grandes violaciones de datos que a diario aparecen en los medios de comunicación, se podría pensar que son pocos los que están expuestos a estos peligros. Sin embargo, la realidad es que la gran mayoría de empresas son vulnerables y no hacen nada por corregir sus vulnerabilidades.

En el afán de producir interfaces y aplicaciones fáciles de usar, centradas en los clientes, la gran mayoría de empresas están dejando expuestos sus datos más sensibles para que los ataque algún delincuente cibernético [4].

Los principales ataques en Ecuador se centran hacia ataques de denegaciones de servicios y atacar vulnerabilidades propias internas, a más de ello se utiliza una modalidad llamada phishing que consiste en obtener los datos de un usuario y suplantar su identidad [5].

Actualmente la Universidad Técnica de Ambato no cuenta con buenas políticas de seguridad informática, tales como el manejo adecuado de las cuentas de usuario para evitar uso de nombres y contraseñas por defecto, balanceo de carga cuando son realizadas una gran cantidad de peticiones, manejo de datos de credenciales en canales inseguros. Dados éstos fallos existen vulnerabilidades de ataques de negaciones de

servicios, accesos no autorizados, y una gran posibilidad de que información sensible sea robada.

1.3 DELIMITACIÓN

1.3.1. DELIMITACIÓN DE CONTENIDOS

El campo de la investigación está basado en la Tecnología Informática:

Área académica: Hardware y Redes

Línea de investigación: Sistemas administradores de recursos

Sub línea de investigación: Seguridad Informática

1.3.2. DELIMITACIÓN ESPACIAL

El presente proyecto de investigación se realizará en Ambato, en la Universidad Técnica de Ambato

1.3.3. DELIMITACIÓN TEMPORAL

La investigación se desarrollará durante el semestre Octubre 2016 – Marzo 2017

1.4 JUSTIFICACIÓN

La presente investigación es de sumo interés para la comunidad universitaria actual ya que, en ésta se encuentran repositorios de las clases impartidas por los docentes hacia los estudiantes, así mismo como la revisión de sus trabajos y la realización de evaluaciones acordes a los temas observados.

En la actualidad no se ha explorado a profundidad el campo de la seguridad informática dentro de las páginas web propias de la universidad, es por lo cual el presente proyecto representa una innovación adecuada para la comunidad universitaria.

Para la investigación necesaria se contará con la asesoría de los encargados del control de la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato, en donde se realizarán posteriores pruebas de los diferentes tipos de ataques que hoy en día son los más peligrosos para las comunidades virtuales.

Los principales beneficiarios del presente proyecto será la comunidad universitaria en general, los estudiantes tendrán la seguridad de que sus datos personales tales como repositorios y archivos se encuentran seguros de una intrusión, a más de dar confiabilidad de que la página se mantendrá siempre a pesar de ser atacada mediante múltiples peticiones (ddos), los docentes tendrán la confiabilidad de que los trabajos enviados no serán vulnerados y los archivos recibidos estarán procesados de mejor manera, a más de asegurar la realización de evaluaciones acordes con la enseñanza impartida, finalmente los administradores de la página web podrán estar seguros de

que no existan ataques que sean un peligro para los servidores, y de haberlos contarán con metodologías que permitan reducir éstos ataques de manera sencilla sin alterar el funcionamiento principal de la página.

El presente proyecto de investigación es factible dado que se cuenta con los recursos tecnológicos, humanos y económicos necesarios para su realización

1.5 OBJETIVOS

1.5.1 GENERAL

Analizar las vulnerabilidades existentes y diseñar procesos correctivos para la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato.

1.5.2 ESPECÍFICOS

- Realizar los estudios preliminares acerca de las tecnologías utilizadas por la universidad para la creación y manejo de sus páginas web y sus repositorios virtuales
- Establecer los tipos de ataques más comunes y peligrosos para páginas web
- Definir tecnologías necesarias y realizar los diferentes tipos de ataques en la página web de la Dirección de Educación a Distancia y Virtual
- Diseñar procesos correctivos para reducir el impacto de los ataques realizados y mitigar ataques futuros.

CAPÌTULO 2

MARCO TEÓRICO

2.1 ANTECEDENTES INVESTIGATIVOS

En el entorno tecnológico actual, el cual avanza a cada momento, es necesario asegurar la información de las personas, es por ello que el presente proyecto de investigación se encargará de mitigar las diferentes amenazas existentes dentro de una red a ser atacada, es por lo cual se ha estudiado casos anteriores de análisis de vulnerabilidades y *hacking ético,* término que será estudiado más adelante.

Como dice Andrés Pazmiño, ex estudiante de la Universidad Técnica de Ambato, en su tesis de graduación, el hacking puede ser usado como una muy útil herramienta de auditoría dentro de una empresa, ya que con él se ven de primera mano las distintas vulnerabilidades que existen ante ataques que pueden llegar a representar grandes pérdidas a niveles empresariales [6].

Es por ello que realizar pruebas de una página web antes de hacerla pública es crucial para una empresa, ya que al seguir éstas políticas de seguridad se tiene un menor riesgo de poder ser atacados, y si lo son, tener una capacidad de respuesta más alta garantizando la integridad y fiabilidad de los datos que [7].

El conocer con qué recursos cuenta una entidad es importante al momento de poder redirigirlos en el caso que se necesite mayor seguridad (compra de servidores por ejemplo), para lo cual un análisis del entorno representará un muy importante aspecto a tomar en consideración [8].

Para encontrar los problemas existentes dentro de una entidad se realizan pruebas de penetración, las cuales están diseñadas específicamente para probar que las vulnerabilidades existen, son reales y peligrosas, por lo cual un diseño de procesos correctivos es imperativo. Una prueba de penetración correctamente realizada no solo demuestra la existencia de sectores vulnerables, sino que añade recomendaciones y correcciones a ser tomadas en cuenta por la entidad en la cual se realizaron los ataques controlados [9].

A fin de mitigar los ataques se debe saber cuáles existen, los que son más comunes y así encontrar soluciones a los problemas que éstos pueda presentar. Por ejemplo uno de los ataques más peligrosos y con un ranking de uso muy alto es el de inyección SQL, el cual se adueña de una página web con permisos de administrador, es decir, el atacante puede realizar cualquier tipo de cambio dentro de una página web [7].

Por lo tanto, algo que se debe tomar en cuenta es que “Nada es absolutamente seguro”, siempre existen puertas traseras o enlaces los cuales permiten a cualquier persona con conocimientos en el campo, entrar sin ser autorizados y muchas veces realizar cambios sin autorización. Es por ello que existen protocolos a seguir, los cuales muchas veces son pasados por alto [10].

Dada éstas incidencias, en la Universidad técnica de Ambato se han propuesto varias tesis anteriores al análisis de vulnerabilidades, mas en los sectores que son utilizados

por el estudiantado se ha pasado por alto el análisis de objetivos los cuales un atacante puede dar de baja o controlarlos a voluntad, siendo la presente, una propuesta para aumentar la efectividad y garantizar mayor seguridad en la página web del aula virtual.

2.2 FUNDAMENTACIÓN TEÓRICA

2.2.1 SEGURIDAD INFORMÁTICA

El objetivo de la seguridad de la información según la norma ISO 27001 es "preservación de la confidencialidad, la integridad y la disponibilidad de la información, además también pueden estar implicados otras propiedades como la autenticidad, la responsabilidad, el no repudio, y la fiabilidad" [11].

Jorge Aguirre, experto en seguridad informática, expone un concepto en su libro que se refiere a "la cualidad de un sistema informático exento de peligro" [12].

Por lo cual un concepto adecuado para la seguridad informática es el otorgar de fiabilidad e integridad tanto a hardware como software, mediante distintos procesos a seguir para así garantizar una protección de los datos de los usuarios a accesos no permitidos.

2.2.2 ANÁLISIS DE VULNERABILIDADES

"Herramientas de análisis para los equipos de toda la red. Determinan servicios que se están ejecutando en un equipo remoto" [13].

2.2.3 PRUEBAS DE PENETRACIÓN

Conjunto de técnicas y metodologías llevadas a cabo para determinar el nivel de seguridad de un sistema [14].

2.2.4 HACKER

Persona que con mucho conocimiento rompe las seguridades de un sistema para obtener conocimiento del mismo sin alterar su funcionalidad [14].

2.2.5 CRACKER

Persona con un alto grado de conocimiento que rompe las vulnerabilidades de un sistema para beneficio propio, alterando funcionalidades, cambiando y eliminando datos [14].

2.2.6 HACKING ÉTICO

Realización de pruebas de penetración para la determinación de vulnerabilidades y corrección de las mismas [14].

2.2.7 AUDITORÍA DE SEGURIDAD INFORMÁTICA

A diferencia del hacking ético, la auditoría se centra en los procesos, no es tan técnica y se basa en el cumplir o no estándares de calidad [14].

2.2.8 TIPOS DE HACKING

- **Sombrero Blanco**

  Terminología usada para referirse a un hacker, el cual solo realiza auditorías en el campo de la seguridad informática con todos los permisos de la misma sin rozar en ninguna evaluación de carácter ilegal; se encarga de verificar la funcionalidad de los sistemas evitando realizar algún cambio en el mismo [14].

- **Sombrero Gris**

  Persona que realiza ataques rozando cierta parte de la ilegalidad de los mismos, realizando cambios en pequeñas partes de un sistema [14].

- **Sombrero Negro**

  Persona malintencionada la cual realiza ataques para dañar un sistema o robar información para lucro personal [14].

2.2.9 TIPOS DE ATAQUES

- **DDoS**

  Una denegación distribuida de servicio es definida como un ataque intencional con la intención específica de negar a los usuarios su uso legítimo de la información mediante el envío de una gran cantidad de paquetes para sobrecargar al servidor [15].

- **Ataques DNS**

  Un ataque DNS consiste en enviar mediante el uso de protocolo de nombres de dominio, las solicitudes hacia servidores distintos a los originales, con intenciones de robar información personal [15].

- **Virus**

  Código malicioso que se pega a un programa determinado, su ataque puede ser hacia distintos lugares dentro de un sistema, puede ser ejecutado sin necesidad de que el usuario lo autorice o sepa de ello [15].

- **Spoofing**

  Suplantación de identidad para realizar entradas ilegitimas hacia un lugar determinado del sistema [16].

- **Trojano**

  Programa destructivo el cual aparece como una aplicación inofensiva, para engañar al usuario y entrar al sistema [15].

- **Gusano**

  Es un programa malicioso cuya característica principal es el de la autoreplicación sin que intervenga ninguna persona [15].

- **Botnet**

  Son programas y fragmentos de código manejados remotamente los cuales pueden estar programados para realizar spam, ataques DDoS y ataques internos, realizados desde el exterior. [17].

- **Ataque de infraestructura**

  Es un ataque el cual se encarga de controlar la parte física de una entidad tales como redes eléctricas, interfaces de red, servicios de control computarizado como control de agua y gas, entre otros. [15].

- **Ingeniería Social**

  Es una técnica que usa el engaño para que la víctima otorgue sus datos y contraseñas a un atacante [15].

2.2.10. APLICACIÓN WEB

Se entiende como aplicación web aquel código construido con un lenguaje de programación determinado que puede ser accedido desde un navegador web e interactúa dinámicamente con el usuario respondiendo sus solicitudes [18].

2.2.11. SITIO WEB

Sitio web, a diferencia de una aplicación web es sólo de lectura, no posee de un código para interactuar con el usuario a más de ser observado [19].

2.2.12. THE OPEN WEB APPLICATION SECURITY PROJECT

The Open Web Application Security Project, OWASP por sus siglas en inglés, es un proyecto generado a partir de las falencias encontradas en diferentes organizaciones a nivel de seguridad informática; usado para recolectar todas las técnicas posibles de evaluación y comprobación de errores.

La metodología es basada en un acercamiento de caja negra en donde quien va a comprobar la seguridad del sitio y/o aplicación web tiene poca o nula información acerca de la misma.

2.3 PROPUESTA DE SOLUCIÓN

El análisis de vulnerabilidades dentro de un entorno web, representa una parte vital de cualquier entidad para garantizar la seguridad de sus datos, a más de agregar políticas internas las cuales crearán un ambiente de integridad y fiabilidad de los datos, repercutiendo en la comunidad que usa el entorno.

CAPÍTULO 3

METODOLOGÍA

3.1 MODALIDAD DE LA INVESTIGACIÓN

Modalidad Bibliográfica

El presente proyecto de investigación es basado en información que es posible hallarla en libros técnicos, informes, artículos, los cuales proporcionarán información relevante para llevar a cabo la misma.

Modalidad Aplicada

Al ser aplicados conocimientos adquiridos a lo largo del estudio académico en lo referente a los módulos de Intranets/Extranets y Seguridad Informática.

Modalidad Campo

Para poder conocer la interacción de los procesos de la institución y el desarrollo del proyecto tanto como para detectar las vulnerabilidades existentes, como para diseñar procesos correctivos, la investigación de campo se desarrollará en la Universidad técnica de Ambato en los departamentos de la Dirección de Educación a Distancia y Virtual.

3.2 POBLACIÓN Y MUESTRA

Por las características de la investigación no se requiere población y muestra

3.3 RECOLECCIÓN DE LA INFORMACIÓN

Para recolectar la información necesaria para el desarrollo de la investigación se contará con herramientas como la auditoría informática en seguridad en sistemas y análisis de grupo focal.

Con la auditoría informática en entorno de seguridad se tendrán en cuenta los procesos relacionados con la seguridad informática, para analizar sus vulnerabilidades y diseñar estrategias de solución.

Con el grupo focal se analizarán las principales dificultades de seguridad informática encontradas a lo largo del trabajo normal del sitio web tales como ataques externos e internos.

3.4 PROCESAMIENTO Y ANÁLISIS DE DATOS

Recopilada la información se organiza y se analiza los procesos tomando en cuenta en primer lugar aquellos que representen un mayor riesgo dentro de la institución. Aplicando procedimientos estadísticos y gráficos los cuales serán expuestos en el Capítulo 4 para facilitar su análisis

3.5 DESARROLLO DEL PROYECTO

Se presentarán a continuación las actividades a realizar para el cumplimiento de los objetivos específicos, para así poder completar el objetivo general propuesto.

Realizar los estudios preliminares acerca de las tecnologías utilizadas por la universidad para la creación y manejo de sus páginas web y sus repositorios virtuales.

- Analizar el medio en que se encuentra creada la página principal de la Dirección de Educación a Distancia y Virtual
- Verificar el tipo de servidores en donde se guarda la información de la página web
- Observar los medios físicos que se disponen para la seguridad de las computadoras y servidores, si es que se dispone de alguno.
- Crear los lineamientos primarios para la realización de una auditoría informática solo en entorno de seguridad informática

Establecer los tipos de ataques más comunes y peligrosos para páginas web

- Definir los distintos tipos de ataques hacia un entorno web, tanto desde cliente como de servidor
- Analizar un histórico de los ataques más comunes realizados a entornos web en el país
- Recolectar datos de los daños más importantes realizados dentro de la Universidad Técnica de Ambato

Definir tecnologías necesarias y realizar los diferentes tipos de ataques en la página web de la Dirección de Educación a Distancia y Virtual

- Conseguir, mediante reuniones, autorización para realizar pruebas de hacking ético a la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato.
- Investigar herramientas que faciliten las pruebas de penetración (PenTesting)
- Iniciar con los ataques más comunes previamente investigados e ir avanzando hacia ataques de mayor complejidad y peligrosidad
- Documentar los resultados de las pruebas de penetración

Diseñar procesos correctivos para reducir el impacto de los ataques realizados y mitigar ataques futuros.

- Analizar los datos obtenidos de las pruebas de penetración
- Investigar herramientas necesarias para mitigación de riesgos en seguridad informática
- Crear documentación acerca de buenos procesos a seguir para garantizar la seguridad informática dentro de una institución
- Instruir al personal acerca de las herramientas necesarias para minimizar los daños causados por ataques informáticos

CAPÍTULO 4

DESARROLLO DE LA PROPUESTA

4.1 TEMA

Análisis de vulnerabilidades y Diseño de procesos correctivos de la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato

4.2 DATOS INFORMATIVOS

Institución: Universidad Técnica de Ambato

Dirección: Dirección de Educación a Distancia y Virtual (DEaDV)

Beneficiario/s: Comunidad Universitaria

Tiempo: El presente proyecto de investigación se desarrollará en el período académico Octubre 2016 – Marzo 2017

Costo: Se tiene un costo estimado de 1350,9 $

Tutor: Ing. Mg. Franklin Mayorga

4.3 ANTECEDENTES DE LA PROPUESTA

Los ataques informáticos no son una novedad hoy en día, a nivel Ecuador existen ataques realizados principalmente a páginas gubernamentales.

Como se pueden observar en temas de tesis ya tratados con anterioridad en la Universidad Técnica de Ambato, dentro de la misma temática, por poner un ejemplo al trabajo del señor Byron Nuela en donde se exponen las vulnerabilidades en seguridad informática a nivel gubernamental local en el Honorable Gobierno Provincial de Tungurahua [20].

Por lo cual se considera muy necesario explorar éste campo dentro de la Universidad ya que muchas veces se ha visto víctima de ataques los cuales dejan inutilizadas muchos de sus sitios web provocando un malestar general, externo al no poder conseguir información de la misma e interno al tener que a cada momento encontrarse restableciendo las páginas caídas

4.4 JUSTIFICACIÓN

La Universidad Técnica de Ambato, específicamente la Dirección de Educación a Distancia y Virtual, a pesar de contar con ciertas medidas de seguridad para reducir ataques informáticos aun suceden, muchas veces provocando un mal funcionamiento de los servidores poniendo en peligro la integridad de los archivos institucionales y provocando pérdidas de recursos en volver a poner en funcionamiento la página en cuestión.

El presente proyecto de investigación tiene como finalidad la detección de las principales vulnerabilidades existentes para un campo web tanto estático como

dinámico para lo cual se realizarán diferentes pruebas y análisis para determinar cuáles son los ataques a los cuales es más propensa la página web a sucumbir.

Posterior a la realización de pruebas se desarrollará un diseño de los procesos que se deben realizar tanto para evitar los ataques como para si algún momento suceden poder mitigarlos utilizando una menor cantidad de recursos de tiempo y personal, en beneficio de la institución.

4.5 OBJETIVOS

4.5.1 GENERAL

Analizar las vulnerabilidades existentes y diseñar procesos correctivos para la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato.

4.5.2 ESPECÍFICOS

- Realizar los estudios preliminares acerca de las tecnologías utilizadas por la universidad para la creación y manejo de sus páginas web y sus repositorios virtuales
- Establecer los tipos de ataques más comunes y peligrosos para páginas web
- Definir tecnologías necesarias y realizar los diferentes tipos de ataques en la página web de la Dirección de Educación a Distancia y Virtual
- Diseñar procesos correctivos para reducir el impacto de los ataques realizados y mitigar ataques futuros.

4.6 ANÁLISIS DE FACTIBILIDAD

El análisis de factibilidad se centra en la existencia o disponibilidad de los recursos necesarios para la realización exitosa del presente proyecto.

Factibilidad Operativa

Dentro de la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato no se ha realizado un análisis de vulnerabilidades, por lo cual resulta imperativo el mismo para poder evitar ataques informáticos o mal funcionamiento de la misma provocando pérdidas de información y recursos al necesitar personal que restablezca al sitio web.

Es por lo cual el presente proyecto de investigación resulta factible para realizar dentro de la presente institución representando un avance para la detección y mitigación de amenazas informáticas mediante el uso de procesos adecuados de manejo de la página web.

Factibilidad Técnica

Para el análisis de vulnerabilidades de la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato se cuenta con el apoyo institucional y de la dirección, el estudiante quien posee los conocimientos suficientes para realizar un análisis de vulnerabilidades con su respectivo informe de corrección de los mismos y los recursos necesarios como son una laptop con un sistema operativo orientado al análisis y seguridad informática y una conexión directa, por lo cual el proyecto resulta factible.

Factibilidad Económica

Los recursos necesarios tales como un computador portátil, memorias flash, hostings virtuales, libros y transporte serán cubiertos por el estudiante investigador. Otros recursos tales como software son gratuitos ya que se utilizará software libre para las investigaciones pertinentes, por lo cual se concluye que el presente proyecto es económicamente factible.

4.7. FUNDAMENTACIÓN TEÓRICA

4.7.1 KALI LINUX

Kali Linux es un Sistema Operativo libre utilizado para auditoría de seguridad informática ya que incorpora más de 300 herramientas utilizadas para la realización de pruebas de penetración, lo cual permite a los administradores el comprobar la efectividad de sus seguridades, riesgos y estrategias de mitigación de los mismos.

Facilita los trabajos de Pentesting, haciéndolos más accesibles para administradores y especialistas de seguridad, su adherencia con estándares Debian hace que sea mucho más sencillo su manejo mediante su interfaz gráfica.

Los usuarios pueden modificar el sistema operativo según sus necesidades y preferencias.

Todos los programas incluidos en el sistema operativo han sido evaluados por efectividad y manejo; incluyen, por ejemplo, Metasploits para pentesting de redes, Nmap para escaneo de puertos y vulnerabilidades, Wireshar para monitorizar el tráfico de la red y Aircrack para la comprobación de seguridades en redes wifi.

Es muy adaptable a distintos tipos de hardware y compatible con numerosos dispositivos Wireless y USB a más de soportar dispositivos ARM [21].

4.7.2 FOOTPRINTING

El término reconocimiento por definición proviene de la estrategia militar que consiste en explorar el territorio enemigo para futuro análisis o ataque. El reconocimiento de un sistema computacional tiene una naturaleza similar, en donde un hacker pretende recolectar la mayor cantidad de información acerca del ambiente del objetivo, su sistema y manejo de archivos para posteriormente atacarlo. Esto es conocido también como establecer el *footprint* de un objetivo [22].

4.7.3 PORT SCANNING

Port scanning o escaneo de puertos es el proceso de determinar los puertos abiertos TCP o UDP en una máquina remota para determinar los más vulnerables o los cuales son posibles atacar, se debe tener un grado de conocimiento alto acerca de los diferentes puertos existentes y los servicios que los mismos manejan [21].

4.7.4 ENUMERACIÓN

La enumeración consiste en la obtención de una mayor cantidad de información mediante la explotación de una vulnerabilidad en los servicios obtenidos mediante *port scanning*.

Mediante la enumeración se puede obtener datos vitales de la empresa tales como cuentas de usuarios, correos electrónicos, recursos compartidos, archivos con hashes de contraseñas, siendo ésta última la más vulnerable ante un atacante [23]. Los protocolos más comunes a ser enumerados son:

- NetBIOS
- DNS
- LDAP
- SNMP

4.7.5 GOOGLE HACKING

El uso de Google para encontrar información, vulnerabilidades o páginas web con deficientes configuraciones fue publicada por Johnny Long en 2001. Desde entonces una base de datos con búsquedas por defecto ha sido creada y compilada para permitir que auditores de seguridad informática encuentren de manera sencilla las configuraciones existentes de un dominio específico [21].

4.7.6 WHOIS

Whois es el nombre para un servicio y herramienta TCP, y en cierta medida una base de datos la cual contiene información acerca del nombre del servidor de un dominio y muchas veces información de contacto de la misma. Las bases de datos son creadas y mantenidas por InterNIC22 y publicadas por servidores whois en el puerto 43 que son accesibles desde un programa cliente whois [21].

4.7.7 THE HARVESTER

La recolección de correos electrónicos es una manera efectiva de recuperar posibles nombres de usuarios para los servidores de una organización. Éstos emails son muy útiles al momento de proveer una lista para realizar ataques del lado cliente, revelando el nombre del posible usuario, o escaneando a todos los usuarios de la organización.

Una de las herramientas que posee Kali Linux para la realización de ésta tarea es The Harvester, el cual utiliza Google, Bing, y otros motores de búsqueda para encontrar correos electrónicos asociados a un dominio en particular [21].

4.7.8 FOCA

Los metadatos son los datos más básicos e información de un objeto, recurso o un data set, en ella incluye la forma en la que está constituido así como el nombre de quien fue recolectado. Los metadatos pueden ser muy útiles para un Pentesting ya que contiene información del sistema en donde fue creado, tales como:

- Nombre de los usuarios conectados al Sistema.
- El software que creó el documento
- El sistema operativo donde fue creado

FOCA es una herramienta de auditoría de seguridad informática la cual examina los metadatos de los dominios. Se puede utilizar FOCA para analizar los archivos encontrados en un sitio web o utilizar archivos locales [22].

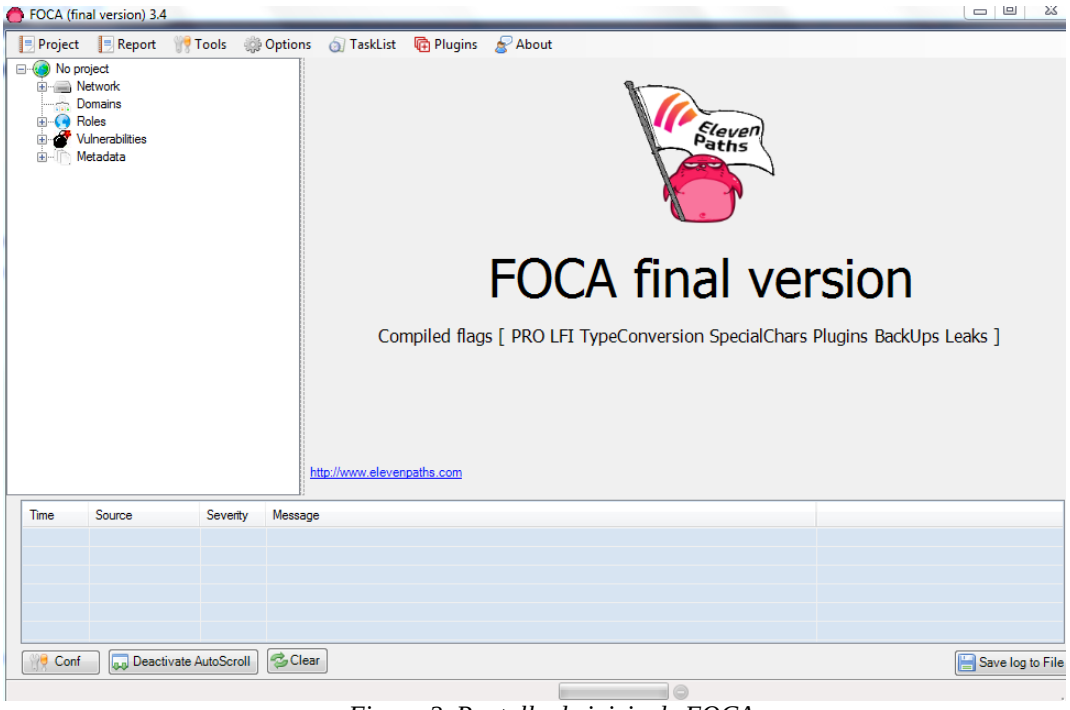


Figura 2. Pantalla de inicio de FOCA

4.7.9 MALTEGO

Maltego es una herramienta de reconocimiento de Kali Linux desarrollada por Paterva, empresa orientada a análisis de datos para la realización de auditorías informáticas creada en el año 2007. Se usa para la recolección de información abierta y pública de internet. También posee reconocimiento DNS, pero lo que le caracteriza es que despliega gráficas de análisis [22].

Dependiendo de la opción de reconocimiento escogida Maltego puede:

- Asociar una dirección e-mail a una persona
- Asociar páginas web a personas
- Verificar direcciones mail
- Recolectar datos de Twitter, incluyendo geolocalización de fotografías

4.7.10 NMAP

Nmap o Network Mapper es usado para escanear hosts y servicios dentro de una red. Ha ido evolucionando de distintas maneras y hoy en día se usa para descubrir las aplicaciones a más de los servicios y los sistemas operativos de los servidores de la red.
Es uno de los escáneres de red más utilizados haciéndolo uno de los más efectivos, pero a su vez es muy detectable debido a la cantidad de banda que consume [22].

4.7.11 ARMITAGE

Se trata de una interfaz gráfica para el manejo de Metasploits, el cual facilita en gran medida su uso al mostrar de una forma visual los objetivos y encontrar los exploits a los que el objetivo del ataque es más vulnerable [24].

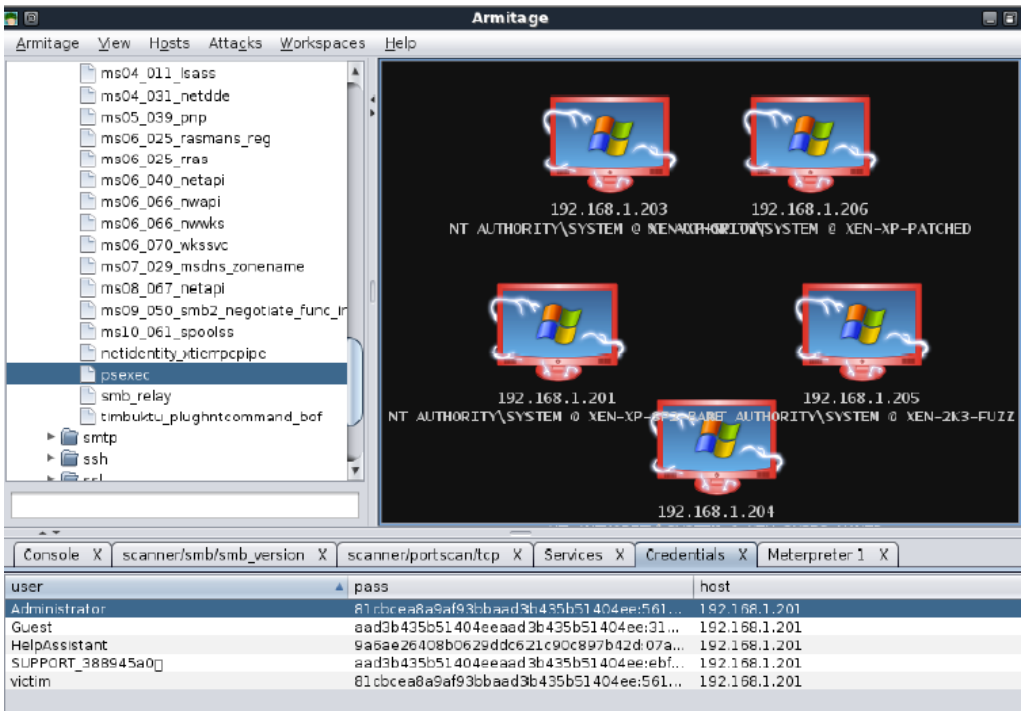


Figura 3. Pantalla de manejo de Armitage [24]

4.7.12 DUMPSEC

DUMPSEC es un programa usado por auditores de seguridad informática el cual permite visualizar vulnerabilidades del sistema, recolectar información de los distintos usuarios y sus permisos.

Es utilizado para recolectar información de sistemas operativos Windows [25].

4.7.13 PHISHING

Resulta en un tipo de ataque el cual utiliza ingeniería social en contra de un usuario quien, mediante engaños, envía su información personal tales como usuarios y contraseñas.

El uso de correos electrónicos con links hacia páginas falsas, las cuales lucen como una página confiable, es la manera más común de éste tipo de ataque [26].

4.7.14 BUFFER OVER FLOW (DOS)

Es el ataque más común que existe hoy en día, y uno de los más difíciles de mitigar; consiste en enviar al objetivo una gran cantidad de peticiones simultáneamente, ésta sobrecarga evita que la respuesta de los recursos del servidor sea la adecuada, o inclusive deje de responder, los ataques pueden ser dirigidos hacia el espacio en discos, ancho de banda, información de configuración (eliminación de tablas de enrutamiento), información de estado (reseteo de sesión TCP), entre otros.

Existe cuatro categorías de ataques DoS:

Ataque Basado en Volumen: Se refiere a inundación de peticiones en protocolos UDP, TCP y aquellos que sean basados en paquetes. El propósito de éste ataque es saturar el ancho de banda del sitio web atacado.

Ataques de Protocolo: Consume los recursos del servidor o del equipo de comunicación, tales como routers, firewalls, balanceadores de carga, entre otros. Un ejemplo muy difundido de éste tipo de ataque es el *"Ping de la muerte"*.

Ataques a la capa de aplicación: Aprovecha el tráfico legítimo de red para detener el servicio web. El ejemplo más difundido es los ataques *"Día Cero"*.

Agotamiento de Sesiones: Al abusar de las limitaciones de sesiones estableciendo muchas sesiones nuevas sin cerrarlas con el objetivo de consumir recursos [22].

4.7.15 LOIC

Low Orbit Ion Cannon (LOIC) es una herramienta utilizada para comprobar qué cantidad de tráfico puede tolerar un objetivo, LOIC permite realizar éste tipo de pruebas desde un navegador web.
Éste software se hizo famoso al ser utilizado por el grupo Anonymous entre los años 2014 y 2016 para facilitar los ataques DDoS en contra de una gran cantidad de sitios web por lo cual muchas leyes condenan el uso de LOIC como una violación a la seguridad computacional [22].

4.7.16 METASPLOIT

Es una de las herramientas más peligrosas contra las vulnerabilidades de un sistema computacional, se trata de pequeños programas los cuales realizan funciones pre programadas dentro de un ambiente, en dependencia del que se utilice, por ejemplo, el devolver una sesión obtenida desde una máquina remota para el control externo de una computadora [23].

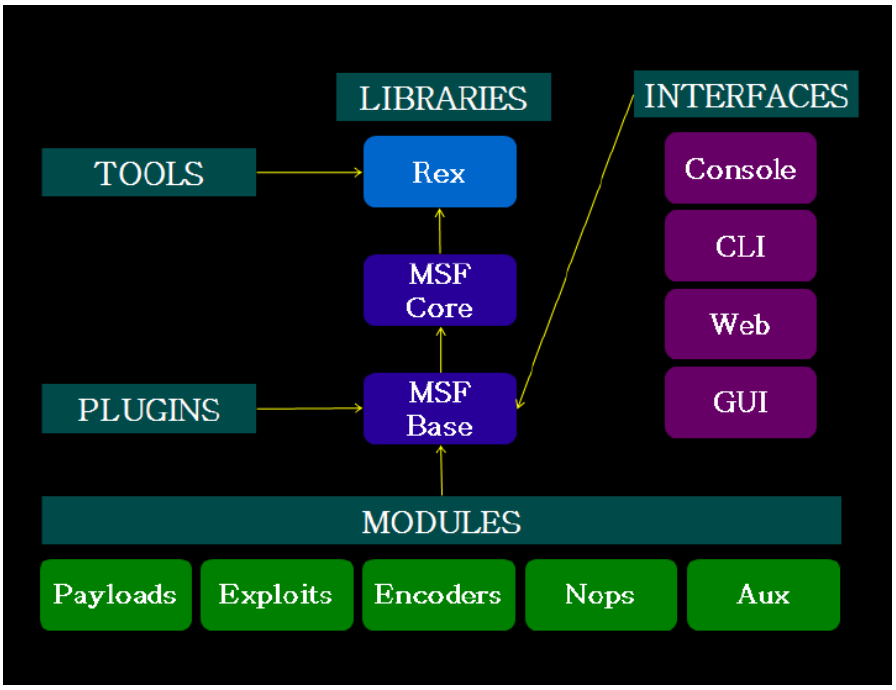


Figura 4. Arquitectura de un Metasploit [24]

4.7.17 SPOOFING

Es la alteración de ciertos elementos de una máquina para poderla hacer pasar por otra, como por ejemplo el cambiar la MAC y la IP de una computadora para hacerla pasar como una propia de la red interna y poder acceder a los recursos propios de dicha máquina, ésta práctica no es tan recomendable debido a la facilidad que existe de ser detectado por el administrador del servidor [26].

4.7.18 NETCRAFT

Es un servicio de internet el cual es usado para obtener información completa de una página web, de la misma manera tiene otras características como prestador de servicios anti phishing, hosting, auditorías de seguridad, entre otras soluciones a nivel de redes y páginas web [27].

4.7.19 OWASP ZAP

Zed Attack Proxy o ZAP por sus siglas en inglés, es una herramienta usada para analizar vulnerabilidades de seguridad informática mediante el escaneo total de la página web, la cual proporciona las vulnerabilidades encontradas y su grado de riesgo, con lo cual el administrador puede realizar los cambios necesarios en la página web [28].

4.7.20 JOOMSCAN

Es un paquete de herramientas que viene instalado por defecto en Kali Linux, desarrollado por la compañía OWASP por lo tanto de software libre, el cual realiza un escaneo de páginas web basadas en el sistema gestor de contenidos Joomla para detectar y reportar vulnerabilidades de seguridad encontradas en la página web [29].

4.7.21 OPENVAS

Open Vulnerability Assessment System (OpenVAS) es una interfaz muy completa que posee una gran cantidad de información con la cual mediante prueba y error descubre todas las vulnerabilidades posibles dentro de una interfaz web, el mismo es el más difundido entre los auditores de seguridad informática, la desventaja principal es que se provoca un gran tráfico inusual dentro de la red por lo cual resulta detectable [30].

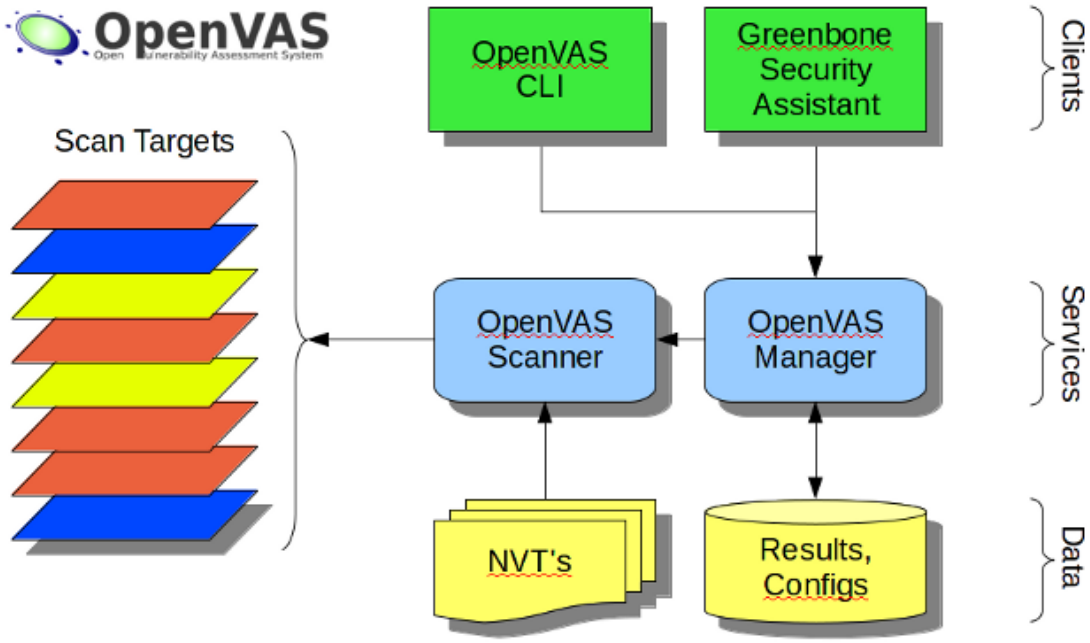


Figura 5. Arquitectura de OpenVAS

4.8 Análisis de la situación actual de la Página Web de la Dirección de Educación a Distancia y Virtual con enfoque en la subpágina perteneciente al aula virtual de la facultad de ingeniería en sistemas, electrónica e industrial

Para poder realizar el presente análisis se procedió a realizar una encuesta a 141 estudiantes de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, a continuación, se listan cada una de las preguntas realizadas con su respectivo porcentaje de respuesta:

1. **¿Con qué frecuencia ha tenido dificultades para ingresar al aula virtual?**

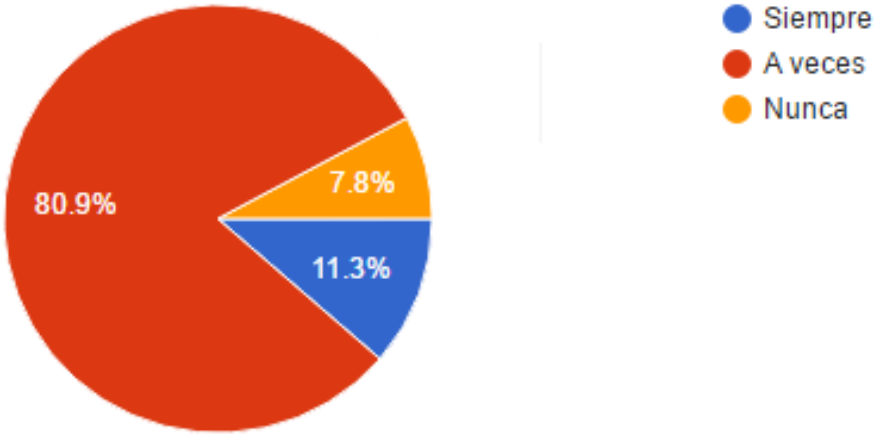


Figura 6. Resultados de la pregunta Nº 1

El 80.9 por ciento, quienes representan a la mayoría del estudiantado manifiestan que a veces existen dificultades para ingresar al aula virtual, un 11.3 por ciento siempre tienen éstas dificultades mientras que a un 7.8 por ciento del total de los 141 estudiantes entrevistados nunca les ha sucedido éste problema.

Existe un gran porcentaje de estudiantes que han tenido dificultades al ingresar al aula virtual, muchas veces se produce al tener una gran cantidad de peticiones simultáneas por lo cual es necesaria una revisión del presente problema.

2. ¿Ha tenido dificultades con subir trabajos a la plataforma virtual?

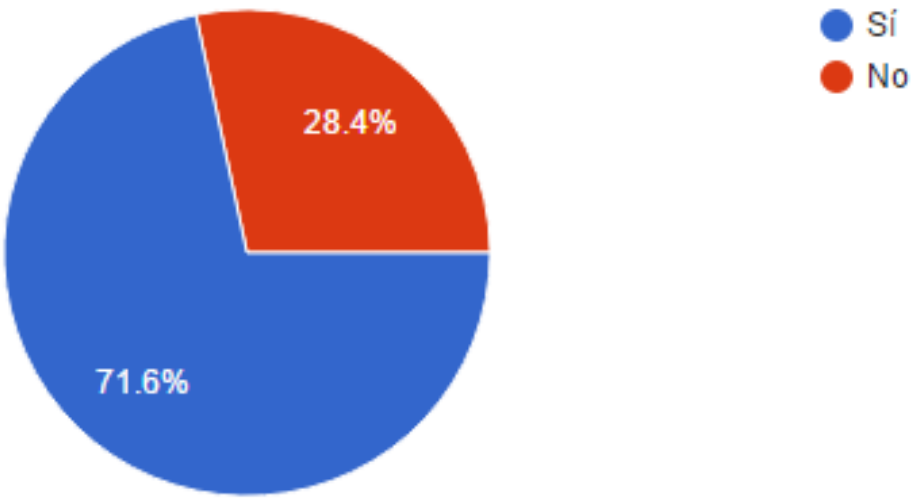


Figura 7. Resultados de la pregunta Nº 2

La gran mayoría del estudiantado entrevistado ha tenido dificultades al subir trabajos a la plataforma virtual mientras que el 28.4% de los estudiantes nunca han presentado éste problema.

Muchas veces por la misma razón que en la anterior respuesta existe un tiempo de respuesta lento, provocando muchas veces pérdida de información.

3. ¿Ha sido evaluado usted mediante la plataforma virtual?

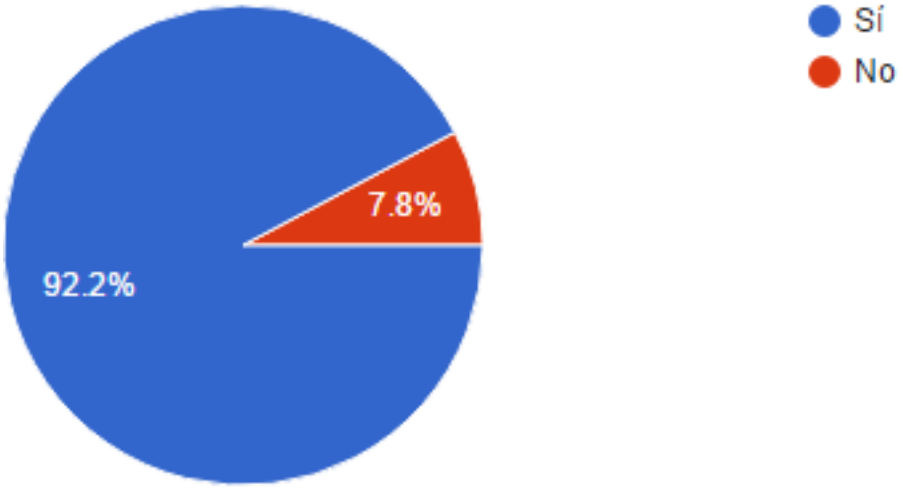


Figura 8. Resultados de la pregunta Nº 3

La presente pregunta fue para diagnosticar la cantidad de docentes usuarios activos de la plataforma, los cuales la utilizan como mecanismo de evaluación a los estudiantes, en éste caso solo 7.8% de entrevistados jamás han sido evaluados mediante la plataforma por lo que se puede utilizar ésta información para encontrar dificultades de funcionamiento de la misma.

4. **¿Se ha sentido perjudicado en cuestión a su calificación final en pruebas virtuales por motivos del aula virtual?**

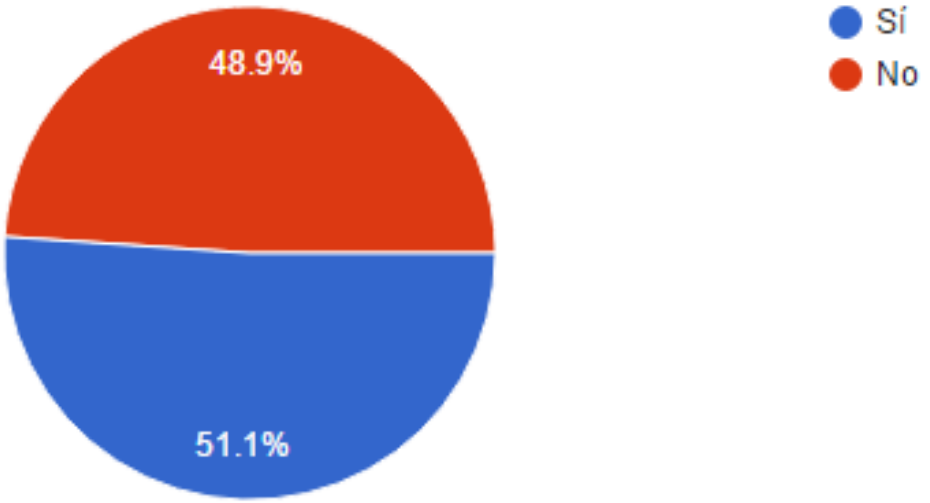


Figura 9. Resultados de la pregunta Nº 4.

La presente pregunta busca determinar si en algún momento los estudiantes han presentado problemas de calificaciones en sus evaluaciones por motivos propios de la plataforma, existe un cuasi equilibrio entre quienes consideran sus notas evaluadas mediante la plataforma vulneradas de alguna manera, sin embargo, la tendencia apunta a la existencia de cierta inconformidad por lo cual se necesita un análisis de ello.

5. ¿En la escala de 1 a 5 cómo calificaría la eficiencia de la plataforma (Siendo 1 poco eficiente y 5 muy eficiente)?

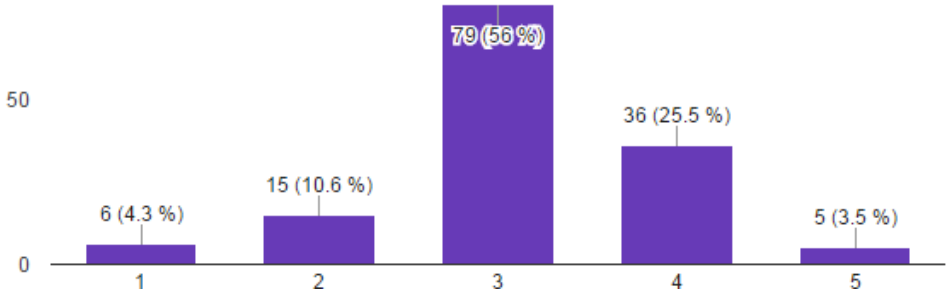


Figura 10. Resultados de la pregunta Nº 5

Se puede observar que existen puntos los cuales mejorar debido a que existe un cierto grado de inconformidad con la eficiencia de la página (principalmente en tiempos de respuesta de la misma), dentro del rango más bajo el cual sería el más preocupante existen 6 estudiantes inconformes con el aula virtual, y en el rango más alto 5 estudiantes están conformes con el manejo de la misma, existe una cantidad superior en una posición neutral dando un total de 79 estudiantes quienes consideran que la plataforma tiene ciertas deficiencias a corregir.

6. ¿Considera adecuado el grado de seguridad general que ofrece la plataforma virtual?

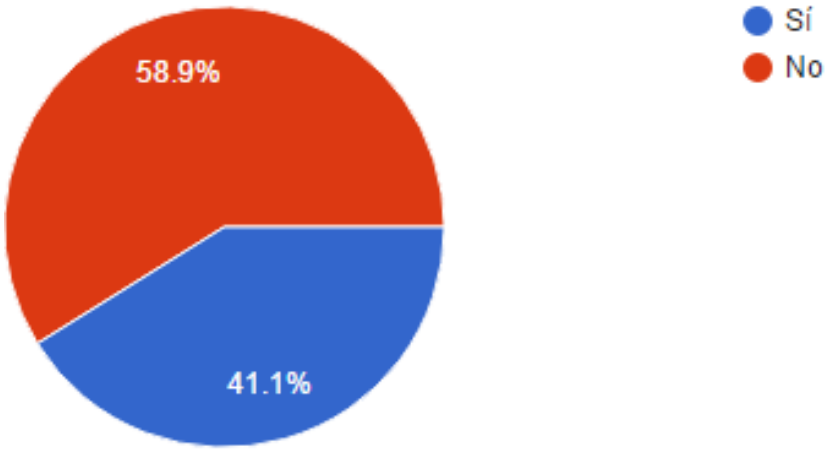


Figura 11. Resultados de la pregunta Nº 6.

Con seguridad general de la plataforma se refiere a la existencia de contramedidas contra vulnerabilidades de aplicaciones web, con la presente pregunta se determina que más de la mitad de los encuestados, en este caso un 58.9% de ellos, encuentran a la página del aula virtual insegura ante ataques web mientras que un 41.1 % sienten que la seguridad manejada es la adecuada.

7. ¿Ha sentido su propia seguridad vulnerada en la plataforma?

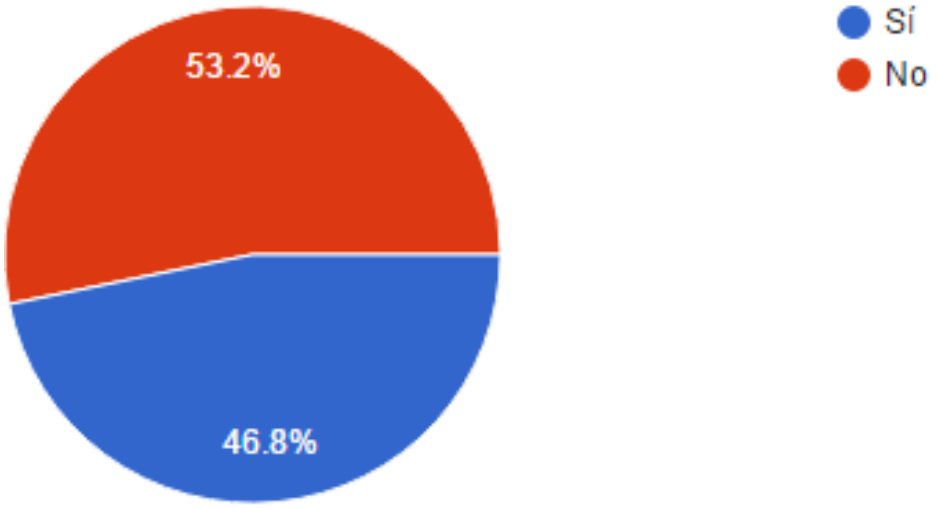


Figura 12. Resultados de la pregunta Nº 7.

En las respuestas presentadas por los encuestados se demuestra cierta confianza en el manejo de datos personales y sensibles dentro del aula virtual, el 53.2% de estudiantes manifiestan que su grado de seguridad dentro del aula virtual es el adecuado mientras que un 46.8% no lo considera así por lo que es necesario comprobar si los procesos del manejo de seguridad de la misma son los adecuados.

8. ¿Con qué frecuencia cambia su contraseña de ingreso a la plataforma virtual?

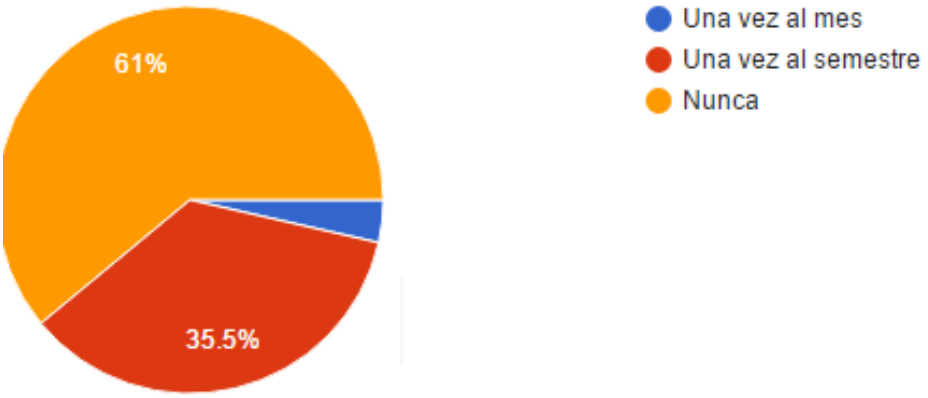


Figura 13. Resultados de la pregunta Nº 8

Ésta es una de las principales dificultades existentes dentro de un sistema computacional, representando un gran riesgo de seguridad para el propio estudiante y para quienes administran la página virtual al existir posibilidades de suplantación de identidad.

Un 61% de los estudiantes nunca ha realizado cambio alguno a su contraseña para ingresar a la plataforma virtual, el 35.5% lo hace una vez al iniciar el semestre mientras que un preocupante 3.5% de estudiantes lo realiza cada mes, cuando éstos datos deberían ser invertidos.

9. Considera su contraseña de acceso al aula virtual como:

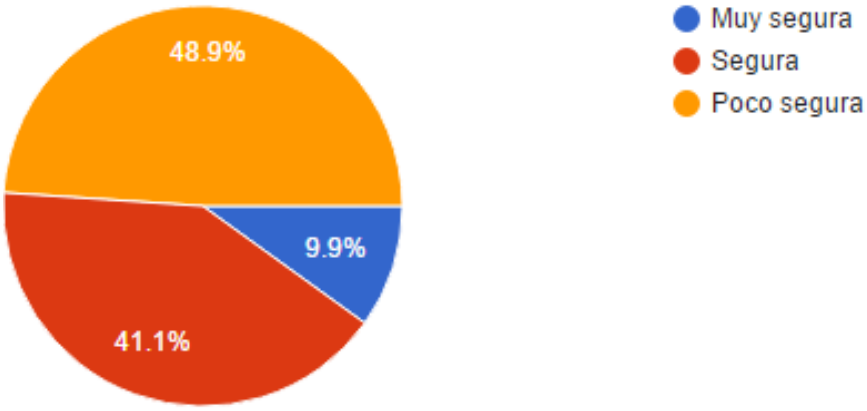


Figura 14. Resultados de la pregunta Nº 9

Por la misma razón anterior se necesitan políticas de seguridad para manejo de contraseñas lo cual garantizaría de mayor manera la seguridad de los datos estudiantiles, son un 48.9% de estudiantes que consideran que su propia contraseña es insegura, muchas veces por desconocimiento de las vulnerabilidades existentes, un 41.1% la considera segura, tal vez por haberla cambiado en algún momento a alguna que no sea fácil de adivinar y un 9.9% muy segura representando una

minoría del estudiantado, lo cual con el presente proyecto de investigación se pretende cambiar.

10. ¿En la escala de 1 al 5 cómo calificaría el grado de seguridad de la plataforma?

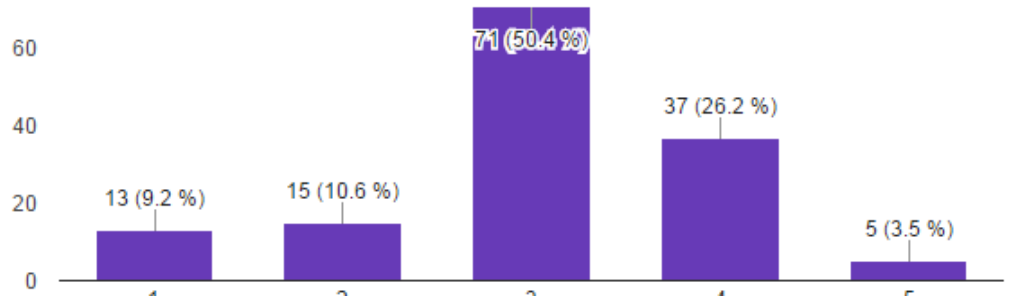


Figura 15. Resultados de la pregunta Nº 10.

De la misma manera es necesario el mejoramiento de la seguridad para el manejo de datos al existir cierta inconformidad por parte de los estudiantes, siendo el 50.4% de ellos que consideran que debe existir un mejoramiento de la misma.

Con el presente proyecto de investigación, se pretende realizar un mejoramiento de los procesos que son manejados dentro de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato, quienes están encargados del manejo de las aulas virtuales universitarias para la mitigación de dificultades y riesgos de seguridad informática.

4.9 METODOLOGÍA

Se evaluan los tipos de ataques más comunes realizados hacia páginas web, ésta investigación se llevó a cabo mediante los reportes realizados por distintas páginas web durante el año 2015 recolectadas en el trabajo de investigación titulado *"Attributing cyber attacks"* tomando en cuenta los más comunes [31].

Nombre	Descripción	Riesgo
Google Hacking	Mediante el uso de la herramienta google sea realiza un análisis completo de la página web en búsqueda de información sensible.	Bajo
Escaneo de Puertos	Es usado para determinad la vulnerabilidad de un puerto en específico para atacar un servicio en especial.	Medio
Ataques de fuerza bruta	Consiste en probar una combinación de credenciales una y otra vez hasta dar con la correcta, produce una gran cantidad de tráfico de red.	Medio
Ataque de hombre en el medio	Se utilizan para capturar todo el tráfico que proviene de un sitio hacia otro, usado para capturar datos no encriptados.	Alto
Denegación de Servicios	Es usado para realizar muchas peticiones a un sitio en específico, provocando su sobrecarga y caída de servicios	Alto
Cross Site Scripting	Es usado para inyectar código ejecutable en una página web no segura para que realice acciones distintas a las programadas.	Alto
Phishing	Un ataque el cual, mediante engaños, busca que un usuario realice una acción en específico, como por ejemplo dar sus credenciales de acceso.	Medio
Inyecciones SQL	Es el ingreso de código tipo SQL que busca que el sitio devuelva información de filas o tablas de la base de datos que usa.	Alto
Ataque mediante referencias inseguras	Se explota la vulnerabilidad mediante el cambio directo de una URL para que la página web devuelva un sitio distinto a la misma, muchas veces puede devolver sitios de administración	Bajo

Tabla 1. Análisis de ataques más comunes hacia páginas web.

Seguido de ello es necesario conocer las diferentes metodologías y herramientas necesarias para llevar a cabo un análisis de vulnerabilidades, por lo que se deben enlistar sus principales ventajas y desventajas, para así poder determinar las mejores herramientas con las cuales el presente proyecto se realiza.

Las consideraciones para el uso de las metodologías y herramientas presentadas son basados en el estudio y análisis de trabajos de titulación anteriormente realizados en la Universidad Técnica de Ambato tales como "Auditoría de la Seguridad Informática para el Honorable Gobierno Provincial de Tungurahua" y "Aplicación de Hacking Ético para la Determinación de Vulnerabilidades de Acceso a Redes Inalámbricas WiFi", tomando en cuenta su eficiencia, grado de profundidad del estudio y considerando que la presente investigación se trata de un análisis de vulnerabilidades de sombrero gris [6] [20].

Nombre	Ventajas	Desventajas	Uso
Metodología OSSTMM	• Hace uso de métricas para determinar impactos y riesgos. • Realiza análisis tanto a la empresa como a sus sistemas, aplicaciones y procesos. • Posee su propio formato de reportes.	• Es necesario realizar una ardua y profunda investigación para obtener los datos y las métricas. • Es necesario una vasta experiencia en análisis de procesos empresariales. • Puede resultar tediosa al tener que analizar no sólo el ámbito digital sino físico y procesos humanos. • Demasiado general.	
Metodología OWASP	• Específica en el ámbito digital, tomando en cuenta aspectos humanos relacionados a aplicaciones web. • Posee herramientas propias para realizar su análisis y pruebas de penetración. • Es más difundido a nivel mundial • Posee metodologías para corregir vulnerabilidades encontradas. • Es más flexible. • Permite el trabajo colaborativo.	• No toma en cuenta procesos empresariales que no tengan relación directa con la aplicación web. • No posee un formato de reportes específico. • Constantes cambios en sus herramientas provocan bugs en las mismas.	
The Harvester	• Permite realizar una búsqueda dentro de todo el sitio web. • Permite exportar las búsquedas a código HTML y XML. • Facilita la realización de reportes.	• Sólo es utilizado para búsqueda de correos electrónicos vinculados a páginas web. • Algunos correos electrónicos no son tomados en cuenta por el programa por lo que no aparecen en su reporte.	

FOCA	• Realiza una búsqueda intensiva de archivos y metadatos de una página web. • Permite descargar todos los archivos encontrados. • Trabaja con distintos formatos de documentos (.pdf, .doc, .xml). • Enlista las todas las redes conectadas a un servidor. • Realiza un análisis de archivos en donde reporta su fecha de creación, servidor y sistema operativo.	• Su interfaz puede resultar en cierta medida complicada.	
Nmap	• Analiza todas las redes vinculadas a una IP. • Puede sobrepasar esquemas de Firewall. • Los paquetes que envía a las diferentes IPs están muy bien construidos. • Realiza sus consultas de manera rápida. • Puede escanear un rango de IPs enlistando todos los servicios. • Configurable.	• Su soporte para Windows es deficiente. • No sobrepasa esquemas de proxys. • Puede resultar muy invasivo creando una cantidad de tráfico inusual en la red.	
Armitage	• Su interfaz gráfica facilita el manejo de sus herramientas. • Contiene una vasta base de datos de exploits para su uso. • Elimina la necesidad de programación del usuario. • Muy usado para análisis de vulnerabilidades con ataques que afectan al servidor.	• Se debe tener un conocimiento bastante grande de exploits y programación. • Al tener exploits pre programados no es transparente en cuestión a lo que realiza cada uno paso a paso.	
Dumpsec	• Permite realizar un análisis de usuarios y roles dentro de una página web.	• Usado únicamente en Windows.	

	• Interfaz muy amigable y fácil de usar. • Permite analizar los servicios que se están ejecutando.	• Existe una falla al momento de enlistar los servicios donde muestra otro puerto en lugar del real.	
LOIC	• Interfaz simple de usar. • Realiza la cantidad de peticiones simultaneas programadas. • Permite visualizar el estado del ataque.	• Provoca tráfico en la red interna de la máquina atacante. • Al no poder ser configurado no garantiza un anonimato por parte del atacante • Únicamente disponible en Windows.	
OpenVAS	• Es de código abierto. • Posee interfaz gráfica. • Permite realizar una auditoría de seguridad informática completa. • Posee herramientas propias para realizar sus funciones. • Posee la facilidad de generación de reportes.	• Plugins limitados. • Es complicado de instalar, configurar y ejecutar. • Complejidad en el manejo, orientado a expertos informáticos. • Toma una gran cantidad de tiempo y recursos poder realizar un análisis de vulnerabilidades.	
OWASP ZAP	• Herramienta de código abierto. • Multi plataforma. • Facilidad de instalación. • Soporte continuo. • Permite realizar análisis de cabeceras de una manera más simple. • Análisis pasivos.	• A pesar de poseer interfaz gráfica su uso puede ser complicado. • No puede sobrepasar esquemas de firewalls. • Está limitado por la velocidad de conexión y es invasivo.	
Joomscan	• Herramienta de código abierto. • Permite realizar un análisis de vulnerabilidades con un simple comando. • La presentación de las vulnerabilidades es clara y concisa.	• Algunos exploits no están incluidos en su base de datos. • No puede sobrepasar esquemas de firewalls.	

	• Detecta el lugar exacto donde fue encontrada la vulnerabilidad y lo expone.	• No posee una herramienta avanzada para análisis de inyección SQL.	

Tabla 2. Análisis de ventajas y desventajas de metodologías y herramientas para Pentesting

Mediante el análisis presentado en la tabla anterior se pudo concluir las herramientas que van a ser utilizadas y realizar una comparativa del por qué es utilizada la metodología OWASP para la investigación.

Para el presente proyecto de investigación se debe definir en primer lugar, lo que representa OWASP (Open Web Application Security Project), la cual es una organización sin fines de lucro; busca ofrecer soluciones y herramientas para crear, operar, desarrollar, mantener y asegurar aplicaciones para su mejoramiento [32].

OWASP, al ser un proyecto de constante crecimiento, se utilizará su última versión 4.0 la cual fue creada el 17 de septiembre de 2014 y actualizada en abril del 2016. [32]

La Guía de Pruebas OWASP posee un apartado específico para la realización de pruebas de penetración *"Web Application Penetration Testing"* en donde especifica todos los puntos necesarios a asegurar dentro de una institución, en el presente proyecto se toma como base a las proposiciones de ésta metodología para una incursión de SOMBRERO GRIS.

Estudio de la metodología OWASP para test de penetración de aplicaciones web

Un test de seguridad es un método de evaluación a una red de sistemas de computadoras mediante la validación metódica y la verificación de la efectividad de los controles de seguridad de la aplicación o página web.

El proceso incluye un análisis activo de las vulnerabilidades de la aplicación, los problemas encontrados deberán ser presentados al dueño del sistema, conjuntamente con el grado de impacto y la propuesta de mitigación o una solución técnica.

El presente test está dividido en dos fases:

Fase 1 Modo Pasivo: En el modo pasivo el analista juega con la aplicación, todos sus botones y características. Se pueden utilizar herramientas para recolección de datos, con el objetivo de conocer las entradas posibles hacia la aplicación.

Fase 2 Modo Activo: En éste momento el analista empieza a utilizar la presente metodología que se irá describiendo a continuación:

- Recolección de Información
- Test de manejo de configuración y desarrollo
- Test de manejo de identidad
- Test de autenticación
- Test de autorización
- Test de manejo de sesiones
- Test de validación de entradas
- Manejo de errores
- Criptografía
- Test de lógica de negocio
- Test de lado cliente

4.10 DESARROLLO DE LA METODOLOGÍA OWASP PARA TEST DE PENETRACIÓN DE APLICACIONES WEB

La presente metodología fue escogida dado a que se analizará tanto al dominio principal de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato para errores sistemáticos y análisis web estático (sitio web), como a su subdominio del Aula Virtual de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial para análisis de errores humanos, procesos deficientes y suplantaciones de identidad en una página web dinámica (aplicación web).

4.10.1. RECOLECCIÓN DE INFORMACIÓN

a) Uso de un motor de búsqueda para verificación de existencia de información vulnerable

Existen elementos directos e indirectos los cuales pueden ser obtenidos mediante un motor de búsqueda si no existe una configuración adecuada. Los elementos directos se refieren a los índices de búsqueda, mientras que los indirectos representan información sensible la cual puede ser utilizada para una explotación.

Objetivo

Comprender el diseño y configuración de la página web, sus aplicaciones y organización y si éste tipo de información se encuentra expuesta directa o indirectamente.

Se realiza una búsqueda compuesta de site: "nombre de la página web" para encontrar las subpáginas que contiene.

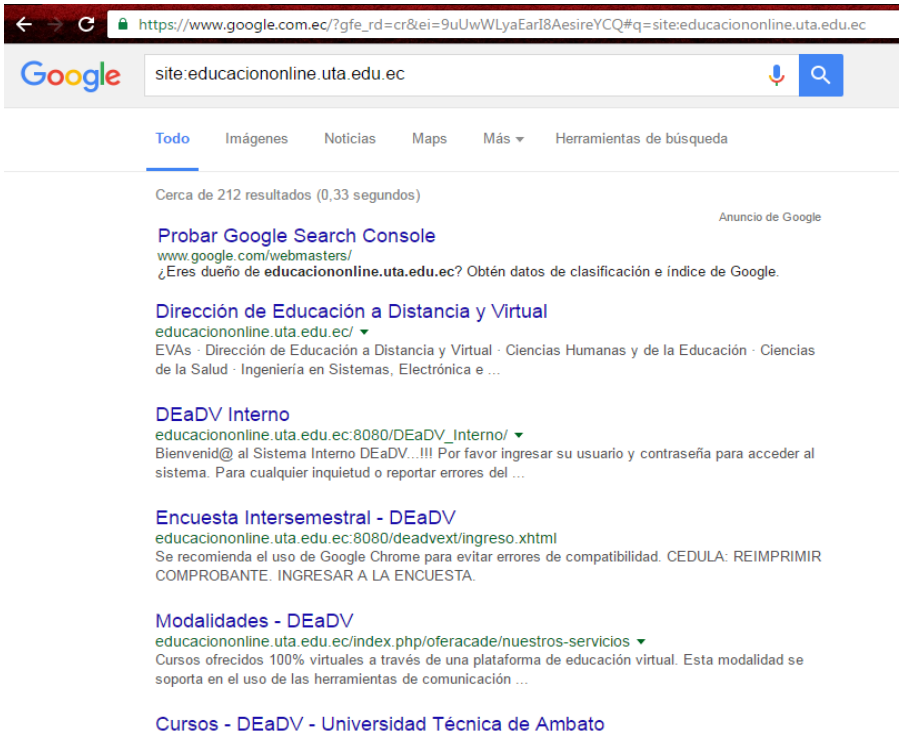


Figura 16. Resultados de la búsqueda del sitio web en google

Entre los primeros datos se obtienen páginas web que pueden ser de utilidad para posteriores explotaciones como son:

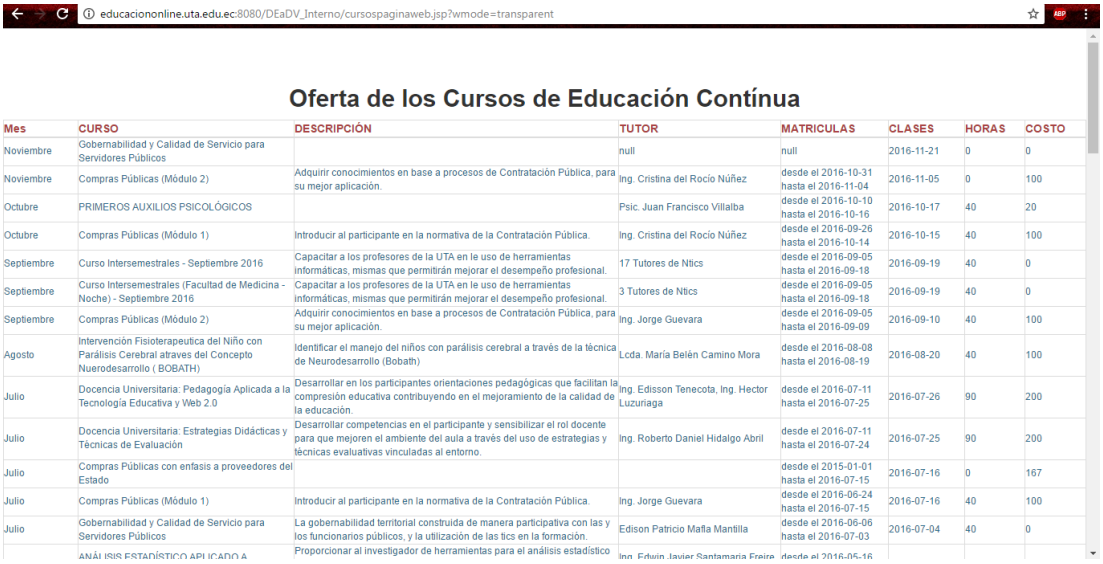
Figura 17. Sitio web interno de la Dirección de Educación a Distancia y Virtual

En la imagen se puede observar que en el URL se presenta el puerto al que se está dirigiendo la consulta, y dirige a una página que requiere autenticación de usuario y contraseña.

Así mismo, como se puede apreciar en la siguiente captura de pantalla, se encuentra una dirección que lleva hacia un ingreso con número de cédula para la realización de una encuesta.

Figura 18. Sitio web de ingreso a encuestas DEaDV

Se encontró información acerca de cursos online que ofrece la unidad de educación continua.



Oferta de los Cursos de Educación Contínua

Mes	CURSO	DESCRIPCIÓN	TUTOR	MATRICULAS	CLASES	HORAS	COSTO
Noviembre	Gobernabilidad y Calidad de Servicio para Servidores Públicos		null	null	2016-11-21	0	0
Noviembre	Compras Públicas (Módulo 2)	Adquirir conocimientos en base a procesos de Contratación Pública, para su mejor aplicación.	Ing. Cristina del Rocío Núñez	desde el 2016-10-31 hasta el 2016-11-04	2016-11-05	0	100
Octubre	PRIMEROS AUXILIOS PSICOLÓGICOS		Psic. Juan Francisco Villalba	desde el 2016-10-10 hasta el 2016-10-16	2016-10-17	40	20
Octubre	Compras Públicas (Módulo 1)	Introducir al participante en la normativa de la Contratación Pública.	Ing. Cristina del Rocío Núñez	desde el 2016-09-26 hasta el 2016-10-14	2016-10-15	40	100
Septiembre	Curso Intersemestrales - Septiembre 2016	Capacitar a los profesores de la UTA en le uso de herramientas informáticas, mismas que permitirán mejorar el desempeño profesional.	17 Tutores de Ntics	desde el 2016-09-05 hasta el 2016-09-18	2016-09-19	40	0
Septiembre	Curso Intersemestrales (Facultad de Medicina - Noche) - Septiembre 2016	Capacitar a los profesores de la UTA en le uso de herramientas informáticas, mismas que permitirán mejorar el desempeño profesional.	3 Tutores de Ntics	desde el 2016-09-05 hasta el 2016-09-18	2016-09-19	40	0
Septiembre	Compras Públicas (Módulo 2)	Adquirir conocimientos en base a procesos de Contratación Pública, para su mejor aplicación.	Ing. Jorge Guevara	desde el 2016-09-05 hasta el 2016-09-09	2016-09-10	40	100
Agosto	Intervención Fisioterapeutica del Niño con Parálisis Cerebral atraves del Concepto Nuerodesarrollo (BOBATH)	Identificar el manejo del niños con parálisis cerebral a través de la técnica de Neurodesarrollo (Bobath)	Lcda. María Belén Camino Mora	desde el 2016-08-08 hasta el 2016-08-19	2016-08-20	40	100
Julio	Docencia Universitaria: Pedagogía Aplicada a la Tecnología Educativa y Web 2.0	Desarrollar en los participantes orientaciones pedagógicas que facilitan la compresión educativa contribuyendo en el mejoramiento de la calidad de la educación.	Ing. Edisson Tenecota, Ing. Hector Luzuriaga	desde el 2016-07-11 hasta el 2016-07-25	2016-07-26	90	200
Julio	Docencia Universitaria: Estrategias Didácticas y Técnicas de Evaluación	Desarrollar competencias en el participante y sensibilizar el rol docente para que mejoren el ambiente del aula a través del uso de estrategias y técnicas evaluativas vinculadas al entorno.	Ing. Roberto Daniel Hidalgo Abril	desde el 2016-07-11 hasta el 2016-07-24	2016-07-25	90	200
Julio	Compras Públicas con enfasis a proveedores del Estado			desde el 2015-01-01 hasta el 2016-07-15	2016-07-16	0	167
Julio	Compras Públicas (Módulo 1)	Introducir al participante en la normativa de la Contratación Pública.	Ing. Jorge Guevara	desde el 2016-06-24 hasta el 2016-07-15	2016-07-16	40	100
Julio	Gobernabilidad y Calidad de Servicio para Servidores Públicos	La gobernabilidad territorial construida de manera participativa con las y los funcionarios públicos, y la utilización de las tics en la formación.	Edison Patricio Mafla Mantilla	desde el 2016-06-06 hasta el 2016-07-03	2016-07-04	40	0
	ANÁLISIS ESTADÍSTICO APLICADO A	Proporcionar al investigador de herramientas para el análisis estadístico	Ing. Edwin Javier Santamaria Freire	desde el 2016-05-16			

Figura 19. Sitio web de oferta de cursos de educación continua

Se encontró una dirección que puede resultar peligrosa al contener información sensible http://educaciononline.uta.edu.ec/curriculums/ y http://educaciononline.uta.edu.ec/descargas/

Index of /curriculums

Name	Last modified	Size	Description
Parent Directory		-	
Curriculo Instructora WILMA GAVILANEZ.pdf	08-Apr-2014 15:06	302K	
Curriculo Instructor eduardofernandez.pdf	01-Apr-2014 16:54	225K	
Eduardo Fernández.pdf	18-May-2015 17:24	1.0M	
Edwin Santamaria.pdf	18-May-2015 17:23	396K	
Mauricio Tenecota.pdf	18-May-2015 17:28	377K	
dhidalgo.pdf	02-Jun-2015 09:14	243K	
edwinsantamaria.pdf	02-Apr-2014 11:42	222K	
hectorhurtado.pdf	13-Aug-2014 12:02	111K	
marceloaldaz.pdf	24-Sep-2014 16:38	179K	
mauriciotenecota.pdf	24-Sep-2014 16:39	182K	
ovaca.pdf	04-Jul-2014 17:32	54K	

Index of /descargas

Name	Last modified	Size	Description
Parent Directory		-	
Acceso_a_la_Plataforma.pdf	16-Jun-2014 12:28	8.1M	
Formulario_Aula_Virtual.pdf	22-Jan-2015 09:32	430K	
Intersemestral_Septiembre_2016.zip	16-Sep-2016 17:52	306M	
Manual_de_usuario_2016.pdf	13-Oct-2016 15:40	15M	
copia_de_seguridad-Aula-Base1617-nu.mbz	13-Oct-2016 10:16	4.8M	

Figura 20. Urls de sitios web con posible información sensible

Con lo cual se puede concluir que existe un proceso el cual se debería corregir y se refiere al sitio web el cual dirige hacia un puerto en específico, dando una pauta a un atacante para focalizar su intrusión.

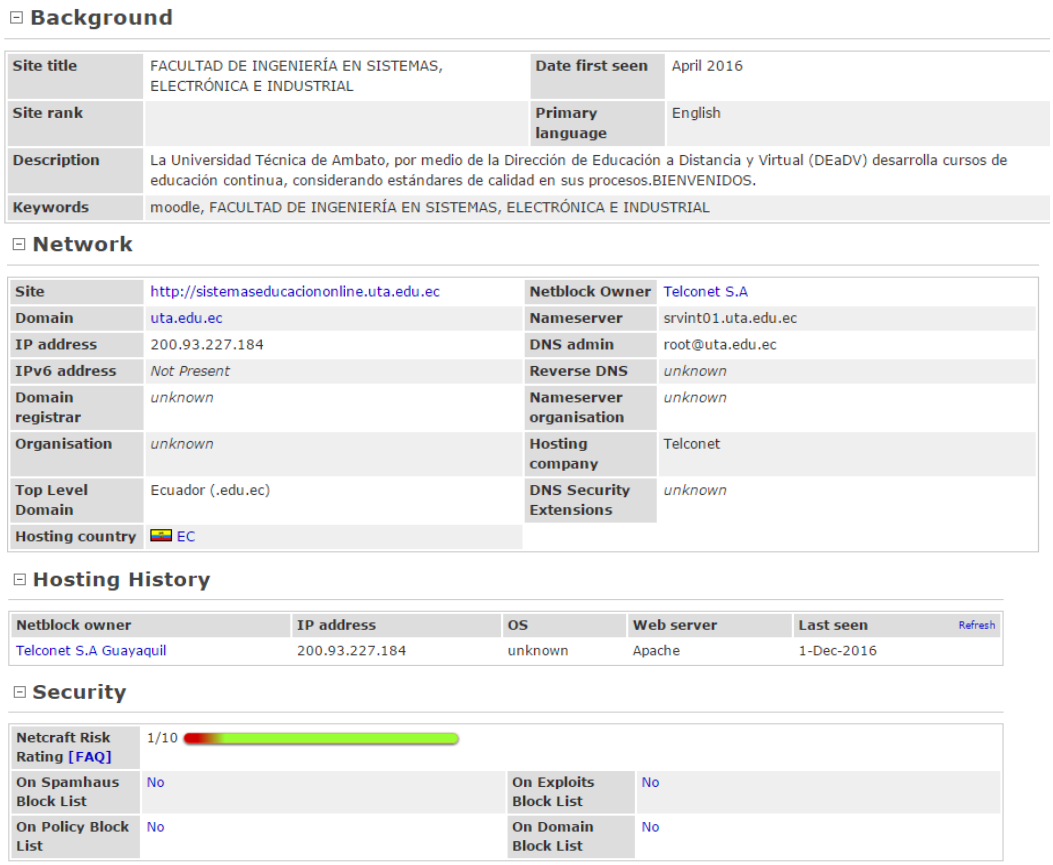
b) Análisis del sitio y servidor web para verificar nombres por defecto

El conocer al sitio web que va a ser atacado es una etapa crítica de un auditor informático, ya que en ésta etapa se encuentra el objetivo que será la *víctima*, así como el tipo de servidor en donde éste corre y su versión.

Objetivo:

Conocer la IP del sitio web a ser atacado como el servidor que lo maneja y su versión.

En primera instancia se hará uso de la herramienta Netcraft, la cual proporciona información básica del sitio web a vulnerar.



Background

Site title	FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL	**Date first seen**	April 2016
Site rank		**Primary language**	English
Description	La Universidad Técnica de Ambato, por medio de la Dirección de Educación a Distancia y Virtual (DEaDV) desarrolla cursos de educación continua, considerando estándares de calidad en sus procesos.BIENVENIDOS.		
Keywords	moodle, FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL		

Network

Site	http://sistemaseducaciononline.uta.edu.ec	**Netblock Owner**	Telconet S.A
Domain	uta.edu.ec	**Nameserver**	srvint01.uta.edu.ec
IP address	200.93.227.184	**DNS admin**	root@uta.edu.ec
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	Telconet
Top Level Domain	Ecuador (.edu.ec)	**DNS Security Extensions**	*unknown*
Hosting country	EC		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Telconet S.A Guayaquil	200.93.227.184	unknown	Apache	1-Dec-2016

Security

Netcraft Risk Rating [FAQ]	1/10		
On Spamhaus Block List	No	**On Exploits Block List**	No
On Policy Block List	No	**On Domain Block List**	No

Figura 21. Información de Netcraft del subdominio de la página web de la DEaDV

Al conocer la IP de la página o aplicación web específica se procede a realizar una consulta, mediante el comando whois en Kali Linux.

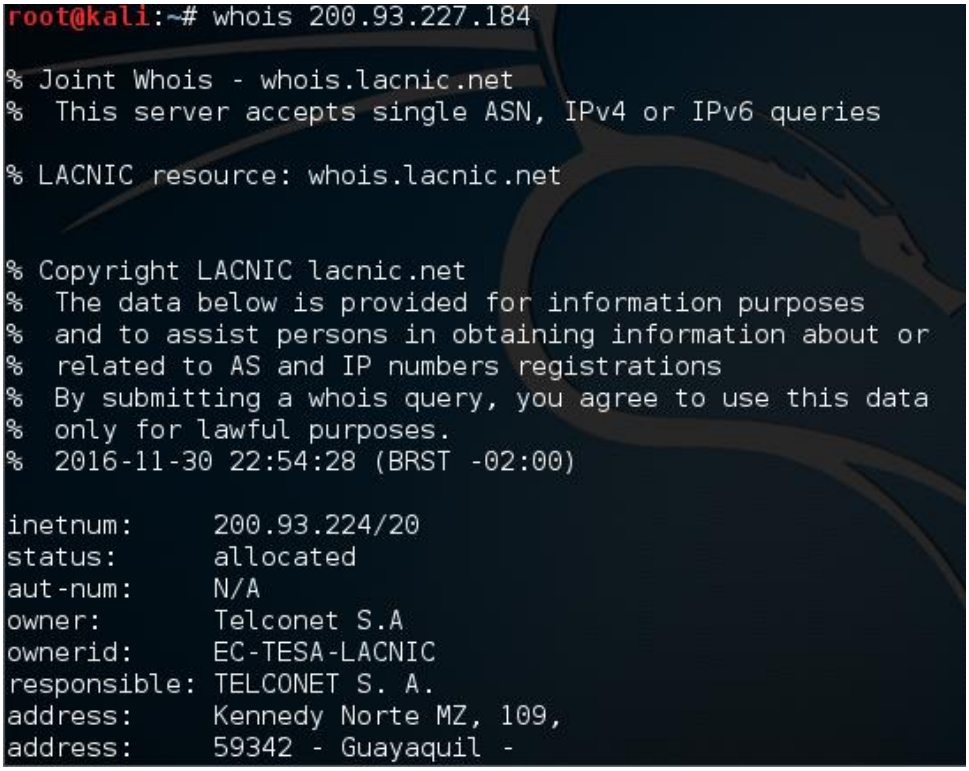


Figura 22. Respuesta del servidor acerca de la consulta whois (1)

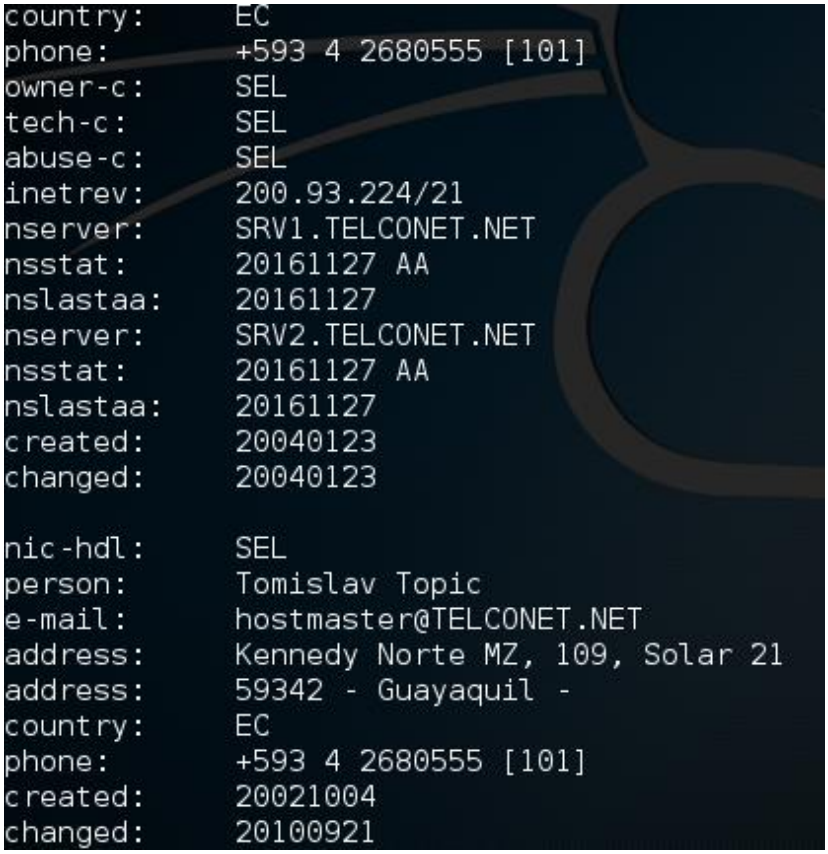


Figura 23. Respuesta del servidor acerca de la consulta whois (2)

De la misma manera se realiza una consulta a las cabeceras de la página web para obtener su información.

```
HTTP/1.1 200 OK
Date: Fri, 09 Dec 2016 14:29:59 GMT
Server: Apache
X-Powered-By: PHP/5.6.28
Set-Cookie: 88b13f49ddef3cf983705838cea21858=uiv5r8prn8jr8j35g2r3t9frg1; path=/; HttpOnly
Expires: Fri, 09 Dec 2016 14:29:59 GMT
Last-Modified: Fri, 09 Dec 2016 14:29:59 GMT
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Access-Control-Allow-Origin: http://educaciononline.uta.edu.ec:8080
Content-Length: 3538
Connection: close
Content-Type: application/javascript; charset=utf-8
```

Figura 24. Respuesta de consulta de cabecera de la página web de la DEaDV

Con las presentes consultas se obtuvo información muy útil para los fines pertinentes a un análisis de vulnerabilidades, tales como:

- Direcciones IP de los servidores
- Direcciones de los proveedores
- Nombre del servidor
- Herramientas de funcionamiento y sus versiones
- Contactos de proveedores y administradores
- Sistema Operativo del servidor

c) Recolección de metadatos de la página web para la comprobación de existencia de información vulnerable

Con la presente prueba se analiza el archivo robots.txt con el fin de encontrar información acerca de las carpetas existentes dentro del servidor y verificar si existe posibilidad de acceder a archivos de información sensible.

Objetivo:

Encontrar las direcciones de carpetas, así como crear una lista de directorios que pueden ser usados para sobrepasar las seguridades.

Para comenzar se ingresa a la URL http://educaciononline.uta.edu.ec/robots.txt en donde se encuentra la siguiente información.

```
#
# robots.txt
#

User-agent: Aboundexbot
Disallow: /

User-agent: BlackWidow
Disallow: /

User-agent: Bot mailto:craftbot@yahoo.com
Disallow: /

User-agent: ChinaClaw
Disallow: /

User-agent: Custo
Disallow: /

User-agent: DISCo
Disallow: /

User-agent: DOC
Disallow: /

User-agent: Download Demon
Disallow: /

User-agent: Download Ninja
Disallow: /

User-agent: eCatch
Disallow: /

User-agent: EirGrabber
Disallow: /

User-agent: EmailSiphon
Disallow: /

User-agent: EmailWolf
Disallow: /

User-agent: Express WebPictures
Disallow: /
```

Figura 25. Archivo robots.txt de la página web de la DEaDV (1)

```
User-agent: ExtractorPro
Disallow: /

User-agent: EyeNetIE
Disallow: /

User-agent: Fetch
Disallow: /

User-agent: FlashGet
Disallow: /

User-agent: GetRight
Disallow: /

User-agent: GetWeb!
Disallow: /

User-agent: Go-Ahead-Got-It
Disallow: /

User-agent: Go!Zilla
Disallow: /

User-agent: GrabNet
Disallow: /

User-agent: Grafula
Disallow: /

User-agent: grub-client
Disallow: /

User-agent: HMView
Disallow: /

User-agent: HTTrack
Disallow: /

User-agent: HTTrack
Disallow: /

User-agent: Image Stripper
Disallow: /
```

Figura 26. Archivo robots.txt de la página web de la DEaDV (2)

Con el presente análisis se puede comprobar todos los recursos deshabilitados de la página web y con un análisis a las mismas encontrar recursos no enlistados los cuales son posibles utilizar.

d) Enumeración de las aplicaciones del servidor web

Dentro de un servidor pueden correr una o más aplicaciones web, es importante conocer todas ellas ya que pueden existir vulnerabilidades en alguna de ellas y puede ser explotado.

Objetivo:

Enumerar las aplicaciones web que posea el servidor de la página web.

Se puede comenzar con una búsqueda en Google para analizar las aplicaciones que contiene el servidor web.

Figura 27. Página de inicio de la aplicación del aula virtual de Ingeniería en Sistemas, Electrónica e Industrial

Fue encontrada la aplicación de aula virtual del DEaDV perteneciente a Ingeniería en Sistemas, Electrónica e Industrial, la misma que será utilizada para comprobación de vulnerabilidades que sean causadas por errores humanos, más adelante en el presente proyecto.

Otra manera de encontrar las aplicaciones que se encuentran dentro de un servidor en específico es mediante el escaneo de puertos utilizando el comando NMAP.

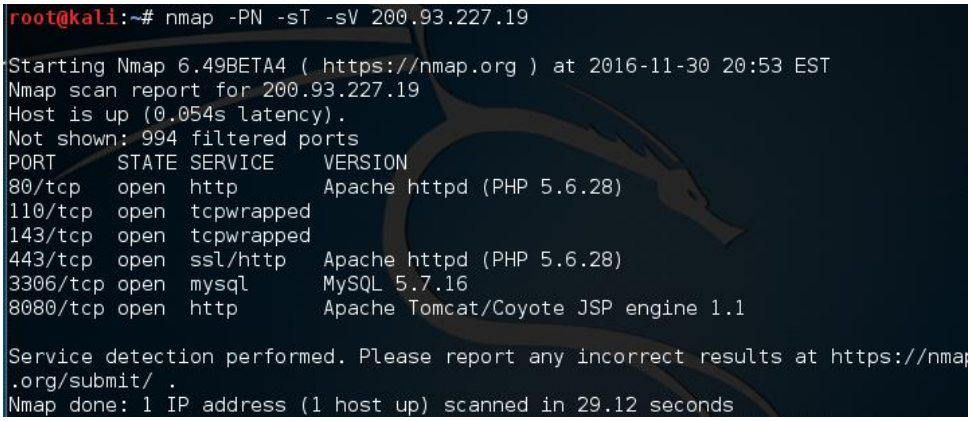


Figura 28. Escaneo de puertos del servidor de la DEaDV

Se puede así mismo comprobar si existe algún tipo de filtrado firewall

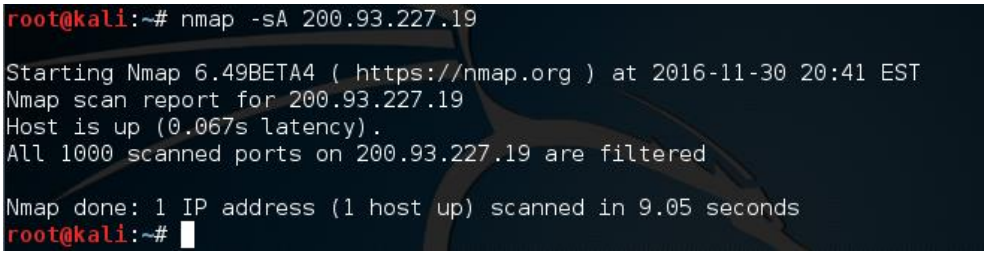


Figura 29. Escaneo de filtro firewall

Se comprueba si existe algún tipo de hosting virtual

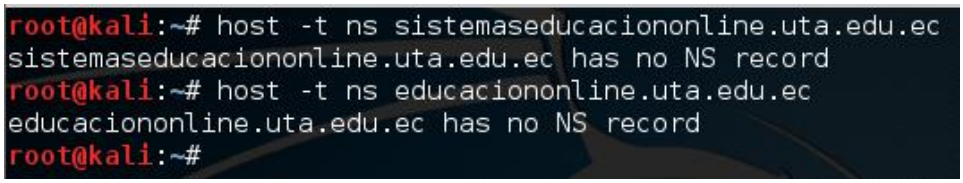


Figura 30. Uso del comando host a los dominios de la DEaDV

Es necesario tener en cuenta a todos los puertos abiertos y manejar la información proporcionada por el escaneo de puertos.

Para el análisis de sombrero gris se solicitó un permiso especial para tener una conexión directa al servidor, seguido de ello, y con el mismo comando, se encontraron puertos no accesibles externamente.

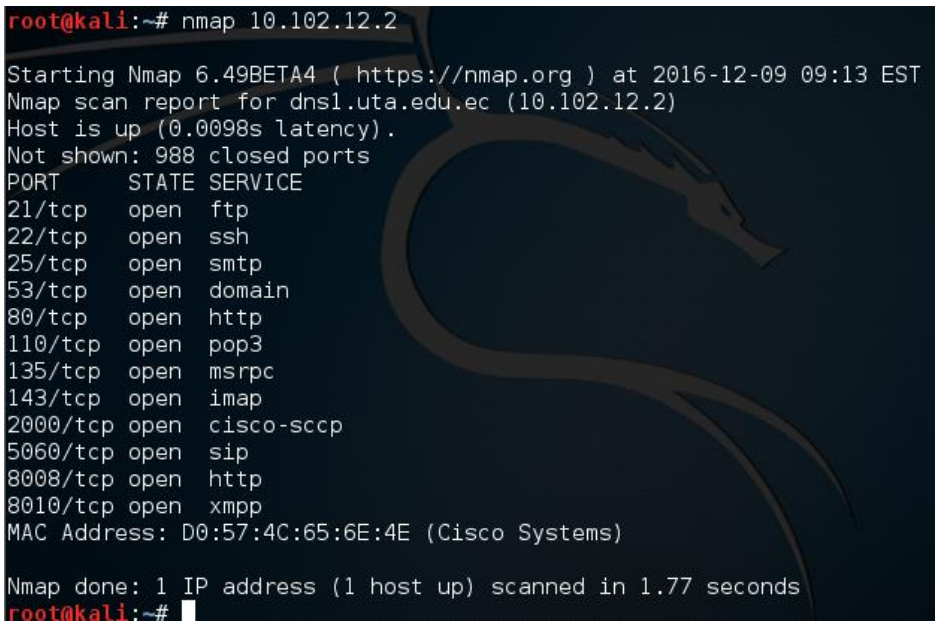


Figura 31. Escaneo de puertos desde red interna

e) Revisión de comentarios y metadata del sitio web para verificación de existencia de información vulnerable

Muchos programadores utilizan comentarios dentro de su código, muchas veces se pueden encontrar comentarios en el código HTML que pueden contener cierta información que puede ser utilizada.
Así mismo, los archivos que son subidos a las páginas web suelen contener datos acerca de quiénes los crearon, información que puede ser útil en caso de realizar ataques de contraseñas.

Objetivo:

Analizar los metadatos obtenidos de la página web de la DEaDV.

Se tomará en un inicio a la herramienta FOCA para analizar los archivos que posea la página web.

Un ejemplo principal se da al analizar la sección de currículums de la página de la DEaDV.

Attribute	Value
File Information	
URL	http://educaciononline.uta.edu.ec/curriculums/dhidalgo.pdf
Local path	C:\Users\PC\Desktop\Análisis Foca\dhidalgo (1).pdf
Download	Yes
Analized	Yes
Download date	07/01/2017 12:40:32
Size	242,72 KB
Users	
Username	OK
Dates	
Creation date	20/04/2015 20:33:59
Modified date	20/04/2015 20:33:59
Other Metadata	
Application	Microsoft Office XP
Software	
Microsoft Office XP	

Figura 32. Análisis de un archivo mediante FOCA.

Existen maneras de determinar al creador, la fecha de creación y el software utilizado para los distintos archivos que tiene una página web.

De la misma manera si se realiza un análisis al código de la página principal, en búsqueda de la existencia comentarios HTML o líneas de código que posean información importante.

```
<html dir="ltr" lang="es-es" slick-uniqueid="3" class="js csstransforms csstransforms3d csstransitions chrome chrome55
responsive responsive-phone" style>
  ▶#shadow-root (open)
  ▶<head>…</head>
  ▼<body>
    ▼<div id="art-main">
      ▶<div id="art-hmenu-bg" class="art-bar art-nav" style="top: 102.396px;" data-bg-top="156.997px" data-bg-height="4px">…</di
      ▼<div class="art-sheet clearfix">
          ::before
        ▼<header class="art-header">
            ::before
          ▶<div class="art-shapes">…</div>
          ▼<div class="art-textblock art-object227400126" data-left="97.63%">
            ▼<form class="art-search" name="Search" action="/index.php" method="post">
                <input type="text" value name="searchword"> == $0
                <input type="hidden" name="task" value="search">
                <input type="hidden" name="option" value="com_search">
                <input type="submit" value name="search" class="art-search-button">
              </form>
            </div>
            ::after
          </header>
        ▶<nav class="art-nav desktop-nav">…</nav>
        ▶<div class="art-layout-wrapper">…</div>
          ::after
        </div>
      ▶<footer class="art-footer">…</footer>
      </div>
    ▼<noscript>
        "<strong>JavaScript is currently disabled.</strong>Please enable it for a better experience of <a
        href="http://2glux.com/projects/jumi">Jumi</a>."
      </noscript>
    ▼<div class="nanogalleryHideElement ozionanocontainer nanogallery_theme_default nanogallery_colorscheme_light
    nanogallery_galleryfullpage_bgcolor_nanoGallery nanogallery_thumbnails_label_align_left">
      ▶<div class="nanoGalleryContainerParent">…</div>
      </div>
    ▶<div id="art-resp">…</div>
    </body>
</html>
```

Figura 33. Código HTML de la página web principal.

Al momento de revisar el código de la página web mediante el navegador no se encontró ningún comentario por parte de algún programador, mas esto es sólo a nivel externo ya que por motivos institucionales no se tuvo acceso al código PHP en donde sí existen comentarios realizados por los desarrolladores.

f) Identificación de puntos de entrada a la aplicación

Enumerar cuales puntos de entrada existen y conocer cada uno de ellos es una parte fundamental para todo analista, para así encontrar vulnerabilidades en las entradas existentes para fortificarlas con distintos procesos.

Objetivos:

Analizar las peticiones y respuestas desde la página web

Mediante el uso de la herramienta OWASP ZAP se obtuvo información de los métodos GET y POST que se pueden realizar en la página web dando como resultado la siguiente información.

Processed	Method	URI	Flags
	GET	http://educaciononline.uta.edu.ec	SEED
	GET	http://educaciononline.uta.edu.ec/robots.txt	SEED
	GET	http://educaciononline.uta.edu.ec/sitemap.xml	SEED
	GET	http://educaciononline.uta.edu.ec/	
	GET	http://educaciononline.uta.edu.ec/index.php/informacion-general/dea...	
	GET	http://educaciononline.uta.edu.ec/index.php/informacion-general/equ...	
	GET	http://educaciononline.uta.edu.ec/index.php/oferacade/listado-de-cur...	
	GET	http://educaciononline.uta.edu.ec/index.php/oferacade/nuestros-serv...	
	GET	http://educaciononline.uta.edu.ec:8080/utasys/faces/inscripciones/re...	
	GET	http://educaciononline.uta.edu.ec:8080/deadvext/apps/appencuesta/...	
	GET	http://educaciononline.uta.edu.ec/index.php/servicios-en-linea/2016-...	
	GET	http://educaciononline.uta.edu.ec:8080/utasys/faces/reportes/consul...	
	GET	http://educaciononline.uta.edu.ec/index.php/servicios-en-linea/2016-...	
	GET	http://educaciononline.uta.edu.ec/index.php/servicios-en-linea/trabaj...	
	GET	http://educaciononline.uta.edu.ec:8080/DEaDV_Interno/	
	GET	http://educaciononline.uta.edu.ec/index.php/servicios-en-linea/fotogr...	

Figura 34. Métodos GET existentes en distintas URL's de la página web de DEaDV (1)

Processed	Method	URI	Flags
	GET	http://educaciononline.uta.edu.ec/index.php/servicios-en-linea/fotogr...	
	GET	http://educaciononline.uta.edu.ec/index.php/component/content/arti...	
	GET	http://educaciononline.uta.edu.ec/index.php/component/content/arti...	
	GET	http://educacioncontinua.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://humanaseducaciononline.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://saludeducaciononline.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://sistemaseducaciononline.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://jurisprudenciaeducaciononline.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://arteseducaciononline.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://civileducaciononline.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://alimentoseducaciononline.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://agronomiaeducaciononline.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://administracioneducaciononline.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://idiomaseducaciononline.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://auditoriaeducaciononline.uta.edu.ec/	OUT_OF_SCOPE
	GET	http://educaciononline.uta.edu.ec/index.php/contacto	

Figura 35. Métodos GET existentes en distintas URL's de la página web de DEaDV (2)

Debido a políticas institucionales no se pudo realizar el análisis de cabeceras mediante el comando telnet, debido a que existe un firewall controlado por el Dirección de Tecnología de la Información y Comunicación, el cual es distinto al departamento donde se realizó el trabajo, pero se utilizó la herramienta OWASP ZAP para análisis de ciertos métodos POST y aquellas cabeceras.

```
POST http://educaciononline.uta.edu.ec/index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Referer: http://educaciononline.uta.edu.ec/index.php
Host: educaciononline.uta.edu.ec
```

Figura 36. Método POST posible en la página principal de la DEaDV

g) Análisis al entorno del sitio web

El conocer el entorno del sitio web es una subtarea muy importante dentro de la recolección de requerimientos, ya que otorga al analista información que puede resultar útil al momento de realizar las distintas pruebas, tales como configuraciones deficientes del entorno o el uso de configuraciones antiguas y sin parches, lo cual representa una vulnerabilidad bastante grave dentro de un sistema.

Objetivo:

Definir el entorno web en donde se maneja el sitio de la DEaDV

En éste caso se utilizó el comando whatweb, el cual devuelve las configuraciones, versiones y tipos de estructura que componen a una determinada dirección web.

```
root@kali:~# whatweb educaciononline.uta.edu.ec
http://educaciononline.uta.edu.ec [200] Apache, Cookies[88b13f49ddef3cf983705838
cea21858,cip_vvisitcounter], Country[ECUADOR][EC], HTTPServer[Apache], HttpOnly[
88b13f49ddef3cf983705838cea21858], IP[200.93.227.19], maybe Joomla, PHP[5.6.28],
 UncommonHeaders[access-control-allow-origin], X-Powered-By[PHP/5.6.28]
root@kali:~# whatweb -a 3 -p joomla educaciononline.uta.edu.ec
http://educaciononline.uta.edu.ec [200] maybe Joomla
root@kali:~#
```

Figura 37. Resultado del comando whatweb a la dirección de la DEaDV

Con ésta búsqueda la información acerca del servidor que corre al sitio web puede ser analizada y conocer bajo que lenguaje fue realizada, su versión y el tipo de sistema de gestión de contenidos que maneja, que en éste caso es Joomla.

Otra manera de analizar las herramientas utilizadas dentro de un entorno web es mediante el análisis de los comentarios del código HTML.

Figura 38. Análisis de código HTML para búsqueda de herramientas

La herramienta usada para el diseño de la página web es Artisteer, es muy necesaria ésta información para poder conocer a fondo al sitio que se va a analizar.

h) Análisis de la aplicación web

Al terminar con el análisis del sitio web es necesario realizar lo mismo con las aplicaciones web que contenga el sitio.

En el presente proyecto se dará enfoque únicamente a la aplicación web del aula virtual correspondiente a la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

De la misma manera como al sitio web se inicia con el análisis mediante el comando whatweb.

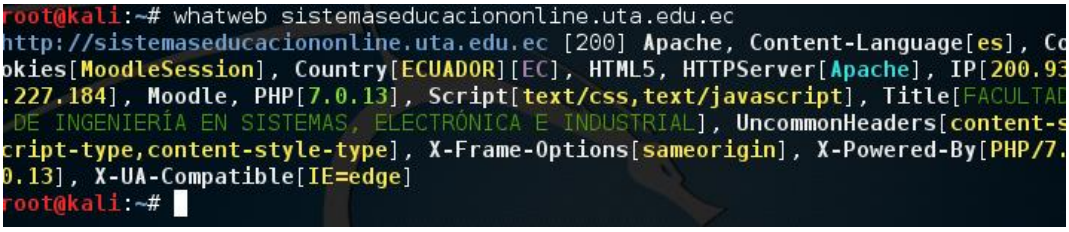


Figura 39. Resultado del comando whatweb realizado a la página del aula virtual

De la misma manera comprobar el entorno en el cual la aplicación es manejada, así como el lenguaje y la versión del mismo, es primordial.

Al ingresar en la página web mencionada se puede observar el sistema de manejo de contenidos para aplicaciones web utilizado.

Figura 40. Sistema de manejo de contenidos de la página del aula virtual

Así mismo mediante el análisis del código HTML se determina el tipo de lenguaje utilizado para la aplicación, en éste caso siendo javascript.

Figura 41. Análisis de código HTML a la página del aula virtual

i) Análisis y mapa de la arquitectura de la aplicación

La complejidad de la infraestructura de un sitio web puede resultar en gran medida complicado de analizar paso a paso, pero representa un pilar fundamental dentro del análisis de seguridad ya que un simple error de configuración puede recaer en la pérdida total de los datos de una institución.

Objetivo:

Determinar la infraestructura utilizada dentro del sitio web de la DEaDV

Para el análisis se hará uso la herramienta OWASP ZAP la cual proporciona un análisis a fondo de la estructura de la página web.

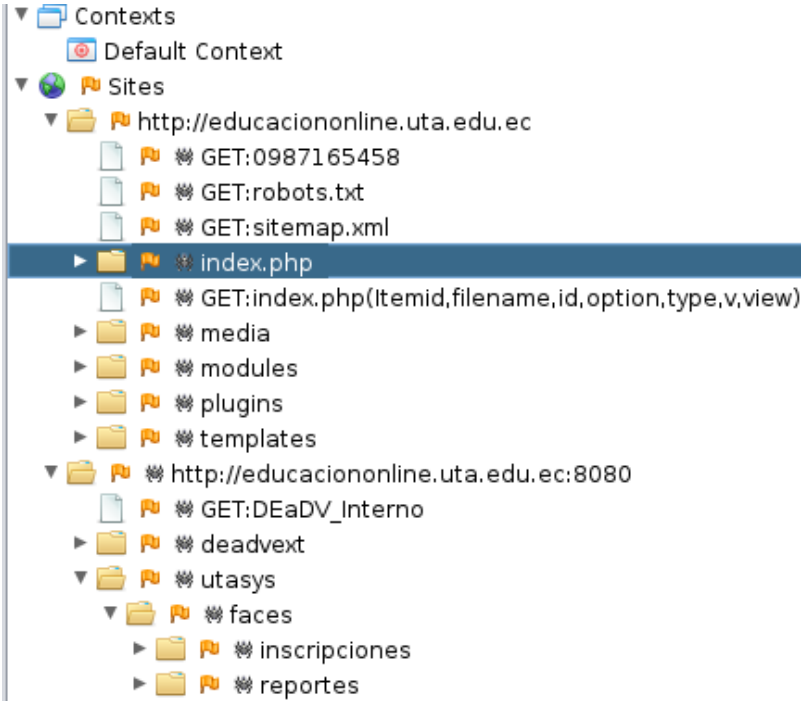


Figura 42. Estructura de la página web de la DEaDV

4.10.2. TEST DE MANEJO DE CONFIGURACIÓN Y DESARROLLO

a) Test de configuración e infraestructura de la red

Dentro de las herramientas administrativas existentes para el manejo de contenidos de un sitio web es necesario establecer las configuraciones adecuadas para cada una ya que, muchas veces, el mínimo error conlleva a un riesgo de seguridad considerable.

Entonces se analizan las herramientas administrativas que utiliza la página web, en éste caso Joomla

Figura 43. Inicio de la página de acceso a la administración

Al conocer las herramientas para manejo de contenidos se procede a realizar un análisis exhaustivo de las vulnerabilidades de la página web.

Gracias al análisis realizado en los puntos anteriores se pudo determinar la herramienta utilizada para el manejo de contenidos, por lo cual es posible utilizar joomscan, el cual analiza vulnerabilidades de la herramienta para manejo de contenidos Joomla.

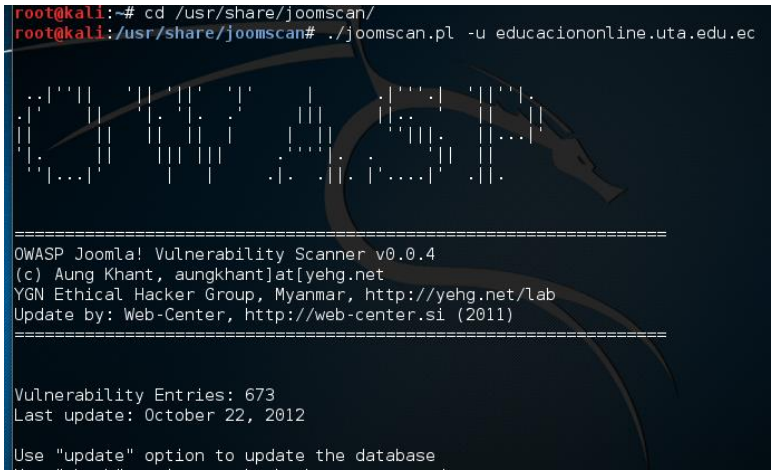


Figura 44. Inicio de la herramienta Joomscan

Entonces la herramienta enumera las posibles vulnerabilidades de su base de datos y si éstas fueron encontradas o no dentro de un dominio en específico.

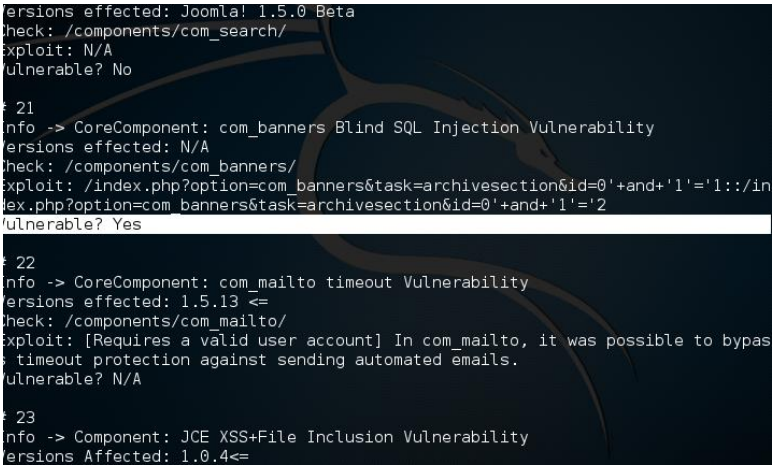


Figura 45. Vulnerabilidad encontrada

Los logs del sistema se tiene conocimiento de que nunca son borrados, son archivados dentro de otro servidor de almacenamiento, el mismo que se encuentra conectado en red con salida a internet.

b) Test de las extensiones de los archivos que manejan información sensible

Las extensiones de los archivos utilizados en los servidores pueden determinar que tecnologías, lenguajes y plugins utilizados para completar peticiones. El uso de extensiones de archivos estándar puede otorgar al analista información útil acerca del funcionamiento interno de un sitio web.

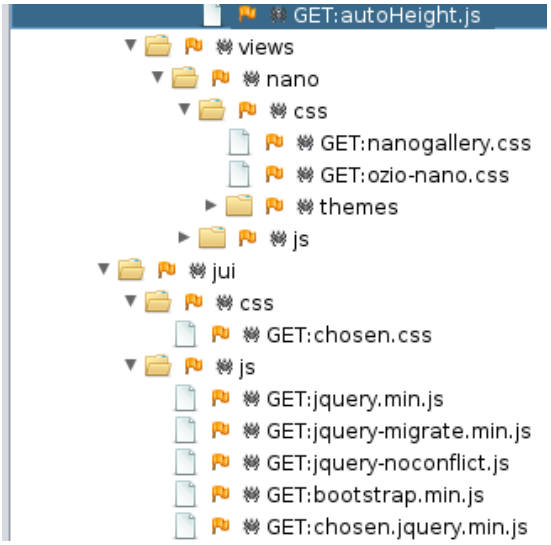


Figura 46. Archivos encontrados en la página web

En éste caso existe una buena configuración de la página web ya que los archivos encontrados son sólo del tipo de lenguaje empleado para las peticiones y para el diseño de la presente.

Si se encontraran archivos con extensión *.asa* o *.inc* tendría un grave problema de seguridad debido a que éste tipo de archivos son utilizados para almacenar información de configuraciones de base de datos así como otro tipo de información sensible.

c) Revisión de archivos viejos, de backup o no referenciados para verificación de información sensible

Muchas veces los archivos ya no utilizados son olvidados dentro de la página web sin tener en cuenta que muchos de ellos pueden contener información sensible o importante para un atacante.

Todos estos archivos dan a los atacantes una pauta para empezar su ataque tales como credenciales, muchas veces claves, configuraciones, entre otros.

Con el análisis realizado en el punto 4.10.1 subsección *A* se demuestra la existencia direcciones dentro del sitio web con información que puede resultar importante.

Figura 47. Archivos obtenidos del sitio web

En uno de éstos archivos se encontró información de configuración lo que representa un riesgo de seguridad de nivel alto.

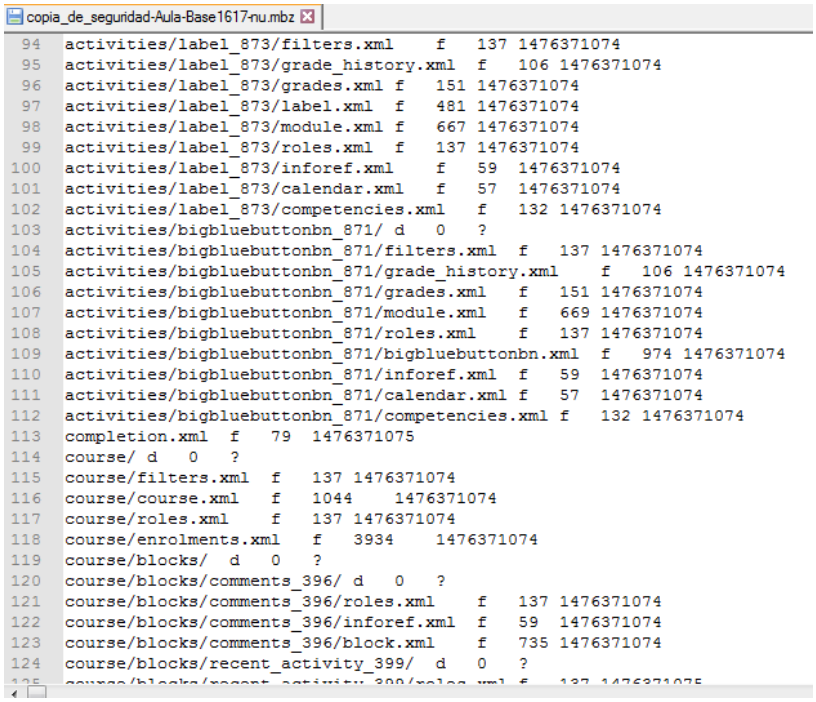


Figura 48. Archivo de configuración hallado

d) Enumeración de las interfaces de administrador

Los administradores tienen la oportunidad de realizar cambios en la página web interna, es necesario conocer cómo trabajan, bajo qué configuraciones y cómo realizan cambios en la misma; para ello se realiza un ingreso a la url http://educaciononline.uta.edu.ec/administrator en donde se despliega un formulario de ingreso.

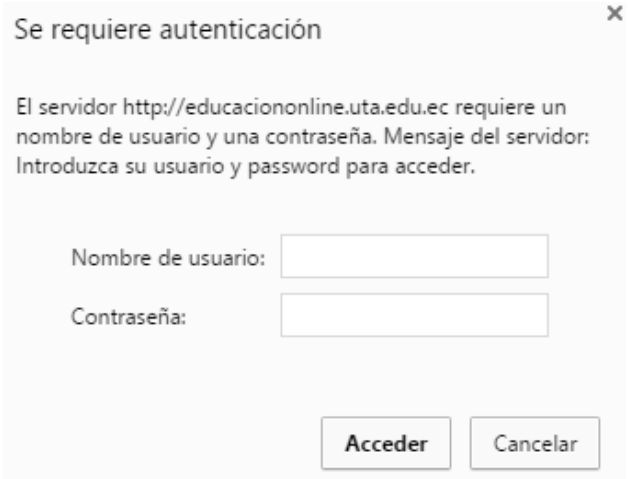


Figura 49. Formulario de acceso a la herramienta de administración de página web

Mediante los permisos institucionales otorgados por la Dirección de Educación a Distancia y Virtual se tuvo un acceso completo a ésta herramienta para realizar un análisis de sombrero gris.

La página web despliega la pantalla principal de manejo de Joomla, donde se obtuvo un permiso especial para análisis de las interfaces de administrador.

Figura 50. Inicio de la página de acceso a la administración

Al ingresar como un usuario con privilegios de administrador se muestra la pantalla principal.

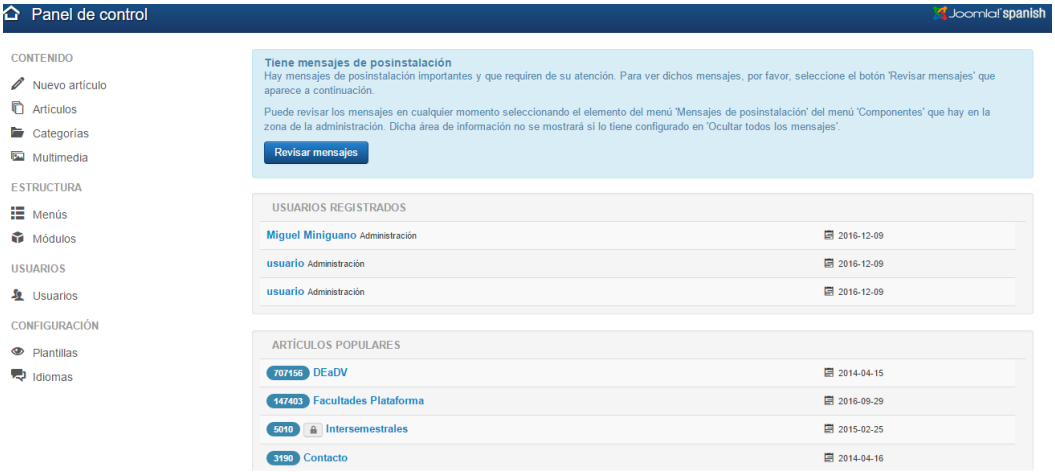


Figura 51. Panel de control del sitio web de la DEaDV

En ésta página se encuentra también información de las herramientas utilizadas

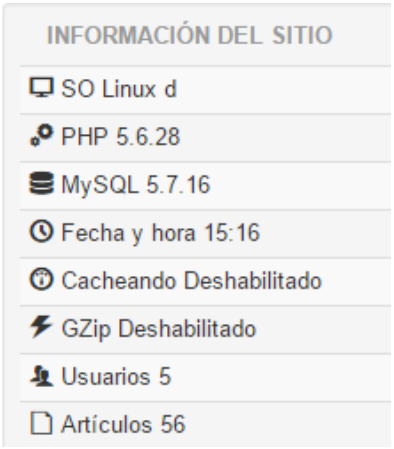


Figura 52. Información de las herramientas del sitio web

Y la manera de editar las diferentes páginas del sitio web

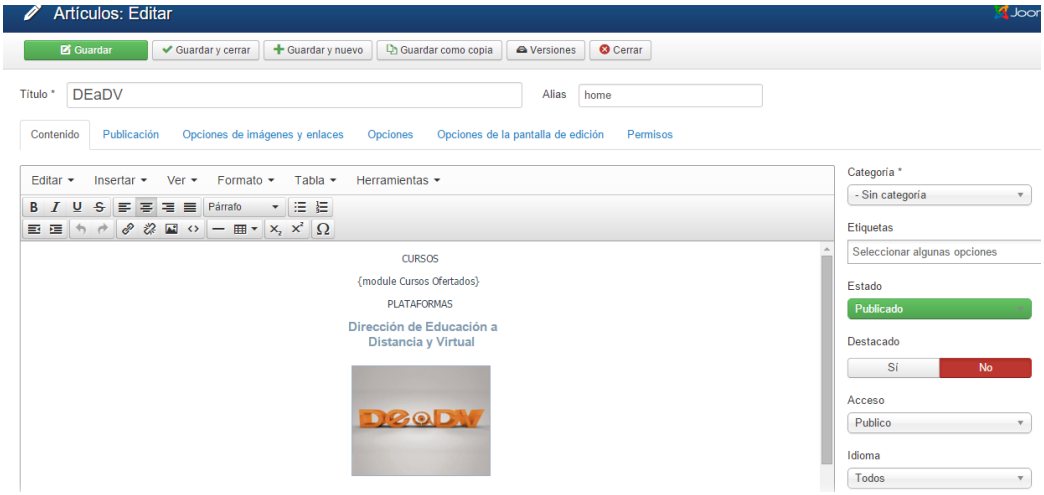


Figura 53. Página de edición del sitio web (1)

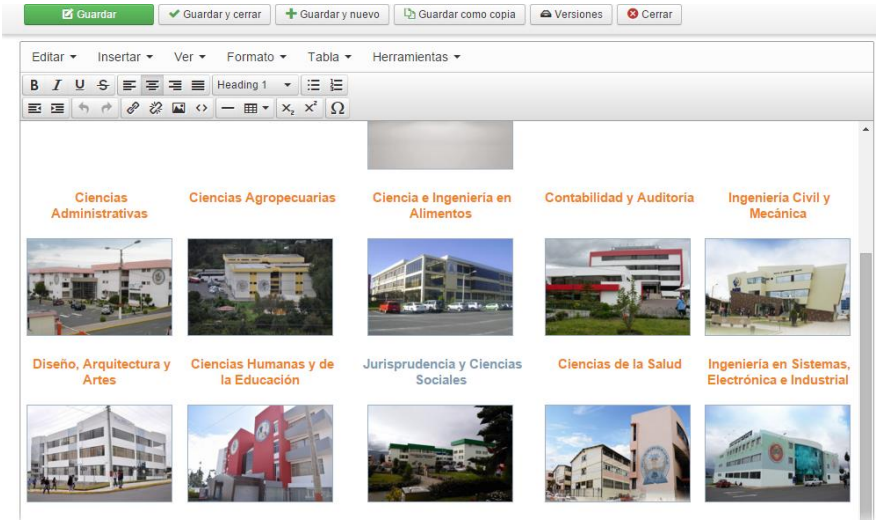


Figura 54. Página de edición del sitio web (2)

De igual manera existe la página de administración de las aulas virtuales, debido a políticas institucionales no se pudo tener acceso a la misma, pero se presenta la pantalla de ingreso a la misma.

Figura 55. Página de ingreso para administración de aulas virtuales

e) Test de métodos HTTP

Los métodos HTTP son aquellos en donde, mediante el análisis y la obtención de las cabeceras de un sitio web, se puede editarlos y encontrar mayor información de los mismos o, gracias a ellos, traspasar inicios de sesión.

Dentro de la página web de la DEaDV se puede obtener información de las cabeceras gracias a la herramienta OWASP ZAP al realizar un análisis tipo GET a la página web se pudo obtener la siguiente información:

```
GET http://educaciononline.uta.edu.ec/index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: http://educaciononline.uta.edu.ec/index.php/component/content/article
Host: educaciononline.uta.edu.ec
```

Figura 56. Consulta realizada a la página web principal de la DEaDV

```
HTTP/1.1 200 OK
Date: Mon, 09 Jan 2017 17:00:29 GMT
Server: Apache
X-Powered-By: PHP/5.6.28
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Access-Control-Allow-Origin: http://educaciononline.uta.edu.ec:8080
Set-Cookie: 88b13f49ddef3cf983705838cea21858=9rj91s8u1icocnqoe7svdsqu57; path=/; HttpOnly
Set-Cookie: cip_vvisitcounter=MTg2LjQ2LjIyNC43MQ%3D%3D; expires=Mon, 09-Jan-2017 17:15:30 GMT; Max-Age=900
Expires: Mon, 1 Jan 2001 00:00:00 GMT
Last-Modified: Mon, 09 Jan 2017 17:00:31 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
```

Figura 57. Respuesta a consulta tipo GET de la página principal del sitio de la DEaDV

De la misma manera al realizar una petición tipo POST

```
POST http://educaciononline.uta.edu.ec/index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Referer: http://educaciononline.uta.edu.ec/index.php
Host: educaciononline.uta.edu.ec
```

Figura 58. Consulta tipo POST realizada a la página web principal de la DEaDV

```
HTTP/1.1 200 OK
Date: Mon, 09 Jan 2017 17:01:04 GMT
Server: Apache
X-Powered-By: PHP/5.6.28
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Access-Control-Allow-Origin: http://educaciononline.uta.edu.ec:8080
Set-Cookie: 88b13f49ddef3cf983705838cea21858=e2tqjcjtdkbnduefirst0hpg67; path=/; HttpOnly
Set-Cookie: cip_vvisitcounter=MTg2LjQ2LjIyNC43MQ%3D%3D; expires=Mon, 09-Jan-2017 17:16:05 GMT; Max-Age=900
Expires: Mon, 1 Jan 2001 00:00:00 GMT
Last-Modified: Mon, 09 Jan 2017 17:01:05 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
```

Figura 59. Respuesta a la consulta POST por parte de la página web de la DEaDV

Otro tipo de pruebas HTTP resultan imposibles en el presente proyecto de investigación dado que el servicio telnet y netcraft son manejados por el firewall perteneciente a la Dirección de Tecnología de la Información y Comunicación, departamento que es diferente al cual se realizan las pruebas de vulnerabilidades por lo que los permisos obtenidos fueron de análisis para la presente sección.

f) Test de transporte de seguridad estricto HTTP

El transporte de seguridad estricto o HSTS es la forma mediante la cual se comunica la página web con el navegador de una manera cifrada [32].

Mediante un simple análisis a la página web se pudo determinar que la misma no posee HSTS.

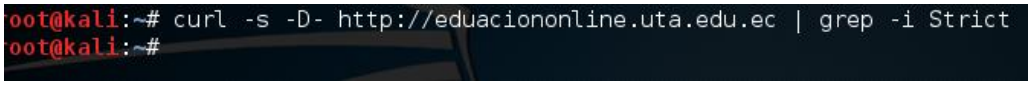


Figura 60. Análisis de existencia de HSTS

Mientras que el resultado esperado de la página web es

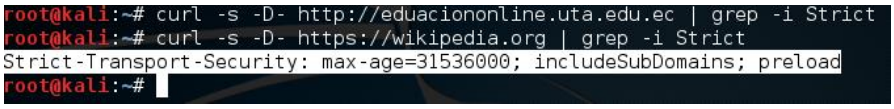


Figura 61. Resultado esperado HSTS

De ésta manera se garantiza que la información proporcionada desde el navegador a la página web es cifrada.

La línea de *max-age = 31536000* sirve para realizar un control de caché, en donde el número es la cantidad de milisegundos que una petición se considera fresca, caso contrario expira y tiene que volver a cargarse.

4.10.3. TEST DE MANEJO DE IDENTIDAD

a) Test de definición de roles

Dentro de toda entidad se definen los roles del sistema con el objetivo de determinar las autorizaciones que tienen los administradores y usuarios que manejan el sitio web interno. Los roles son los que permiten el acceso a información sensible del sitio web, con la posibilidad de realizar cambios que afecten a la página principal manejada por Joomla.

Es por lo cual se necesita un análisis al flujograma de autorizaciones correspondiente a una entidad, para así poder definir las acciones que se pueden o no realizar dentro de un sistema web.

Dentro del sistema de administración Joomla se enlistan los usuarios y roles existentes, el usuario con el que se obtuvo el ingreso tiene permisos de administrador.

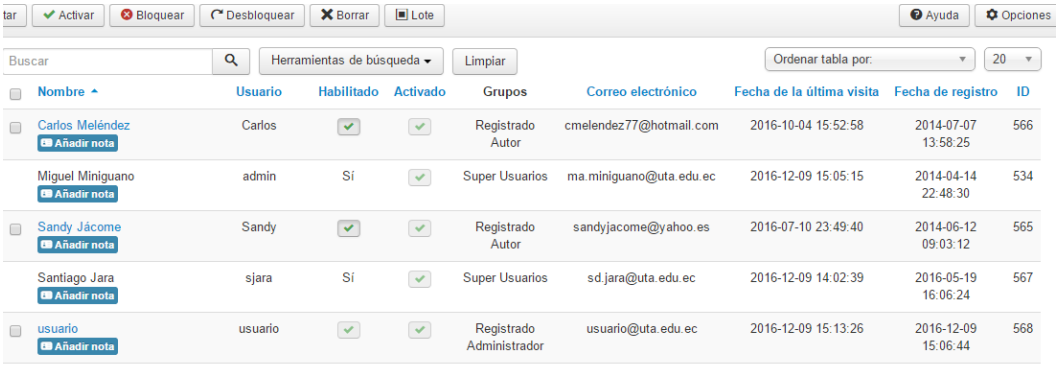


Figura 62. Listado de usuarios y roles de administración de la página de la DEaDV

Así mismo cada rol está definido con las acciones que puede realizar.

Figura 63. Niveles de acceso y roles de la DEaDV

Figura 64. Grupos de usuarios

Una de las principales seguridades que tiene la administración del sistema de la DEaDV es mediante el cual sólo el usuario que crea una entrada o página, es el único que puede eliminarla, si es administrador, ya que el super usuario tiene acceso total.

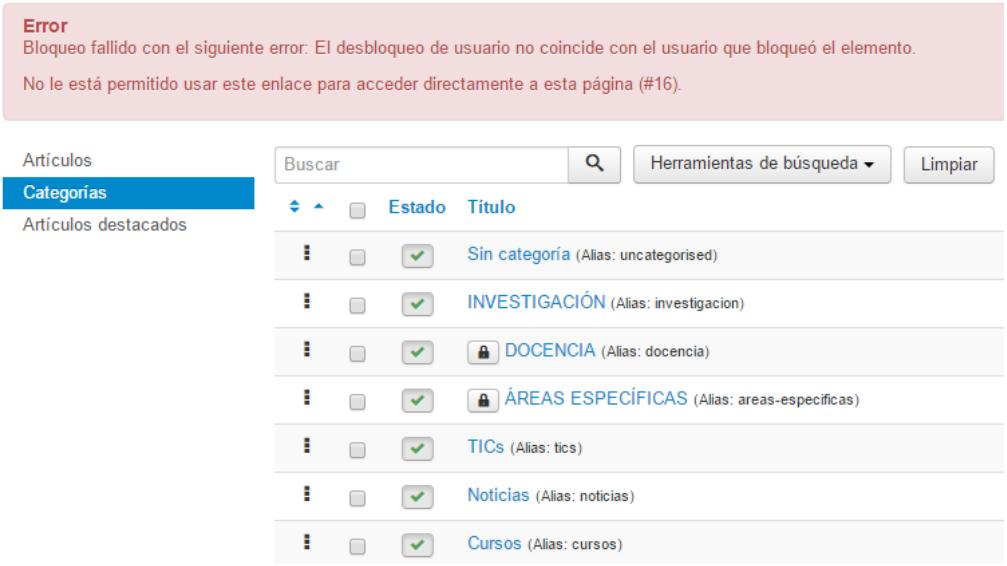


Figura 65. Intento de eliminación de publicación

b) Test de proceso de registro de nuevos usuarios

Para el registro de nuevos usuarios es necesario tener privilegios de administrador, ya que solo usuarios con éste rol puede crear a nuevos usuarios.

Joomla ofrece un registro de usuarios con una interfaz gráfica muy simple con la cual guía paso a paso la definición de un nuevo usuario.

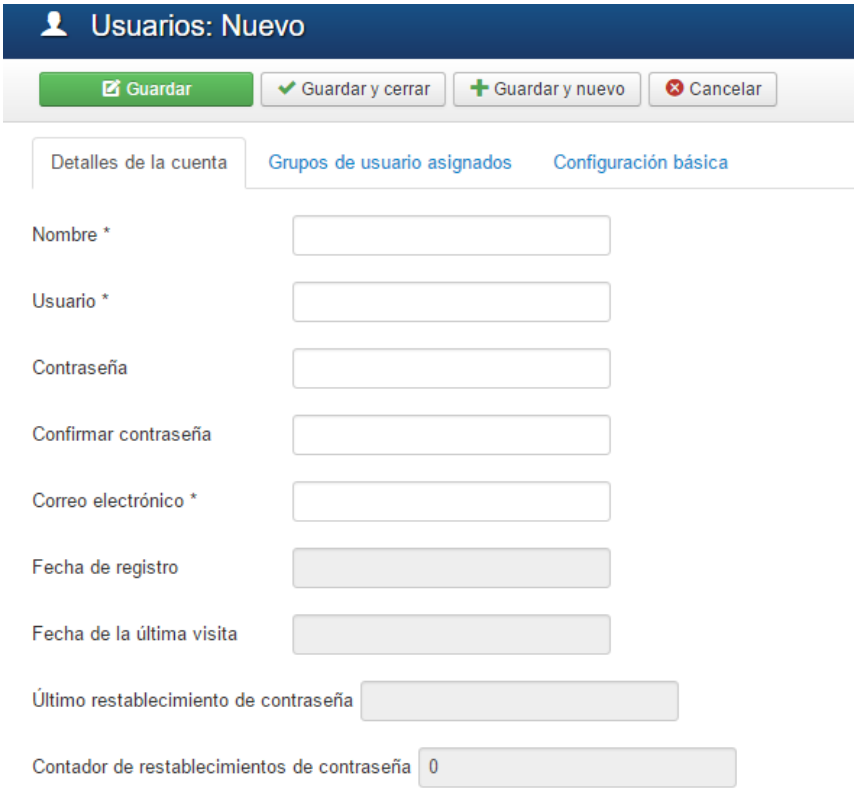


Figura 66. Pantalla de registro de nuevo usuario (1)

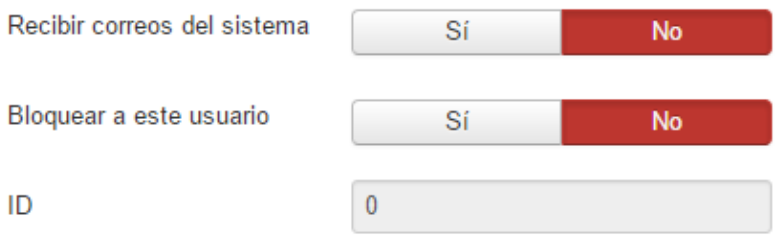


Figura 67. Pantalla de registro de nuevo usuario (2)

c) Test de procesos de creación de nuevas cuentas

Al crear una nueva cuenta también se le debe otorgar el rol y los permisos necesarios para que pueda funcionar con normalidad, en el punto anterior se observó cómo se crea una nueva cuenta, es entonces cuando existen las configuraciones de usuarios.

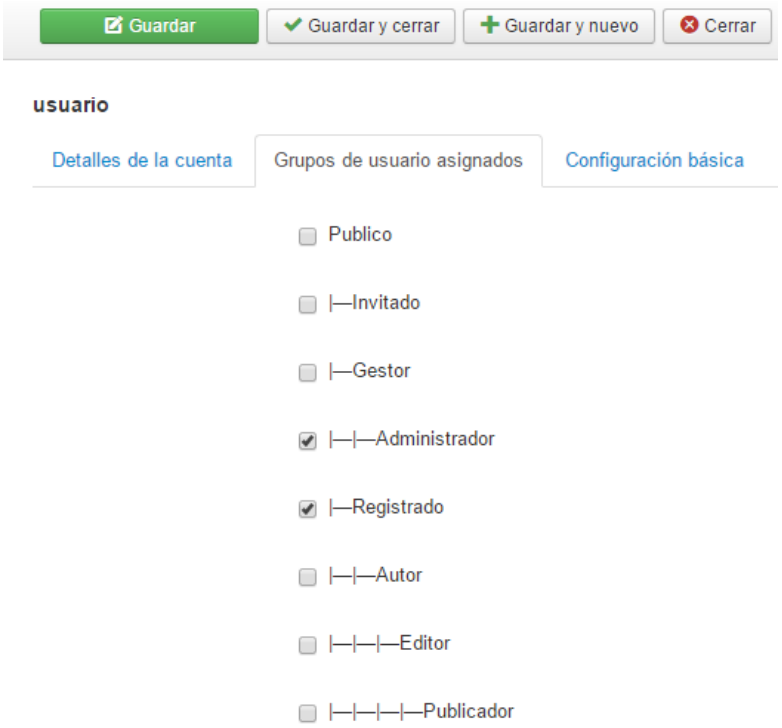


Figura 68. Configuración de grupos de usuario

Al configurar al usuario en el grupo adecuado se le asignan los roles y acciones que puede realizar el mismo, cada rol posee acciones distintas para o cual es necesario el conocimiento de las mismas al momento de asignación del grupo.

De la misma manera en las configuraciones básicas se encuentran aquellas que se van a mostrar al usuario para el manejo de la aplicación, tales como tipo de estilo y métodos de utilización de pantallas.

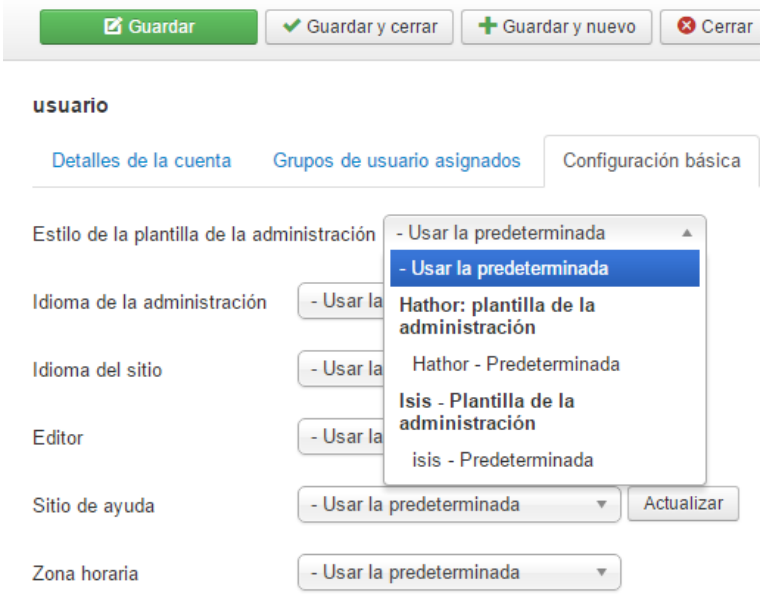


Figura 69. Configuración básica de usuario, plantillas

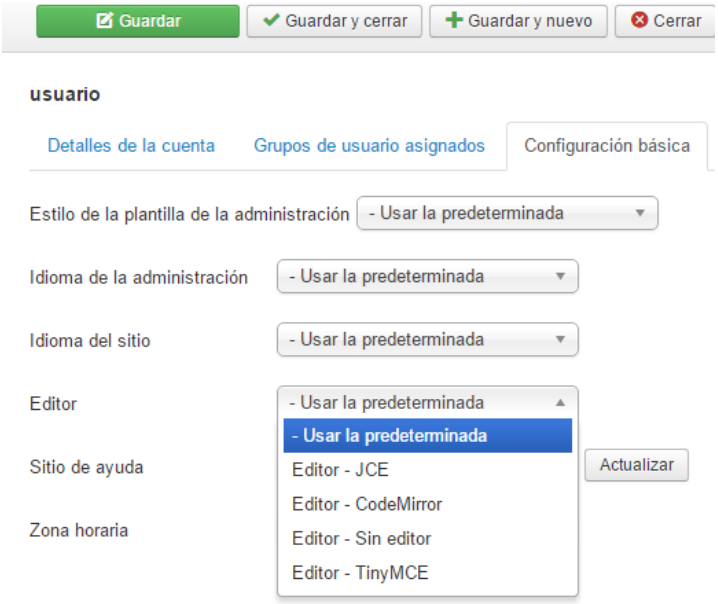


Figura 70. Configuración básica de usuario, estilos.

d) Test de enumeración de cuentas y cuentas de usuario con nombres por defecto

En la creación de cuentas se debe tener en cuenta los nombres de usuario, y tratar de evitar a toda costa que sean fáciles de adivinar o acceder; nombres como: usuario, administrador, admin, entre otros son muy comúnes y por defecto, dichos nombres de usuario no son recomendables.

Al realizar un análisis a los usuarios se obtuvo la siguiente imagen:

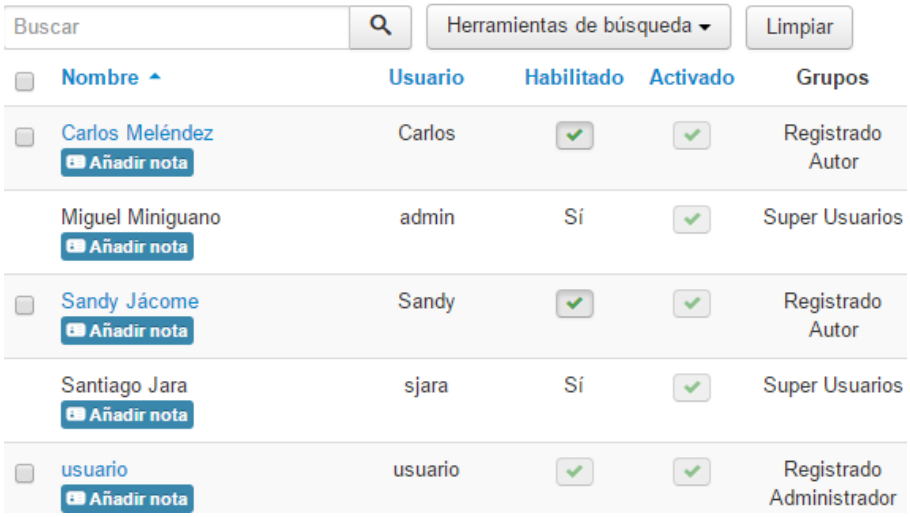


Figura 71. Listado de usuarios que manejan el sistema interno de la página de la DEaDV

Por lo cual existen procesos que deben ser revisados y modificados para evitar riesgos de seguridad.

e) Test para políticas de uso de nombres de usuarios débiles o sin seguridades

Para evitar el uso de los nombres de usuario incorrectos, muchas entidades tienen políticas para creación de nombres de usuarios distintos a los usados por defecto, teniendo en cuenta su complejidad, más aún si es para el manejo de un sistema y una página web.

Los usuarios creados en el sitio de administración de la página web, tienen riesgo de ser vulnerados dado a que son usados por defecto, por lo que la política de nombres de usuario débiles tiene que ser mejorada.

Debido a políticas institucionales las cuales no permiten que estudiantes manipulen al servidor principal de las aulas virtuales, debido a la posibilidad de alterar el funcionamiento del mismo, con el riesgo de pérdida de datos, se procedió a realizar un análisis de fallos humanos al aula virtual correspondiente a la Facultad de Ingeniería en Sistemas Electrónica e Industrial, por lo cual el presente test fue factible.

Entonces se determinó que la creación de nuevos usuarios mediante la plataforma virtual y su acceso está limitada por su número de cédula.

Figura 72. Ingreso al aula virtual

Al utilizar el número de cédula como nombre de usuario puede repercutir en un riesgo de seguridad dentro de la aplicación web, mas el correcto uso de claves puede ser una forma de mitigación bastante útil en el presente caso.

4.10.4. TEST DE AUTENTICACIÓN

La autenticación dentro de un entorno web representa la parte vital del mismo, es necesario tener en cuenta todas las credenciales existentes y qué métodos se utilizan para la comprobación de las mismas.

Mediante la colaboración con la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato y los recursos otorgados por las autoridades pertinentes, se procede a analizar el presente proceso dentro del entorno del Aula Virtual de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, por lo cual se analizaron errores humanos y de credenciales, existentes en ésta aplicación web.

a) Test de credenciales transportadas en un canal encriptado

La encriptación de datos es necesaria debido a que un atacante puede realizar un análisis completo de la red e intervenir peticiones que son realizadas hacia una aplicación web, si las mismas no se encuentran cifradas, el atacante tiene un fácil acceso a información sensible, en el caso del presente proyecto de investigación, se pueden obtener usuarios y contraseñas del aula virtual, un riesgo muy grave en un entorno educativo.

Para la comprobación correspondiente se realizará una petición tipo POST a la página web.

```
POST http://sistemaseducaciononline.uta.edu.ec/login/index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Referer: http://sistemaseducaciononline.uta.edu.ec/login/index.php
Host: sistemaseducaciononline.uta.edu.ec
```

Figura 73. Petición post realizada al aula virtual

Como se puede observar, la respuesta viene de un servicio HTTP y no un HTTPS lo que comprueba que la información enviada no se envía sobre un canal encriptado.

b) Test de credenciales por defecto

Al momento de crear nuevos usuarios, muchas veces son creados con nombres de usuario y contraseñas generadas por defecto, en el caso del aula virtual en primera instancia se crean usuarios con el acceso de usuario = número de cédula y su contraseña = número de cédula, un error bastante grave y el que tiene el mayor riesgo dentro del presente proyecto de investigación, en éste punto se vulnerará a profundidad el error de mantener las credenciales por defecto.

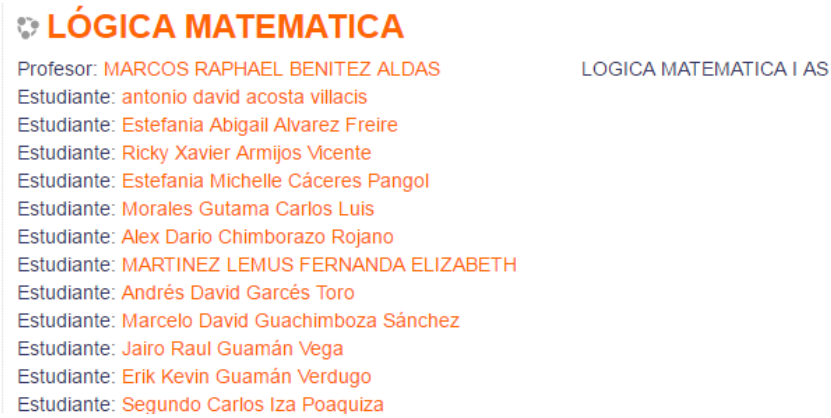
Después del primer ingreso al aula virtual como nuevo usuario, el mismo, es solicitado para realizar un cambio de clave por una más segura, éste paso es omitido por la gran mayoría de las personas, tanto estudiantes como profesores, como se pudo observar en la pregunta número 9 de la encuesta realizada las contraseñas utilizadas en su mayoría son débiles, y casi nunca son cambiadas por los mismos usuarios.

Para determinar los nombres de usuario, en éste caso los números de cédula se procedió a realizar dos tipos de análisis, el primero es mediante el análisis de archivos con información sensible encontrados en la página web, en donde existía un listado de profesores y su número de cédula.

8	18	[redacted]
9	18	[redacted]
10	17	[redacted]
11	17	[redacted]
12	17	[redacted]
13	05	[redacted]
14	18	[redacted]
15	06	[redacted]
16	180	[redacted]
17	05	[redacted]
18	18	[redacted]
19	18	[redacted]
20	09	[redacted]
21	18	[redacted]
22	05	[redacted]
23	17	[redacted]
24	180	[redacted]

Figura 74. Listado de profesores con sus números de cédula

De la misma manera un riesgo que tiene de forma visual el aula virtual es el mostrar el listado, con nombres completos, de los estudiantes y profesores que cursan una materia en específico.



LÓGICA MATEMATICA

Profesor: MARCOS RAPHAEL BENITEZ ALDAS — LOGICA MATEMATICA I AS
Estudiante: antonio david acosta villacis
Estudiante: Estefania Abigail Alvarez Freire
Estudiante: Ricky Xavier Armijos Vicente
Estudiante: Estefania Michelle Cáceres Pangol
Estudiante: Morales Gutama Carlos Luis
Estudiante: Alex Dario Chimborazo Rojano
Estudiante: MARTINEZ LEMUS FERNANDA ELIZABETH
Estudiante: Andrés David Garcés Toro
Estudiante: Marcelo David Guachimboza Sánchez
Estudiante: Jairo Raul Guamán Vega
Estudiante: Erik Kevin Guamán Verdugo
Estudiante: Segundo Carlos Iza Poaquiza

Figura 75. Estudiantes y profesores universitarios.

Si bien la información tal como números de cédula, nombres y apellidos, es pública, el hecho de mostrar nombres completos dentro de una materia específica facilita el trabajo de algún atacante, enfocándolo directamente hacia su objetivo.

Al obtener el listado con números de cédula de los profesores pertenecientes a la Facultad de Ingeniería en Sistemas, Electrónica e Industrial se procedió a la

realización del ataque en cuestión, probando como nombre de usuario y contraseña al número de cédula, obteniendo resultados con un riesgo alto.

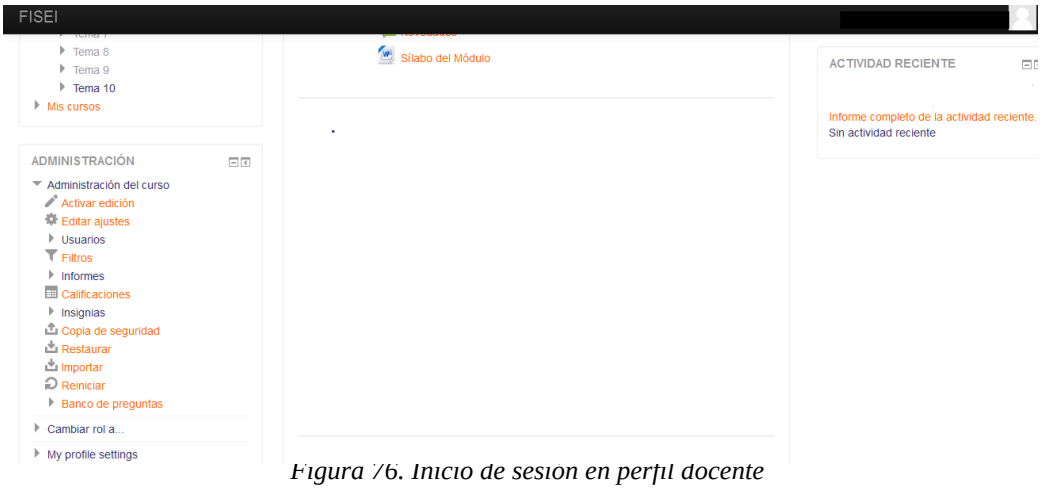


Figura 76. Inicio de sesión en perfil docente

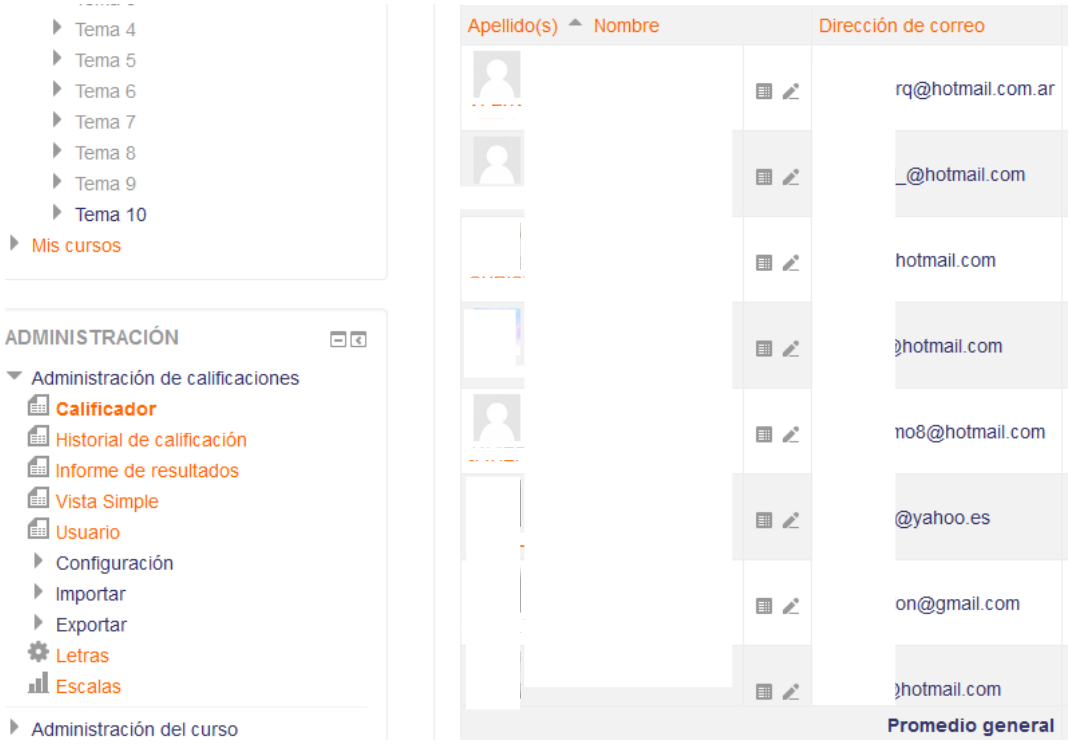


Figura 77. Pantalla de administración de calificaciones

Figura 78. Ingreso a banco de preguntas de examen (1)

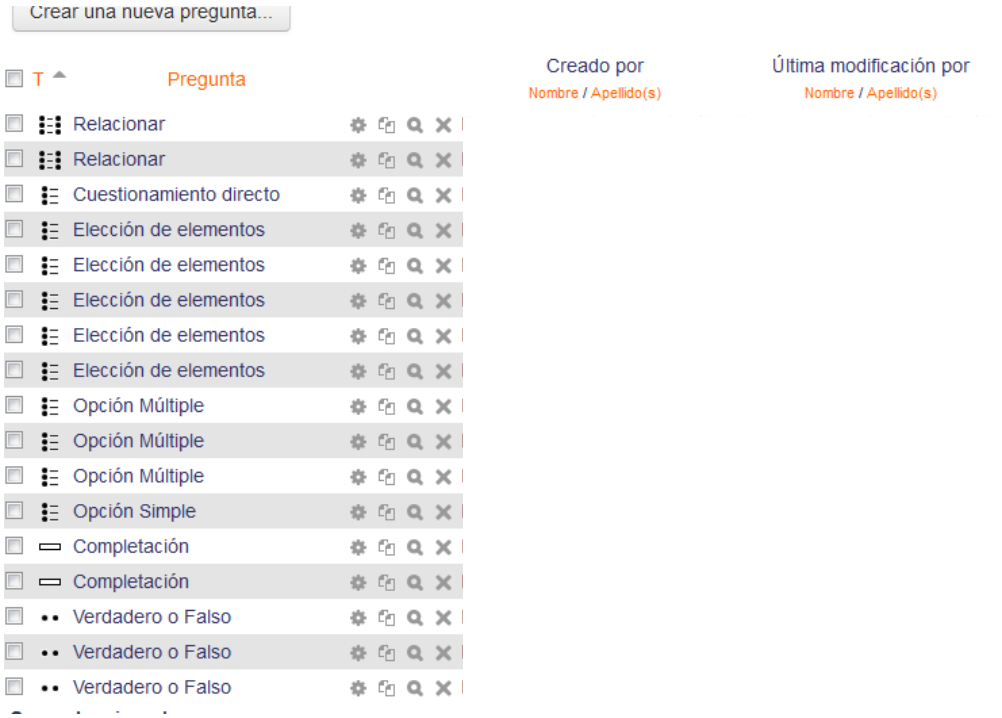


Figura 79. Ingreso a banco de preguntas de examen (2)

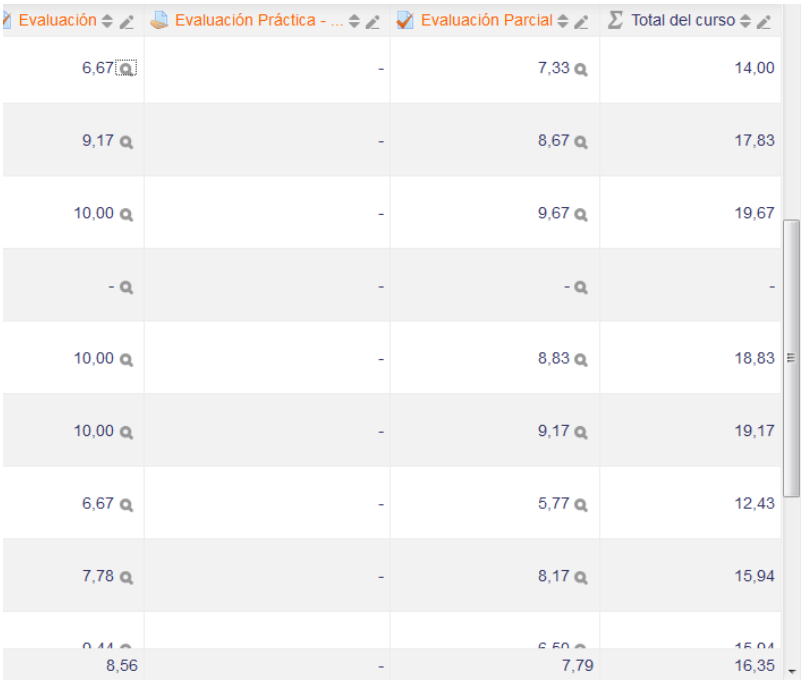


Figura 80. Ingreso a panel de modificación de notas

El análisis presentado es el más grave existente dentro de la aplicación, y son vulnerables tanto alumnos como profesores dado su propio manejo de sus cuentas y el mantener la misma contraseña creada por defecto.

c) Test de debilidades de mecanismos de cierre

El mecanismo de cierre se refiere al manejo de la aplicación para ataques de fuerza bruta, mediante el mecanismo de cierre la cuenta que está siendo vulnerada se bloquea automáticamente después de un número determinado de intento de ingreso utilizando credenciales incorrectas.

La metodología OWASP propone una serie de pasos a seguir para la verificación del correcto mecanismo de cierre [32]:

- Intentar ingresar al sistema con datos incorrectos 3 ocasiones
- Ingresar normalmente al sistema, demuestra que no se ha disparado un mecanismo de cierre
- Intentar ingresar al sistema con datos incorrectos 4 ocasiones
- Ingresar normalmente al sistema, demuestra que no se ha disparado un mecanismo de cierre
- Intentar ingresar al sistema con datos incorrectos 5 ocasiones
- Si se dispara un mecanismo de cierre se habrá bloqueado la cuenta
- Intentar ingresar correctamente después de 5 minutos, si se logra el mecanismo de cierre se desactiva a los 5 minutos de bloqueo
- Intentar ingresar correctamente después de 10 minutos, si se logra el mecanismo de cierre se desactiva a los 10 minutos de bloqueo

- Intentar ingresar correctamente después de 15 minutos, si se logra el mecanismo de cierre se desactiva a los 15 minutos de bloqueo

En el aula virtual se intentó realizar los pasos anteriormente presentados mas después de 20 intentos fallidos la cuenta no se bloqueó.

Figura 81. Intento Nº 20 de ingreso con datos erróneos

Inmediatamente se intentó entrar con los datos correctos comprobando que no existió un bloqueo de la cuenta; por lo tanto, la página es vulnerable a ataques de fuerza bruta.

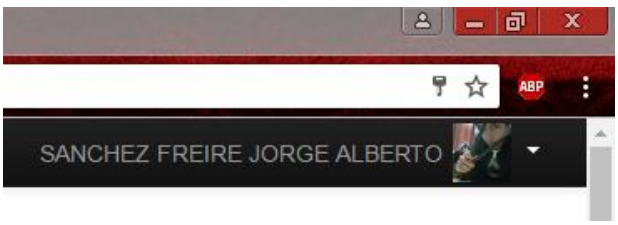


Figura 82. Ingreso exitoso al aula virtual

d) Test para sobrepasar el esquema de autenticación

Existen varias maneras de sobrepasar los esquemas de autenticación, tales como inyecciones SQL, ataques de fuerza bruta o análisis de archivos hash.

En el caso de la página web de la DEaDV el esquema de autenticación es de dos niveles, uno javascript y otro de inicio de sesión del sistema de manejo de contenidos, como se puede apreciar en el punto *4.10.2 subsección b.*

Por lo cual el proceso se considera correcto y el análisis realizado no fue exitoso debido al grado de seguridad de la página web.

e) Test de funcionalidad de recordar contraseñas

Cuando una página web tiene cookies activadas, muchas veces se guardan las contraseñas y el estado de la sesión para facilitar el ingreso de una persona, el análisis de las mismas es necesario para determinar si están cifradas para que un atacante no pueda obtener dichas contraseñas de forma fácil mediante el robo de las cookies del navegador.

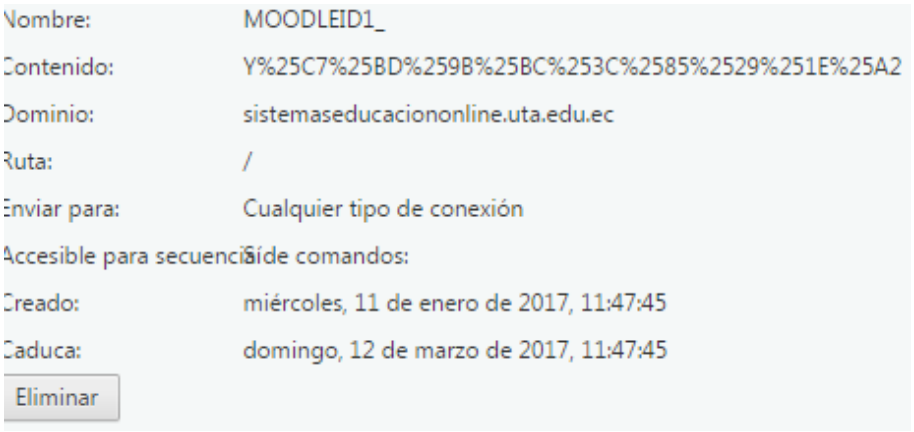


Figura 83. Análisis de cookie de navegación del aula virtual

Como se puede apreciar en la imagen anterior, el contenido se encuentra cifrado por lo cual representa una gran seguridad dentro de un entorno web.

f) Test de vulnerabilidades en la caché del navegador

Muchas veces, información delicada puede guardarse en la caché del navegador, hay que determinar que el historial de un navegador no es igual que la memoria caché del mismo, se distinguen en que la memoria caché es temporal, donde se bajan archivos de un determinado sitio web hacia archivos temporales para tener un acceso a ellos mucho más rápido, varios de éstos archivos pueden ser tokens de sesión los cuales pueden mantener una sesión activa, permitiendo a un atacante suplantar la identidad de una víctima.

Mediante un test bastante simple se puede analizar la existencia de memoria caché vulnerable dentro de una página web, al cerrar la sesión, en este caso del aula virtual, se retorna a la página anterior en el navegador.

Figura 84. Cerrar sesión en aula virtual

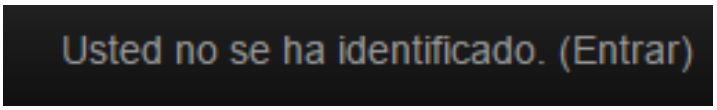


Figura 85. Salida exitosa

Es entonces cuando se regresa a la página anterior del navegador, para comprobar si existe alguna vulnerabilidad en el caché.

Figura 86. Demostración de vulnerabilidad de caché

Cabe recalcar que al momento de realizar una actualización de los datos la aplicación vuelve a pedir las credenciales de ingreso del usuario.

g) Test de políticas de contraseñas débiles

Para el manejo de las contraseñas, las empresas poseen reglas o métodos por los cuales evitar la existencia de contraseñas débiles o fáciles de adivinar.

Dentro del aula virtual de la Universidad Técnica de Ambato, también existen éstas políticas, al momento de creación de usuarios, se les provee de una clave temporal la cual debe ser cambiada por el usuario en su primer ingreso a la plataforma; en éste caso Moodle otorga parámetros que deben ser cumplidos para un cambio exitoso de contraseña, en el caso de la DEaDV, estableció que para el primer cambio de contraseña se debe otorgar una que contenga mayúsculas, minúsculas, al menos un digito numérico, al menos un digito no alfanumérico y de una longitud mínima de 8 caracteres.

h) Test de preguntas de seguridad débiles

Para poder recuperar una cuenta o entrar a alguna, existen preguntas de seguridad, en gran mayoría, generadas por la misma aplicación.

Si bien muchas veces se utiliza de una manera correcta ya que es información que, se supone, que sólo el usuario conoce, como por ejemplo la edad de su madre, el nombre de su mejor amigo de la infancia, entre otros, existen vulnerabilidades en las mismas cuando son muy simples de adivinar por un atacante. Es más, existen

muchas aplicaciones que permiten generar al usuario sus propias preguntas de seguridad, lo cual es un arma de doble filo a nivel de seguridad informáticas.

En el presente proyecto se investigó acerca de preguntas de seguridad utilizadas, tanto en el sitio web de administración de la DEaDV, como en el aula virtual, para así poder acceder o resetear las contraseñas, pero las preguntas de seguridad en ambas partes están desactivadas.

La no presencia de preguntas de seguridad no representa una vulnerabilidad latente, lo que sería tomado como riesgo sería la presencia de preguntas de seguridad débiles dentro de la misma.

i) Test de funcionalidades de reseteo de contraseñas

La reacción del sistema ante un cambio de contraseña es necesario para determinar los distintos cambios que ha tenido dicho sistema.

La metodología OWASP propone una serie de pasos a seguir para determinar la seguridad existente en el reseteo y cambio de contraseñas.

Reseteo de contraseña

¿Qué información es necesaria para resetear una contraseña?

Dentro del sistema de manejo de la DEaDV se pide dar una dirección de correo electrónico a donde será enviada la información del reseteo de contraseña

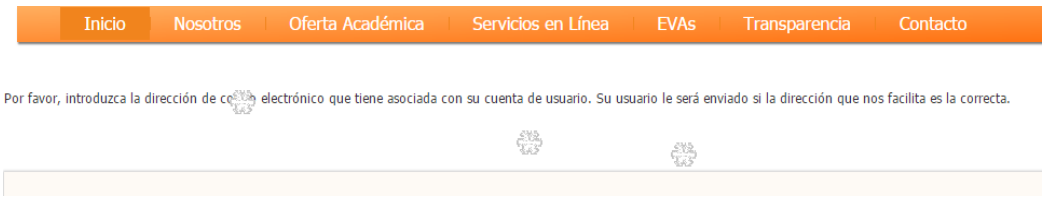


Figura 87. Solicitud de correo electrónico por parte de la página de la DEaDV

Mientras que, en el aula virtual, se pide el nombre de usuario relacionado al aula virtual o su correo electrónico para su reactivación

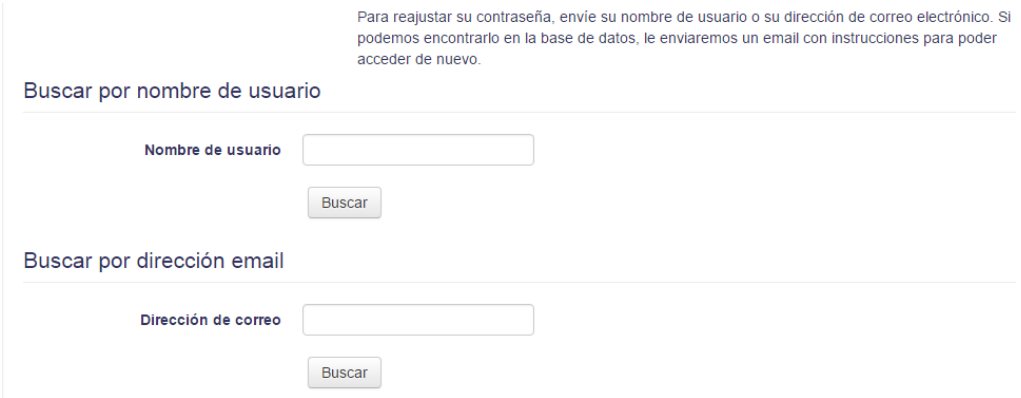


Figura 88. Solicitud de información de la aplicación del aula virtual

¿Cómo se comunica al usuario el restablecimiento de la contraseña?

Con un mensaje al correo electrónico asociado con las cuentas del usuario.

Test de cambio de contraseña

Para el cambio de contraseña se solicita la contraseña anterior para poder modificarla.

Figura 89. Cambio de contraseña

Entonces, en el presente caso, se deseaba realizar un cambio de contraseña cumpliendo con el único parámetro presentado que se refiere a que la nueva contraseña debe ser mayor a 8 caracteres.

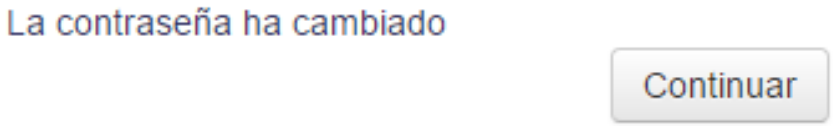


Figura 90. Cambio exitoso a contraseña débil

Por lo cual debe existir una política por parte tanto del sistema como de los usuarios del mismo para el correcto manejo de contraseñas, debido a la gravedad de la vulnerabilidad presentada en el presente proyecto de investigación.

j) Test de autenticación en un canal alternativo

Muchas páginas web utilizan canales alternativos para proveer los mismos servicios, tales como:

- Página web para dispositivos móviles
- Accesibilidad a páginas web optimizadas
- Páginas web para distintos lenguajes
- Sitios web paralelos que utilizan las mismas sesiones
- Versiones beta de las mismas páginas web

Es por ello que se necesita una verificación de los distintos puntos de acceso a un mismo recurso, dentro de la página de la DEaDV y el análisis realizado a la aplicación del aula virtual no se encontró otro tipo de acceso, haciendo pruebas desde varios dispositivos por lo cual el presente test no se realizó ya que no representa una vulnerabilidad la inexistencia de éstos canales de acceso.

4.10.5. TEST DE AUTORIZACIÓN

En los test de autorización se definen nuevamente los roles existentes y cada una de las funciones que tienen los mismos dentro de un área específica, el presente test está enfocado a la página de administración de Joomla de la DEaDV.

a) Test para sobrepasar el esquema de autorización

El presente test se basa en las acciones que pueden realizar los usuarios dentro del sistema, cada usuario y su nivel de autorización están definidos en el proceso 4.10.3 subproceso a, en donde los roles son definidos con las acciones que los mismos pueden realizar.

Para llegar al esquema de autorización se debe primero sobrepasar la seguridad javascript existente, después de ella el inicio de sesión Joomla, por lo cual se considera que el esquema de autorización del sitio web de administración de la página de la DEaDV se encuentra configurado de manera adecuada, por lo que no existen vulnerabilidades de seguridad encontradas dentro del presente test.

De la misma manera al analizar si existe manera de regresar a un estado anterior después de haber finalizado una sesión se dispara un error de cache.

Figura 91. Respuesta de la página al querer reingresar después de finalizada la sesión

b) Test de escala de privilegios

En cada etapa en donde el usuario pueda crear información que se almacene en una base de datos es muy necesario el registro de cambios existentes dentro del sitio web y en los logs del sistema debe constar qué usuario realizó los cambios, desde qué máquina y cuáles fueron dichos cambios, y si existió un cambio del sistema accesible por el usuario el cual no poseía el rol acorde al mismo.

Dentro de la escala de privilegios de un sistema web es necesario el análisis de los cambios realizados y del usuario en cuestión para la determinación de los procesos a tomar si el mismo tuvo acceso a roles o acciones no permitidas para su tipo.

Dentro del manejo de la DEaDV no existe dificultad encontrada acerca de la escala de privilegios, vista desde una perspectiva no invasiva, en donde las pruebas fueron realizadas como usuario administrador, siendo fallido el intento de escalar privilegios hacia superusuario sin alterar el funcionamiento del servidor.

c) Test de referencias inseguras de objetos directos

Para la comprobación de ésta vulnerabilidad se utilizará el mapeo realizado en la recolección de datos encontrando referencias a objetos directos. Por ejemplo, la localización de entradas que usen como parámetro un nombre de tabla, nombre de una fila, lo que puede representar un error muy común de seguridad.

Se realizó un análisis a fondo de la página web de la DEaDV en búsqueda de objetos directos.

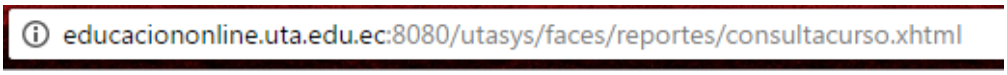


Figura 92. Búsqueda de Objetos Directos en la página de la DEaDV

En la misma imagen se puede observar que no existe una referencia a un objeto directamente, sino utilizando *friendly urls* que no es más que un enmascaramiento del objeto directo para que no pueda ser visto.

De la misma manera se realizó el mismo análisis a la aplicación de la DEaDV que es el aula virtual teniendo como resultado:

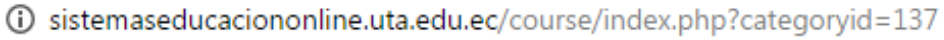


Figura 93. Búsqueda de Objetos Directos en el aula virtual

En donde se obtuvo el nombre de una fila de una base de datos y el objeto directo puede ser cambiado para tener acceso hacia otros recursos de la misma.

4.10.6. TEST DE MANEJO DE SESIONES

a) Test para sobrepasar el esquema de manejo de sesiones y atributos de cookies

Dentro de una página web, las sesiones muchas veces son guardas en las cookies presentes en el navegador, con una correcta configuración de las mismas, cuando existen, son cifradas o, en varios casos, se encuentran bloqueadas.

En el área de trabajo de la administración de la página web de la DEaDV, primero se realiza un análisis del tipo de cookies que se están utilizando mediante un método GET o POST de las cabeceras de la página web.

```
HTTP/1.1 303 See other
Date: Fri, 09 Dec 2016 14:29:23 GMT
Server: Apache
X-Powered-By: PHP/5.6.28
Set-Cookie: 88b13f49ddef3cf983705838cea21858=02qiqn7u2lqieq4i95gdmfi405; path=/; HttpOnly
Location: /index.php/component/search/?searchword=ZAP&searchphrase=all&Itemid=101
Vary: Accept-Encoding
Access-Control-Allow-Origin: http://educaciononline.uta.edu.ec:8080
Content-Length: 0
Connection: close
Content-Type: text/html; charset=utf-8
```

Figura 94. Análisis a cookies manejadas por la página web de la DEaDV

Al analizar la cookie se puede observar el tipo de criptografía utilizado por la misma, en éste caso es en MD5.

De la misma manera al analizar las cookies guardadas por el navegador.

Contenido:	s475i64f7eaoglkofs1affg9f2
Dominio:	sistemaseducaciononline.uta.edu.ec
Ruta:	/
Enviar para:	Cualquier tipo de conexión
Accesible para secuencias de comandos:	
Creado:	miércoles, 11 de enero de 2017, 11:47:45
Caduca:	Al finalizar la sesión de navegación

Figura 95. Cookie de sesión guardada por el navegador

Después de las pruebas realizadas se puede concluir que el manejo de sesiones está llevado de una manera adecuada, la criptografía utilizada debe ser mejorada ya que MD5 puede tener ciertas vulnerabilidades dado que ya es un tipo de encriptación obsoleto, el traspasar el esquema de manejo de sesiones no puede ser fácilmente realizado por un atacante sin afectar el funcionamiento del servidor.

b) Test de arreglo de sesiones

Cuando una aplicación no renueva la cookie de sesión después de la autenticación de un usuario, existe la posibilidad de encontrar la vulnerabilidad de arreglo de sesiones, que consiste en forzar al usuario a utilizar una cookie ya conocida y descifrada por un atacante. Las principales razones por la que éstos ataques pueden resultar exitosos son cuando: el sitio web vuelve a iniciar otra sesión sin previamente finalizar la sesión activa o cuando un atacante es capaz de forzar un ID de sesión ya conocida de algún usuario, por lo tanto, cuando el usuario se autentica, el atacante tiene acceso a ésta sesión.

Al analizar el manejo de sesiones por parte de la administración se determinó que los tokens de sesión son cambiados en cada sesión, por lo cual, al terminar una sesión éste token queda inutilizable en un intento de inicio de sesión próximo; de la misma manera al autenticarse un usuario existe una renovación de cookies, por lo que no existe posibilidad de volver a iniciar sesión si finalizar la actual.

De la misma manera las sesiones deben ser guardadas dentro de un log, y deben ser visibles a los administradores para poder llevar un correcto registro de cambios, claro que muchas veces las sesiones pueden ser establecidas mediante un proxy el cual enmascara la dirección original quien envía la solicitud a la página web, de ésta manera fueron realizados los test de autenticación en el apartado 4.10.4.

Último acceso	Última dirección IP	Acción
Current session	193.90.12.87	
hace 4 horas	172.21.121.29	Salir

Figura 96. Registro de cambios del aula virtual

En donde fue detectada la dirección IP del proxy escondiendo al atacante.

c) Test de funcionalidad de cerrar sesión

La finalización de una sesión es una parte crucial del ciclo de vida de una sesión. Reducir al mínimo el tiempo de vida de los tokens utilizados para evitar una falsificación de sesiones. Con éste test y su corrección también se pueden utilizar para prevenir ataques tipo Cross Site Scripting y Cross Site Request Forgery, los cuales se basan muchas veces en una sesión activa presente de un usuario.

Para el presente test se evaluó la presencia de un botón de logout en cada pantalla, el mismo que debe ser siempre visible y accesible sin necesidad de moverse en la pantalla.

Figura 97. Pestaña de finalizar sesión

La pestaña se encuentra siempre visible, inclusive si se desplaza hacia el final de la página la cabecera se mantiene, lo cual representa visualmente, un buen proceso, el cual ayuda a evitar que el usuario se olvide de finalizar su sesión al terminar el trabajo realizado.

Después de ello se realiza un análisis de la capacidad de regresar hacia pantallas de usuario mediante el regtorno a la página anterior en el navegador, en el apartado *4.10.5 subsección a* se realizó el test dando como resultado un error de caché al no poder reenviar el formulario.

Se puede concluir que la funcionalidad de cierre de sesión de la página web de la DEaDV se encuentra configurada de manera adecuada.

d) Test de tiempo de espera de sesión

El tiempo de espera de sesión se refiere a cuánto tiempo una sesión puede permanecer activa mientras no se está realizando ninguna actividad en la misma.

Es necesario éste test debido a que; si existe, por parte del usuario, un error al finalizar la sesión, o el simple hecho de haber olvidado hacerlo, automáticamente el sistema cierra la sesión del usuario.

Dentro de joomla existe un cierre de sesión automático después de media hora de inactividad, no se da una razón en específico de la finalización de la sesión, sólo se regresa a la pantalla de inicio de sesión.

En el manejo del aula virtual por parte de Moodle, después de media hora de inactividad, ésta vez se aprecia un mensaje el cual solicita los datos del usuario si se requiere ingresar de nuevo.

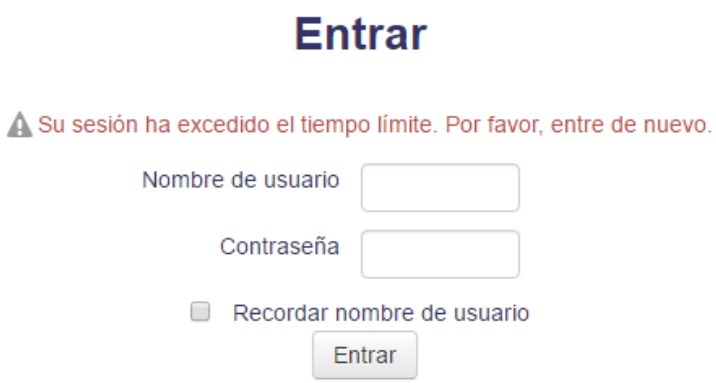


Figura 98. Solicitud de datos del usuario al finalizar la sesión

Con la finalización de la sesión se debe tener en cuenta que los tokens de sesión deben quedar inutilizables, el servidor se encarga de verificar el estado de la sesión y realizar las acciones correspondientes.

4.10.7. TEST DE VALIDACIÓN DE ENTRADAS

Las vulnerabilidades más comunes existentes dentro de un entorno web son la falla en la validación de datos del lado del cliente antes de utilizarlos. Éstas vulnerabilidades pueden llevar a grandes riesgos de seguridad informática de un sistema tales como inyecciones de código, ataques a archivos de sistema y sobrecarga de buffer.

Muchos de los test presentados a continuación y por motivos institucionales, no fueron posibles realizarlos ya que interfieren con el servidor, alterando el funcionamiento correcto del mismo provocando molestias a la comunidad universitario, mas son mostrados para ser analizados y sus posibles repercusiones de ser posibles.

a) Test de Cross Site Scripting

O XSS por sus siglas en inglés, ocurren cuando un atacante inyecta código ejecutable en el navegador para esperar una respuesta HTTP. El código inyectado no afecta directamente a la aplicación sino a un usuario que puede abrir un link incorrecto de la página clonada, el código es incluido en ésta nueva página dentro de la URL o en los parámetros HTTP [32].

Con un simple test se puede verificar si existe una vulnerabilidad de éste tipo, se inyecta código javascript en la url del sitio web.

Figura 99. Inyección de código en url de la página web

El sitio ignora el código ingresado y toma en cuenta sólo la url de la página web, lo que representa una buena medida de seguridad por parte de la administración del sitio web.

b) Test de falsificación HTTP

Al reemplazar parámetros HTTP con diferentes nombres, puede causar que una aplicación interprete los valores de maneras no anticipadas. Mediante la explotación de ésta vulnerabilidad, un atacante puede sobrepasar las validaciones de atributos de entrada, activar mensajes de error o modificar variables internas.

De la misma manera que el apartado anterior, el método de test de la presente vulnerabilidad se lo realiza en la URL del sitio web, en donde se añade un nuevo parámetro con el cual se espera conseguir un resultado distinto.

Primero se realiza una búsqueda dentro del sitio para obtener resultados, en éste caso se buscará la palabra cursos.

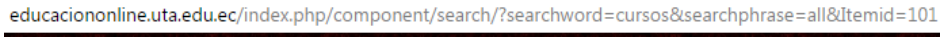


Figura 100. URL de búsqueda

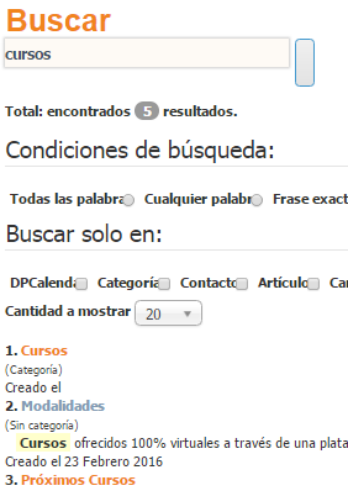


Figura 101. Resultado de la búsqueda

Entonces se procede a añadir un parámetro extra a la búsqueda esperando un resultado que combine ambas búsquedas

Figura 102. URL búsqueda arreglada

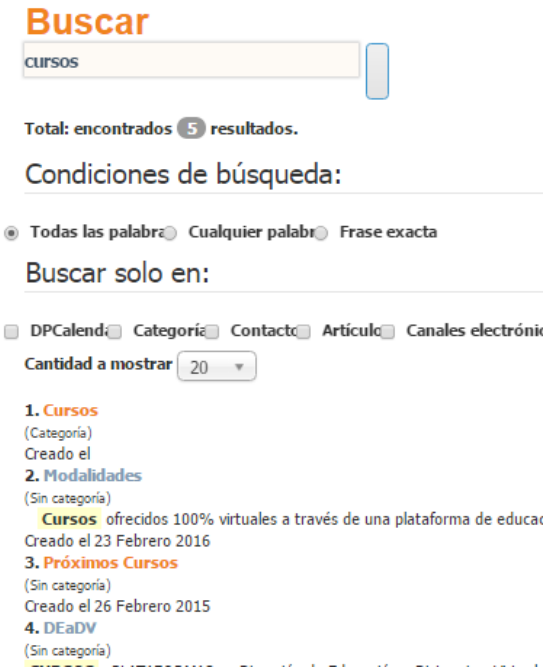


Figura 103. Resultado de la búsqueda arreglada

El manejo de las validaciones es correcto y al añadir el nuevo parámetro fue ignorado por el sitio web, por lo cual se considera un grado de seguridad muy bueno.

c) Inyección SQL

Una inyección SQL consiste en la inserción parcial o completa de una consulta SQL vía entrada de datos por parte del cliente hacia la aplicación, para tener un acceso a los datos manejados por el servidor. Una inyección SQL exitosa puede devolver como respuestas información sensible de la base de datos del servidor, modificar la base de datos, ejecutar operaciones administrativas y recuperar contenido de un archivo existente en la base de datos [32].

Existen distintas maneras de comprobar éste tipo de vulnerabilidad, como se pudo comprobar en los test realizados, los comandos y caracteres ajenos a la URL son ignorados por lo que un test a la URL queda descartado; mediante la herramienta de Kali Linux, SQLMAP se realiza un análisis de la existencia de la presente vulnerabilidad, las inyecciones de cualquier tipo de datos, al ser un análisis que compromete al servidor, sólo se presentará la interfaz de la herramienta mencionada.

Figura 104. Interfaz sqlmap

La misma puede ser más focalizada al conocer, mediante recolección de datos, la base de datos que maneja al servidor principal la cual es Mysql 5.7.16.

d) Inyección LDAP

El protocolo de acceso a directorios de peso ligero es usado para guardar información acerca de usuarios, hosts y distintos objetos de éste tipo; es un ataque del lado del servidor el cual permite modificar o insertar datos y objetos dentro de un archivo modificando los hosts y los usuarios válidos dentro de un servidor [13].

Para el mismo es necesario realizar una inyección SQL con el objetivo de recabar información de tablas en donde se puede alojar éste tipo de información.

e) Inyección XML

Se produce cuando un atacante intenta inyectar un documento de tipo XML a la aplicación.

Se realiza en la URL del sitio web y se intenta ingresar un documento de éste tipo con parámetros de usuario y contraseña para obtener accesos no autorizados.

El sitio web de la DEaDV rechaza todo tipo de solicitudes ajenas a la URL original, es por lo que el presente test no pudo ser realizado y representa una gran seguridad por parte del manejo del sitio web, mas como ejemplo es citado a continuación un intento de inyección XML realizado como ejemplo en la guía de metodología OWASP, para detección de vulnerabilidades en aplicaciones web [32].

Primero se analiza un archivo XML obtenido de una base de datos

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
        <user>
                <username>gandalf</username>
                <password>!c3</password>
                <userid>0</userid>
                <mail>gandalf@middleearth.com</mail>
        </user>
        <user>
                <username>Stefan0</username>
                <password>w1s3c</password>
                <userid>500</userid>
                <mail>Stefan0@whysec.hmm</mail>
        </user>
</users>
```

Figura 105. Ejemplo de archivo XML [32]

Después de ello se intenta inyectar mediante la URL de un sitio no seguro, un fragmento del código, en el mismo formato analizado

```
http://www.example.com/addUser.php?username=tony&password=Un6R34kb!e&email=s4tan@hell.com
```

Figura 106. Ejemplo de inyección XML [32]

Se generando un nuevo archivo

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
        <user>
                <username>gandalf</username>
                <password>!c3</password>
                <userid>0</userid>
                <mail>gandalf@middleearth.com</mail>
        </user>
        <user>
                <username>Stefan0</username>
                <password>w1s3c</password>
                <userid>500</userid>
                <mail>Stefan0@whysec.hmm</mail>
        </user>
        <user>
                <username>tony</username>
                <password>Un6R34kb!e</password>
                <userid>500</userid>
                <mail>s4tan@hell.com</mail>
        </user>
</users>
```

Figura 107. Archivo XML alterado [32]

En el cual constan las nuevas credenciales ingresadas.

f) Sobrecarga de Buffer (DOS)

Se trata de una de las vulnerabilidades más graves para un sistema manejado en web, no existe una forma total de prevenir éstos ataques, ya que, debido a la evolución de la tecnología, de la misma manera evolucionan las maneras de vulnerar y las herramientas para el mismo.

El ataque DOS puede ser dirigido a un servicio específico de un servidor o a todas sus funcionalidades, siendo éste el más peligroso; se debe tomar en cuenta la diferencia entre DOS y DDOS, mientras que DOS es en pequeña escala y dirigido para un ataque pequeño, un DDOS (Distributed Denial of Services) está enfocado en provocar un daño más persistente y duradero.

En el test realizado se emplearon tres maneras de realizar un ataque DOS dirigido al sitio web de la DEaDV.

Se utilizó la herramienta goldeneye la cual es propia de Kali Linux.

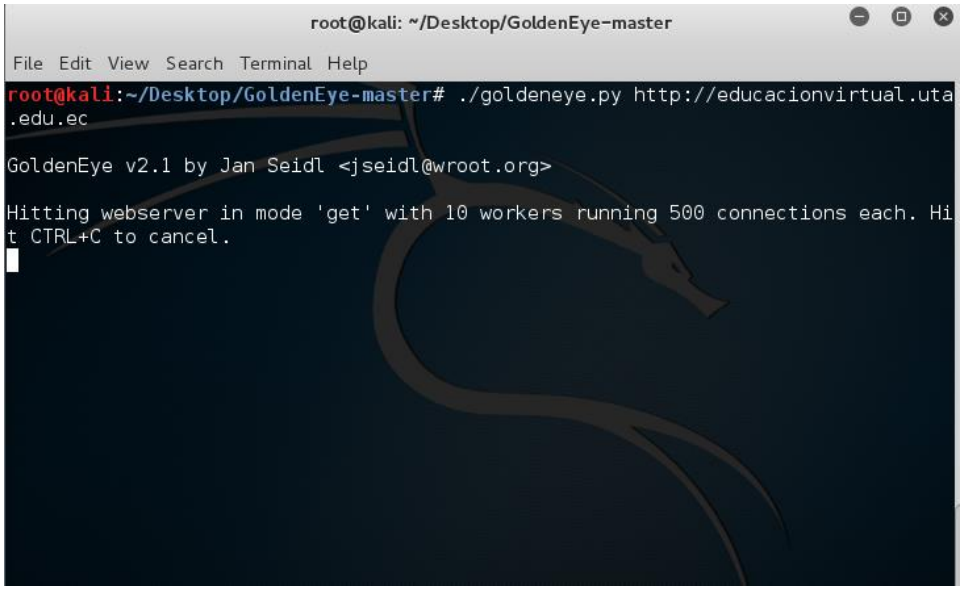


Figura 108. Uso de la herramienta goldeneye

De la misma manera se utilizó un exploit con el mismo fin

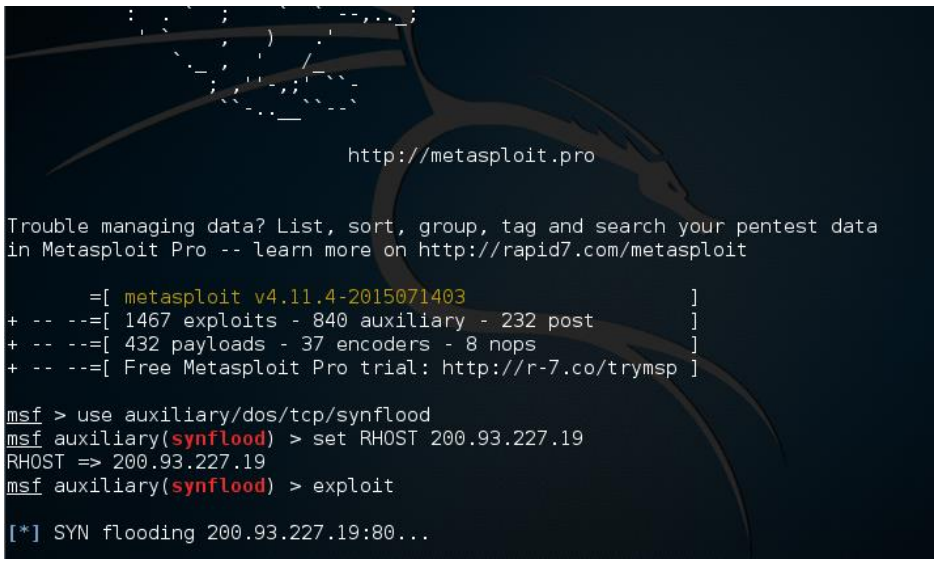


Figura 109. Uso de exploit para crear un DOS

Finalmente se utilizó la herramienta LOIC que la cual es una herramienta de Windows con interfaz gráfica

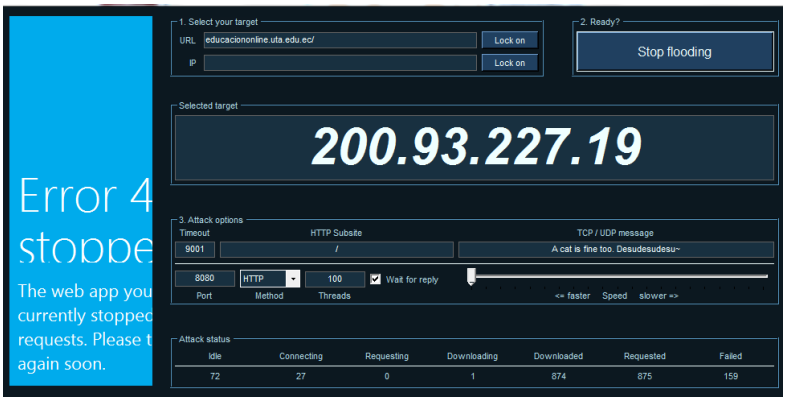


Figura 110. Interfaz de la herramienta LOIC

Con las tres herramientas se obtuvo el resultado esperado, el cual fue el detener al sitio web, mas al terminar el ataque el sitio web recupera su normalidad.

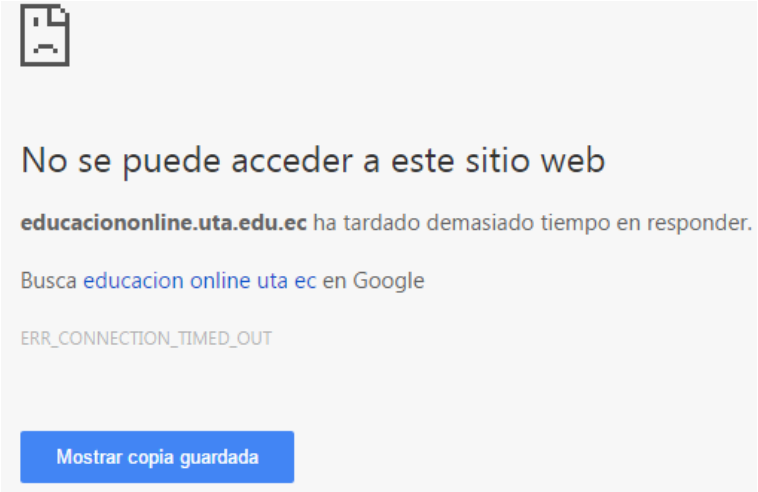


Figura 111. Comprobación del éxito del test

La vulnerabilidad a éste tipo de ataques es la más difundida a nivel mundial, por lo que son necesarias medidas de mitigación para éstos existentes riesgos.

4.10.8. MANEJO DE ERRORES

A menudo, durante un análisis de vulnerabilidades hacia un sitio o aplicación web, se generan muchos errores; es posible causar éstos errores mediante solicitudes particulares, éstos errores son muy importantes para un analista debido a que los mismos revelan mucha información acerca de la base de datos, bugs y componentes tecnológicos relacionados con la aplicación y el sitio web.

Muchas veces los errores son manejados por el servidor, como por ejemplo, al realizar una petición que el mismo no reconoce y devuelve información acerca del sitio en cuestión tal como el error 404 Not Found, el mismo que se puso a prueba en la página web de la DEaDV.

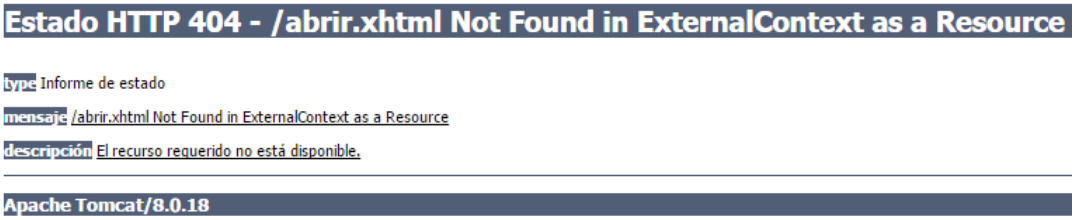


Figura 112. Error 404 Not Found

Con la información de que el servidor utiliza Apache Tomcat 8.0.18 se puede focalizar más un ataque dirigido al servidor, el manejo de éste tipo de errores, es el que debe ser analizado y tomado en cuenta por los administradores del sistema

De la misma manera se pueden generar errores propios de la aplicación, la cual los maneja sin necesidad de ingresar al servidor como por ejemplo los de contraseñas incorrectas; éstos errores si bien no aportan con información clara de las herramientas o tecnologías utilizadas por el servidor, si se puede utilizar para buscar maneras de vulnerar a la misma.

Figura 113. Generación de error de aplicación

4.10.9. CRIPTOGRAFÍA

Datos sensibles deben ser protegidos cuando son transmitidos a través de la red; datos como nombres de usuarios y contraseñas.

El sitio y la aplicación no debe transportar información sensible en canales que no contengan la encriptación correcta,

En el apartado *4.10.4 subsección A* se demuestra que los datos enviados no son transmitidos a través de un canal seguro al no tener un certificado HTTPS, lo cual puede resultar en riesgos de seguridad informática.

En el apartado *4.10.6 subsección A*, se analiza la encriptación de una cookie, si bien se encuentra encriptada, la metodología usada para la misma es MD5 la cual es muy vulnerable hoy en día.

Los certificados utilizados por un sitio web son parte fundamental para garantizar la seguridad del transporte de datos como por ejemplo la utilizada por la página de la Universidad Técnica de Ambato,

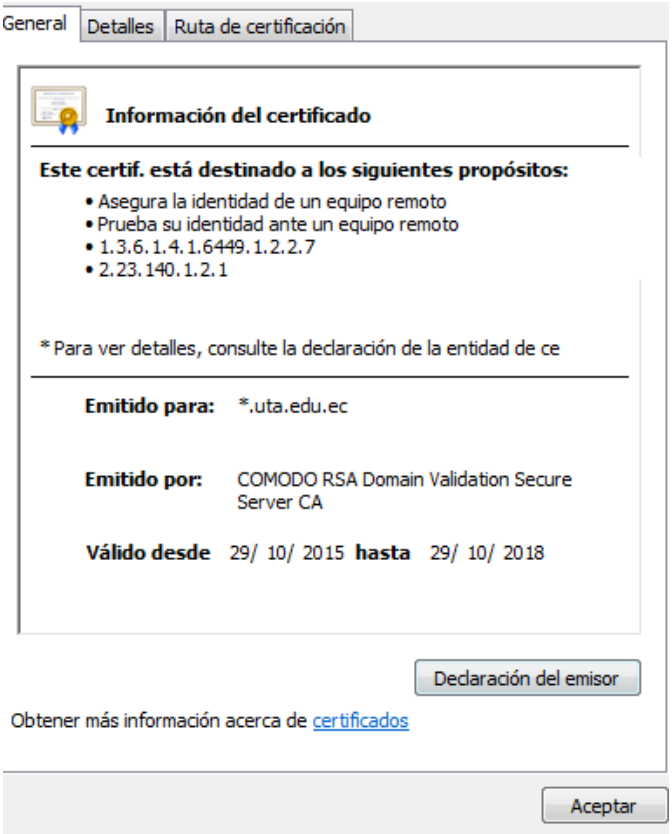


Figura 114. Certificado utilizado por la página https://uta.edu.ec

Por lo cual el análisis de encriptación es necesario para cada entidad y, como fue demostrado en puntos anteriores debe existir un refuerzo en las mismas.

4.11 DISEÑO DE PROCESOS CORRECTIVOS PARA MITIGACIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA

Después de un análisis a la página web de la Dirección de Educación a Distancia y Virtual y a la aplicación web correspondiente al aula virtual de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, y utilizando las vulnerabilidades encontradas, se procede a realizar el diseño de procesos correctivos para dichas vulnerabilidades, las cuales serán citadas en orden de impacto hacia un sistema web siguiendo la metodología descrita en el punto anterior; de la misma manera, se citará el grado de impacto o riesgo existente ante la presencia de las vulnerabilidades y los procesos que se deben seguir para su corrección.

Mediante la investigación realizada, la metodología OWASP propone distintos parámetros de solución para varias de las vulnerabilidades encontradas, en el caso de la presente investigación y para los fines pertinentes de llevar a cabo soluciones inmediatas, se listan los procesos primordiales a llevar a cabo por los administradores de la página para solucionar de la mejor manera posible las distintas vulnerabilidades encontradas.

Éstos procesos fueron diseñados a partir de las soluciones ya establecidas por la metodología OWASP, tomando en cuenta el rango de tiempo para el cumplimiento de los mismos y su eficiencia.

Vulnerabilidad:	Uso de archivos por defecto para la configuración	
Apartado: 4.10.1		**Subsección:** B
Descripción:	Los archivos de configuración por defecto que vienen en los servidores no han sido cambiados	
Riesgo:	**Bajo**	
Proceso(s) Correctivo(s):	• Cambiar a nombres propios de la entidad a los archivos de configuración por defecto • Redirigir los enlaces internos a éstos archivos	

Tabla 3. Vulnerabilidad Nº 1

Vulnerabilidad:	Presencia de nombres de usuario administrador por defecto	
Apartado: 4.10.1		**Subsección:** B
Descripción:	Existe el nombre de usuario administrador manejado por defecto, en éste caso root.	
Riesgo:	**Bajo**	
Proceso(s) Correctivo(s):	• Crear un nuevo usuario con privilegios de administrador. • Borrar los usuarios por defecto creados por el sistema operativo.	

Tabla 4. Vulnerabilidad Nº 2

Vulnerabilidad:	Versión de PHP muy antigua	
Apartado: 4.10.1		**Subsección:** D
Descripción:	Se pueden explotar vulnerabilidades ya encontradas por los mismos desarrolladores de PHP, principalmente de ataques DOS	
Riesgo:	**Bajo**	
Proceso(s) Correctivo(s):	• Actualizar PHP a su versión más actual y estable • Aconsejable 7.1.1	

Tabla 5. Vulnerabilidad Nº 3

Vulnerabilidad:	Inexistencia de transporte HTTP de estricta seguridad HSTS	
Apartado: 4.10.2		**Subsección:** F
Descripción:	La información traspasada por éste canal no se encuentra encriptada	
Riesgo:	**Bajo**	
Proceso(s) Correctivo(s):	• Implementar dentro del código de la página web los apartados de *max-age = segundos* para prevenir ataques de hombre en el medio. • Verificar la red ante posibles comportamientos de recolección de información mediante sniffers	

Tabla 6. Vulnerabilidad Nº 4

Vulnerabilidad:	Cuentas de usuario con nombres por defecto	
Apartado: 4.10.3		**Subsección:** D
Descripción:	Se encuentra varias cuentas de usuario nombradas de la misma manera que el usuario en cuestión y el administrador con un nombre por defecto	
Riesgo:	**Bajo**	
Proceso(s) Correctivo(s):	• Realizar un análisis de cuentas de usuario para evitar la utilización de nombres predefinidos o de fácil acceso	

Tabla 7. Vulnerabilidad Nº 5

Vulnerabilidad:	Creación de usuarios de la aplicación web son débiles o por defecto	
Apartado: 4.10.3		**Subsección:** E
Descripción:	La creación de los usuarios del aula virtual están limitados a su número de cédula	
Riesgo:	**Bajo**	
Proceso(s) Correctivo(s):	• Redefinir las reglas de la creación de usuarios nuevos • Crear usuarios tomando en cuenta una mayor cantidad de parámetros para que sea más complicado su acceso • Se sugiere primera letra del nombre, apellido y últimos cuatro dígitos de la cédula.	

Tabla 8. Vulnerabilidad Nº 6

Vulnerabilidad:	Aplicación web de Moodle muestra datos completos de alumnos y profesores	
Apartado: 4.10.4		**Subsección:** B
Descripción:	Al mostrar todos los datos de los estudiantes y profesores se puede realizar un ataque más enfocado hacia una persona o materia en particular	
Riesgo:	**Bajo**	
Proceso(s) Correctivo(s):	• Configurar a la aplicación para que sólo muestre a éstos usuarios a usuarios validados e ingresados.	

Tabla 9. Vulnerabilidad Nº 7

Vulnerabilidad:	Referencias inseguras a objetos directos en la aplicación web de Moodle	
Apartado: 4.10.5		**Subsección:** C
Descripción:	Existe la posibilidad de cambiar ciertos parámetros de la URL e ingresar a recursos distintos	
Riesgo:	**Bajo**	
Proceso(s) Correctivo(s):	• Implementar *friendly urls* para enmascarar los recursos que están siendo compartidos a los usuarios • Se puede implementar en el htaccess o en el servidor	

Tabla 10. Vulnerabilidad Nº 8

Vulnerabilidad:	Manejo de errores usado por el propio servidor web por defecto en la página web de Joomla	
Apartado: 4.10.8		**Subsección: -**
Descripción:	Al dejar que por defecto los errores sean manejados por el servidor web se puede otorgar información valiosa a un invasor y enfocar su ataque	
Riesgo:	**Bajo**	
Proceso(s) Correctivo(s):	• Reconfigurar el archivo de configuración web por defecto • Crear páginas de mensajes de error propias	

Tabla 11. Vulnerabilidad Nº 9

Vulnerabilidad:	Referencia a sitios web que no deberían ser accesibles en la página web administrada por Joomla	
Apartado: 4.10.1		**Subsección:** A
Descripción:	Mediante la búsqueda en google se obtuvieron páginas que no deben ser accedidas	
Riesgo:	**Medio**	
Proceso(s) Correctivo(s):	• Respaldar y eliminar las páginas web antiguas u obsoletas • Quitar todo vínculo a dichas páginas • Realizar una depuración a fondo del sitio web	

Tabla 12. Vulnerabilidad Nº 10

Vulnerabilidad:	Almacenamiento riesgoso de logs del sistema	
Apartado: 4.10.2		**Subsección:** A
Descripción:	Los logs antiguos son transportados a un servidor con acceso a la red y a internet.	
Riesgo:	**Medio**	
Proceso(s) Correctivo(s):	• Reservar un servidor para almacenamiento y recuperación el cual no tenga acceso a la red, mucho menos a internet.	

Tabla 13. Vulnerabilidad Nº 11

Vulnerabilidad:	Credenciales transportadas en un canal inseguro	
Apartado: 4.10.4		**Subsección:** A
Descripción:	Al carecer de un protocolo https existe la posibilidad de que los datos sean robados a través de un sniffer y al no estar cifrados ser utilizados por un atacante	
Riesgo:	**Medio**	
Proceso(s) Correctivo(s):	• Conseguir una certificación SSL (Capa de conexión segura). • Configurar a las páginas sitio web que transportan información sensible para usar la nueva certificación para la comunicación de sus datos. • Editar los enlaces a los elementos de la página web para utilizar el nuevo protocolo	

Tabla 14. Vulnerabilidad Nº 12

Vulnerabilidad:	Falta de control de cambio de contraseñas en la aplicación web de Moodle	
Apartado: 4.10.4		**Subsección:** I
Descripción:	Existe la posibilidad de cambiar una contraseña fuerte por una débil sin controles adecuados	
Riesgo:	**Medio**	
Proceso(s) Correctivo(s):	• Implementar las mismas políticas de contraseñas existentes al realizar el cambio la primera vez, tal como ingresar una contraseña con mayúsculas, minúsculas, al menos un dígito numérico y al menos un dígito no alfanumérico. • Concienciar a los usuarios acerca de las presentes políticas	

Tabla 15. Vulnerabilidad Nº 13

Vulnerabilidad:	Vulnerabilidad a sobrecarga de buffer (Ataque DOS)	
Apartado: 4.10.7		**Subsección:** F
Descripción:	Existe la posibilidad de realizar éste tipo de ataques y dar de baja tanto la página como al servidor web	
Riesgo:	**Medio**	
Proceso(s) Correctivo(s):	• Analizar el código para verificar si existen líneas del mismo que permitan éste tipo de ataques (no verificación de entradas). • Utilizar la última versión de los recursos web ya que poseen parches para mitigar éste tipo de ataques. • Escaneo periódico a la red para verificar fluctuaciones de la misma. • Bloqueo de la IP atacante al detectar una cantidad anormal de peticiones y realizar una revisión de la misma (si es un ataque interno). • Como sugerencia adicional se podría hacer uso de las características propias de Moodle para realizar un balanceo de carga entre las entidades capaces de manejarlo.	

Tabla 16. Vulnerabilidad Nº 14

Vulnerabilidad:	Existencia de archivos con información sensible en la página web de Joomla	
Apartado: 4.10.2		**Subsección:** C
Descripción:	Mediante exploración de metadatos de la página web se obtuvieron archivos personales y de configuración	
Riesgo:	**Alto**	
Proceso(s) Correctivo(s):	• Respaldar y eliminar dichos archivos de la página web • Respaldar los archivos en servidores que no tengan salida a la red, mucho menos a internet.	

Tabla 17. Vulnerabilidad Nº 15

Vulnerabilidad:	Uso de usuarios y contraseñas débiles o por defecto en la aplicación web de Moodle	
Apartado: 4.10.4		**Subsección:** B
Descripción:	Se manejan credenciales predecibles con un alto impacto a la integridad de los datos existentes en la aplicación	
Riesgo:	**Alto**	
Proceso(s) Correctivo(s):	• Utilizar mecanismos de seguridad al momento de la creación de los usuarios • Al crear usuarios realizarlo con claves seguras, aleatorias e indetectables que sean enviadas a los correos electrónicos de los usuarios • Se sugiere utilizar el PIN usado para el acceso a UTA Mático	

Tabla 18. Vulnerabilidad Nº 16

Vulnerabilidad:	Debilidad de mecanismo de cierre en la aplicación web de Moodle	
Apartado: 4.10.4		**Subsección:** C
Descripción:	Existe la posibilidad de insertar un usuario y contraseña de manera errónea una gran cantidad de veces permitiendo ataques de fuerza bruta	
Riesgo:	**Alto**	
Proceso(s) Correctivo(s):	• Activar un mecanismo de cierre que bloquee temporalmente la página para no poder ingresar usuario y/o contraseña nuevamente en un tiempo determinado • En caso de existir un ataque hacia un usuario en específico, bloquear la cuenta temporalmente al tercer intento fallido • Si se insiste con un usuario correcto pero una clave incorrecta bloquear la cuenta y solicitar al usuario acercarse al administrador • Se sugiere realizar el bloqueo definitivo al tener entre 5 y 7 intentos fallidos.	

Tabla 19. Vulnerabilidad Nº 17

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- El análisis de vulnerabilidades es un proceso necesario para toda entidad. La Universidad Técnica de Ambato debe poner énfasis en la misma para garantizar la seguridad informática de todos sus dominios y aplicaciones web.

- Mediante el uso de herramientas de fácil acceso y de software libre fueron los resultados acerca de las vulnerabilidades tanto a la página web realizada en Joomla como a la aplicación web manejada por Moodle.

- Tras la obtención de las vulnerabilidades existentes, se llevó a cabo un informe dirigido hacia el director y los administradores de la Dirección de Educación a Distancia y Virtual para su corrección.

- Los objetivos planteados en el presente proyecto fueron cumplidos mediante el análisis, explotación y corrección de las distintas vulnerabilidades encontradas.

- El uso de la metodología OWASP de acuerdo a sus distintos pasos, se llevó a cabo mediante la obtención de información crucial de la entidad, consiguiendo así focalizar el estudio y realizar los distintos análisis a varios sectores del sitio web y de la aplicación que es manejada por la Dirección de Educación a Distancia y Virtual.

5.2. RECOMENDACIONES

- Se recomienda a la entidad realizar periódicamente un análisis de seguridad informática para evitar riesgos, y garantizar el correcto funcionamiento de la página web a los usuarios, de la misma manera garantizar la seguridad del transporte de los datos personales de los estudiantes y docentes usuarios de la aplicación web.

- Se sugiere trabajar conjuntamente con la Dirección de Tecnologías de la Información y Comunicación para realizar auditorías de seguridad, ya que la entidad es encargada de la comunicación y el manejo de firewalls y proxys.

- Resulta crítico el realizar un análisis de vulnerabilidades enfocándolo en ataques DOS, ya que representa un impacto negativo en los servidores.

- Es recomendado analizar el tipo de herramientas que se va a utilizar para el análisis de un entorno web, ya que muchas de ellas son muy intrusivas, provocando congestión en la red y un funcionamiento anómalo en la misma como por ejemplo realizar una consulta muy grande mediante el comando de Linux NMAP.

- Para un posterior análisis del sitio y la aplicación web es recomendada la metodología OWASP ya que su análisis conlleva distintos elementos y procesos de la entidad y son analizados a fondo, incluyendo servidores los cuales, en el presente proyecto de investigación, y por políticas institucionales, no pudieron ser atacados para analizar sus vulnerabilidades.

REFERENCIAS

[1] L. &. G. S. Tauscher, «How people revisit web pages: Empirical findings and implications for the design of history systems,» *nternational Journal of Human-Computer Studies,,* vol. 4, nº 21, pp. 97-137, 1997.

[2] J. M. Myerson, «Identifying enterprise network vulnerabilities.,» *International Journal of Network Management,* vol. 3, nº 12, pp. 135-144, 2002.

[3] Acutenix Enterprises, «Acutenix Enterprises,» Acutenix, 2015. [En línea]. Available: http://www.acunetix.com/acunetix-web-application-vulnerability-report-2015/. [Último acceso: 15 Abril 2016].

[4] J. Freire, «Ecuador, el cuarto país de la región que recibe más ataques cibernéticos,» *El Universo,* p. Sección Dr. Tecno, 3 Octubre 2015.

[5] L. A. Gómez, «Análisis de Ia Tecnología Honeypot y su Aplicación en la Detección y Corrección de Vulnerabilidades en la Red de Datos del Gobierno Autónomo Descentralizado de la Provincia de Chimborazo,» Riobamba, 2012.

[6] A. P. Caluña, «Aplicación de Hacking Ético para la Determinación de Vulnerabilidades de Acceso a Redes Inalámbricas WiFi,» Ambato, 2012.

[7] C. D. N. L. C. Dennis Applet, «Automated testing for SQL injection vulnerabilities: an input mutation approach,» *ACM Digital Library,* pp. 259-269 , 2014.

[8] F. Quisaguano, «Implementación de hacking ético para el análisis de vulnerabilidades, métodos de prevención y protección aplicados a la infraestructura de red de la empresa Construlec Cía. Ltda,» Quito, 2015.

[9] P. Engebretson, The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing made easy, Elsevier, 2013.

[10] Y. Malhotra, «A Risk Management Framework for Penetration Testing of Global Banking & Finance Networks VoIP Protocols,» *Social Science Research Network,* 2014.

[11] I. 27001, «Estándar Internacional,» 2015.

[12] J. Aguirre, Breve Introducción a la Seguridad Informática, España, 2006.

[13] C. Tori, Hacking Ético, Rosario Argentina: Carlos Tori, 2008.

[14] K. Beaver, Hacking for dummies, Wiley, 2013.

[15] J. E. Mehan, Cyberwar, Cyberterror, Cybercrime, It Governance Publishing, 2008.

[16] E. W. B. D. D. D. &. W. D. S. Felten, «Web spoofing: An internet con game.,» *Software World,* vol. 28, nº 2, pp. 6-8.

[17] US CERT, «Quarterly Trends and Analysis Report.,» 2007.

[18] W. Georgia, Penetration Testing A Hands-On Introduction to Hacking, San Francisco - EEUU: No Starch Press, Inc, 2014.

[19] B. Sheila, Web Hacking, claves para desarrolladores y administradores de sitios, Buenos Aires - Argentina: Fox Andina, 2013.

[20] B. D. Nuela Guananga, AUDITORÍA DE LA SEGURIDAD INFORMÁTICA PARA EL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA, Ambato, 2015.

[21] Offensive Security Ltd., Penetration Testing with Kali Linux, 2014.

[22] A. L. Joseph Muniz, Web Penetration Testing with Kali Linux, Birmingham: Packt Publishing, 2013.

[23] K. A. B., *HACKING ÉTICO 101,* Guayaquil, 2013.

[24] Offensive-Securitty, *Tutorial de Metasploit Framework,* 2013.

[25] L. E. DOS, «La Extensión DOS,» 23 Mayo 2013. [En línea]. Available: http://laextensiondos.blogspot.com/2013/05/software-de-auditoria-dumpsec.html. [Último acceso: 14 Noviembre 2016].

[26] J. F. R. Buendía, Seguridad informática, Aracava (Madrid): McGraw-Hill/Interamericana de España, S. L., 2013.

[27] Netcraft Company, «About us,» [En línea]. Available: https://www.netcraft.com/about-netcraft/. [Último acceso: 07 Marzo 2017].

[28] S. Bennetts, «Owasp zed attack proxy,» de *AppSec*, USA , 2013.

[29] The Open Web Application Security Project, «OWASP Joomla Vulnerability Scanner Project,» [En línea]. Available: https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project. [Último acceso: 7 Marzo 2017].

[30] OpenVAS, «OpenVAS,» [En línea]. Available: http://www.openvas.org/about.html.

[31] T. &. B. B. Rid, «Attributing cyber attacks,» *Journal of Strategic Studies,* vol. 38, nº 1-2, pp. 4-37, 2015.

[32] Open Web Application Security Project Foundation, Guía de Pruebas OWASP, 2015.

ANEXOS Y APÉNDICES

Anexo A

Aprobación para realizar el proyecto de investigación

DEaDV | DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL

Ambato septiembre 08, 2016
Oficio DEaD-D-296-2016

Señor
Jorge Alberto Sánchez Freire
ESTUDIANTE DÉCIMO SEMESTRE
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS
FACULTA DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
UNIVERSIDAD TÉCNICA DE AMBATO
Presente

De mis Consideraciones:

Reciba un cordial y atento saludo, una vez revisado el proyecto de investigación de tesis con el tema: **"Análisis de vulnerabilidades y Diseño de procesos correctivos de la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato",** autorizo a usted el poder de efectuar la mencionada investigación, en el período de Octubre 2016- Marzo 2017, para lo cual es necesario coordinar con esta Dirección las fechas a efectuar las pruebas.

Con sentimientos de consideración y estima.

Atentamente,

DIRECCION DE EDUCACION A DISTANCIA Y VIRTUAL DEaDV U.T.A

Ph.D. Carlos Meléndez Tamayo
DIRECTOR

CMT/lch

UTA | UNIVERSIDAD TÉCNICA DE AMBATO

Edificio Epsilón, Campus Huachi (Av. Los Chasquis y Río Payamino)
educacionvirtual@uta.edu.ec | educaciononline.uta.edu.ec
(03) 2401618 ext. 124 | WhastApp: 0 987165458

Anexo B

Certificado de Culminación del proyecto de investigación

DE@DV | DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL

Ambato, 12 de abril de 2017

CERTIFICACIÓN –DEaDV-021-2017

En calidad de DIRECTOR DE EDUCACIÓN A DISTANCIA Y VIRTUAL de la Universidad Técnica de Ambato, certifico que el Sr. SÁNCHEZ FREIRE JORGE ALBERTO, con Cédula de Ciudadanía N° 180455705-4 realizó el trabajo de investigación: "Análisis de vulnerabilidades y diseño de procesos correctivos de la página web de la Dirección de Educación a Distancia y Virtual", de conformidad a los intereses de esta Dirección.

Por la atención que se sirva dar al presente, me suscribo de usted.

Atentamente,

DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DEaDV U.T.A.

Ph.D. Carlos Meléndez Tamayo
DIRECTOR

Anexo C

Informe tipo checklist presentado a la entidad

Checklist: Fase 1 Recolección de Información

Identificación de la auditoría

Institución auditada: Universidad Técnica de Ambato / Dirección de Educación a Distancia y Virtual

Proyecto:
ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Tipo de auditoría: ❒ Interna
❒ Externa

Auditor

Nombre Jorge Alberto Sánchez Freire

e-mail jorsanfre@gmail.com | **Fono 0984505439**

Checklist

¿ Existe vulnerabilidad ?	Sí	No
a) Uso de un motor de búsqueda para verificación de existencia de información vulnerable	X	
b) Análisis del sitio y servidor web para verificar nombres por defecto	X	
c) Recolección de metadatos de la página web para la comprobación de existencia de información vulnerable		X
d) Enumeración de las aplicaciones del servidor web	X	
e) Revisión de comentarios y metadata del sitio web para verificación de existencia de información vulnerable		X
f) Identificación de puntos de entrada a la aplicación		X
g) Análisis al entorno del sitio web	X	
h) Análisis de la aplicación web	X	
i) Análisis y mapa de la arquitectura de la aplicación		X

Checklist: Fase 2 Test de manejo de configuración y desarrollo

Identificación de la auditoría

Institución auditada: Universidad Técnica de Ambato / Dirección de Educación a Distancia y Virtual

Proyecto:
ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Tipo de auditoría: ❒ Interna
❒ Externa

Auditor

Nombre Jorge Alberto Sánchez Freire

e-mail jorsanfre@gmail.com | **Fono 0984505439**

Checklist

¿ Existe vulnerabilidad ?	Sí	No
a) Test de configuración e infraestructura de la red	X	
b) Test de las extensiones de los archivos que manejan información sensible		X
c)Revisión de archivos viejos, de backup o no referenciados para verificación de información sensible	X	
d) Enumeración de las interfaces de administrador		X
e) Test de métodos HTTP		X
f) Test de transporte de seguridad estricto HTTP	X	

Checklist: Fase 3 Test de manejo de identidad

Identificación de la auditoría

Institución auditada: Universidad Técnica de Ambato / Dirección de Educación a Distancia y Virtual

Proyecto:
ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Tipo de auditoría: ❒ Interna
❒ Externa

Auditor

Nombre Jorge Alberto Sánchez Freire

e-mail jorsanfre@gmail.com | **Fono 0984505439**

Checklist

¿ Existe vulnerabilidad ?	Sí	No
a) Test de definición de roles		X
b) Test de proceso de registro de nuevos usuarios		X
c) Test de procesos de creación de nuevas cuentas		X
d)Test de enumeración de cuentas y cuentas de usuario con nombres por defecto	X	
e) Test para políticas de uso de nombres de usuarios débiles o sin seguridades	X	

Checklist: Fase 4 Test de autenticación

Identificación de la auditoría

Institución auditada: Universidad Técnica de Ambato / Dirección de Educación a Distancia y Virtual

Proyecto:
ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Tipo de auditoría: ❒ Interna
❒ Externa

Auditor

Nombre Jorge Alberto Sánchez Freire

e-mail jorsanfre@gmail.com | **Fono 0984505439**

Checklist

	¿ Existe vulnerabilidad ?	Sí	No
a)	Test de credenciales transportadas en un canal encriptado	X	
b)	Test de credenciales por defecto	X	
c)	Test de debilidades de mecanismos de cierre	X	
d)	Test para sobrepasar el esquema de autenticación		X
e)	Test de funcionalidad de recordar contraseñas		X
f)	Test de vulnerabilidades en la caché del navegador	X	
g)	Test de políticas de contraseñas débiles		X
h)	Test de preguntas de seguridad débiles		X
i)	Test de funcionalidades de reseteo de contraseñas	X	
j)	Test de autenticación en un canal alternativo		X

Checklist: Fase 5 Test de autorización

Identificación de la auditoría

Institución auditada: Universidad Técnica de Ambato / Dirección de Educación a Distancia y Virtual

Proyecto:
ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Tipo de auditoría: ❒ Interna
❒ Externa

Auditor

Nombre Jorge Alberto Sánchez Freire

e-mail jorsanfre@gmail.com | **Fono 0984505439**

Checklist

¿ Existe vulnerabilidad ?		Sí	No
a)	Test para sobrepasar el esquema de autorización		X
b)	Test de escala de privilegios		X
c)	Test de referencias inseguras de objetos directos	X	

Checklist: Fase 6 Test de manejo de sesiones

Identificación de la auditoría

Institución auditada: Universidad Técnica de Ambato / Dirección de Educación a Distancia y Virtual

Proyecto:
ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Tipo de auditoría: ❒ Interna
❒ Externa

Auditor

Nombre Jorge Alberto Sánchez Freire

e-mail jorsanfre@gmail.com | **Fono 0984505439**

Checklist

¿ Existe vulnerabilidad ?		Sí	No
a)	Test para sobrepasar el esquema de manejo de sesiones y atributos de cookies		X
b)	Test de arreglo de sesiones		X
c)	Test de funcionalidad de cerrar sesión		X

d)	Test de tiempo de espera de sesión		X

Checklist: Fase 7 Test de validación de entradas

Identificación de la auditoría

Institución auditada: Universidad Técnica de Ambato / Dirección de Educación a Distancia y Virtual

Proyecto:
ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Tipo de auditoría: ❒ Interna
❒ Externa

Auditor

Nombre Jorge Alberto Sánchez Freire

e-mail jorsanfre@gmail.com **Fono 0984505439**

Checklist

¿ Existe vulnerabilidad ?		Sí	No
a)	Test de Cross Site Scripting		X
b)	Test de falsificación HTTP		X
c)	Inyección SQL		X
d)	Inyección LDAP		X
e)	Inyección XML		X
f)	Sobrecarga de Buffer (DOS)	X	

Checklist: Fase 8 Manejo de errores

Identificación de la auditoría

Institución auditada: Universidad Técnica de Ambato / Dirección de Educación a Distancia y Virtual

Proyecto:
ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Tipo de auditoría: ❒ Interna
❒ Externa

Auditor

Nombre Jorge Alberto Sánchez Freire

e-mail jorsanfre@gmail.com **Fono 0984505439**

Checklist

¿ Existe vulnerabilidad ?		Sí	No
a)	Existencia de un manejo propio de errores	X	

Checklist: Fase 9 Criptografía

Identificación de la auditoría

Institución auditada: Universidad Técnica de Ambato / Dirección de Educación a Distancia y Virtual

Proyecto:
ANÁLISIS DE VULNERABILIDADES Y DISEÑO DE PROCESOS CORRECTIVOS DE LA PÁGINA WEB DE LA DIRECCIÓN DE EDUCACIÓN A DISTANCIA Y VIRTUAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Tipo de auditoría: ❒ Interna
❒ Externa

Auditor

Nombre Jorge Alberto Sánchez Freire

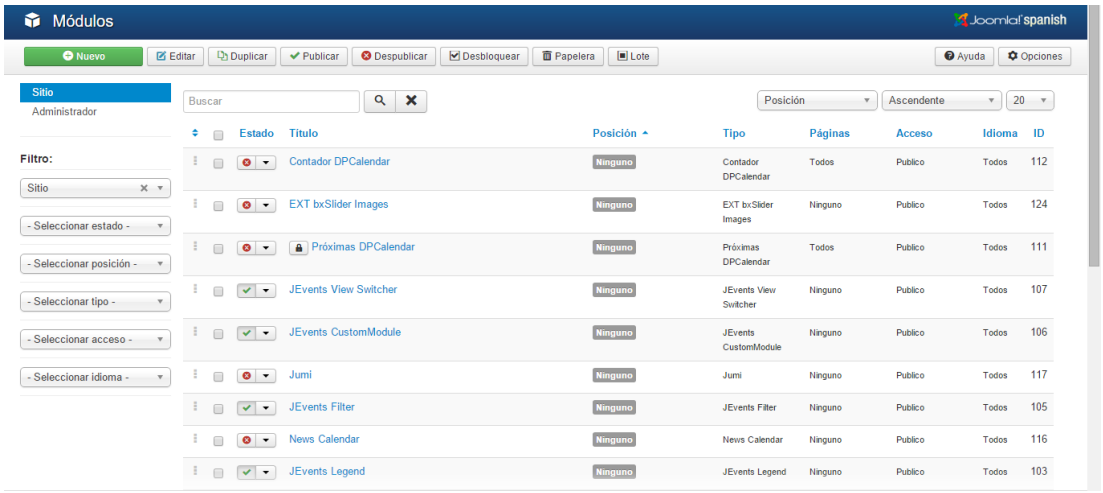
e-mail jorsanfre@gmail.com | **Fono 0984505439**

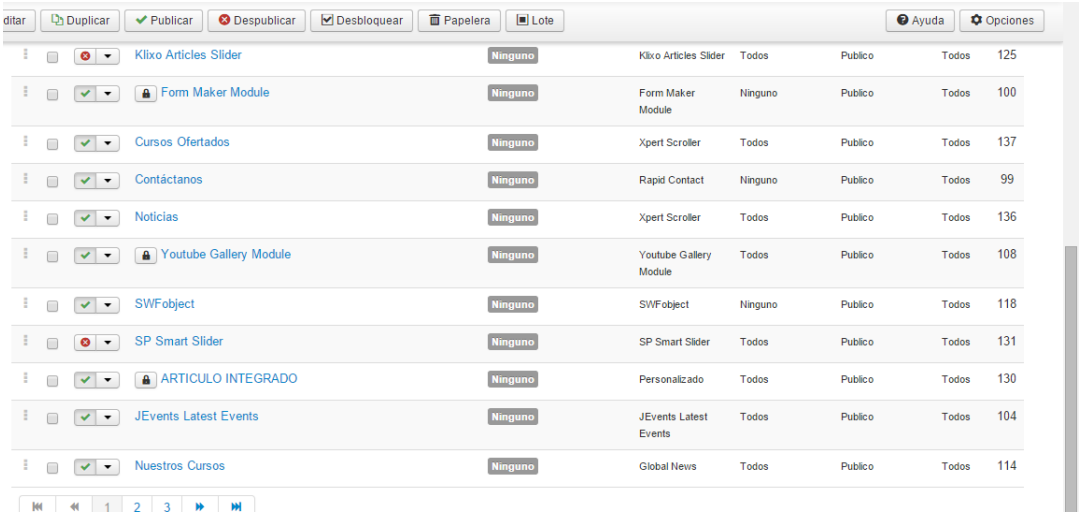
Checklist

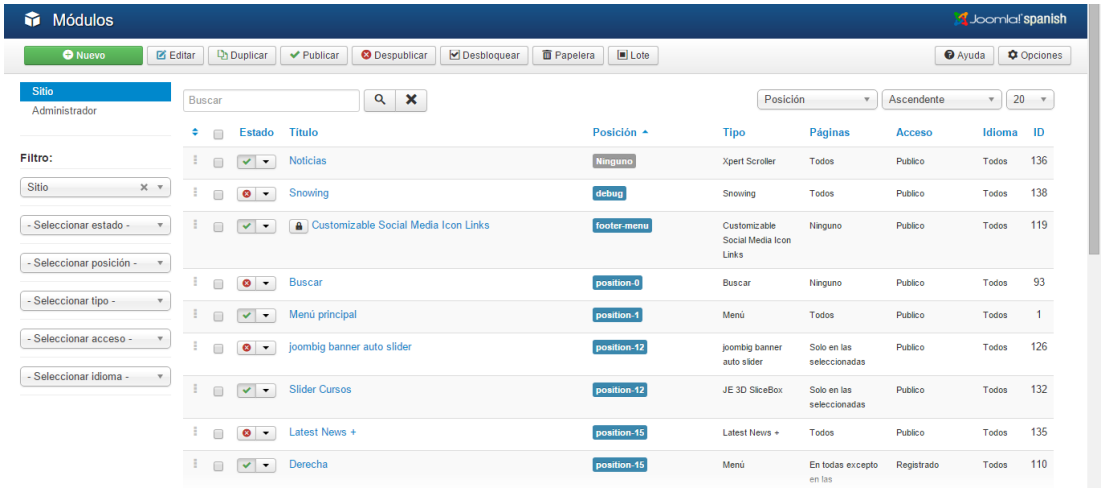
	¿ Existe vulnerabilidad ?	Sí	No
a)	Existencia de certificados para encriptación de datos	X	

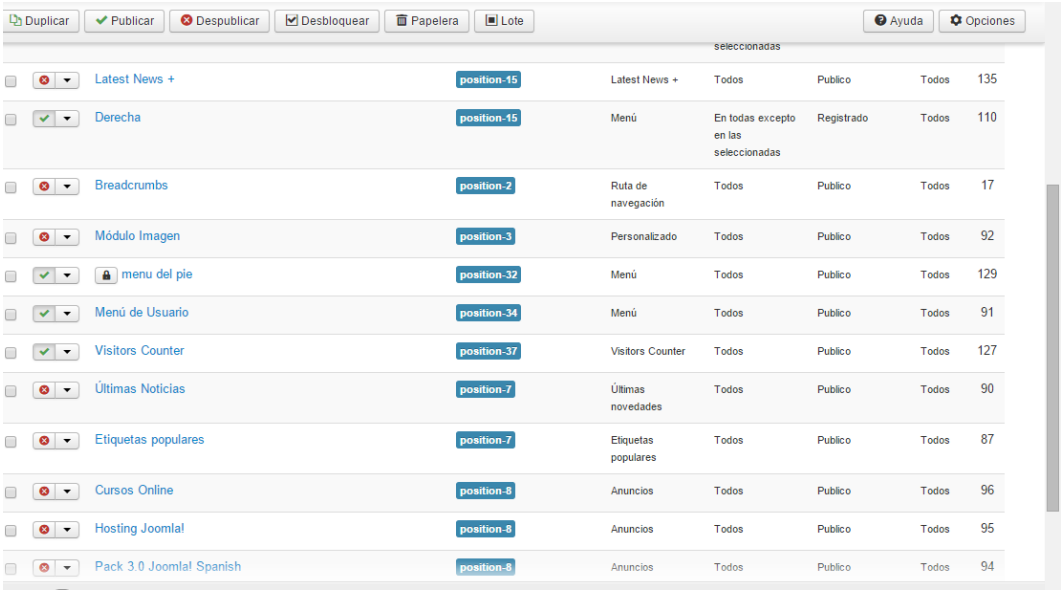
Anexo D

Imágenes de herramientas Joomla usadas por el sitio web






Módulos
Joomla!spanish
Nuevo
Editar
Duplicar
Publicar
Despublicar
Desbloquear
Papelera
Lote
Ayuda
Opciones
Sitio
Administrador
Filtro:
Sitio
- Seleccionar estado -
- Seleccionar posición -
- Seleccionar tipo -
- Seleccionar acceso -
- Seleccionar idioma -
Buscar
Posición
Ascendente
20
Estado
Titulo
Posición
Tipo
Páginas
Acceso
Idioma
ID
Noticias
Ninguno
Xpert Scroller
Todos
Publico
Todos
136
Snowing
debug
Snowing
Todos
Publico
Todos
138
Customizable Social Media Icon Links
footer-menu
Customizable Social Media Icon Links
Ninguno
Publico
Todos
119
Buscar
position-0
Buscar
Ninguno
Publico
Todos
93
Menú principal
position-1
Menú
Todos
Publico
Todos
1
joombig banner auto slider
position-12
joombig banner auto slider
Solo en las seleccionadas
Publico
Todos
126
Slider Cursos
position-12
JE 3D SliceBox
Solo en las seleccionadas
Publico
Todos
132
Latest News +
position-15
Latest News +
Todos
Publico
Todos
135
Derecha
position-15
Menú
En todas excepto en las
Registrado
Todos
110


Duplicar
Publicar
Despublicar
Desbloquear
Papelera
Lote
Ayuda
Opciones
seleccionadas
Latest News +
position-15
Latest News +
Todos
Publico
Todos
135
Derecha
position-15
Menú
En todas excepto en las seleccionadas
Registrado
Todos
110
Breadcrumbs
position-2
Ruta de navegación
Todos
Publico
Todos
17
Módulo Imagen
position-3
Personalizado
Todos
Publico
Todos
92
menu del pie
position-32
Menú
Todos
Publico
Todos
129
Menú de Usuario
position-34
Menú
Todos
Publico
Todos
91
Visitors Counter
position-37
Visitors Counter
Todos
Publico
Todos
127
Últimas Noticias
position-7
Últimas novedades
Todos
Publico
Todos
90
Etiquetas populares
position-7
Etiquetas populares
Todos
Publico
Todos
87
Cursos Online
position-8
Anuncios
Todos
Publico
Todos
96
Hosting Joomla!
position-8
Anuncios
Todos
Publico
Todos
95
Pack 3.0 Joomla! Spanish
position-8
Anuncios
Todos
Publico
Todos
94