# UNIVERSIDAD ANDINA DEL CUSCO

**FACULTAD DE INGENIERÍA Y ARQUITECTURA**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

TESIS

# "VULNERABILIDADES INFORMÁTICAS EN EL PORTAL WEB DE LA UNIVERSIDAD ANDINA DEL CUSCO"

**Presentado por:**

**Bach. Edderson Jair Hernández Mechate.**

**Para optar al Título Profesional de**

**Ingeniero de Sistemas.**

**Asesor:**

**Mgt. Edwin Carrasco Poblete.**

**CUSCO - PERÚ**

**2020**

## Agradecimiento

A Dios, por permitirme realizar las cosas que día a día me trazo, y que cada vez que estoy por caer, me ayuda a levantarme e intentarlo de nuevo.

A mi abuela Epifania, a mis padres Jessica y Jorge, que fueron la principal inspiración y motor espiritual de mi vida.

A mi asesor Mg. Ing. Edwin Carrasco Poblete, por su orientación y disposición durante todo el proceso de trabajo de investigación.

Y a mis amigos que de alguna forma colaboraron y participaron en la ejecución de la presente. Les doy mi más extensivo y sincero agradecimiento.

Edderson Jair Hernández Mechate

## Dedicatoria

A mi abuela Epifania, mis padres Jorge y Jessica, mi tía Katherin, mis hermanas Angie y Jely, mi enamorada Paula y docentes de la universidad los cuales estaban atentos a cada etapa de este proyecto y me daban palabras de aliento y regaños en los momentos precisos. A todos ustedes muchas gracias.

A mi gran amigo que también pertenece al mundo de la ingeniería de sistemas que contribuyo con sus conocimientos en la presente investigación, Mgt. Ing. Mijhael Gamarra Morveli.

A los autores y sus libros correspondientes que me ayudaron como superación personal, tomando sus palabras y sucesos anecdóticos como ejemplo.

Edderson Jair Hernández Mechate

# Índice General

Pág.

# Índice de Tablas

# Índice de Figuras

## Resumen

El presente estudio se desarrolló teniendo como objeto de pruebas el portal Web de la Universidad Andina del Cusco (www.uandina.edu.pe); el punto de partida esta dado en la afirmación de que no se puede garantizar la seguridad o la estabilidad total de un sistema informático; es así que se desarrolló persiguiendo el objetivo de identificar vulnerabilidades informáticas mediante la aplicación de las herramientas de detección de vulnerabilidades en el portal Web de la Universidad Andina del Cusco. El diseño de investigación usado es experimental, de tipo descriptivo. Se aplicó para las pruebas de vulnerabilidad los programas informáticos Kali-Linux y Acunetix Web Vulnerability Scanner. La hipótesis principal afirma la existencia de vulnerabilidades en el portal Web; los resultados de los análisis realizados muestran que el portal Web de la Universidad Andina del Cusco presenta vulnerabilidades de nivel medio/alto, tanto en vulnerabilidades de diseño, implementación y uso; por lo que la hipótesis fue confirmada.


Palabras clave: sistema informático, vulnerabilidad, sitio Web, detección.

## Abstract

The present study was carried out with the purpose of testing the Web portal of the Andean University of Cusco (www.uandina.edu.pe); the starting point is given in the statement that the security or total stability of a computer system cannot be modified; This is how they are detected in order to identify computer vulnerabilities through the application of vulnerability detection tools in the Web portal of the Andean University of Cusco. The research design used is experimental, descriptive. The Kali-Linux and Acunetix Web Vulnerability Scanner software were applied for problem testing. The main hypothesis affirms the existence of vulnerabilities in the web portal; The results of the analyzes performed show the Web portal of the Andean University of Cusco presents medium / high level vulnerabilities, both in design, implementation and use vulnerabilities; So the hypothesis was confirmed.


Keywords: computer system, disability, website, detection.

# Capítulo I

# Aspectos Generales

## 1.1 Descripción de la Situación Actual

En sus inicios el internet solo brindaba lugares Web compactos en archivos de información comprendida en documentos irreversibles; se hicieron las páginas Web como manera de restauración y observación de información.

El movimiento de información se daba en una única dirección: del servidor al navegador; más actualmente la situación ha cambiado mucho debido a que las páginas Web modernas "tienen funciones relevantes dentro de un dominio, y dependen del movimiento de información en dos direcciones tanto del servidor al navegador como del navegador al servidor. Sosteniendo registro de inicio de sesión, transacciones financieras, búsqueda y todo tipo de información dependiendo del cliente" (Romaniz, S.F., págs. 1-2).

En lo contemporáneo el peligro para los sistemas informáticos ha incrementado dado que hay un aumento en la dificultad en las tecnologías de la información. En la actualidad cualquier tecnología conectada a la red está comprometida a distintos ataques. Un efecto es el crecimiento en la cantidad de ataques informáticos. La manera de evitar es proceder con anticipación, descubriendo las vulnerabilidades de mayor riesgo que pueden ser utilizadas por los hacker (Hernández Saucedo & Mejia Miranda, 2015).

Para Prevenir las vulnerabilidades informáticas se hace uso de auditorías de seguridad o hacking ético con el objetivo de comprobar y explorar vulnerabilidades en una red o sistema, poniendo a prueba los sistemas de seguridad existentes, para así poder subsanar los fallos encontrados antes de que sean aprovechados por un hacker (Martí Talón, 2016).

Actualmente la seguridad de la información es sumamente importante el cual debe de ser analizado, debido a las condiciones que se van transformando con el tiempo en

relación de las nuevas tecnologías, permitiendo establecer nuevos horizontes dando como resultado, la manifestación de nuevas ataques tecnológicos que pueden poner en peligro los activos de información (Pintado Cuji & Hurtado Valero, 2015).

Como dice Carbajal (Globalteksecurity, 2007, pág. 5) en el libro Tecnologías Globales para la seguridad de la Información, un sistema de información se considera seguro si: se encuentra libre de todo peligro y daño, pero esto es poco probable, porque es imposible dar garantía a la seguridad total de un sistema; he aquí una de las razones por las que surge investigar sobre las vulnerabilidades informáticas que pueden afectar el portal Web de la Universidad Andina del Cusco.

La Universidad Andina del Cusco (UAC) es una institución educativa referente tanto en la región como a nivel nacional por los grandes logros alcanzados a nivel académico, con la reciente acreditación institucional y de diversas escuelas profesionales con las que cuenta. En el año 2016 esta Universidad tenía un total de 16643 alumnos matriculados en pregrado, en sus 20 escuelas profesionales (Dirección de Planificación y Desarrollo Universitario, 2017, pág. 143).

La Universidad Andina del Cusco hace uso de las Tecnologías de Información y Comunicación (TIC) para la prestación del servicio educativo, tanto en sus procesos internos como a la hora de brindar información a sus estudiantes y otros grupos de interés. En los procesos internos tienen programas informáticos y sistemas como el ERP University (sistema integrado), Tempus (sistema de control para personal administrativo), SCA (sistemas de control docente y administrativo), entre otros. Asimismo, en cuanto a brindar información y acceso a ciertos servicios (sobre todo de consulta) cuenta con el portal Web cuyo dominio es www.uandina.edu.pe; donde acceden los más de 16000 estudiantes en algún momento. No solo es consulta de información sino también solicitada en diversos momentos de la prestación del servicio educativo. Dada la cantidad de usuarios que

interactúan con el portal Web y lo importante en la prestación del servicio educativo de la UAC, resulta útil realizar un diagnóstico de las posibles vulnerabilidades que podrían existir en portal Web; más aun sabiendo que durante el año 2017 se han reportado casos donde agentes desconocidos intentaron vulnerar la seguridad. Este dato fue brindado por la encargada de administrar el portal Web, en la Dirección de Tecnologías de Información de la Universidad Andina del Cusco (Universidad Andina del Cusco, 2017).

## 1.2 Formulación de Problemas

### 1.2.1 Problema general

- ¿Cuáles son las vulnerabilidades informáticas del portal Web de la Universidad Andina del Cusco?

### 1.2.2 Problemas específicos

- ¿Cuáles son las vulnerabilidades de diseño del portal Web de la Universidad Andina del Cusco?
- ¿Cuáles son las vulnerabilidades de implementación del portal Web de la Universidad Andina del Cusco?
- ¿Cuáles son las vulnerabilidades de uso del portal Web de la Universidad Andina del Cusco?

## 1.3 Justificación

### 1.3.1 Conveniencia

Debido a la cantidad de usuarios que tiene el portal Web de la Universidad Andina del Cusco, la abundante y delicada información que se maneja, además de ser soporte y portal de acceso a enlaces Web con los que cuenta esta institución, es conveniente realizar hacking ético.

### 1.3.2 Relevancia social

Las instituciones necesitan ofrecer y transmitir información rápida, confiable y aplicando en lo factible de conservar su información de forma segura, utilizando nuevas tecnologías que no muestren gastos económicos sino que contribuyan a un manejo de información reservado, favoreciendo a los estudiantes, profesores y administrativos que forman parte de la universidad.

### 1.3.3 Implicancias prácticas

El hacking ético es medio utilizado a nivel mundial para encontrar la existencia de vulnerabilidades en cualquier sistema, evaluarlas y determinar el grado de riesgo con respecto a la seguridad de la información, ofreciendo de esta manera posibles soluciones, ayudando a advertir al administrador de la red de un posible ataque.

### 1.3.4 Valor teórico

Los temas que se abordan se enfocaran de acuerdo al Sistema de Gestión de la Seguridad de la Información (SGSI) que es el conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

### 1.3.5 Utilidad metodológica

La utilidad metodológica de la investigación que se pretende realizar se da, debido a que se formuló un conjunto de pasos para evaluar el portal Web de la Universidad Andina del Cusco, con las características que tiene el objeto de

estudio. Este método podrá ser aplicado por otros investigadores que encuentren una problemática similar a la estudiada, en otros ámbitos académicos, utilizando las mismas herramientas.

## 1.4 Objetivos de Investigación

### 1.4.1 Objetivo general

- Identificar vulnerabilidades informáticas mediante la aplicación de las herramientas de detección de vulnerabilidades en el portal Web de la Universidad Andina del Cusco.

### 1.4.2 Objetivos específicos

- Identificar vulnerabilidades de diseño mediante la aplicación de las herramientas de detección de vulnerabilidades en el portal Web de la Universidad Andina del Cusco.
- Identificar vulnerabilidades de implementación mediante la aplicación de las herramientas de detección de vulnerabilidades en el portal Web de la Universidad Andina del Cusco.
- Identificar vulnerabilidades de uso mediante la aplicación de las herramientas de detección de vulnerabilidades en el portal Web de la Universidad Andina del Cusco.

## 1.5 Delimitación del Estudio

### 1.5.1 Delimitación espacial

Esta investigación se ejecutó en el dominio perteneciente al portal Web de la Universidad Andina del Cusco (www.uandina.edu.pe).

### 1.5.2 Delimitación temporal

El desarrollo de esta investigación se efectuó durante el tiempo comprendido de febrero del 2017 a abril del 2018.

# Capítulo II

# Marco Teórico

## 2.1 Antecedentes de la Investigación

**Título 1:** Diagnóstico de las vulnerabilidades informáticas en los sistemas de información para proponer soluciones a la rectificadora Gabriel Mosquera s.a.

**Autores:** Karen Andrea Pintado Cují y Cesar Luis Hurtado Valero

**Lugar:** Universidad Politécnica Salesiana Sede Guayaquil

**Año:** 2015

**Resumen:** En esta investigación se hace una evaluación de las vulnerabilidades informáticas en los sistemas informáticos para plantear soluciones de seguridad en la empresa Retigamos S.A. Las soluciones serán detalladas en la propuesta técnica que se realiza como resultado a los informes y estudios investigados, esta información fundamentada recolecta de forma notoria las políticas de seguridad y el cargo de conciencia de cada uno de los miembros en el desarrollo informático, así como las medidas y los métodos que puedan evitar, encontrar y responder a los riesgos actuales dentro de la empresa.

Siendo de suma importancia el resguardo de los sistemas que utilizan información frágil y delicada de la empresa Retigamos S.A, los miembros de la actual investigación pretenden realizar una evaluación de metodologías MSAT y OCTAVE –S. Se seleccionaron estas herramientas por lo que son elementales en las mejores prácticas de seguridad generalmente admitidas, es decir, estándares como las normas ISO 27001, 17799 y NIST-800.x. Estas metodologías son diseñadas específicamente para organizaciones menores a 100 trabajadores y que la red de datos tiene recursos limitados. (Pintado Cuji & Hurtado Valero, 2015)

**Conclusiones:**

- Se corrobora que los activos importantes más valiosos para el desarrollo de negocio de la empresa son el sistema contable, exportaciones, servidor de base de datos y correo electrónico.
- Se precisa que la información evidente que utiliza la empresa, son los datos que se realizan en el sistema contable, correos electrónicos y los documentos de clientes y proveedores.
- Se extrajo una lista de los activos valiosos de Retigamos S.A, desde el punto de vista real de la empresa para confrontar a cada una de las áreas de práctica de seguridad y un perfil de riesgo para cada activo crítico.
- La realización de perfiles de amenaza hace posible tener una idea clara de posibles circunstancias dentro de los cuales los activos críticos podrían estar expuestos.
- Se establece que las áreas más notables, y que requieren un diseño de seguridad con suma urgencia son las áreas de gerencia, contabilidad y taller.
- El diseño de seguridad sirve para realizar una base que prevenga posibles riesgos a posteriores ataques. La herramienta emplea la experiencia del equipo de análisis, y los riesgos de ataques anteriores, para precisar la probabilidad de que una amenaza pueda acontecer y establecer los correctivos necesarios.
- Una financiación externa sería precisa para ejecutar la implementación del plan de seguridad y asegurar la continua gestión sobre el cumplimiento de los planes establecidos y la actualización permanente sobre los mismos.
- La compresión y comunicación entre los integrantes del equipo de análisis es muy importante para realizar la evaluación de una manera adecuada y ordenada.

**Título 2:** Análisis de vulnerabilidades esteganográficas en protocolos de comunicación IP y HTTP

**Autor:** Pablo Andrés Deymonnaz

**Lugar:** Universidad de Buenos Aires

**Año:** 2012

**Resumen:** En este trabajo de investigación se indaga la esteganografía, comprendida como la técnica de comunicar mensajes entre dos puntos, de modo que la comunicación pase desprevenida por quienes tengan permiso al canal de comunicación.

El objetivo primordial de la investigación se basa en el estudio detallado de los protocolos de comunicación IP y HTTP para detectar aplicaciones de técnicas esteganográficas sobre los mismos. Se comprende por técnica esteganográfica sobre un protocolo a cada una de las interpretaciones o modificaciones que se coloca a un mensaje del protocolo que permita comunicar un mensaje de manera inadvertida, fuera de las reglas del protocolo. A la posibilidad de aplicación de esas técnicas sobre los protocolos se las denominará "vulnerabilidades esteganográficas" de los protocolos. (Deymonnaz, 2012)

**Conclusiones:**

- Se da perfección a un dispositivo de comunicación esteganográfica que incluye algunas de las técnicas estudiadas sobre ambos protocolos. Se ha desarrollado un guardián activo para prevenir la transmisión de los mensajes esteganográficos con las técnicas establecidas y se han presentado los resultados de las pruebas efectuadas.
- La realización del artefacto pudo inspeccionar la factibilidad de la aplicación de las técnicas establecidas para la comunicación esteganográfica. Al mismo tiempo, la elaboración del guardián activo pudo prevenir la aplicación de las técnicas puestas

en funcionamiento. Se visualizó que, en todas las pruebas, las comunicaciones basadas en los protocolos funcionaron adecuadamente.

- Mientras se hizo los análisis a los protocolos de comunicación se ha observado que las vulnerabilidades esteganográficas presentes en ellos contestan principalmente a ambigüedades, vaguedades o libertades en las especificaciones de los mismos.
- El principal desafío que presenta el análisis de vulnerabilidades esteganográficas, está en que las técnicas utilizadas para la unión de mensajes dentro de portadores son ad hoc, es decir, específicas del protocolo y de cada una de sus definiciones.

El aporte que da los antecedentes mencionas son: el primer antecedente ayuda en lo que es la elaboración de los informes, así como las medidas y los métodos que pueden evitar, encontrar y responder a las vulnerabilidades encontradas. El manejo de algunas herramientas de hacking ético, analizando las vulnerabilidades informáticas para prevenir algunos ataques. El segundo antecedente ayuda a prevenir vulnerabilidades informáticas que se presentan en los protocolos de comunicación IP y HTTP.

## 2.2 Bases Teóricas

### 2.2.1 BuiltWith

BuiltWith es un recurso integral de tecnologías que la web ha estado utilizando desde el 2010, permitiendo introducir una URL y dando como resultado información acerca de la infraestructura con la que ha sido diseñada una página web.

BuiltWith te permite saber qué servidor web utilizan, qué gestor de contenidos (puedes saber incluso la versión que utilizan y la plantilla), el framework, los certificados SSL, el proveedor de hosting, el sistema de analytics y rendimiento web, librerías de javascript, plugins, librerías de media Query, entre otras cosas más.

El objetivo de BuiltWith es ayudar a los desarrolladores web, investigadores y diseñadores a rastrear qué tecnologías están utilizando otros sitios web, lo que puede ayudarlos para decidir qué tecnologías implementar ellos mismos. (Built With, 2008)

### 2.2.2 Universidad Andina del Cusco

La Universidad Andina del Cusco (UAC) es una de las instituciones educativas referentes en el medio regional y nacional por los grandes logros alcanzados a nivel académico, como la reciente acreditación institucional y de diversas escuelas profesionales con las que cuenta. En el año 2016 esta Universidad tenía un total de 16643 alumnos matriculados en pregrado, en sus 20 escuelas profesionales (Dirección de Planificación y Desarrollo Universitario, 2017, pág. 143).

La Universidad Andina del Cusco hace uso de la TIC's para la prestación del servicio educativo, tanto en sus procesos internos como a la hora de brindar información a sus estudiantes y otros grupos de interés. En los procesos internos tienen programas informáticos y sistemas como el ERP University (sistema integrado), Tempus (sistema de control para personal administrativo), SCA (sistemas de control docente y administrativo), entre otros. Asimismo, en cuanto a brindar información y acceso a ciertos servicios (sobre todo de consulta) cuenta con el portal Web cuyo dominio es www.uandina.edu.pe; donde acceden los más de 16000 estudiantes en algún momento. No solo es consulta de información sino también solicitada en diversos momentos de la prestación del servicio educativo (Universidad Andina del Cusco, 2017).

Prosiguiendo con la descripción se mostrara información que contiene el portal Web de la Universidad Andina del Cusco utilizando la herramienta BuiltWith:

Al utilizar la herramienta BuiltWith, se da a conocer la información general actual del portal Web de la Universidad Andina del Cusco cuya URL es www.uandina.edu.pe, de los cuales se mencionó solo la información más relevante:


*Figura 1.* Contenido analítico y rastreo.
**Fuente:** Contenido de la página BuiltWith uandina.edu.pe.

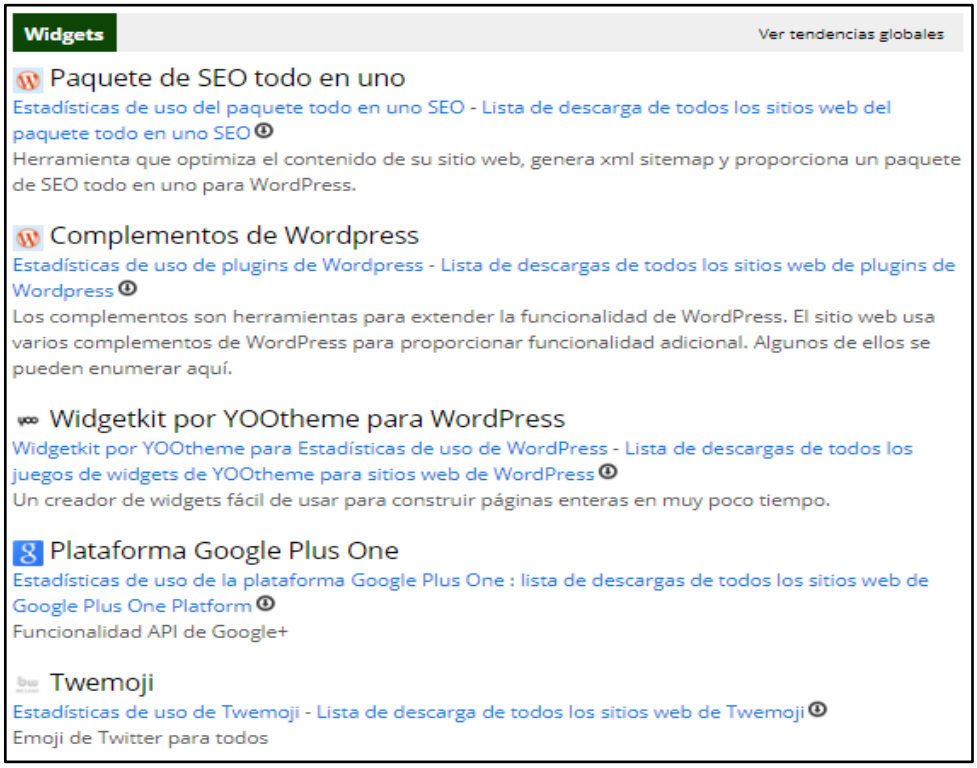



*Figura 2.* Contenido de widgets.
**Fuente:** Contenido de la página BuiltWith uandina.edu.pe.

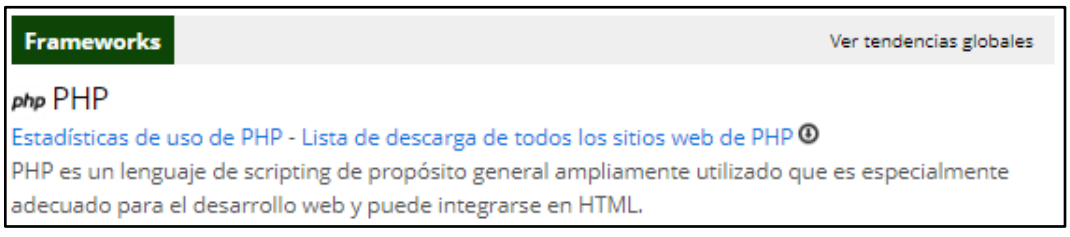



*Figura 3.* Contenido de frameworks.
**Fuente:** Contenido de la página BuiltWith uandina.edu.pe.

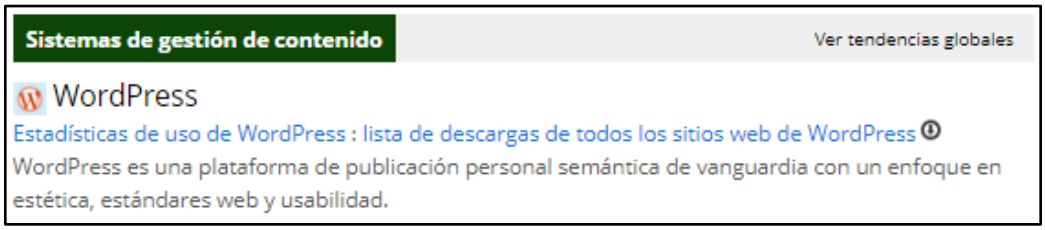



*Figura 4.* Contenido de sistema de gestión de contenido.
**Fuente:** Contenido de la página BuiltWith uandina.edu.pe.


*Figura 5.* Contenido de biblioteca javascript.
**Fuente:** Contenido de la página BuiltWith uandina.edu.pe.

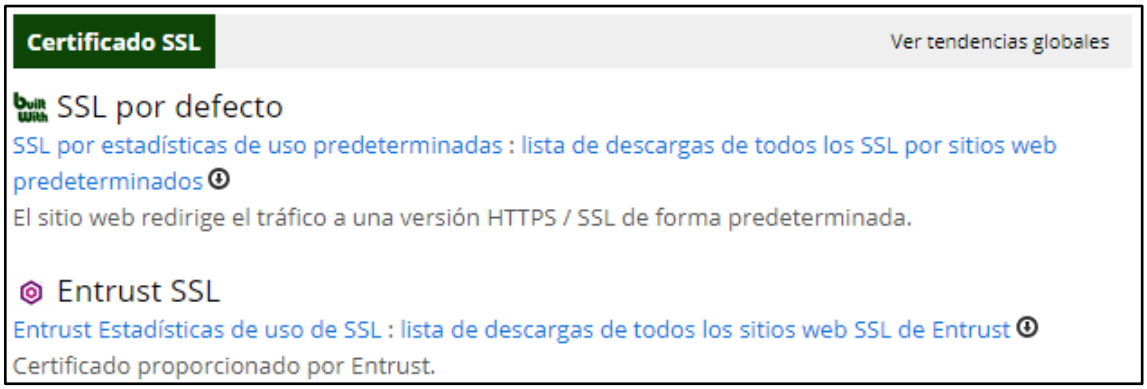



*Figura 6.* Contenido de certificado SSL.
**Fuente:** Contenido de la página BuiltWith uandina.edu.pe.

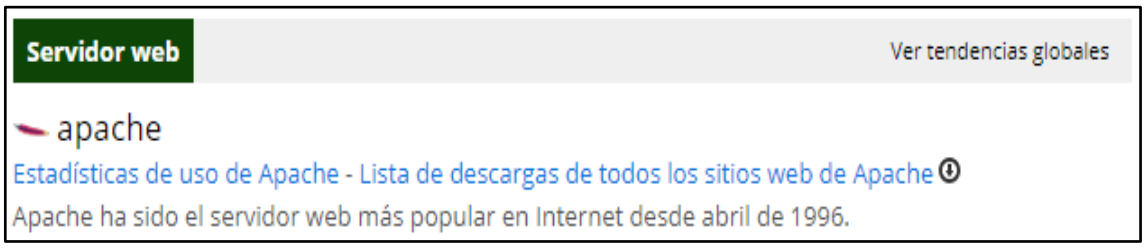



*Figura 7.* Contenido del servidor Web.
**Fuente:** Contenido de la página BuiltWith uandina.edu.pe.

La Universidad Andina del Cusco cuenta con el protocolo HTTPS. Este protocolo es más confiable y apropiado para poder ingresar a las páginas que provee Internet, ya que al insertar cualquier dato o información será cifrado, lo que da garantía que no podrá visualizarse por nadie más que el cliente y el servidor; haciendo posible de esta forma que no sea mal utilizada; puesto que el que intente visualizar el contenido sólo encontrará datos que no podrá descifrar. La desventaja de utilizar https es la rapidez para mostrar los datos es un poco lenta, esto se debe a que la labor de cifrado y descifrado que hace con los datos genera un mayor consumo de banda.

La Universidad Andina del Cusco cuenta con el sistema de gestión de contenido WordPress y Widgets a WordPress, utiliza el lenguaje de programación PHP, servidor Apache HTTP SERVER, protocolo HTTPS, entre otras cosas más.

### 2.2.3 Tecnologías de información y comunicación

Para (Cabero, 1998) las TIC: Se podría mencionar que las recientes tecnologías de la información y comunicación se centran relacionadas a tres recursos básicos: la informática, la microelectrónica y las telecomunicaciones; pero estas no solo se encuentran de manera separada, sino que se encuentran de manera mutuamente conectadas, lo que posibilita lograr nuevas formas de comunicación.

Las características que representan a las TIC son:

a) Inmaterialidad: Se puede mencionar que las TIC ejecutan la elaboración, el desarrollo y la comunicación de la información. Esta información es simplemente intangible y puede ser dirigida de forma clara.

b) Interactividad: Es probablemente la cualidad más fundamental de las TIC para su utilidad en el campo pedagógico. Por medio de las TIC se obtiene intercambiar información entre el usuario y la computadora. Estas cualidades permiten acomodar los bienes utilizados a las necesidades de las personas.

c) Interconexión: hace referencia a la elaboración de nuevos medios tecnológicos comenzando de la relación entre dos tecnologías.

d) Instantaneidad: Las TIC, ha dado posibilidad al uso de servicios permitiendo la comunicación y transmisión de la información, entre sitios apartados físicamente, de una forma dinámica.

e) Altos parámetros en la calidad de imagen y de sonido: El desarrollo y transferencia de la información comprende diverso tipo de información: textos, imágenes y sonidos, por lo que los progresos han ido encaminándose a alcanzar transferencias multimedia de gran importancia, siendo simplificado por la técnica de digitalización.

f) Digitalización: Su finalidad es que la información de diverso tipo (sonido, texto, imagen, animación, entre otros) puedan ser transferida por el mismo canal al estar manifestada en un formato exclusivo universal.

g) Elevada Influencia en los procesos que en los productos: Es factible que al utilizar las diversas aplicaciones de la TIC muestren un dominio sobre los desarrollos mentales que ejecutan los usuarios para adquirir conocimientos, más que los propios conocimientos obtenidos. En los diversos análisis efectuados, sobre la sociedad de la información, se destaca el valor excesivo de la incontable información a la que se puede tener acceso en Internet. Aunque, como otros muchos indican, los medios que ofrecen las TIC presumen un cambio cualitativo en el desarrollo más que en los productos. Estas dos magnitudes esenciales son las que presumen transformaciones cuantitativas y cualitativas en los desarrollos propios y de educación al emplear las TIC.

h) Penetración en todos los sectores (cultural, económico, educativo, industrial, entre otros): La impresión de las TIC no se manifiesta de forma única en un individuo, grupo, sector o país, sino que, se amplía a la agrupación de las sociedades del planeta.

i) Innovación: Las TIC están realizando, innovación y cambios periódicos en todos los entornos sociales. Pero, es de replicar que estas transformaciones no siempre indican resistencia a las tecnologías o medios, sino que en algunos casos se realiza una clase de fusión con otros medios.

j) Tendencia hacia automatización: Las dificultades conllevan a manifestar distintas posibilidades y herramientas que accedan a un manejo simplificado de la información en diferentes diligencias personales, de profesión y social. La

obligación de tener información estructurada hace que incrementen gestores personales o corporativos con diversas finalidades.

k) Diversidad: Los beneficios de las tecnologías puede ser muy diversos, desde la comunicación entre usuarios, hasta el desarrollo de la información para hacer informaciones nuevas.

Se podría definir TIC como: Tecnologías para almacenar, recuperar, procesar y comunicar la información.

Hay diversas herramientas electrónicas que encajan dentro del concepto de TIC, la tv, el móvil, los videos, la computadora. Pero sin lugar a duda, los bienes más característicos de la presente sociedad son las computadoras que hacen posible probar distintas aplicaciones informáticas y propiamente dichas las redes de comunicación, en pocas palabras, Internet.

### 2.2.4 Desarrolladores Web

Los Desarrolladores Web diseñan, crean y realizan mantenimiento a páginas y aplicaciones web, en tal sentido, trabajan en sitios de internet y de intranet. Por lo general, son empleados por empresas especializadas en el desarrollo de programas especializados o en consultoría informática. Estos profesionales tienen la opción de trabajar directamente para la corporación o de manera independiente o a destajo.

La mayoría de los Desarrolladores Web trabajan en el software, en la base de datos o en la codificación de un sitio web. Por otro lado, hay otros quienes lidian con el diseño y la interfaz de la página. Sin embargo, hay expertos del área con la capacidad de asumir los aspectos antes descritos, ofreciendo un servicio más completo, conocidos como Desarrolladores Full Stack.

Un desarrollador web se divide en tres tipos principales de desarrolladores, los cuales son front-end, back-end y full-stack. Los desarrolladores front-end son responsables por las partes del sitio web que las personas ven e interactúan, los desarrolladores back-end se encargar por el

código detrás de escenas que controla cómo carga y se ejecuta un sitio web, y los desarrolladores full-stack hacen un poco de todo.

Un desarrollador front-end es alguien que toma el diseño de un website de un cliente o un equipo de diseño y escribe el código necesario para implementarlo en la web. Un buen desarrollador web front-end sería competente en al menos tres lenguajes de programación – HTML, CSS, y JavaScript.

HTML les permite añadir contenido al sitio web y dividirlo en titulares, párrafos y tablas. CSS le permite al buen desarrollador estilizar el contenido y cambiar cosas como colores, tamaños y bordes. JavaScript permite añadir elementos interactivos, así como botones pulsadores.

Los desarrolladores back-end se ocupan del lado del servidor, esto significa que tienen que crear el código y los programas que impulsan el servidor de la página web, las bases de datos y cualquier aplicación que contenga. La función más importante de un desarrollador back-end es la habilidad de crear código limpio y eficiente que haga lo que se requiere de la manera más rápida posible. Como la velocidad de un sitio web es un aspecto fundamental cuando se trata de optimización en motores de búsqueda (SEO), es un factor importante en el desarrollo back-end.

Los desarrolladores back-end utilizan una amplia y distinta variedad de lenguajes del lado del servidor para crear programas complejos. Algunos de los programas más populares incluyen PHP, Python, Java, y Ruby. JavaScript se está difundiendo cada vez más como un lenguaje de desarrollo back-end, mientras que SQL se usa generalmente para la gestión y análisis de datos en bases de datos de páginas web.

Un desarrollador back-end debe ser flexible, capaz de crear programas diferentes, y deben tener un entendimiento claro y profundo de los lenguajes que utilizan. Es muy importante que se aseguren que pueden ejecutar el método más eficiente al crear el programa requerido, asimismo cerciorarse que es seguro, escalable y fácil de mantener.

Los desarrolladores full-stack utilizan tanto estrategias front-end como back-end y procesos, lo que significa que están perfectamente situados para supervisar el proceso completo.

En el caso de páginas web sencillas que no cuentan con un gran presupuesto para su desarrollo, un desarrollador full-stack será generalmente contratado para crear el sitio web por completo. En este caso, es extremadamente importante para ellos tener un entendimiento completo y profundo tanto de desarrollo front-end como back-end y cómo funcionan. (bitdegree.org, 2019)

### 2.2.5 Páginas Web

World Wide Web (WWW): Es el medio de descripción de la información más empleado en Internet. Sus importantes características son:

- **Hipertexto**: Es un escrito o figura que se presentan en pantallas relacionadas en diferentes páginas del propio sitio o de sitios extraños.
- **Multimedia**: En las páginas muestran texto, imágenes, videos, audios, animaciones, etc.
- **Universalidad**: Se puede ingresar desde distintos equipos con cualquier sistema operativo (Windows, Linux, Mac), utilizando diferentes navegadores y en cualquier parte del mundo.
- **Pública**: La información está dividida en miles de servidores que brindan un lugar para guardarla. La información es pública y comúnmente disponible para distintos usuarios.
- **Dinámica**: Demasiada información, y así este guardada, se puede actualizar por el público que la consulte sin que el usuario necesite saber detalles técnicos de su mantenimiento.
- **Navegador**: Es el programa que se emplea para ingresar a los contenidos de Internet. Debe de estar apto para comunicarse con un servidor y entender el lenguaje de todas las herramientas que utiliza la información de Web.

- **Servidor**: Es el computador encargado de ofrecer al navegador los documentos y medios que requiere, para que puedan ser utilizados.
- **HTTP (HyperText Transfer Protocol):** Es el reglamento de comunicación empleado para notificar las solicitudes y documentos por medio de Internet entre el servidor y el navegador.
- **URL (Universal Resource Locator):** Es la dirección donde se ubica una petición en Internet.

Una página Web, en el transcurso de navegación por Internet, sigue el siguiente proceso: el usuario, puesto en el equipo cliente, teclea la URL en la casilla la dirección del navegador y presiona la tecla Enter; la solicitud se direcciona a los servidores DNS que transforman esta URL a una dirección IP. Por ejemplo: www.uandina.edu.pe -> 190.119.204.68. Es factible poner en la casilla del navegador esta dirección IP aunque sea más compleja. Luego, la solicitud llega al servidor que tiene esa IP; el servidor muestra la página solicitada, el archivo HTML y los multimedia referenciados se guardan en la carpeta caché del navegador. Cuando se han descargado estos archivos, el usuario puede ver la página y sus elementos.

#### *2.2.5.1 HTML (HyperText Markup Language)*

Es el lenguaje de diseño de las páginas y que se observan por medio del navegador. Este lenguaje está basado en etiquetas y atributos. Una página HTML implica texto en formato real y relaciones a archivos externos abarcando imágenes, sonidos, animaciones, etcétera. El archivo HTML se emplea para detallar información que se observara a través del navegador. Esta información se almacena en un documento con extensión HTM o HTML. Fundamentalmente la información escrita en HTML está compuesta de texto y etiquetas. Las etiquetas autorizan para determinar el formato del texto, el título que se

exhibirá en la barra de título del navegador, los componentes multimedia que se mostrarán introducidos en el documento pero se guardan en archivos externos, etc.

Las aplicaciones Web acarrean nuevos y relevantes ataques en la seguridad, por lo que cada aplicación es distinta y puede incluir vulnerabilidades exclusivas; muchas de las aplicaciones son realizadas y mantenidas por equipos internos y, en muchos ocasiones, por desarrolladores que poseen limitado conocimiento respecto de los problemas de seguridad que pueden aparecer en el código que están elaborando (Romaniz, S.F., págs. 1-2).

a) Funcionalidades comunes de un servidor Web: Las aplicaciones Web han sido elaboradas para realizar casi todas las funciones posibles en línea. Además, han sido ampliamente aceptadas por las organizaciones para efectuar funciones internas permanentes. Y regularmente se las emplea para ofrecer una interfaz de administración en los dispositivos de hardware y software. (Romaniz, S.F., pág. 2)

b) Beneficios de las aplicaciones Web: Son muchos los componentes técnicos y comerciales que contribuyen en la manera de cómo usar la Internet: HTTP, el protocolo de comunicaciones central para tener acceso al World Wide Web, es ligero y sin conexión; pone resistencia en la comunicación en caso de fallos y previene que el servidor mantenga en apertura una conexión de red para cada cliente; además, HTTP puede ser proxeado y tunelizado con otros protocolos, realizando una comunicación certera en distintas configuraciones divididas; todos los clientes Web ya tienen un navegador instalado por defecto en su trabajo; las aplicaciones Web extienden su interface de usuario dinámicamente dentro del entorno del navegador, previniendo así la necesidad de dividir y de ejecutar un elemento de software (cliente); las transformaciones puestas en la interfaz sólo deben ser ejecutados una vez, en el servidor, teniendo efecto de forma instantánea; los navegadores vigentes contienen múltiples funcionalidades, facilitando la elaboración de interfaces de usuario ricas y satisfactorias; las interfaces Web emplean métodos de

navegación y estándares de control de acceso, previniendo la necesidad de estudiar cómo se ejecutan las aplicaciones particulares; el método de scripting del lado del usuario hace posible que las aplicaciones desplacen parte de su procesamiento hacia el lado del cliente, y las virtudes de los navegadores se pueden ampliar de manera parcial usando componentes del cliente donde resulte necesario; las tecnologías y los lenguajes fundamentales empleados para desarrollar aplicaciones Web son referentemente sencillo; comprende un extenso rango de plataformas y herramientas de desarrollo que hacen más fácil la elaboración de aplicaciones de elevada efectividad por parte de desarrolladores de poca experiencia, y se puede ingresar a una valiosa cantidad de código fuente abierto y otros recursos para su integración en aplicaciones desarrolladas a medida. (Romaniz, S.F., pág. 2)

#### *2.2.5.2 Entradas GET y POST*

La definición GET es conseguir información del servidor. Adquirir datos que están en el servidor, siendo archivos o una base de datos del usuario. Imparcialmente de que para eso se tenga que mandar algún dato que será procesado para luego retornar la respuesta esperada.

POST en cambio manda información desde el usuario para que sea procesada y actualizada o se añada información en el servidor. Cuando se mandan datos a través de un formulario, estos son procesados y luego retornar información.

#### *2.2.5.3 Enlaces Rotos*

Un enlace roto es un término informal que hace referencia cuando un sitio Web ya no está disponible en Internet pero si almacenado en los servidores. En ocasiones, también se anuncia a los enlaces que han sido cambiados a otros servidores; de esta manera cuando un enlace está desactualizado se le conoce como un vínculo roto.

### 2.2.6 WordPress

WordPress es un sistema de gestión de contenidos (CMS) que hace posible crear y diseñar un blog u otro tipo de Web.

Con amplia experiencia y más de un millar de temas plantillas disponibles en su Web publica, no solo es un sistema fácil e interactivo para elaborar un blog personal, también permite desarrollar toda clase de Web más complicadas.

WordPress es un sistema idóneo para un sitio Web que este en constante actualización. Si se redacta contenido con frecuentemente, cuando alguien ingresa al sitio Web, puede descubrir todos esos contenidos ordenados progresivamente.

WordPress tiene un sistema de plugins, que hace posible extender las capacidades de WordPress, de esa forma se consigue un CMS más manejable.

Inicialmente WordPress fue desarrollado para que funcione como un blog. Con el pasar de los tiempos se trasformó en el gestor de blogs por excelencia y a día de hoy con WordPress se puede desarrollar cientos de proyectos diversos. Entre lo más comunes se encuentran: (webempresa, 2016)

- Blog. Esta es su principal función y es por la que ganó su popularidad. Ofrece funciones típicas de un blog como listar artículos, categorizar y etiquetar los artículos, gestión de comentarios entre otras.
- Página Web. Mediante WordPress se pueden crear páginas Web corporativas, sin tener que ser un blog, con la cual ofrecer productos y servicios de manera estática.
- Tienda online. Existen otros gestores de contenido especializados 100% en el desarrollo de tiendas online pero la ventaja de usar WordPress es la sencillez y la funcionalidad que ofrece en comparación con otros gestores de contenido.

A diferencia de otros gestores, con WordPress se tiene todo en uno; es decir, una página Web que además incluya un blog y un carrito de compras mediante una única instalación y en el mismo dominio, cosa que no ofrecen la mayoría del resto de gestores.

Además de estas funciones, WordPress ofrece la posibilidad de crear páginas de reservas de hoteles y viajes, periódicos digitales, foros mediante bbPress, plataformas de eLearning (como Moodle) y una plataforma del tipo red social mediante BudyPress entre otras.

Un proyecto en WordPress puede ser creado en 2 plataformas diferentes y esto se presta a la confusión de muchos usuarios con frecuencia:

- **Wordpress.com**: mediante esta plataforma, se pueden crear blogs y páginas Web en WordPress que se suelen diferenciar por un subdominio. Esta plataforma ofrece un servicio gratuito (con subdominio) y servicios PREMIUM en los que puedes registrar un dominio, instalar plantillas y plugins entre otros aunque su principal desventaja es que tiene muchas limitaciones ya que dependes al 100% de lo que la plataforma te permita hacer.

  Ventajas:

  - Es gratis
  - Es fácil de usar y tiene poca complejidad.

  Desventajas:

  - El cliente no tiene disposición de su propio dominio Web, sino que escoge un subdominio dentro de la plataforma de WordPress.com, con las restricciones que ello soporta.
  - Inasequible de incluir anuncios en la Web para generar dinero en el blog.

- Poca facultad de personalizar los diseños, lo que en ocasión causa una imagen menos profesional del sitio Web, por lo que no es recomendable para páginas de empresas.

– **Wordpress.org**: Accediendo a wordpress.org, se puede descargar el paquete básico de instalación de WordPress mediante el cual podemos crear con libertad cualquier tipo de proyecto sin depender de ninguna otra plataforma.

Ventajas:

- Es muy escalable: esto se refiere que este CMS es completamente útil para pequeños sitios Web personales, pequeñas empresas o profesionales, sin embargo puede desarrollarse en paralelo con dicha Web hasta obtener una magnitud realmente grande. No solo permite agregar muchas funciones, sino también determinar una estructura de usuarios jerarquizada mediante un sistema de permisos bien definido que va desde el administrador primordial hasta el más esencial de los editores.
- Es de código abierto: cualquier cliente puede colaborar a la elaboración de WordPress con sus adecuadas contribuciones.
- Gran variedad de diseños: hay muchos diseñadores individuales o las agencias de diseño que elaboran su propia plantilla y pueden utilizar del resto de clientes, algunas gratuitas u otras de pago.
- Numerosos plugins: los plugins son herramientas elaboradas por desarrolladores externos que ingresan a un sitio Web de WordPress para adjuntar una nueva funcionalidad o mejorar una existente.
- Panel de control amplio: elaborar y administrar nuevas páginas, menús, categorías o cualquier otro detalle de la Web es verdaderamente sencillo desde el panel de control. Además, tiene funcionamiento en la Nube, por lo que se

puede ingresar desde un navegador en cualquier parte y con cualquier dispositivo.

- CMS mobile friendly: tanto el panel de control para la ejecución del contenido como la mayoría de los diseños útiles en WordPress son responsive, esto quiere decir, que se visualizan perfectamente en cualquier tipo de dispositivo, algo cada vez más importante en la actualidad.
- Soporte técnico: con respecto a WordPress existe una amplia comunidad de desarrolladores capacitados para asistir a otros clientes a solucionar problemas correspondientes con la plataforma. En algunos casos son ayudas gratuitas mediante foros de discusión, pero otras veces se pueden contratar servicios particulares de soporte para dar soluciones a problemas concretos.
- Comportamiento SEO: el código HTML es transparente y comprensible para los motores de búsqueda, primordialmente de Google, por lo que si se trabaja de forma adecuada en el contenido, al registrar y posicionar en los buscadores se tendrá grandes posibilidades de éxito.
- Actualizaciones: WordPress cambia constantemente con las actualizaciones, lo que hace posible solucionar errores o defectos de todo tipo.

Desventajas:

- Flexibilidad de diseño limitada: aunque haya variedad de plantillas, si se busca un diseño totalmente a medida, será necesario contratar los servicios de un diseñador Web, al que se le podrá decir las ideas para que pueda elaborar una Web cien por ciento a medida.

### 2.2.7 Hacking ético

Se define a través de lo que hacen los profesionales que se dedican a ello, es decir, los piratas informáticos éticos. Estas personas son contratadas para hackear un sistema e identificar y

reparar posibles vulnerabilidades, lo que previene eficazmente la explotación por hackers maliciosos. Son expertos que se especializan en las pruebas de penetración de sistemas informáticos y de software con el fin de evaluar, fortalecer y mejorar la seguridad.

Este tipo de pirata informático a menudo se denomina como hacker de 'sombrero blanco' (White hat), con el fin de diferenciarlos de los piratas informáticos criminales, que se conocen como hackers de 'sombrero negro'.

Una de las armas más poderosas en la lucha contra los ciber delincuentes ha sido la de los piratas informáticos. Los profesionales con un profundo conocimiento de cómo penetrar en la seguridad de una infraestructura en línea se implementan comúnmente para encontrar vulnerabilidades que aquellos del otro lado del espectro de piratería moral buscarían explotar.

Dentro de la comunidad de seguridad cibernética, los piratas informáticos se dividen en tres campos: piratas informáticos 'sombrero negro' y 'sombrero blanco'.

Los sombreros negros piratean sus objetivos por razones egoístas, como ganancias financieras, para vengarse o simplemente para causar estragos.

Los piratas informáticos de sombrero blanco, en cambio, apuntan a mejorar la seguridad, encontrar agujeros en ella y notificar a la víctima para que tenga la oportunidad de arreglarlos antes de que un hacker menos escrupuloso los explote.

La forma que utilizan estos profesionales para ganar dinero también explica qué es el hacking ético. Los que lo practican, con bastante frecuencia son empleados por las compañías de seguridad cibernética, o dentro de los departamentos de seguridad de las organizaciones más grandes. El hecho de que ellos sepan cómo operan los atacantes, a menudo les da una valiosa perspectiva sobre cómo prevenir los ataques.

Otra forma con la que los hackers éticos pueden ganarse la vida es mediante la recopilación de "recompensas de errores". Las grandes empresas, en particular las de tecnología como Facebook, Microsoft y Google, ofrecen una recompensa a los investigadores o hackers que descubren agujeros de seguridad dentro de sus redes o servicios.

Por otro lado, los piratas informáticos de los hackers negros en general ganan su dinero a través del robo, el fraude, la extorsión y otros medios nefastos.

En conclusión el hacking ético nace como medida para combatir a los piratas informáticos con malas intenciones. Las empresas contratan a estos profesionales porque necesitan probar su seguridad. Al otorgar su permiso, efectivamente cubren sus ojos y oídos corporativos mientras se llevan a cabo estas pruebas. (Tecnologias paralos negocios, 2016)

### 2.2.8 Vulnerabilidades en aplicaciones Web

La Vulnerabilidad es una falla de distinto tipo que afecta la seguridad del sistema informático.

Las vulnerabilidades de los sistemas informáticos (SI) se pueden asociar en función al: Diseño, implementación y uso.

La sociedad de seguridad regularmente admite vulnerabilidades de diseño como deficiencias en la estructura del software y datos característicos, se pueden encontrar en las estipulaciones de la etapa de análisis o en la preparación de la etapa de diseño. En la etapa de vulnerabilidades de implementación se relaciona a fallos de seguridad perpetuados por los creadores cuando están elaborando los módulos u elementos del sistema para efectuar con sus diferencias. La etapa de vulnerabilidad de uso hace referencia a los fallos que aparecen en la demostración y la conformación del sistema en un medio exclusivo (Universidad Internacional de la Rioja , 2015).

#### *2.2.8.1 Ataques de vulnerabilidad de diseño*

- Ataque de hombre en medio: El hacker imposibilita la comunicación entre dos hosts, remplazando la identidad de cualquiera de ellos.
- Ataque de condiciones de carrera: Se puede dar en una ocasión muy diminuta, para que un hacker sustituya el documento original encontrado por otro documento.

- Ataque con sniffer: Un sniffer toma los paquetes del tráfico de la red con la finalidad de adquirir nombres de usuario y passwords que se transfieren en clave. (Universidad Internacional de la Rioja , 2015)

#### *2.2.8.2 Ataques de vulnerabilidad de implementación*

- Ataque de buffer overflow: No examinar el tamaño del área de ingreso de una aplicación puede generar un incremento en la memoria y direccionar la ejecución de código maligno que puede incluirse en los datos que ingresan.
- Ataque de inyección de SQL: Son muy frecuentes en aplicaciones Web, emplean la categoría de vulnerabilidades de entradas anuladas y logran obtener o incluso eliminar información de la base de datos cambiando el código de la consulta, porque el área de ingreso no se ha autentificado y no tienen diferencia las palabras clave que forman parte de la consulta SQL de lo que son solamente datos de entrada.
- Ataques de puerta-atrás: Hay que instituir un conveniente procedimiento de seguridad de calidad de código que imposibilite que un hacker malintencionado escriba código que permita pasar por alto el control de entrada. (Universidad Internacional de la Rioja , 2015)

#### *2.2.8.3 Ataques de vulnerabilidad de uso*

- Ataques de denegación de servicio: Un sistema, un equipo o una red se pueden ver dañados por múltiples solicitudes de servicio, teniendo como ejemplo las solicitudes de conexión telnet, ftp, http. Las constantes solicitudes que transcurren en un tiempo dado, gastan la memoria y con cada intento de conexión puede llegar a la caída del sistema.
- Ataque aprovechando configuraciones por defecto: en un inicio cuando se instalan sistemas operativos, servicios o aplicaciones hay que eliminar las cuentas de

usuario por defecto, servicios como servidores web, conmutadores, servidores ftp, etc.

- Ataque por descubrimiento de contraseñas: Debido a las defectuosas preferencias de los passwords y por emplear programas que manejan notaciones y repertorios que acaban por crackear los passwords almacenados. (Universidad Internacional de la Rioja , 2015)

Las aplicaciones Web presentan distintos ataques que tienen de acuerdo a los servicios que ofrecen. De acuerdo con la OWASP (Open Web Application Security Project), los ataques en aplicaciones Web más empleados al concluir el año 2009, fueron las siguientes:

- Cross Site Scripting (XSS).
- Ataques de inyección de código.
- Ejecución de archivos maliciosos.
- Ataques Cross Site Request Forgery (CSRF).
- Robo de identidad de autenticación.
- Almacenamiento criptográfico inseguro.
- Acceso a URLs ocultas no restringidas de manera adecuada.

El sitio del Departamento de Seguridad en Cómputo de la UNAM nombra en su lista de ataques más comunes a las siguientes:

- Cross Site Scripting (XSS).
- SQL Injection.
- Buffer Overflow.

Se considera que, en las precedentes listas, los ataques en aplicación Web en común es el ataque Cross Site Scripting (XSS). (Castro Jaime & Hernández Muñoz, 2012)

Para este trabajo de investigación se estudiaron los ataques en aplicaciones Web más frecuentes porque representan riesgo tanto para los servidores Web, como para las bases de datos del portal Web de la Universidad Andina del Cusco.

a) **XSS (Cross Site Scripting):** hace referencia al ataque de inyección de código por parte del cliente en el que un hacker puede ejecutar scripts maliciosos en un sitio Web o aplicación Web. XSS se encuentra entre las vulnerabilidades más desenfrenadas de las aplicaciones Web y sucede cuando una aplicación Web emplea un ingreso de usuarios no validada o no codificada dentro de la salida.

Al aprovechar XSS, un hacker no ataca directamente a una víctima. En cambio, un hacker podría explotar una vulnerabilidad dentro de un sitio Web o aplicación Web que la víctima visitaría, esencialmente utilizando el sitio Web vulnerable como un vehículo para entregar un script malicioso al navegador de la víctima.

Mientras que XSS se puede aprovechar dentro de VBScript, ActiveX y Flash (aunque ahora se considera heredado o incluso obsoleto), incuestionablemente, el más abusado es JavaScript, principalmente porque JavaScript es fundamental para la mayoría de las experiencias de navegación.

Funcionamiento de scripting entre sitios: Para poder ejecutar código JavaScript malicioso en el navegador de una víctima, un hacker primero debe encontrar una forma de inyectar una carga en una página Web que la víctima visita. Por supuesto, un hacker podría usar técnicas de ingeniería social para convencer a un usuario de visitar una página vulnerable con una carga útil de JavaScript inyectada.

Para que se origine un ataque XSS, el sitio Web vulnerable debe contener directamente la entrada del usuario en sus páginas. Un hacker puede insertar una cadena que se usará dentro de la página Web y será tratada como código por el navegador de la víctima.

Lo peor que un hacker puede hacer en SQL: Las consecuencias de lo que puede hacer un hacker con la capacidad de ejecutar JavaScript en una página Web no se destacan inmediatamente, especialmente porque los navegadores ejecutan JavaScript en un entorno muy controlado y JavaScript tiene acceso limitado al sistema operativo del usuario y los archivos del usuario.

Sin embargo, cuando se considera que JavaScript tiene acceso a lo siguiente, es más fácil entender cómo pueden obtener los hackers creativos con JavaScript.

- JavaScript malicioso tiene acceso a todos los mismos objetos que el resto de la página Web, incluida el acceso a las cookies. Las cookies se utilizan a menudo para almacenar tokens de sesión, si un hacker puede obtener una cookie de sesión de usuario, pueden suplantar a ese usuario.
- JavaScript puede leer y realizar modificaciones arbitrarias en el DOM del navegador (dentro de la página que se está ejecutando JavaScript).
- JavaScript puede usar XMLHttpRequest para enviar solicitudes HTTP con contenido arbitrario a destinos arbitrarios.
- JavaScript en los navegadores modernos puede aprovechar las API de HTML5, como el acceso a la geolocalización, la cámara Web, el micrófono e incluso los archivos específicos del sistema de archivos del usuario. Si bien la mayoría de estas API requieren la aceptación por parte de los usuarios, XSS junto con una ingeniosa ingeniería social puede llevar al hacker un largo trecho. (Acunetix Vulnerability Scanner, 2017)

**b) CSRF (Cross Site Request Forgery):** La falsificación de solicitudes cruzadas (CSRF) es un ataque mediante el cual una entidad malintencionada engaña a una víctima para que realice acciones en nombre del hacker. El impacto del ataque dependería del nivel de permisos que tenga la víctima explotada. Las acciones perpetradas por el hacker

seguramente tendrán un mayor efecto si la víctima que realiza las acciones está en un nivel administrativo frente a un usuario de bajo nivel, con menos privilegios. Los ataques CSRF aprovechan el hecho de que una aplicación Web confía completamente en un usuario, una vez que puede confirmar que el usuario es realmente quien dice ser.

Hay dos partes principales en la ejecución de un ataque CSRF: la primera parte es engañar a la víctima para que haga clic en un enlace o cargue una página. Esto se hace normalmente a través de la ingeniería social, que funciona excepcionalmente bien para aprovechar la curiosidad de la víctima de hacer clic en enlaces maliciosos. La segunda parte es enviar una solicitud elaborada en el navegador de la víctima, que enviará una solicitud de búsqueda legítima a la aplicación Web. La solicitud se enviará con los valores que desea el hacker, incluidas las cookies que la víctima haya asociado con ese sitio Web. De esta forma, la aplicación Web sabe que esta víctima puede realizar ciertas acciones en el sitio Web y cualquier solicitud enviada con estas credenciales HTTP o Cookies, será considerada como legítima, aunque la víctima envíe la solicitud por el comando del hacker.

Cuando se realiza una solicitud a una aplicación Web, el navegador comprobará si tiene alguna cookie asociada con el origen de la aplicación Web que deberá enviarse con la solicitud. Si es el caso, estos datos de autenticación, como las cookies, por ejemplo, se incluirán en cualquier solicitud que se envíe a esta aplicación Web. Esto se hace para proporcionar a la víctima una experiencia fluida, por lo que no se les exigirá volver a autenticarse para cada página que visiten. Si el sitio Web aprueba que se envíe la cookie y considera que la sesión sigue siendo válida, un hacker puede usar CSRF para enviar solicitudes como si la víctima las enviara, sin que el sitio Web pueda distinguir entre las solicitudes enviadas por el hacker o por la víctima, ya que las solicitudes siempre son enviadas por la víctima con su propia Cookie.

Un ataque CSRF simplemente aprovecha el hecho de que el navegador envía la cookie a la aplicación Web automáticamente con cada solicitud.

La falsificación de solicitudes entre sitios (CSRF) solo será efectiva si la víctima está autenticada. Esto significa que la víctima deberá iniciar sesión para que el ataque tenga éxito. Dado que los ataques CSRF se utilizan para eludir el proceso de autenticación, puede haber algunos elementos que no se ven afectados por los ataques CSRF, a pesar de que no están protegidos contra él, como los que son de acceso público. Estos no requieren que una víctima haya iniciado sesión para enviar la solicitud, ya que cualquiera puede hacer esto. (Acunetix Vulnerability Scanner, 2017)

c) **Inyección SQL (SQL Injection):** hace referencia en el que un hacker ejecuta sentencias SQL malintencionadas que espían el servidor de bases de datos de una aplicación Web. Sabiendo que una vulnerabilidad de Inyección SQL alterara a cualquier sitio Web o aplicación Web que emplee una base de datos hecha en SQL, la inyección de SQL es una de las más antiguas, perdurables y perjudiciales de las vulnerabilidades en las aplicaciones Web.

Al utilizar una vulnerabilidad de Inyección SQL, un hacker puede utilizarla para esquivar los mecanismos de autenticación y autorización de una aplicación Web y rescatar el contenido de una base de datos integra. Otras de las formas que se puede utilizar la inyección SQL son para agregar, modificar y eliminar registros en una base de datos.

El funcionamiento de SQL Injection es para ejecutar consultas SQL maliciosas contra un servidor de base de datos, un hacker primero debe encontrar una entrada dentro de la aplicación Web que se incluye dentro de una consulta SQL.

Para que se de origen a un ataque de inyección SQL, el sitio Web vulnerable debe contener de forma directa la entrada del usuario dentro de una declaración SQL. Un hacker

puede introducir una carga útil que se adjuntara como parte de la consulta SQL y se realizara contra el servidor de la base de datos.

Tomando en cuenta lo descrito anterior, considerando lo siguiente, es más sencillo comprender cuan beneficioso puede ser un ataque de inyección SQL exitoso para un hacker.

- Un hacker puede usar SQL Injection para evitar ser autenticado o incluso reemplazar usuarios característicos.
- Un ataque de inyección SQL permitiría la difusión integra de los datos que están en el servidor de base de datos.
- Un hacker puede usar la Inyección SQL para cambiar los datos guardados en una base de datos. La alteración de los datos varía la integridad de los datos y puede provocar problemas de repudio.
- Un hacker puede usar un ataque de inyección SQL para borrar datos de una base de datos. Aun si se emplea un manejo de respaldo apropiado, los de datos borrados se verían afectados y no estarían disponibles las aplicaciones hasta que se repare la base de datos.
- Algunos servidores de bases de datos están diseñados para autorizar la realización parcial de comandos del sistema operativo en el servidor de la base de datos. (Acunetix Vulnerability Scanner, 2017)

**d) Pingback.** Se encontró una vulnerabilidad en el protocolo XML-RPC en WordPress, o ataque pingback, mediante el cual un hacker tendría 4 formas posibles de ocasionar daños a través de xmlrpc.php, el archivo incorporado en WordPress para dar soporte al protocolo XML-RPC.

El protocolo XML-RPC viene activo por defecto en WordPress desde la versión 3.5 y sin modo aparente de desactivarlo.

Hay 4 maneras que el protocolo XML-RPC de WordPress pueda ser dañada por un hacker:

- Recolección interna: El hacker puede experimentar puertos específicos en la red interna. Esto pueden usar los hacker para tratar de ingresar a hosts dentro de una red interna. De este modo, los hackers podrían emplear URLs para ver si el host está en la red interna.
- Escaneo de puertos: El hacker puede hacer un escaneo de hosts en la red interna. Si se logra detectar la URL original, WordPress intentara conectar con el puerto específico en esa URL. Las respuestas serán distintas si el puerto se encuentra cerrado o abierto, y justamente por eso esta funcionalidad puede utilizarse para escanear hosts dentro de la red interna.
- Ataques DoS (denegación de servicio): El hacker puede hacer pingback desde una desmedida cantidad de lugares, o usar equipos con conexión a internet, para hacer un ataque DoS.
  - GitHub es un soporte de desarrollo de software que contribuye en albergar proyectos usando el sistema de control de versiones Git.

  El código se manifiesta para todos los usuarios, no obstante se puede realizar de forma personal, pagando una cuenta.

  GtiHub almacena archivos de código y ofrece herramientas muy eficientes para el trabajo en grupo, dentro de un proyecto.
- Hackeo del router: El hacker puede volver a configurar un router interno de la red. Y es que WordPress soporta URLs con credenciales. (WordPress, 2013)

Tabla 1.
*Ataque DoS al protocolo XML-RPC.*

| **Nombre** | **Ataque DoS al protocolo XML-RPC** |
|---|---|
| **Descripción breve** | En WordPress, el protocolo XMLRPC se comporta como API para aplicaciones externas y se relaciona con instalaciones de WordPress manejando aplicaciones o servicios externos.<br>Al ejecutarse como una interfaz externa es como una puerta de entrada por lo que esta puerta puede ser atacada de manera sencilla desde el exterior, provocando un elevado consumo de recursos al realizarse una y otra vez el proceso de autentificación. |
| **Impacto** | - Escaneo de hosts en la red interna.<br>- Realizar pingback desde una enorme cantidad de sitios para realizar un ataque de tipo DOS.<br>- Configurar un router interno de la red.<br>- Probar puertos específicos en la red interna. |

**Fuente:** Elaboración propia con información de WordPress.

#### *2.2.8.4 Gravedad de un ataque*

La gravedad de un ataque facilita la labor del auditor porque permiten ejecutar desde una sola interfaz escaneos y enumeraciones sobre el objetivo, a la vez que identifican las vulnerabilidades presentes en dichos sistemas y las clasifican de acuerdo al nivel de riesgo presente.

La identificación se realiza de acuerdo a la versión del sistema operativo y de los servicios y aplicaciones detectados comparándolos contra una base de datos de vulnerabilidades que se actualiza frecuentemente conforme nuevos huecos de seguridad son descubiertos.

Los niveles de riesgo se clasifican usualmente en: bajo, medio y alto, conforme a la siguiente escala:

- Riesgo Alto: el equipo tiene una o más vulnerabilidades críticas que podrían ser explotadas fácilmente por un atacante y que podrían conllevar a tomar control total del sistema o comprometer la seguridad de la información de la organización. Los equipos con este nivel de riesgo requieren acciones correctivas inmediatas.

- Riesgo Medio: el equipo tiene una o más vulnerabilidades severas que requieren una mayor complejidad para poder ser explotadas y que podrían no brindar el mismo nivel de acceso al sistema afectado. Los equipos con riesgos severos requieren atención a corto plazo.
- Riesgo Bajo: el equipo tiene una o más vulnerabilidades moderadas que podrían brindar información a un atacante, la cual podría utilizarse para realizar ataques posteriores. Estos riesgos deben ser mitigados adecuadamente, pero no tienen un nivel de urgencia alto.

### 2.2.9 Seguridad en aplicaciones Web

Se entiende como sistema de seguridad al grupo de componentes lógicos y físicos, que tiene la finalidad de prevenir o disminuir peligros que puedan suscitarse en distintas situaciones. Una de sus particularidades más valiosas es que es dinámico, para poder proteger la más posible cantidad de vulnerabilidades. Un sistema de seguridad eficiente ofrece el soporte necesario en las organizaciones, disminuyendo las tareas de corrección y recuperación. (Herrera, 2012, págs. 4-11)

**a) Niveles de seguridad.** Un sistema de seguridad, debe emplear diversos periodos importantes, con los cuales obtenga una beneficiosa estimación en las evaluaciones para determinar el nivel de garantía de los elementos que se estén protegidos.

- ***Seguridad física:*** Se define como la aplicación de inconvenientes física y metodológica de control como medidas preventivas y proteger la seguridad de los recursos e información confidencial.
- ***Protección de hardware:*** Está compuesta por uno de los activos de mayor costo para las organizaciones para tener absoluta garantía, es uno de los primordiales factores que debe proteger los sistemas de seguridad.

- ***Seguridad lógica:*** Posterior al análisis de las probables causas que puedan alterar cualquier sistema desde el punto de vista de seguridad física, también se debe analizar desde el punto de vista lógico y es en este punto donde están enfocadas la mayoría de ataques.

**b) Componentes de seguridad.** Todos los sistemas de seguridad, para que funcionen correctamente ante los ataques, a las que se muestran los componentes de valor que forman las organizaciones y guardan el cuidado de estos, es necesario que dichos sistemas incluyan las siguientes cualidades para garantizar su importancia y de esta manera, ofrecer un correcto nivel de seguridad a las organizaciones.

- ***Confidencialidad****:* Este elemento tiene divisiones, cumpliendo los niveles de apartamiento que se quieran emplear dentro de la organización, siendo éstos; público, donde cualquier usuario puede tener acceso a la información; privado, solo usuarios aptos pueden ingresar a la información, teniendo un valor no tan alto; rigurosamente confidencial, solo usuarios restringidos pueden ingresar a esta información, la pérdida o acceso de usuarios no autorizados pueden perjudicar la organización.
- ***Integridad****:* Este elemento indica que, solo las entidades que tienen permiso son las delegadas de cambiar la información, observando para que en la información sean inexistentes los datos incorrectos.
- ***Disponibilidad****:* Hace referencia para que los recursos del sistema sean útiles, para las organizaciones previamente autorizadas, en el momento que estas lo requieran y no tengan que esperar.

### 2.2.10 Herramientas de hacking ético

Las principales herramientas de hacking ético que se utilizó son Nmap (Kali Linux) y Acunetix.

#### *2.2.10.1 Nmap ("mapeador de redes")*

Es una herramienta libre que examina redes y hace auditoría de seguridad. Se creó con la finalidad de analizar de forma rápida grandes redes, aunque funciona perfectamente con equipos individuales. Nmap emplea paquetes IP en formas originales para señalar que los equipos estén aptos en la red, qué contenido brindan, qué sistemas operativos desempeñan, qué tipo de filtros de paquetes o cortafuegos se están empleando así como docenas de otras características.

La salida de Nmap es una lista de objetivos analizados, con información agregada para cada uno, dependiendo de las alternativas empleadas. La información fundamental es la tabla de puertos. La tabla hace un listado del número de puerto y protocolo, el nombre ordinario del servicio, y su estado. El estado puede ser open, filtered, closed, o unfiltered. Open indica que la aplicación en la máquina de llegada está esperando conexión o paquetes en ese puerto. Filtered indica que un cortafuego, filtro, u otro impedimento en la red está impidiendo el ingreso a ese puerto, por lo que Nmap no sabe si está abierto o cerrado. Los puertos closed no cuentan con ninguna aplicación prestando atención en los mismos, sin embargo se pueden abrir en cualquier momento. Los clasificados como unfiltered son aquellos que dan respuesta a la exploración de Nmap, pero para los que Nmap no puede decidir si se encuentran abiertos o cerrados. Nmap notifica de las combinaciones de estado open-filtered y closed-filtered cuando no puede decidir en cuál de los dos estados está un puerto. La tabla de puertos también puede contener especificaciones de la versión de la aplicación cuando se requiere detección de versiones. Nmap brinda información de los protocolos IP soportados, en vez de puertos abiertos, cuando se requiere un análisis de protocolo IP.

Además de la tabla de puertos sugerido, Nmap brinda información complementario sobre los objetivos, adjuntando el nombre de DNS según la resolución opuesta de la IP, un

listado de sistemas operativos probables, los tipos de dispositivo, y direcciones MAC (Nmap.org, 2007).

#### *2.2.10.2 Acunetix*

Acunetix WVS (Web Vulnerability Scanner) tiene la capacidad de escanear cualquier sitio Web o aplicación Web que tenga acceso mediante el protocolo HTTP/HTTPS. A pesar de ello, no todas las pruebas se pueden efectuar de forma automática, Acunetix ofrece herramientas de penetración manuales para pruebas específicas. (Acunetix Vulnerability Scanner, 2017)

- Acunetix es una herramienta automatizada de pruebas de seguridad de aplicaciones Web.
- Examina distintas vulnerabilidades. Hasta el momento Acunetix verifica más de 500 vulnerabilidades diferentes.
- Acunetix puede escanear cualquier sitio Web que tenga acceso a través del protocolo HTTP/HTTPS, fundamentalmente, que el sitio Web este visible en un navegador.
- Brinda herramientas de pruebas de penetración manuales que incrementan y colaboran con las pruebas preestablecidas.

Tecnologías propiedad de Acunetix

- AcuMonitor: Es una función intercesora que ayuda al cliente a encontrar vulnerabilidades que están introducidas en la Website pero no son visibles hasta que se realizan algo propio de la Website, haciendo que la vulnerabilidad se active.
- Acusensor: Es un plugin que adquiere más información del código; de la creación de las Websites y lo envía a WVS. Ayuda a encontrar más vulnerabilidades mientras genera menos fallos.

- DeepScan: Es la última adquisición tecnológica de Acunetix Web Vulnerability Scanner, escanea y analiza HTML5 y aplicaciones Web realizadas en JavaScript. Las Aplicaciones Web realizadas en HTML5 están empleando una gran diversidad de bibliotecas complejas de JavaScript como Angular.js, Backbone.js, Ember.js y SproutCore.

Funcionamiento de Acunetix WVS

- Crawling (rastreador): El rastreador examnina la Website en su totalidad desde la URL principal para encontrar todos los directorios y archivos.
- Acunetix escaneo de vulnerabilidades: Acunetix WVS mandará una serie de ataques de vulnerabilidades a cada página.
- Escaneo muestra de Alertas: Todas las vulnerabilidades descubiertas se indicaran con información detallada en la interfaz gráfica del software en la zona de alerta.
- Creación de informes y remediación: Acunetix presenta las vulnerabilidades encontradas en una variedad de informes distintos. Y al comprobar o escanear de alertas específicas hace posible fijar y probar las vulnerabilidades de forma individual en vez de volver a realizar una exploración o escaneo completo.

**Procedimiento Acunetix para escanear una página Web por defecto**

**Introducción**

Los registros del servidor Web mostrarán los escaneos y cualquier ataque realizado por Acunetix WVS. Si no es el único administrador del sitio Web, asegúrese de advertir a otros administradores antes de realizar un análisis. Algunos escaneos pueden hacer que un sitio Web se bloquee, lo que requiere un reinicio del sitio Web. (Acunetix Vulnerability Scanner, 2017)

**Paso 1: Seleccione el objetivo (s) para escanear**

Haga clic en File > New > New Website Scan para iniciar el Asistente de escaneo, o presione en el botón New Scan en la esquina superior izquierda de la barra de menú de Acunetix WVS.

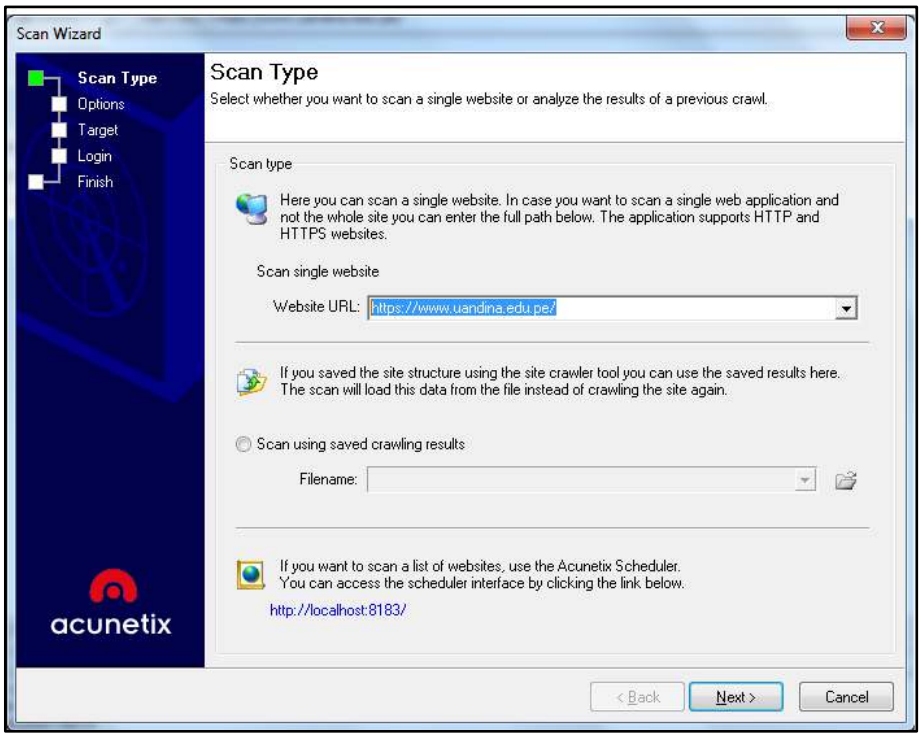



*Figura 8.* Asistente de escaneo Seleccione el tipo de escaneo.
**Fuente:** Contenido de la página Web Acunetix.

Especifique el (los) sitio (s) Web (s) a escanear. Las opciones de destino de escaneo son:

- Escanear sitio Web individual: ingrese la URL de un sitio Web objetivo, https://www.uandina.edu.pe/.
- Escanear utilizando resultados de rastreo guardados: si realizó un rastreo previamente en un sitio Web, puede usar los resultados guardados para iniciar un análisis en lugar de tener que rastrearlo nuevamente.

Nota: Acunetix WVS se puede utilizar para explorar múltiples sitios Web al mismo tiempo, ya que inicia una instancia de Acunetix WVS por cada exploración simultánea.

- Presione siguiente para continuar.

**Paso 2: Especifique el perfil de escaneo, la plantilla de configuración de escaneo y las opciones de rastreo.**

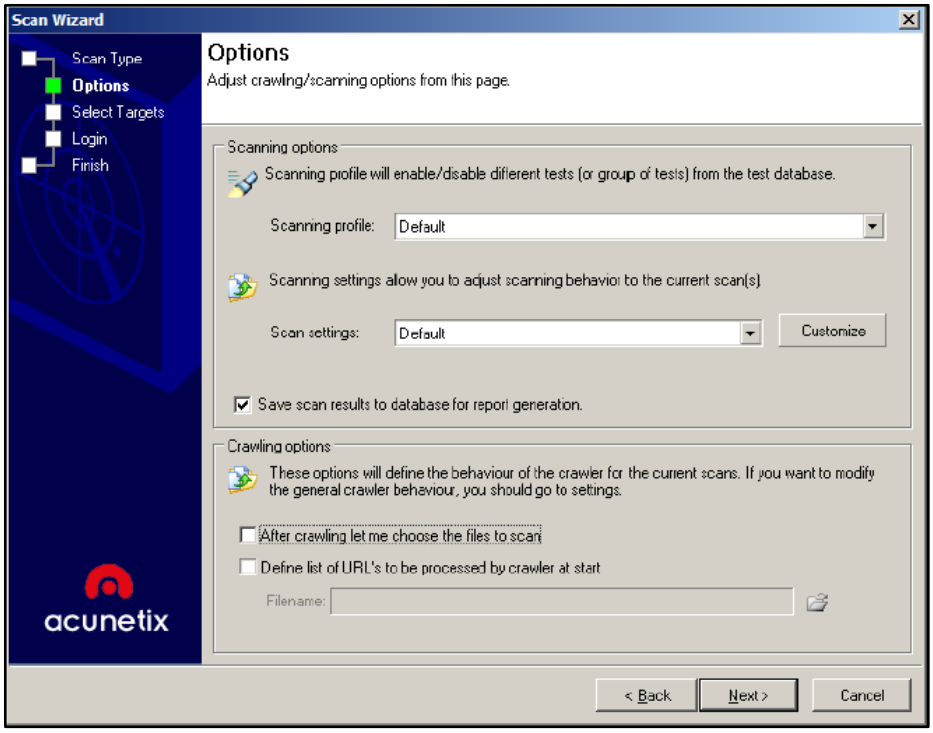



*Figura 9.* Perfil de escaneo y plantilla de configuración de escaneo.
**Fuente:** Contenido de la página Web Acunetix.

Perfil de escaneo (Scanning Profile): El perfil de exploración determinará qué pruebas se lanzarán contra el sitio Web de destino. Por ejemplo, si solo desea probar su (s) sitio (s) Web para inyección SQL, seleccione el perfil sql_injection. No se realizarán pruebas adicionales. El perfil de escaneo predeterminado probará su sitio Web para detectar cualquier vulnerabilidad Web conocida.

Plantilla de configuración de escaneo (Scan Settings template): La plantilla Configuración de escaneo determinará qué Crawler (protocolo HTTP, rastreo avanzado) y la configuración del escáner se usarán durante un escaneo.

Guardar resultados de escaneo (Save scan Results): Si desea guardar automáticamente los resultados de escaneo en la base de datos de informes, habilite Guardar resultados de escaneo en la base de datos para la opción de generación de informes.

Opciones de rastreo (Crawling Options): Marque la opción Después de rastrear, puede elegir qué archivos escanear si desea seleccionar / no seleccionar archivos del escaneo de seguridad del sitio Web automatizado, en lugar de escanear todo el sitio Web. Marque la opción Definir lista de URL para que el rastreador la procese al inicio si desea rastrear una URL específica antes que cualquier otra.

Nota: Si el escaneo se inicia desde un resultado de rastreo guardado, la opción Definir lista de URL estará oculto porque un escaneo automático comenzará inmediatamente sin el rastreo.

**Paso 3: confirmar los objetivos (Targets) y las tecnologías detectadas**

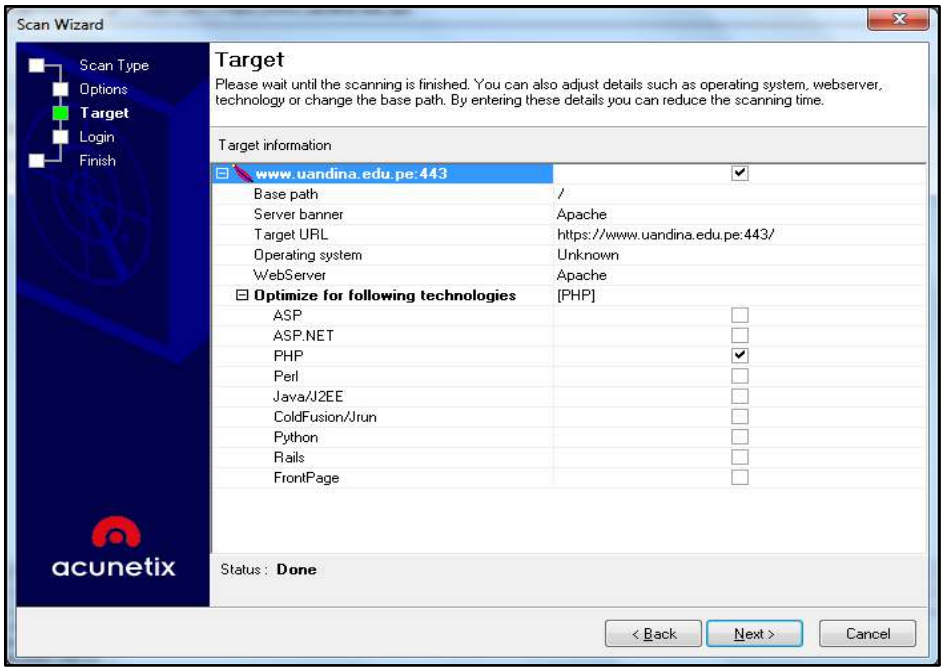



*Figura 10.* Asistente de escaneo Selección de objetivos y tecnologías.
**Fuente:** Contenido de la página Web Acunetix.

Acunetix WVS automáticamente tomará las huellas dactilares de los sitios Web de destino para obtener detalles básicos, como el sistema operativo y del servidor Web, las tecnologías del servidor Web y la página personalizada de error 404 en uso. Si se usa una página de error 404 personalizada, Acunetix WVS la detectará automáticamente y determinará un patrón para ella, eliminando la necesidad de configuración manual.

El escáner de vulnerabilidad Web optimizará y reducirá el tiempo de escaneo para las tecnologías seleccionadas al reducir el número de pruebas realizadas. Por ejemplo: Acunetix WVS no lanzará las comprobaciones de seguridad de IIS (Internet Information Services) contra un sistema Linux que ejecute un servidor Web Apache.

Haga clic en el campo correspondiente y cambie la configuración de las casillas de verificación provistas si desea agregar o eliminar escaneos para tecnologías específicas.

**Paso 4: Inicio de sesión: configure los detalles de entrada / inicio de sesión para áreas protegidas con contraseña o formularios HTML**

2 tipos de mecanismos de inicio de sesión se utilizan comúnmente en la Web:

- Usar secuencia de inicio de sesión pregrabada (Use pre-recorded login sequence): Si su sitio Web requiere autenticación de formularios, debe registrar los pasos necesarios para iniciar sesión en el sitio Web. Esto será como un archivo de secuencia de inicio de sesión y se puede usar más adelante. También puede especificar una sección del sitio Web que no desea rastrear (por ejemplo, enlaces que lo desconectarán del sitio Web).

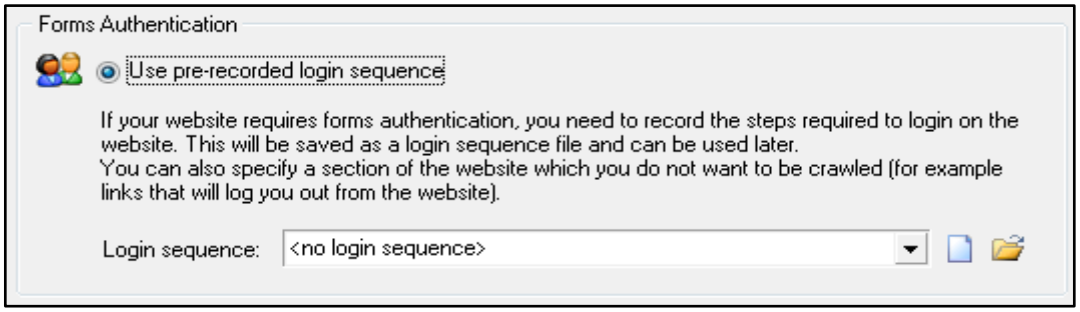



*Figura 11.* Secuencia de inicio de sesión pregrabada.
**Fuente:** Contenido de la página Web Acunetix.

- Intente iniciar sesión automáticamente en el sitio (try to auto-login into the site): La autenticación de formularios del sitio Web en algunos casos puede identificarse automáticamente. La detección automática intentará identificar los pasos necesarios para iniciar sesión, los enlaces restringidos en los que no se debe hacer clic para

mantener la sesión y el patrón mediante el cual se puede identificar una sesión válida.

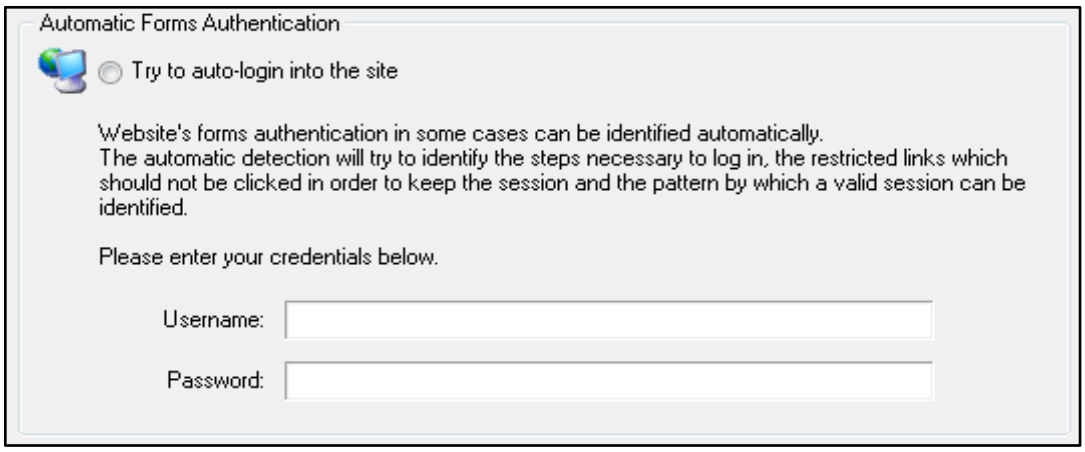



*Figura 12.* Sesión automática en el sitio.
**Fuente:** Contenido de la página Web Acunetix.

**Paso 5: opciones finales del asistente**

En el último paso del asistente de escaneo, se le presenta una descripción general de las opciones de escaneo y se le informa si se requieren más acciones.

Lista de todas las opciones posibles que se le pueden presentar:

- Si se encuentra un error al conectarse al servidor de destino, recibirá una alerta con los detalles completos del error.
- Si el sitio Web de destino está utilizando páginas de error Custom 404, se detectarán automáticamente, por lo tanto, no se requieren más acciones. Si Acunetix WVS no puede detectar automáticamente una página de error 404 personalizada y un patrón para reconocerla automáticamente, deberá configurar una regla de página de error 404 personalizada haciendo clic en el botón Personalizar (Customize).
- Si el servidor de destino utiliza URL insensibles a CASE, también recibirá una alerta con la opción de forzar el rastreo insensible a mayúsculas y minúsculas.

- Si la tecnología AcuSensor está habilitada y el servidor de destino es PHP o .NET, se le solicitará la opción de configurar la tecnología AcuSensor. Presione el botón Personalizar (Customize) para instalar AcuSensor en el servidor de destino.
- Acunetix WVS también lo alertará si se han descubierto hosts adicionales; es decir, otros sitios Web a los que se vinculan su sitio Web. De manera predeterminada, Acunetix WVS no rastreará y escaneará hosts adicionales que estén enlazados desde su sitio Web. Marque el o los hosts que Acunetix WVS debe rastrear y escanear automáticamente.
- Si ha realizado cambios en la plantilla Configuración de escaneo, también puede guardar las modificaciones en la plantilla nueva o existente.

**Paso 6: completar el escaneo**

Haga clic en Finalizar (Finish) para iniciar el escaneo automático. Dependiendo del tamaño del sitio Web, el perfil de escaneo y el tiempo de respuesta del servidor, un escaneo puede tomar varias horas. Estos factores no pueden ser controlados por Acunetix WVS.

**Paso 7: seleccionar los archivos y directorios para escanear**

Si la opción Después de rastrear (After crawling), está marcada en las opciones de rastreo, puede elegir los archivos para escanear, una ventana con la estructura del sitio rastreado aparecerá automáticamente al final del rastreo automatizado, lo que le permitirá seleccionar qué archivos escanear.

**Alertas (vulnerabilidades) descubiertas**

Uno de los componentes clave de los resultados del análisis es la lista de todas las vulnerabilidades encontradas en escanear el objetivo durante el escaneo. Dependiendo del tipo de análisis, estos pueden ser Alertas Web o alertas de red, y las alertas se clasifican según 4 niveles de gravedad:

- Alerta de alto riesgo nivel 3: vulnerabilidades categorizadas como las más peligrosas, que ponen el objetivo de escaneo con el máximo riesgo de piratería y robo de datos.
- Nivel medio de alerta de riesgo 2: vulnerabilidades causadas por la mala configuración del servidor y defectos de codificación del sitio, que facilitan la interrupción e intrusión del servidor.
- Alerta de bajo riesgo Nivel 1: vulnerabilidades derivadas de la falta de cifrado del tráfico de datos o divulgaciones de la ruta del directorio
- Alerta informativa: estos son elementos que se han descubierto durante el escanear y que se consideran de interés; se descubrió durante el análisis la posible divulgación de una IP interna dirección o dirección de correo electrónico, o hacer coincidir una cadena de búsqueda encontrada en Google Hacking.

Según el tipo de vulnerabilidad, se muestra información adicional sobre la vulnerabilidad cuando haces clic en un nodo de categoría de alerta:

- Vulnerability description: una descripción de la vulnerabilidad descubierta.
- Affected ítems: la lista de archivos o componentes que se ven afectados por la alerta.
- The impact of this vulnerability: nivel de impacto en el sitio Web, el servidor Web o servidor perimetral si esta vulnerabilidad es explotada.
- Attack details: detalles sobre los parámetros y las variables utilizados para probar este vulnerabilidad.
- How to fix this vulnerability: orientación sobre cómo solucionar la vulnerabilidad.
- Classification: Además de la clasificación Acunetix, esta sección proporciona clasificación por CVSS (v2 y v3) puntaje y enumeración id CWE.

- Detailed information: información extra sobre lo que está causando el informe vulnerabilidad.
- Web references: una lista de enlaces Web a fuentes externas que brindan más información sobre la vulnerabilidad para ayudarlo a comprenderlo y solucionarlo.

## 2.3 Marco Conceptual

### 2.3.1 Análisis dinámico de código.

Tiene comunicación con la aplicación Web mediante la interfaz de aplicación para identificar vulnerabilidades de seguridad y fallos en la arquitectura de la aplicación Web. (Hernández Saucedo & Mejia Miranda, 2015, págs. 7-8)

### 2.3.2 Análisis estático de código.

Es un método mediante el cual no se requiere ejecutar el programa, este hace un análisis de código fuente directo para señalar fallas en la seguridad. (Hernández Saucedo & Mejia Miranda, 2015, págs. 7-8)

### 2.3.3 Pruebas de penetración.

Simula un ataque de los malignos outsiders (los sistemas de la organización) e insiders (que tienen algún nivel de acceso permitido). El desarrollo implica un análisis activo del sistema para la búsqueda de probables vulnerabilidades que pueden dar resultado de la configuración defectuosa o impropia del sistema. (Hernández Saucedo & Mejia Miranda, 2015, págs. 8-9)

### 2.3.4 Vulnerabilidad de diseño.

Son deficiencias en la arquitectura del sistema de software y datos característicos, se puede encontrar en la estipulación de la fase de análisis o en la determinación de la fase de diseño. (Universidad Internacional de la Rioja , 2015)

### 2.3.5 Vulnerabilidad de implementación.

Son lógicamente fallos de seguridad realizados por los programadores cuando están realizando los módulos u objetos del sistema para satisfacer sus especificaciones. (Universidad Internacional de la Rioja , 2015)

### 2.3.6 Vulnerabilidad informática.

Se define "Vulnerabilidad Informática" como un error de software que puede utilizar directamente el hacker para ganar acceso a un sistema de información. (Carvajal, 2007, págs. 42-43)

### 2.3.7 Vulnerabilidad de uso.

Son fallos que aparecen en el desglose y la configuración del sistema desarrollado en un medio propio. (Universidad Internacional de la Rioja , 2015)

## 2.4 Hipótesis

### 2.4.1 Hipótesis general

$H_1$: Con la aplicación de herramientas de hacking ético se identificó vulnerabilidades informáticas en el portal Web de la Universidad Andina del Cusco.

$H_0$: Con la aplicación de las herramientas de hacking ético no se identificó vulnerabilidades informáticas en el portal Web de la Universidad Andina del Cusco.

### 2.4.2 Hipótesis específicas

$He_1$: Con la aplicación de las herramientas de hacking ético se identificó vulnerabilidades de diseño en el portal Web de la Universidad Andina del Cusco.

$He_2$: Con la aplicación de las herramientas de hacking ético se identificó vulnerabilidades de implementación en el portal Web de la Universidad Andina del Cusco.

$He_3$: Con la aplicación de las herramientas de hacking ético se identificó vulnerabilidades de uso en el portal Web de la Universidad Andina del Cusco.

## 2.5 Variable e Indicadores

### 2.5.1 Variable:

- Vulnerabilidad informática.

### 2.5.2 Indicadores:

- Análisis estático de código.
- Análisis dinámico de código.
- Pruebas de penetración.

# Capítulo III

# Metodología

## 3.1 Tipo de Investigación

Según (Sampieri Hernandez, 1998), los estudios descriptivos permiten detallar situaciones y eventos, es decir cómo es y cómo se manifiesta determinado fenómeno y busca especificar propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis.

Este proyecto de investigación se considera de carácter **descriptivo** en cuanto permite describir todos los procesos y errores que son causados al momento de efectuar actividades en las cuales son incurridas grandes cantidades de datos y la forma que afecta directa e indirectamente en el progreso de las actividades desarrolladas diariamente dentro del portal Web de la Universidad Andina del Cusco.

## 3.2 Diseño de la Investigación

El diseño de investigación es no experimental porque el objetivo de estudio es observado en contexto natural, en su realidad día a día sin realizarse cambios, analizándolos como se efectúan naturalmente en su ambiente en el que estos ocurren. En el enfoque **cuantitativo**, el investigador utiliza su diseño para analizar la certeza de las hipótesis formuladas en un contexto en particular o para aportar evidencia respecto los lineamientos de la investigación.

A continuación se presenta los gráficos de los procesos para la obtención de las vulnerabilidades encontradas en el portal Web de la Universidad Andina del Cusco.

**Configuración de procesos**

Instalación del software Acunetix Web Vulnerability Scanner 10.5.

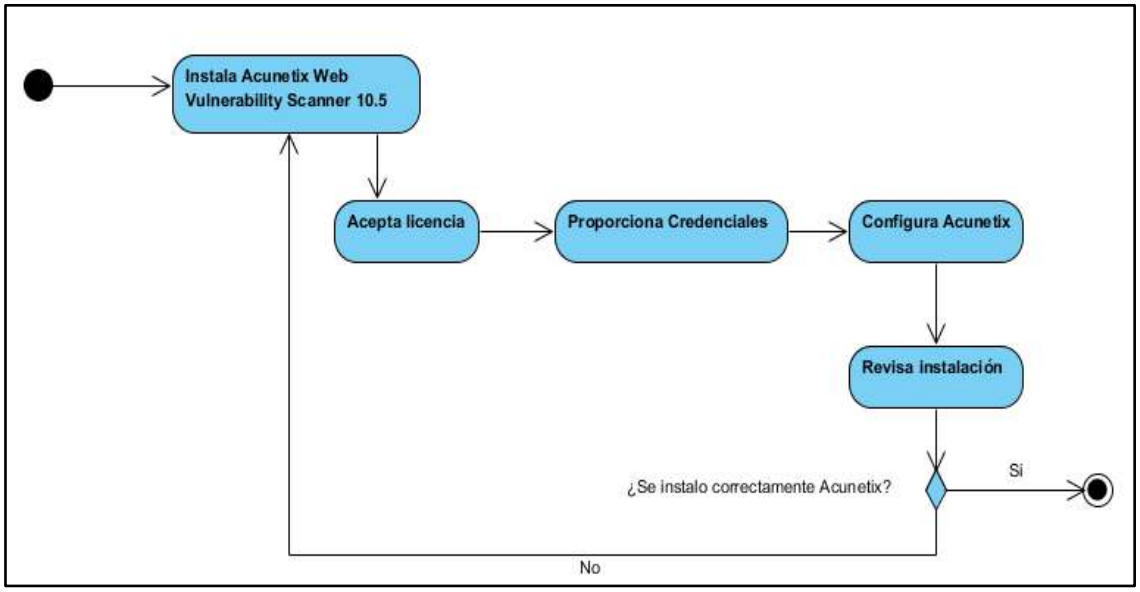



*Figura 13.* Diagrama de instalación del Software Acunetix.
**Fuente**: Elaboración Propia con el software Visual Paradigm.

Diseño de pruebas para vulnerabilidades de implementación con Acunetix para ataques SQL injection, XSS y CSRF.

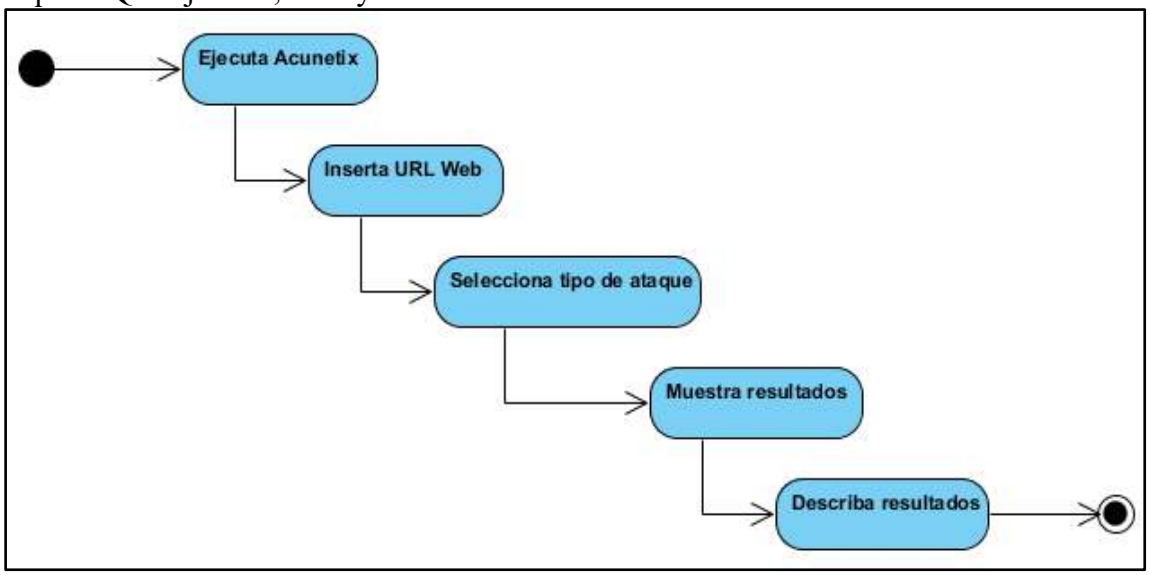



*Figura 14.* Diagrama de pruebas para vulnerabilidades de implementación.
**Fuente**: Elaboración Propia con el software Visual Paradigm.

Instalación del software VMware Workstation Pro.

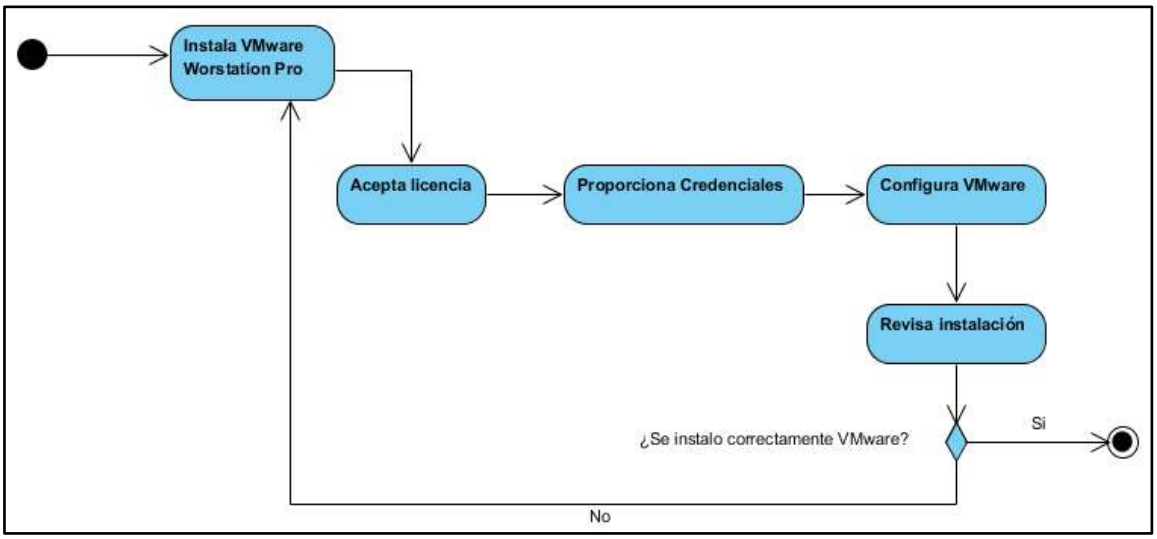



*Figura 15.* Diagrama de instalación del software VMware.
**Fuente:** Elaboración Propia con el software Visual Paradigm.

Instalación de Kali-Linux dentro del Software VMware Worstation Pro.

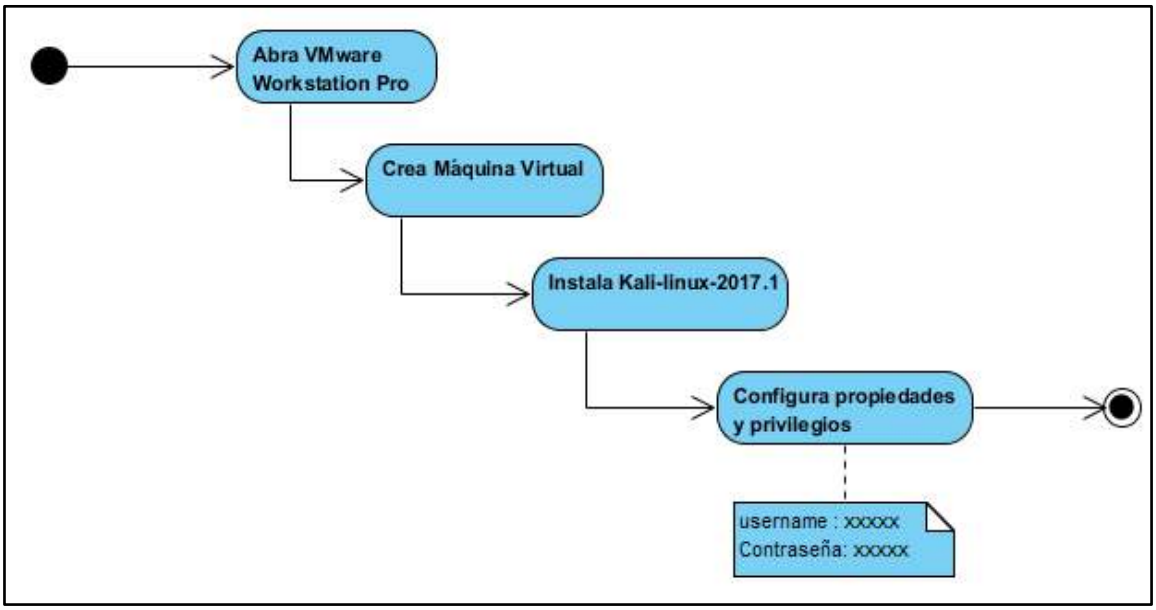



*Figura 16.* Diagrama de instalación del software Kali-Linux.
**Fuente:** Elaboración Propia con el software Visual Paradigm.

Diseño de pruebas para vulnerabilidades de diseño con Kali-Linux para ataques Sniffer con Nmap.

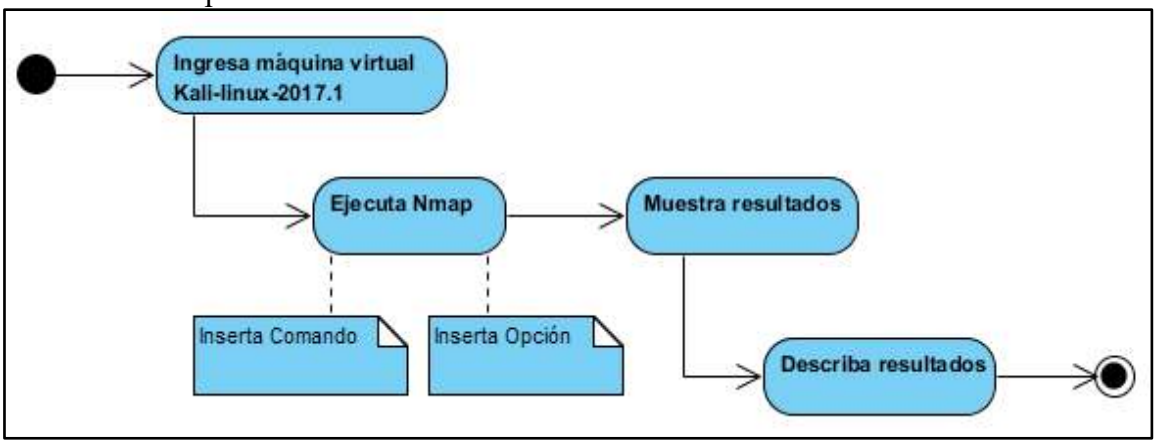



*Figura 17.* Diagrama de pruebas para vulnerabilidades de diseño.
**Fuente:** Elaboración Propia con el software Visual Paradigm.

Diseño de pruebas para vulnerabilidades de uso con Kali-Linux para ataques de Denegación de Servicios (DoS).

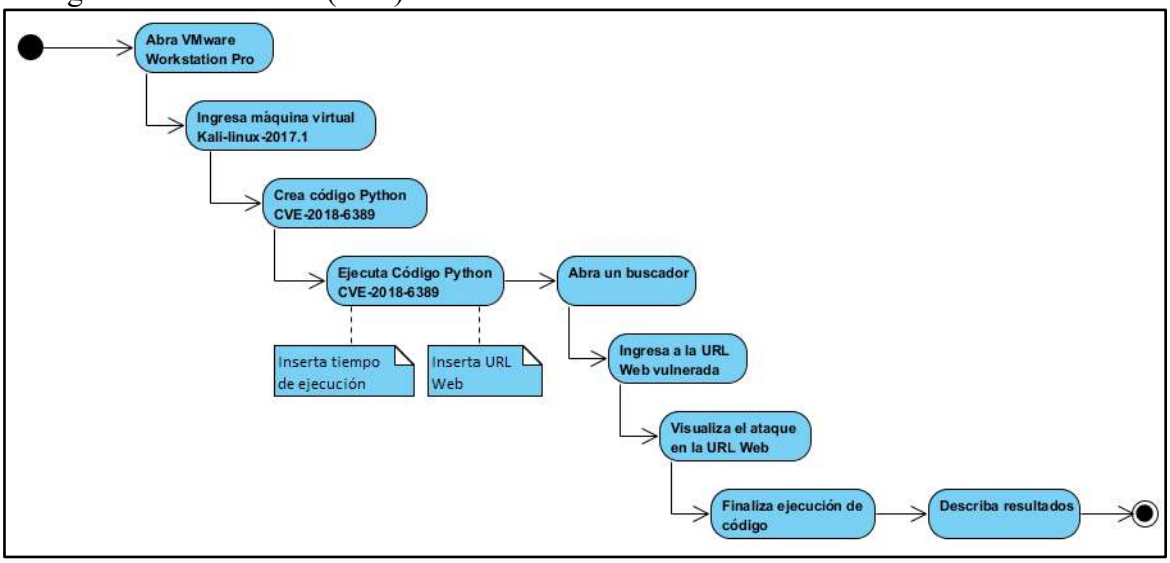



*Figura 18.* Diagrama de pruebas para vulnerabilidades de uso.
**Fuente:** Elaboración Propia con el software Visual Paradigm.

## 3.3 Población y Muestra

### 3.3.1 Población:

El personal de la Dirección de Tecnologías de Información (DTI), quien tiene la información y conoce los procesos actuales dentro de la Universidad Andina del Cusco

La Dirección de Tecnologías de Información de Universidad Andina del Cusco se encuentra integrada por las siguientes unidades.


*Figura 19.* Organigrama estructural de la Dirección de Tecnologías de Información.
**Fuente:** Elaboración de la Dirección de Tecnologías de Información.

El estudio que se ha realizado, está dirigida a toda la Dirección de Tecnologías de Información y que hace uso de las tecnologías de información y comunicación.

3.3.2 Muestra:

La Dirección de Tecnologías de Información está conformada por tres unidades; pero la que se encarga de administrar el portal Web de Universidad Andina del Cusco es la Unidad de Diseño y Programación.

## 3.4 Técnicas de Recolección de Datos

| Técnicas |
|---|
| Análisis estático de código |
| Análisis dinámico de código |
| Pruebas de penetración |

## 3.5 Técnicas de Procesamiento de Datos

| Instrumentos de recolección de datos |
|---|
| Nmap |
| Acunetix |

# Capitulo IV

# Pruebas y Resultados

## 4.1 Resultados Respecto a los Objetivos Específicos

Todos los análisis realizados fueron a través del software Kali Linux y Acunetix Web Vulnerability Scanner, aplicado al portal Web www.uandina.edu.pe. Su fecha de aplicación cubre el periodo entendido entre el 02 de febrero del 2017 y el 25 de marzo del 2018. Encontrando los siguientes resultados:

**DISEÑO PARA LA VULNERABILIDAD DE DISEÑO**

- En la vulnerabilidad de diseño uno de sus ataques es el de Sniffer, el formato que se presenta a continuación es para completar los resultados de Sniffer con Nmap dependiendo de la opción a ejecutar.

Tabla 2.
*Sniffer con Nmap opción: ‘’.*

| **Sniffer con Nmap opción: ‘’** | |
|---|---|
| **Herramienta** | Nmap |
| **Comando** | Código a ejecutar en Kali-Linux. |
| **Opción** | Se describirá la opción a ejecutar. |
| **Objetivo** | Breve descripción de la opción que se ejecutara. |
| **Número de Pruebas** | Cantidad de veces que se usó la opción. |
| **Tiempo de Ejecución** | Tiempo de demora que lleva ejecutar la opción. |

**Fuente**: Elaboración Propia.

## RESULTADOS DE LA VULNERABILIDAD DE DISEÑO

### Sniffer con Nmap

La herramienta Nmap brinda diversos métodos para analizar un sistema. En este caso, se realizó una investigación usando el nombre de host www.uandina.edu.pe para descubrir todos los puertos abiertos, estados y servicios del sistema.

### Opción –v

Tabla 3.
*Opción nmap -v.*

| Sniffer con Nmap opción: -v | |
|---|---|
| **Herramienta** | Nmap |
| **Comando** | `nmap -v www.uandina.edu.pe` |
| **Opción** | `-v` |
| **Objetivo** | Escanear un nombre de host con información más detallada. |
| **Número de Pruebas** | 1 |
| **Tiempo de Ejecución** | 2 minutos aprox. |

**Fuente:** Elaboración propia.

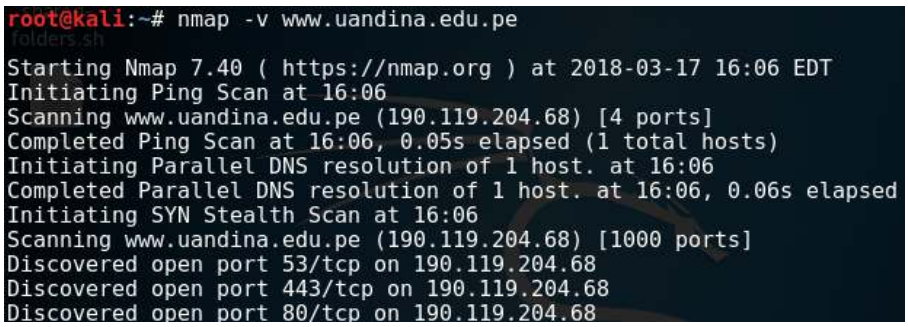



*Figura 20.* Opción nmap –v.
**Fuente:** Elaboración propia con el software Kali-Linux.

**Comentario:** Se encontró el puerto 53, 443 y 80 en estado abierto en la dirección IP "192.119.204.68", en algunos casos al hacer la consulta de puertos abiertos, muestran puertos abiertos los cuales podrían ser vulnerables; en este caso el portal Web de la UAC cuenta con los puertos abiertos necesarios para su funcionamiento.

**Opción –A**

Tabla 4.
*Opción nmap -A.*

| **Sniffer con Nmap opción: -A** | |
|---|---|
| **Herramienta** | Nmap |
| **Comando** | `nmap -A www.uandina.edu.pe` |
| **Opción** | `-A` |
| **Objetivo** | Detectar el sistema operativo y su versión, la exploración de la escritura y la Ruta de seguimiento. |
| **Número de Pruebas** | 1 |
| **Tiempo de Ejecución** | 5 minutos aprox. |

**Fuente:** Elaboración propia.

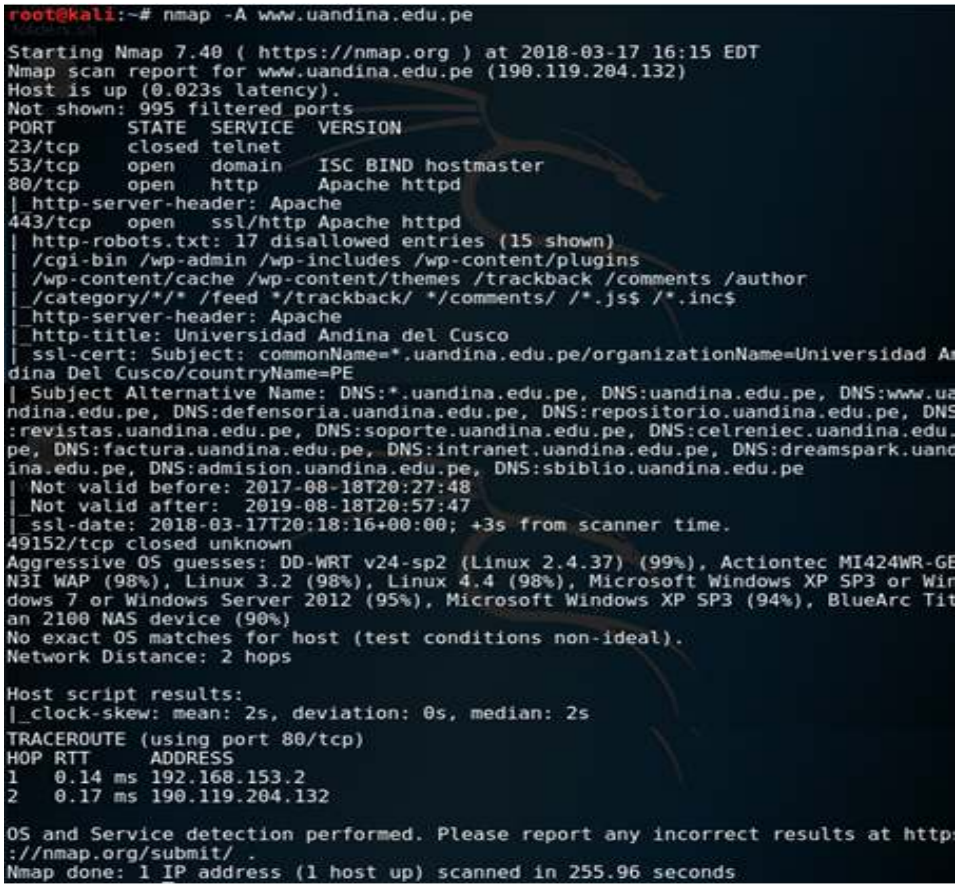



*Figura 21.* Opción nmap –A.
**Fuente:** Elaboración propia con el software Kali-Linux.

**Comentario:** Los sistemas operativos y sus versiones que maneja la Universidad Andina del Cusco son: DD-WRT v24-sp2 (Linux 2.4.37), Actiontec MI424WR-GEN3I WAP, Linux 3.2, Linux 4.4, Microsoft Windows XP SP3 – Windows 7 – Windows Server 2012, Microsoft Windows XP SP3, BluArc Titan 2100 NAS.

**Opción –sA**

Tabla 5.
*Opción nmap -sA.*

| Sniffer con Nmap opción: -sA | |
|---|---|
| **Herramienta** | Nmap |
| **Comando** | `nmap -sA www.uandina.edu.pe` |
| **Opción** | `-sA` |
| **Objetivo** | Encontrar los filtros de paquetes o Firewall que se emplean por el anfitrión. |
| **Número de Pruebas** | 1 |
| **Tiempo de Ejecución** | 1 minutos aprox. |

**Fuente:** Elaboración propia.

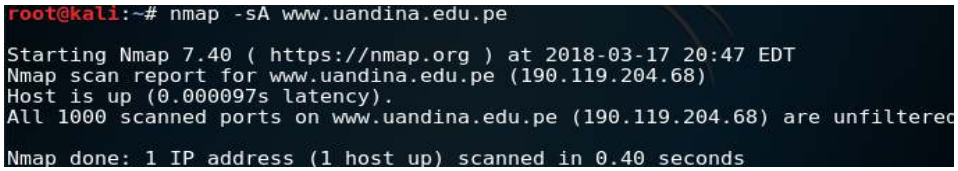



*Figura 22.* Opción nmap –sA.
**Fuente:** Elaboración propia con el software Kali-Linux.

**Cometario:** En este caso la opción –sA no puedo extraer información de los paquetes no del Firewall.

**Opción –sV**

Tabla 6
*Opción nmap –sV.*

| Sniffer con Nmap opción: -sV | |
|---|---|
| **Herramienta** | Nmap |
| **Comando** | `nmap -sV www.uandina.edu.pe` |
| **Opción** | `-sV` |
| **Objetivo** | Encontrar versiones de servicios que se realizan en máquinas remotas |
| **Número de Pruebas** | 1 |
| **Tiempo de Ejecución** | 3 minutos aprox. |

**Fuente:** Elaboración propia.

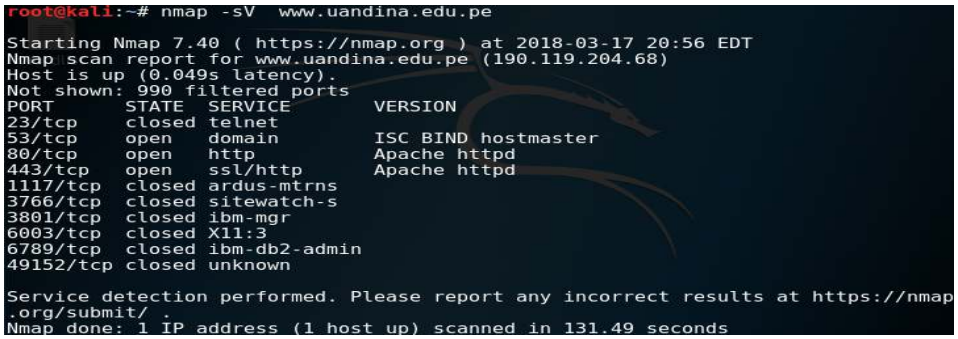



*Figura 23.* Opción nmap –sV.
**Fuente:** Elaboración propia con el software Kali-Linux.

**Comentario:** Se encontró el puerto 53 con servicio "domain" y la versión "ISC BIND hostmaster"; el puerto 80 con servicio "http" y la versión "Apache httpd" y por último el puerto 443 con servicio "ssl/http" y la versión "Apache httpd"; el puerto 443 utiliza un canal cifrado correcto para el tráfico de información delicada.

**Opción –PS**

Tabla 7.
*Opción nmap –PS.*

| **Sniffer con Nmap opción: -PS** | |
|---|---|
| **Herramienta** | Nmap |
| **Comando** | `nmap -PS www.uandina.edu.pe` |
| **Opción** | `-PS` |
| **Objetivo** | Determinar si los filtros de paquetes o Firewall se utilizan por el anfitrión. |
| **Número de Pruebas** | 1 |
| **Tiempo de Ejecución** | 3 minutos aprox. |

**Fuente:** Elaboración propia.

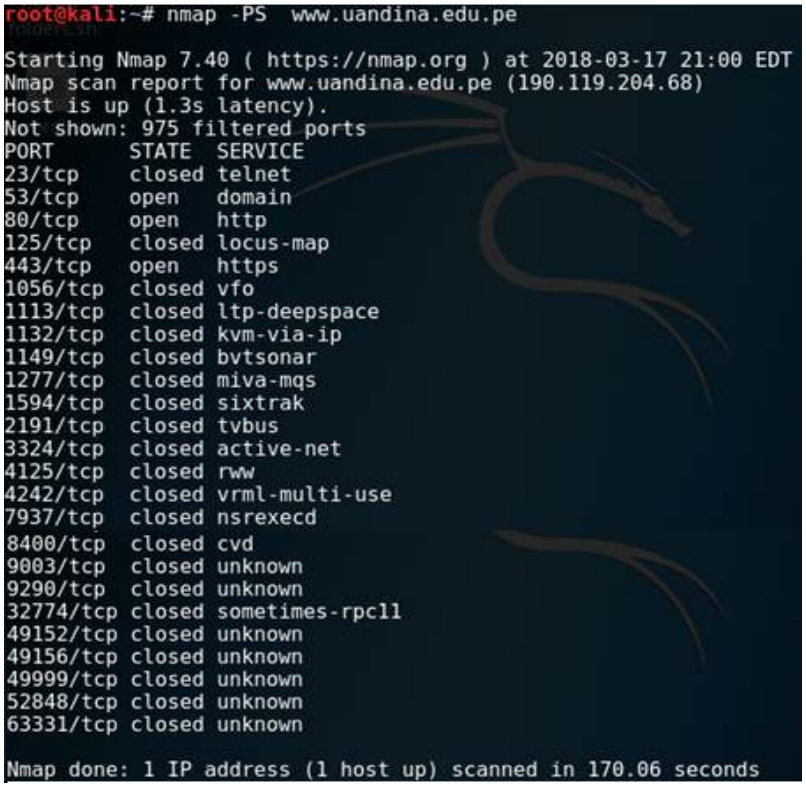



*Figura 24.* Opción nmap –PS.
**Fuente:** Elaboración propia con el software Kali-Linux.

**Comentario:** A veces, los cortafuegos de filtrado de paquetes impide las solicitudes de ping ICMP estándar, con la opción -PS, se utiliza métodos TCP ACK y TCP Syn para escanear hosts remotos; la opción utilizada muestra los puertos con los estados en general (abiertos y cerrados) y los servicios que manejan dichos puertos.

**Combinación de comandos**

Se usó una combinación de comandos para que el análisis sea más intenso con mejores resultados.

**Opción -f -sS -sV - -script auth**

Tabla 8.
*Opción nmap -f -sS -sV --script auth.*

| **Sniffer con Nmap opción: -f -sS -sV - -script auth** | |
|---|---|
| **Herramienta** | Nmap |
| **Comando** | nmap -f -sS -sV --script auth www.uandina.edu.pe |
| **Opción** | -f: fragmentar paquetes.<br>-sS: Análisis TCP.<br>-sV: Sondear puertos abiertos.<br>--script: auth: Para script de autenticación. |
| **Objetivo** | Comprobar la existen usuarios pero con contraseñas vacías. |
| **Número de Pruebas** | 3 |
| **Tiempo de Ejecución** | 15 minutos aprox. |

**Fuente:** Elaboración propia.

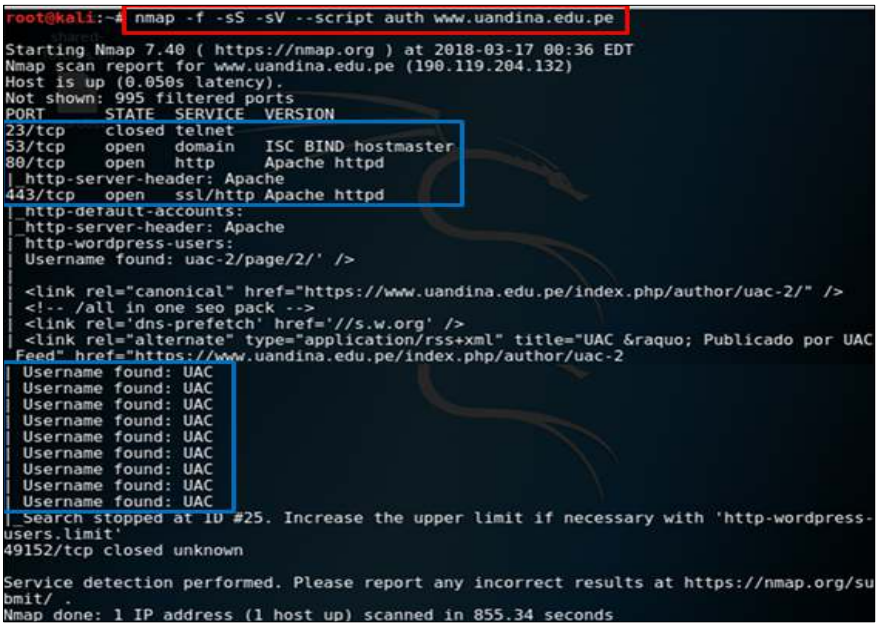



*Figura 25.* Opción nmap -f -sS -sV --script auth.
**Fuente:** Elaboración propia con el software Kali-Linux.

**Comentario**: En el primer recuadro azul se muestra cómo a través de la herramienta se consigue información resaltante. Del mismo modo, en el segundo recuadro azul muestran el listado los usuarios de nombre "UAC" en un tiempo determinado, al tener esta información del nombre de usuario, esto podría prestar a un ataque de fuerza bruta; es por ello que se recomienda quitar el nombre de usuario y prevenir ataques.

**Opción -f -sS -sV - -Script default**

Tabla 9.
*Opción nmap -f -sS -sV --script default.*

| **Sniffer con Nmap opción: -f -sS -sV - -Script default** | |
|---|---|
| **Herramienta** | Nmap |
| **Comando** | nmap -f -sS -sV --script default www.uandina.edu.pe |
| **Opción** | -f: fragmentar paquetes.<br>-sS: Análisis TCP.<br>-sV: Sondear puertos abiertos.<br>--script: default: Para script por defecto. |
| **Objetivo** | Escanar los scripts por defecto. |
| **Número de Pruebas** | 1 |
| **Tiempo de Ejecución** | 4 minutos aprox. |

**Fuente**: Elaboración propia.

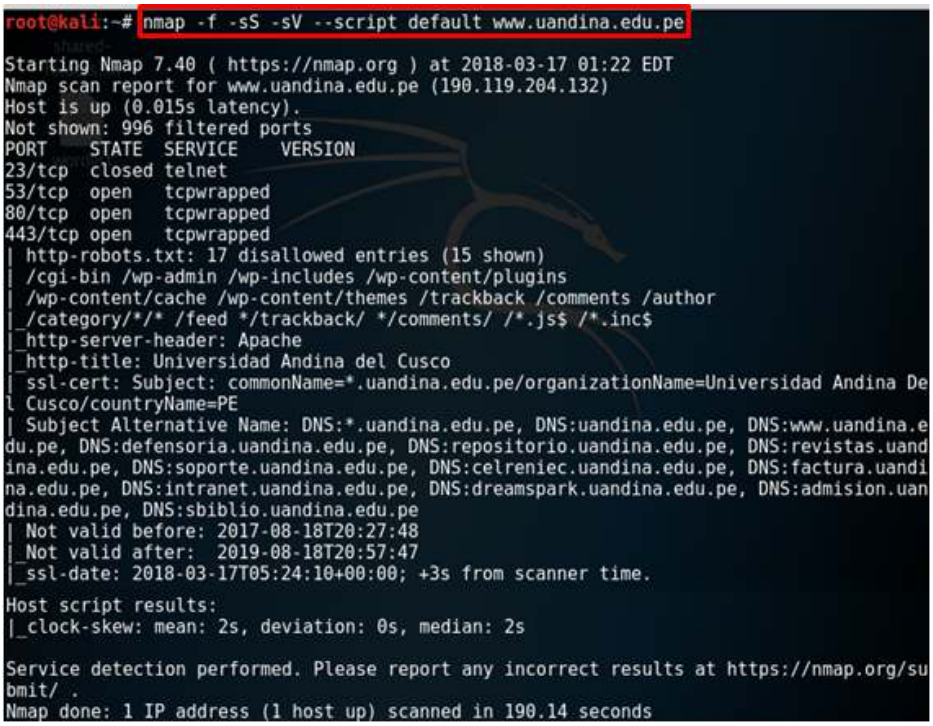



*Figura 26.* Opción nmap -f -sS -sV --script default.
**Fuente:** Elaboración propia con el software Kali-Linux.

**Comentario**: El comando muestra el análisis tcp que comprenden los puertos 23, 53, 80 y 443, los estados en general (abiertos y cerrados) y los servicios que manejan los puertos (telnet y tcpwrapped).

**Opción -f - -Script safe**

Tabla 10.
*Opción nmap -f --script safe.*

| **Sniffer con Nmap opción: -f - -Script safe** | |
|---|---|
| **Herramienta** | Nmap |
| **Comando** | `nmap -f --script safe www.uandina.edu.pe` |
| **Opción** | -f: fragmentar paquetes.<br>--script safe: ejecuta secuencias de commandos. |
| **Objetivo** | Descubrir la dirección IP del router, el nombre de dominio de la red y más información. |
| **Número de Pruebas** | 1 |
| **Tiempo de Ejecución** | 5 minutos aprox. |

**Fuente:** Elaboración propia.

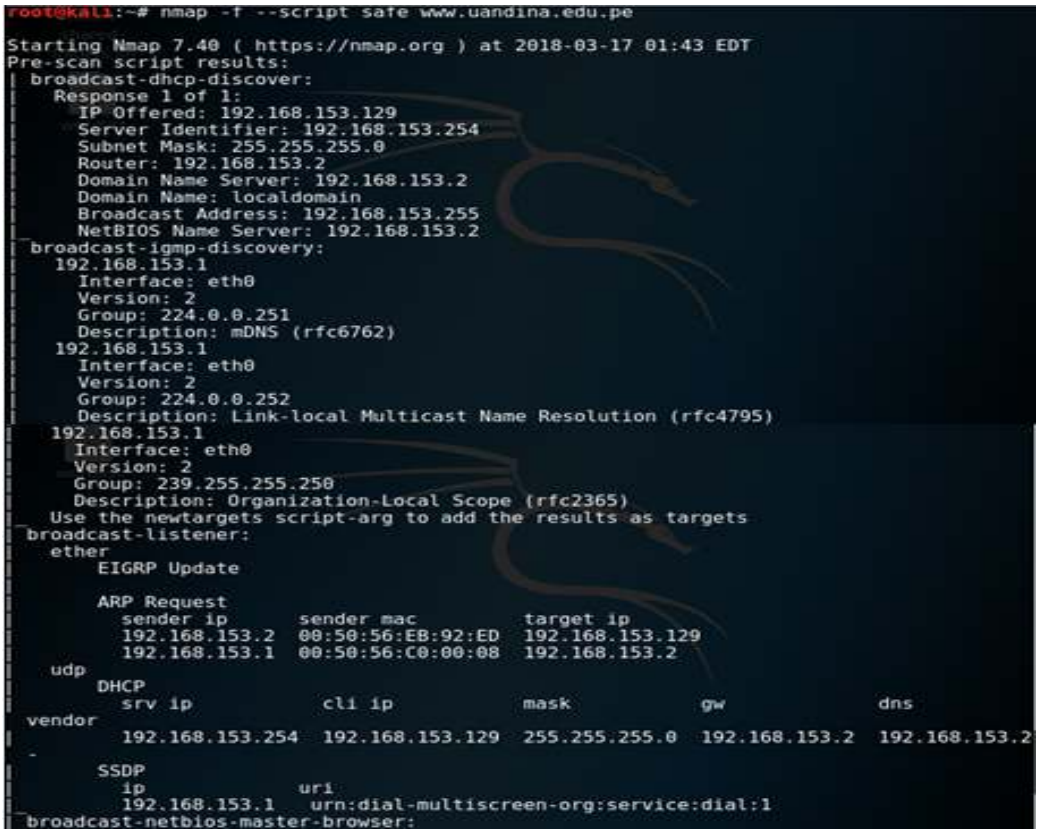



*Figura 27.* Opción nmap -f --script safe.
**Fuente:** Elaboración propia con el software Kali-Linux.

**Comentario:** Se encontró la dirección IP del router "192.168.153.2"; el nombre de dominio de la red "localdomain" y demás información.

**Opción -f - -Script vuln**

Tabla 11.
*Opción nmap -f --script vuln.*

| **Sniffer con Nmap opción: -f - -Script vuln** | |
|---|---|
| **Herramienta** | Nmap |
| **Comando** | `nmap -f --script vuln www.uandina.edu.pe` |
| **Opción** | -f: fragmentar paquetes.<br>--script vuln: permite conocer vulnerabilidades. |
| **Objetivo** | Descubrir si el equipo presenta alguna vulnerabilidad. |
| **Número de Pruebas** | 4 |
| **Tiempo de Ejecución** | 10 minutos aprox. |

**Fuente:** Elaboración propia.

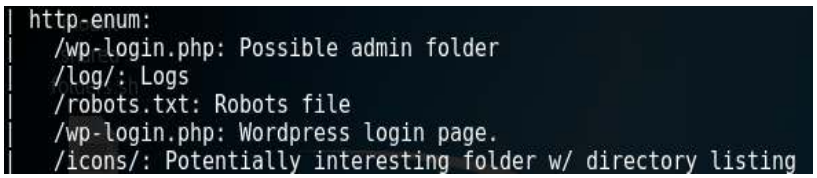



*Figura 28*. Opción nmap -f --script vuln.
**Fuente:** Elaboración propia con el software Kali-Linux.

**Comentario**: Al utilizar el comando detecta que hay una vulnerabilidad en la página de login de Wordpress de la UAC "`/wp-login.php`", eso quiere decir que se puede realizar ataques y perjudicar la información de la página.

**DISEÑO PARA LA VULNERABILIDAD DE IMPLEMENTACIÓN**

– En la vulnerabilidad de Implementación se trabajó con ataques de SQL injection, XSS y CSRF, el formato que se presenta a continuación es para completar los resultados dependiendo del ataque.

Tabla 12.
*Tipo de ataque (SQL injection, XSS y CSRF)*

| **Tipo de Ataque (SQL injection, XSS y CSRF)** | |
|---|---|
| **Fecha de inicio** | Fecha en que inicializa la ejecución. |
| **Fecha de finalización** | Fecha en la que termina la ejecución. |
| **Tiempo de escaneo** | Tiempo de demora que lleva ejecutar el ataque. |
| **Perfil** | Nombre del tipo de ataque. |
| **Portal Web a Vulnerar** | www.uandina.edu.pe |
| **Número de Pruebas** | Cantidad de veces que se aplicó el ataque. |
| **Nivel de Vulnerabilidad** | Nivel de Gravedad en la que se encuentra el ataque. |
| **Información del servidor** | |
| **Responsive** | True |
| **Server banner** | Apache |
| **Server OS** | Unknown |

**Fuente**: Elaboración propia.

**Listado de ataques que puede realizar Acunetix. (Acunetix Vulnerability Scanner, 2017)**

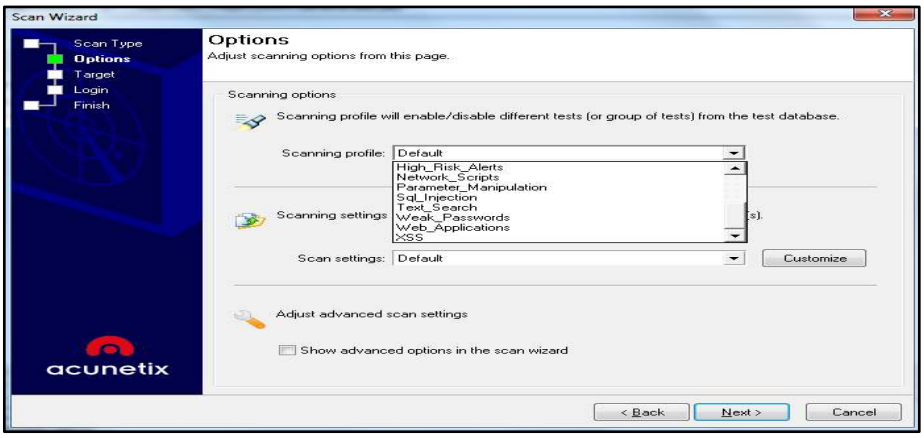



*Figura 29.* Listado de ataques de Acunetix.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario:** En ajustes de escaneo se encuentra la opción por defecto 'Default', al hacer click en 'customize' mostró la opción programada por defecto que utiliza Acunetix para todos los ataques.

**Scanning Options (opción de escaneo)**

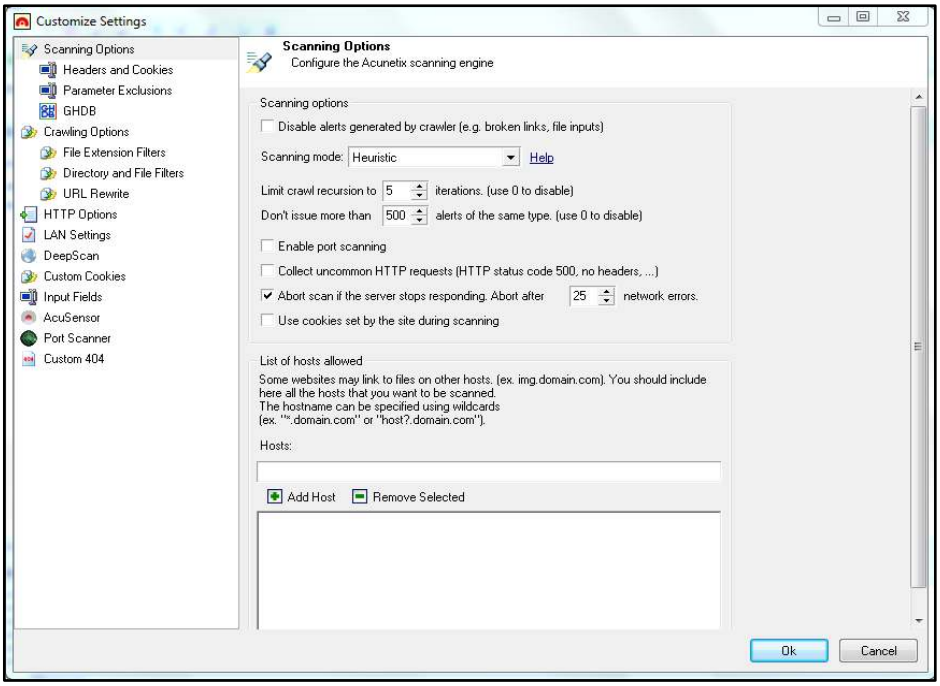



*Figura 30.* Contenido de la opción Scanning Options.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario:** En la opción de escaneo (Scanning Options) se muestra en el modo de escaneo tres opciones: Quick, Heuristic y Extensive; donde Quick es rápido, Heuristic es heurístico y Extensive es extensivo. En este caso la configuración por defecto viene con Heuristic. Descripción de las opciones completadas por defecto: El limitador de iteraciones de repeticiones de rastreo con un valor de 5. No se puede publicar más de 500 alertas del mismo tipo. Anular la exploración si el servidor deja de responder. Anular después de 25 errores de red.

**Headers and Cookies (encabezados y coockies)**

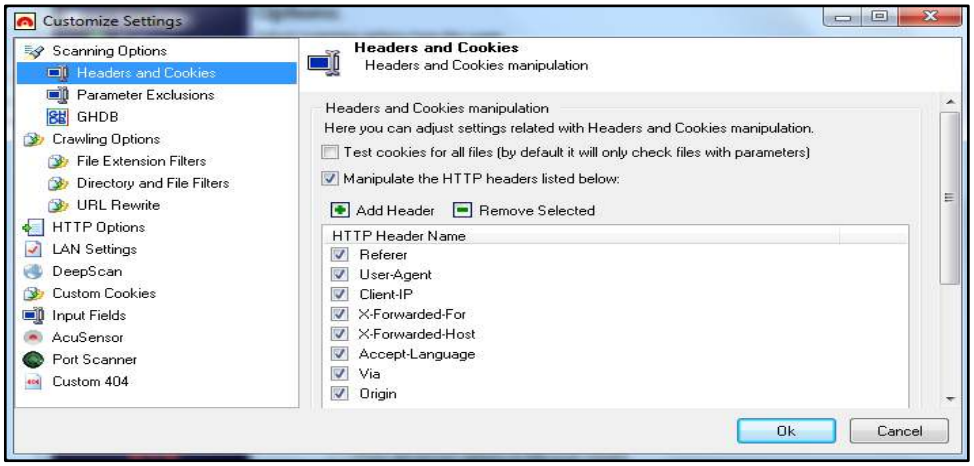



*Figura 31.* Contenido de la opción Headers and Cookies.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: En la opción Headers and Cookies se puede ajustar la configuración relacionada con la manipulación de encabezados y cookies. Descripción de las opciones completadas por defecto: Se puede manipular los encabezados HTTP enumerados seleccionados.

**Parameter Exclusions (exclusiones de parametros)**

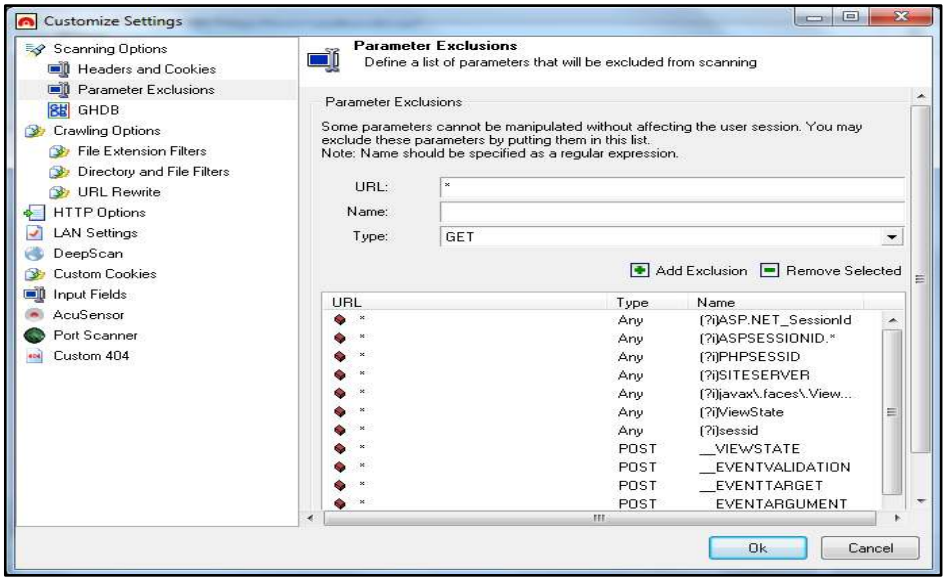



*Figura 32.* Contenido de la opción Parameter Exclusions.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Algunos parámetros no pueden ser manipulados sin afectar la sesión del usuario. Se pueden excluir estos parámetros al ponerlos en la lista.

**GHDB – Google Hacking Database**

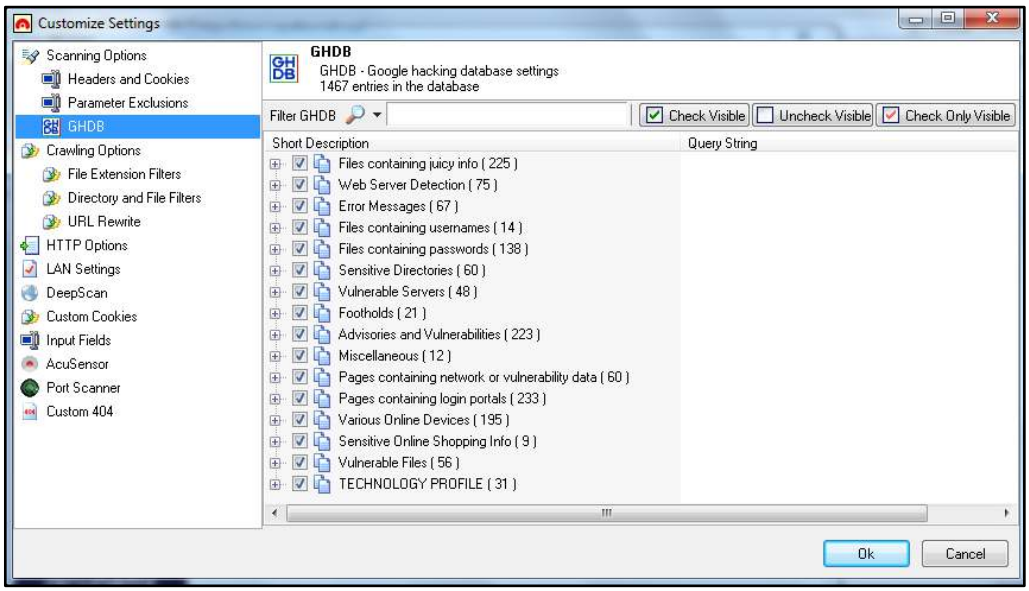



*Figura 33.* Contenido de la opción GHDB.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Con la opción de Google Hacking Database Settings se puede configurar las entradas de las bases de datos.

**Crawling Options**

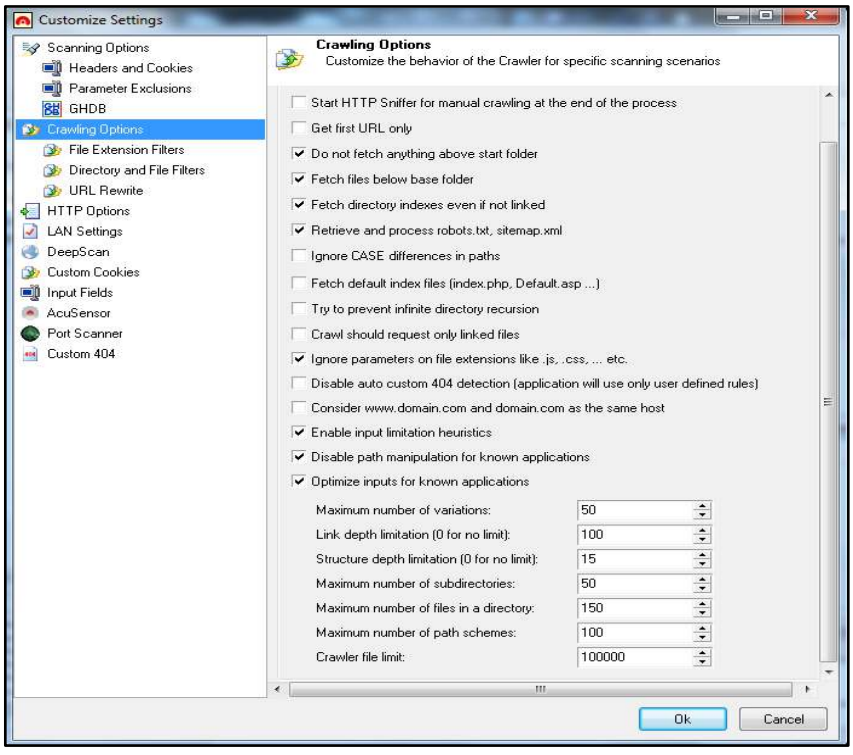



*Figura 34.* Contenido de la opción Crawling Options.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Se puede personalizar el comportamiento del rastreador para escenarios de escaneo específicos. Estas opciones definirán el comportamiento del rastreador. Descripción de las opciones completadas por defecto: No busque nada encima de la carpeta de inicio. Obtener archivos debajo de la carpeta base. Recuperar y procesar robots.txt, sitemap.xml. Ignorar parámetros en las extensiones de archivo. Habilitar la heurística de limitación de entrada. Deshabilitar la manipulación de ruta para aplicaciones conocidas. Optimizar las entradas para aplicaciones conocidas. Número máximo de variaciones 50. Limitación de profundidad del enlace (0 sin límite) 100. Limitación de profundidad de la estructura (0 sin límite) 15. Número máximo de subdirectorios 50. Número máximo de archivos en un directorio 150. Número máximo de esquemas de ruta 100. Límite de archivos de rastreo 100000.

**File Extension Filters (filtros de extensión de archivos)**

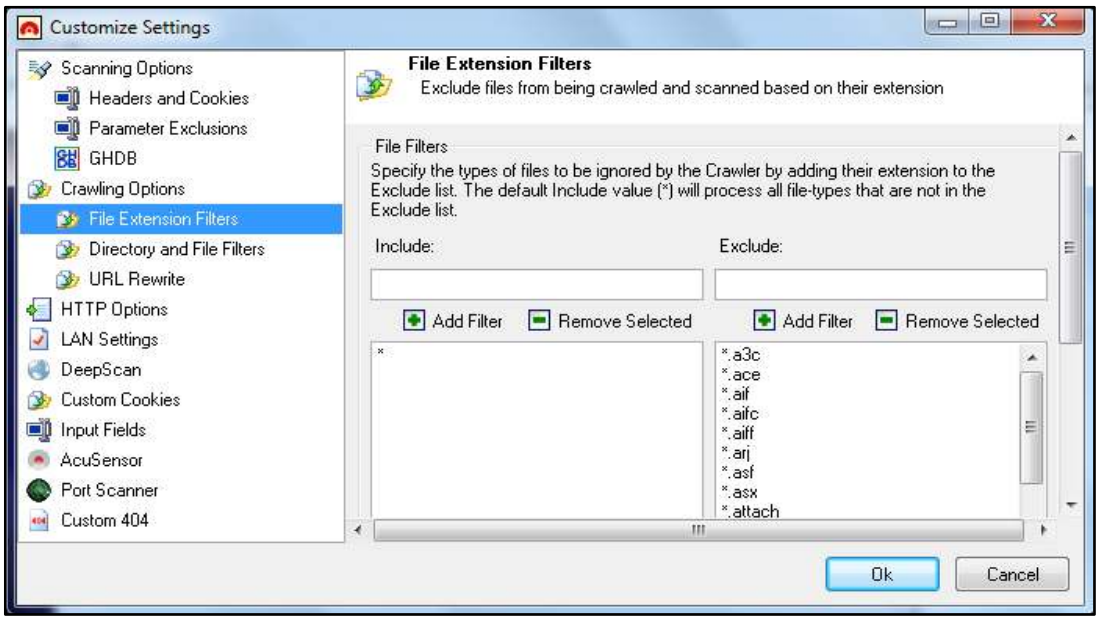



*Figura 35.* Contenido de la opción File Extensions Filters.
**Fuente:** Elaboración Propia con el software Acunetix.

**Cometario**: Se puede especificar los tipos de archivos que el rastreador debe ignorar agregando su extensión a la lista de exclusiones. El valor de inclusión

predeterminado (*) procesará todos los tipos de archivos que no están en la lista de exclusión.

**Directory and File Filters (Directorio y filtros de archivos)**

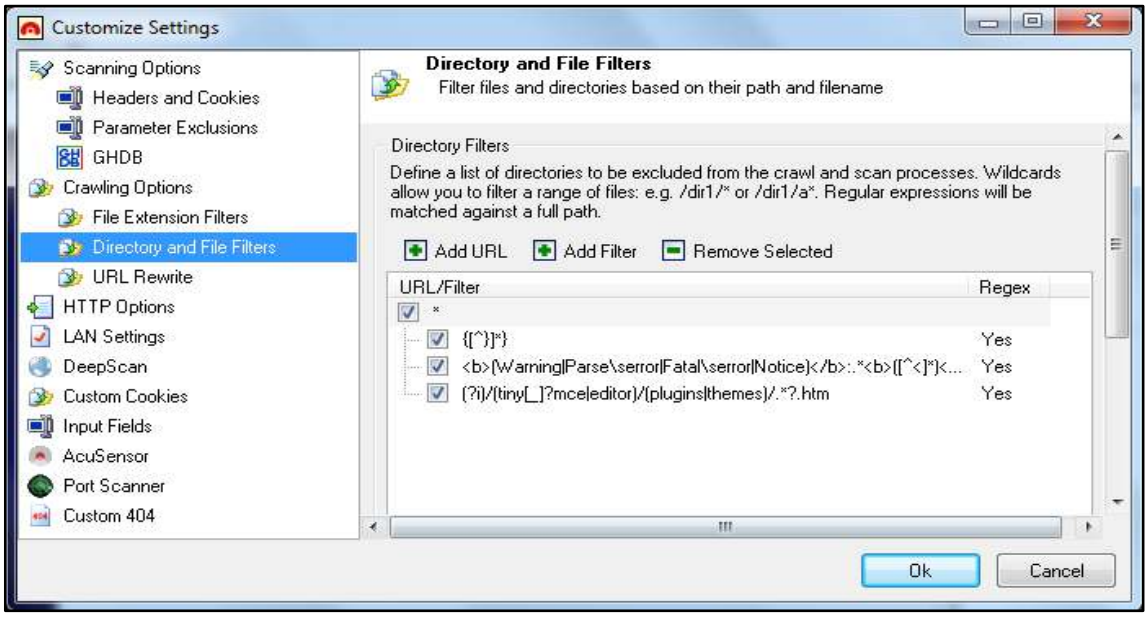



*Figura 36.* Contenido de la opción Directory and File Filters.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Se puede definir una lista de directorios que se excluirán de los procesos de rastreo y exploración. Los comodines le permiten filtrar un rango de archivo. Las expresiones regulares se compararán con una ruta completa.

**URL Rewrite (Reescritura de URL)**

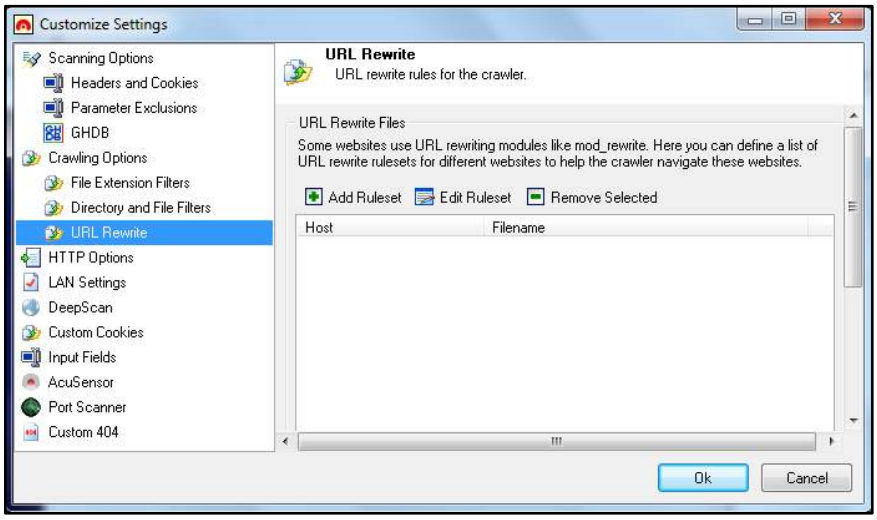



*Figura 37.* Contenido de la opción URL Rewrite.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Algunos sitios Web usan módulos de reescritura de URL como mod_rewrite. En esta opción puede definir una lista de reglas de reescritura de URL para diferentes sitios Web, para ayudar al rastreador a navegar por estos sitios Web.

**HTTP Options**

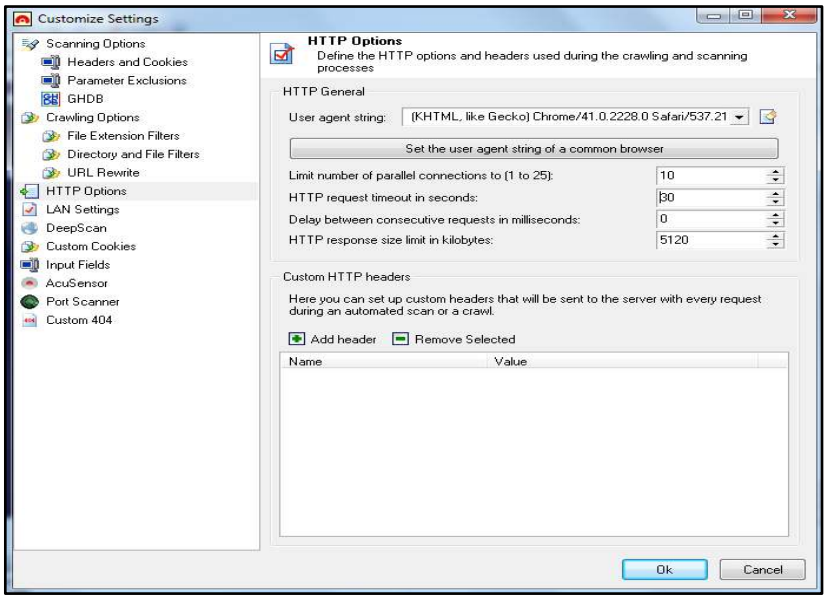



*Figura 38.* Contenido de la opción HTTP Options.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Se puede definir las opciones HTTP y los encabezados utilizados durante los procesos de rastreo y escaneo. Descripción de las opciones completadas por defecto: Cadena de agente de usuario: (Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21). Establezca la cadena del agente de usuario de un navegador común. Limitar el número de conexiones en paralelo a (1 a 25): 10. Tiempo de espera de solicitud de HTTP en segundos: 30. Retardo entre solicitudes consecutivas en milisegundos: 0. Límite de tamaño de respuesta HTTP en kilobytes: 5120.

**LAN Settings**

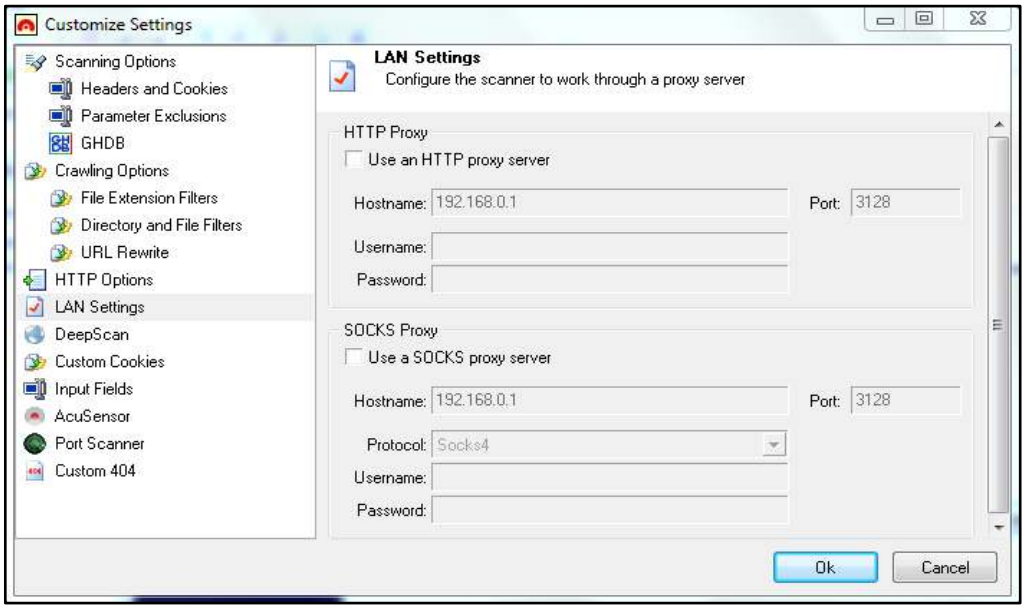



*Figura 39.* Contenido de la opción LAN Settings.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Se puede configurar el escáner para trabajar a través de un servidor proxy.

**DeepScan**

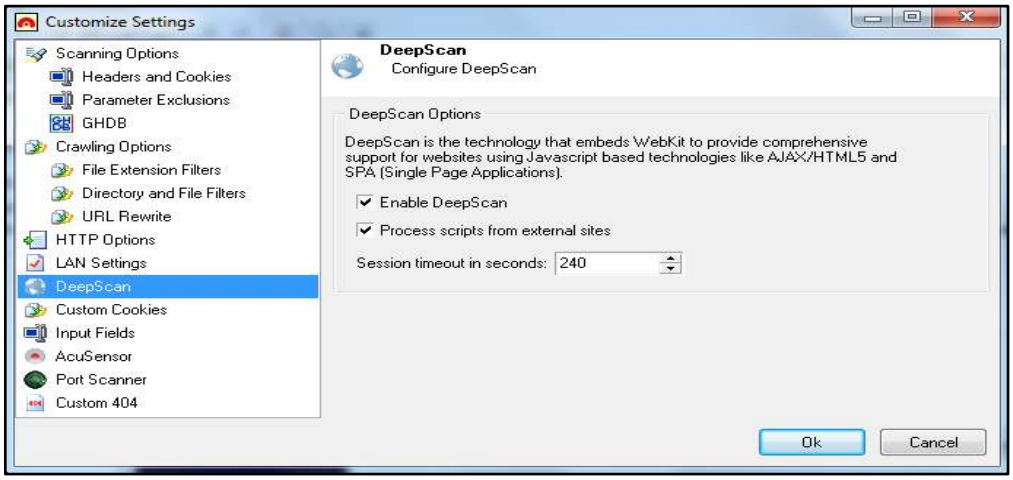



*Figura 40.* Contenido de la opción DeepScan.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: DeepScan es la tecnología que integra Webkit para proporcionar soporte integral para sitios Web que utilizan tecnologías basadas en Javascript como AJAX/HTML5 y SPA (aplicaciones de una sola página). Descripción de las opciones completadas por defecto: permitir un escaneo a fondo. Procesar scripts desde sitios externos. Tiempo de espera de la sesión en segundos: 240.

**Custom Cookies**

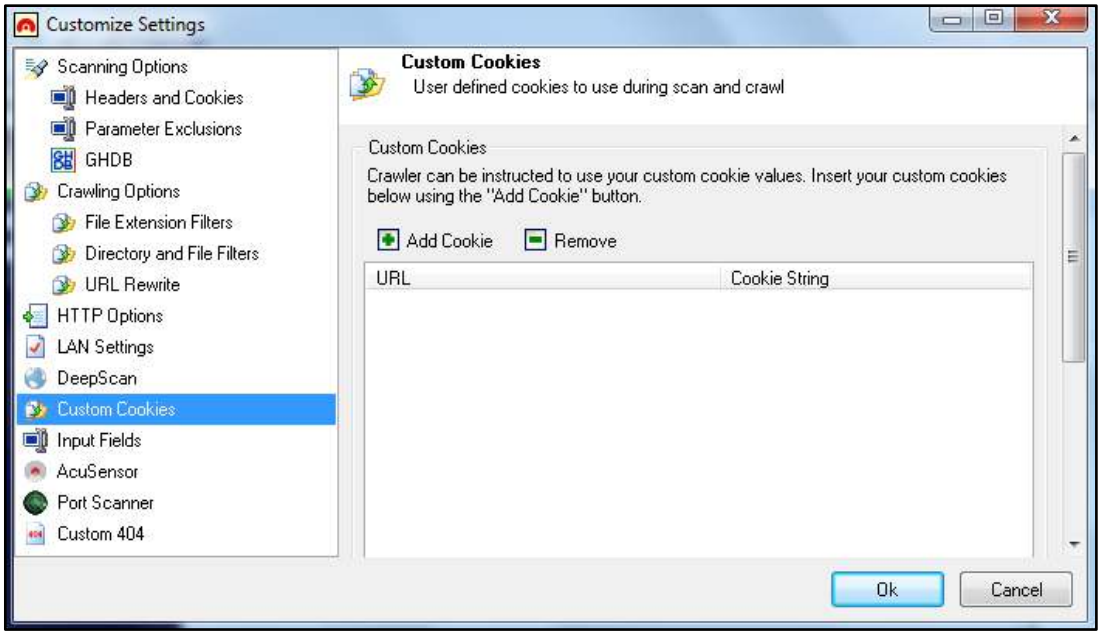



*Figura 41.* Contenido de la opción Custom Cookies.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Se pueden definir Cookies por el usuario para usar durante el escaneo y el rastreo. El rastreador puede ser instruido usando sus valores personalizados de cookies. Para insertar cookies personalizadas puede presionar el botón "Agregar cookie".

**Input Fields**

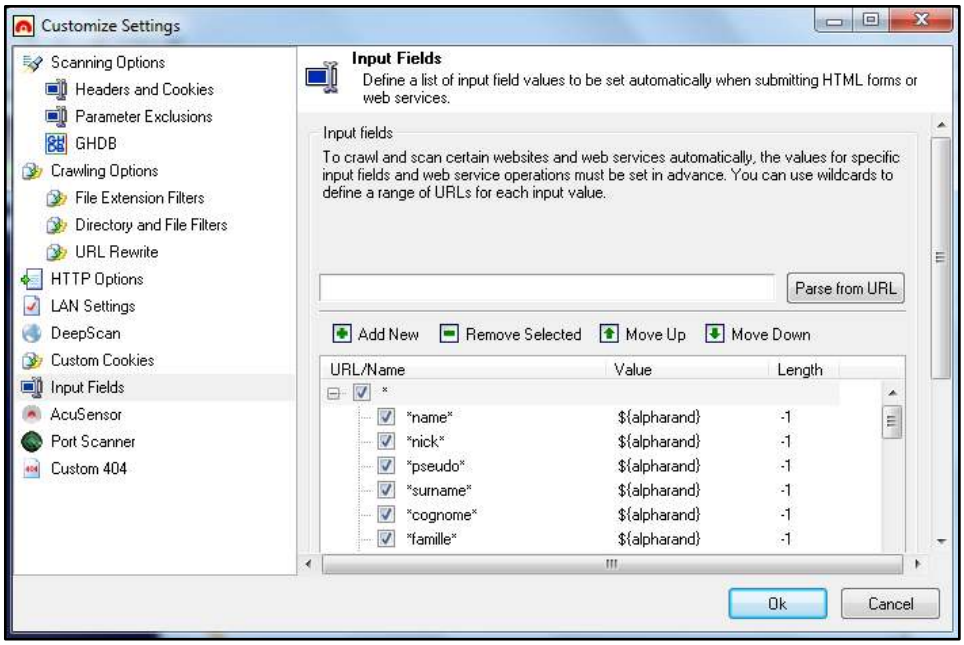



*Figura 42.* Contenido de la opción Input Fields.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Se puede definir una lista de valores de campo de entrada que se establecerán automáticamente al enviar formularios HTML o servicios Web. Para rastrear y escanear ciertos sitios Web y servicios Web automáticamente, los valores para los campos de entrada específicos y las operaciones del servicio Web deben configurarse previamente. Puede usar comodines para definir un rango de URL para cada valor de entrada.

**AcuSensor**

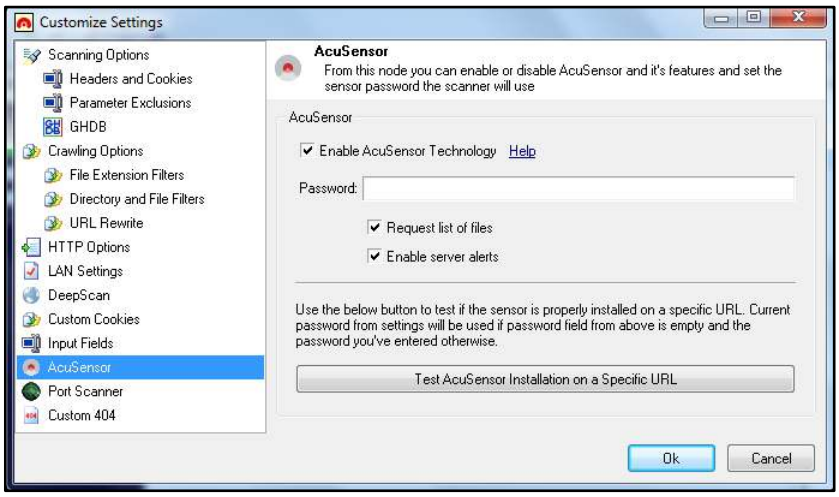



*Figura 43.* Contenido de la opción Acusensor.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Desde esta opción se puede habilitar o deshabilitar AcuSensor y sus funciones y configurar la contraseña del sensor que usará el escáner. Descripción de las opciones completadas por defecto: Habilitar la tecnología AcuSensor. Solicitar lista de archivos. Habilitar alertas del servidor. Use el botón para probar si el sensor está instalado correctamente en una URL específica. La contraseña actual de la configuración se usará si el campo de contraseña de arriba está vacío.

**Port Scanner**

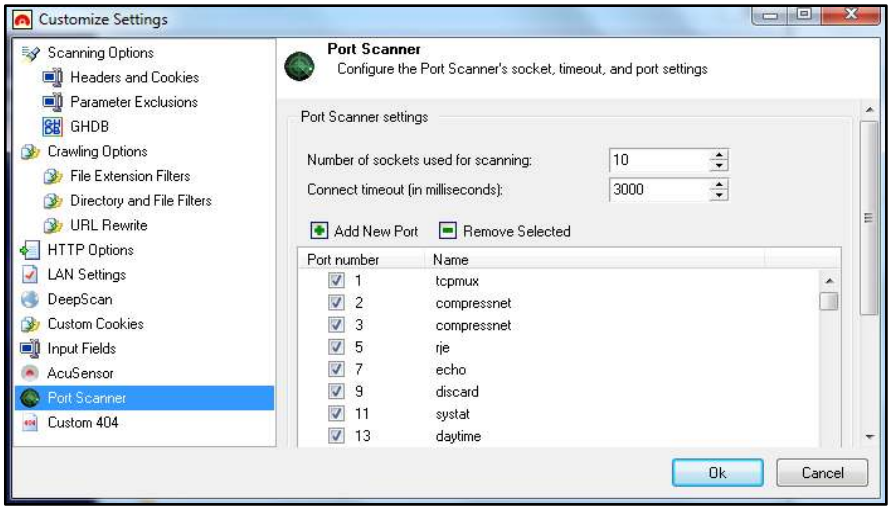



*Figura 44.* Contenido de la opción Port Scanner.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Se esta opción puede configurar el socket del escáner de puerto, el tiempo de espera y la configuración del puerto. Descripción de las opciones completadas por defecto: Número de enchufes utilizados para escanear: 10. Tiempo de espera de conexión (en milisegundos): 3000.

**Custom 404**

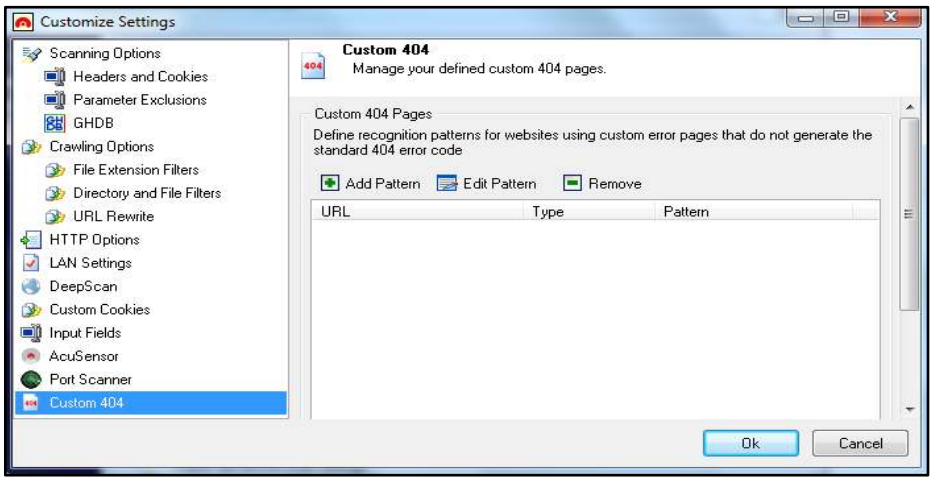



*Figura 45.* Contenido de la opción Custom 404.
**Fuente:** Elaboración Propia con el software Acunetix.

**Comentario**: Se puede administre las páginas 404 personalizadas definidas. Defina patrones de reconocimiento para sitios Web utilizando páginas de error personalizadas que no generan el código de error estándar 404.

## RESULTADOS DE LA VULNERABILIDAD DE IMPLEMENTACIÓN

Según Acunetix Web Vulnerability Scanner las vulnerabilidades serán medidas con la siguiente escala: alta, media y baja.

### a) Ataque de Inyección de código SQL o SQL injection.

**Detalles de Escaneo**

Tabla 13.
*Información SQL injection.*

| **Ataque SQL injection** | |
|---|---|
| **Fecha de inicio** | 10/02/2018 |
| **Fecha de finalización** | 11/02/2018 |
| **Tiempo de escaneo** | 11 horas, 1 minutos |
| **Perfil** | Sql_Injection |
| **Portal Web a Vulnerar** | www.uandina.edu.pe |
| **Número de Pruebas** | 4 |
| **Nivel de Vulnerabilidad** | Medio |
| **Información del servidor** | |
| **Responsive** | True |
| **Server banner** | Apache |
| **Server OS** | Unknown |

**Fuente:** Elaboración propia.

**Selección del Ataque SQL injection**

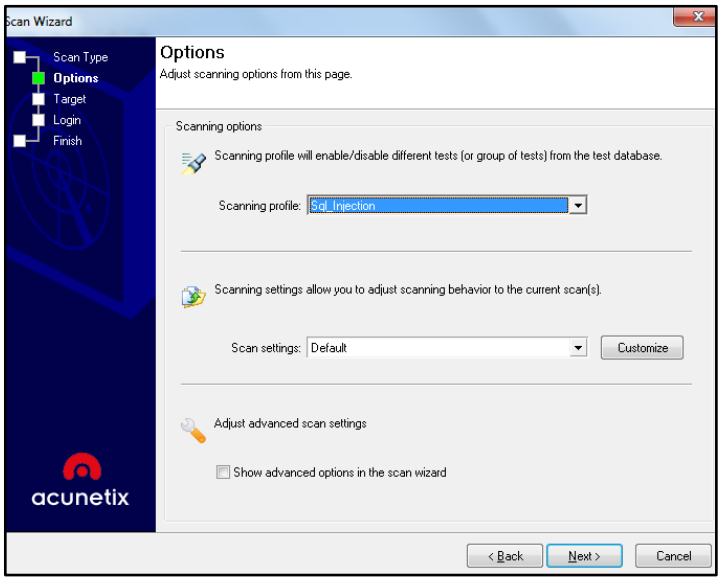



*Figura 46.* Selección del tipo de ataque.
**Fuente:** Elaboración propia con el software Acunetix.

**Configuración de Ataque SQL injection por defecto**

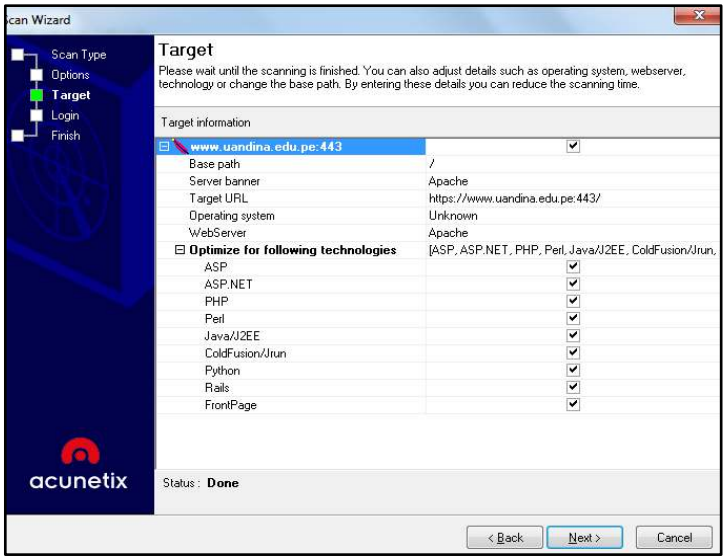



*Figura 47.* Configuración ataque SQL injection.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** Con la configuración por defecto de Acunetix, se pudo seleccionar el ataque y Acunetix se encarga de autocompletar la información del target, y en lo que corresponde a "optimize for following technologies" se seleccionó todas las tecnologías para un escaneo intenso.

**Nivel de Amenaza**

Amenaza Acunetix nivel 2: El escáner descubrió una o más vulnerabilidades de tipo de gravedad media. Debe averiguar cada una de estas vulnerabilidades para garantizar que no pase a problemas severos.


*Figura 48.* Nivel de vulnerabilidad SQL injection.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** La alerta de riesgo 2 que es de vulnerabilidad media, son causadas por la mala configuración del servidor y defectos de codificación del sitio, que facilitan la interrupción e intrusión del servidor.

**Distribución de Alertas**

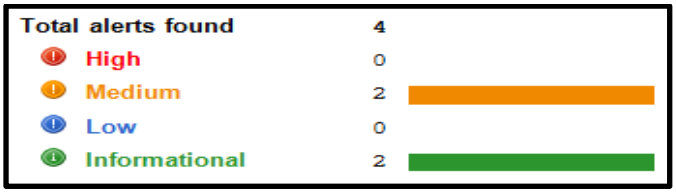



*Figura 49.* Distribución de alertas SQL injection.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** El escáner Acunetix encontró dos vulnerabilidades medias, dando a conocer que esas vulnerabilidades encontradas son causadas por la mala configuración del servidor y defectos de decodificación del sitio.

**Base de Conocimientos**

**Lista de Scripts de clientes**

- /wp-content/themes/yoo_revista_wp/warp/js/search.js
- /wp-content/plugins/widgetkit/widgets/twitter/twitter.js
- /wp-content/plugins/widgetkit/widgets/gallery/js/lazyloader.js
- /wp-content/plugins/widgetkit/widgets/slideset/js/lazyloader.js
- /wp-content/plugins/widgetkit/widgets/accordion/js/accordion.js
- /wp-content/plugins/widgetkit/widgets/slideshow/js/lazyloader.js
- /wp-content/plugins/widgetkit/widgets/map/js/lazyloader.js
- /wp-content/plugins/widgetkit/js/jquery.plugins.js
- /wp-content/plugins/widgetkit/js/responsive.js
- /wp-content/plugins/google-analytics-for-wordpress/assets/js/frontend.min.js
- /wp-includes/js/jquery/jquery.js
- /wp-includes/js/jquery/jquery-migrate.min.js
- /wp-includes/js/wp-embed.min.js

*Figura 50.* Archivos javascript.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** Estos archivos contienen un código Javascript al que se hace referencia desde el sitio Web.

**Lista de archivos con entradas**

- / - 3 inputs
- /index.php/wp-json/oembed/1.0/embed - 2 inputs
- /xmlrpc.php - 1 inputs
- /wp-content/themes/yoo_revista_wp/cache/gzip.php - 1 inputs
- /wp-admin/load-styles.php - 1 inputs
- /wp-admin/load-scripts.php - 1 inputs
- /wp-login.php - 36 inputs

*Figura 51.* Lista de archivos con entradas GET Y POST.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** Estos archivos tienen al menos una entrada GET o POST. Eso quiere decir que los ataques a los archivos con entradas pueden obtener (GET) y enviar (POST) información al servidor. La cantidad total de entradas de GET y POST encontrados son 45, mediante el ataque de SQL injection.

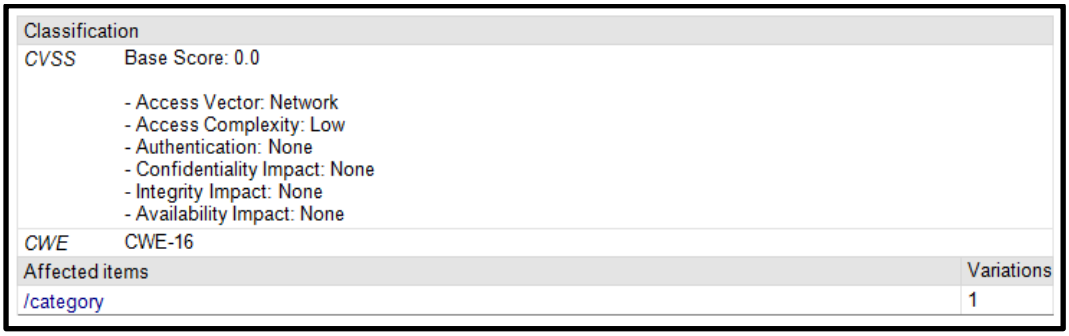
**Lista de hosts externo**


- s.w.org
- goo.gl
- erp.uandina.edu.pe
- campus.uandina.edu.pe
- soporte.uandina.edu.pe
- biblioteca.uandina.edu.pe
- dreamspark.uandina.edu.pe
- repositorio.uandina.edu.pe
- bit.ly
- correo.uandina.edu.pe
- twitter.com
- www.youtube.com
- www.mozilla.org
- mail.google.com
- www.facebook.com
- plus.google.com
- www.weatherlink.com
- windows.microsoft.com
- data
- admision.uandina.edu.pe
- defensoria.uandina.edu.pe
- wordpress.org
- www.ifeanet.org
- www.nesst.org
- www.4shared.com
- www.lan.com
- www.servir.gob.pe
- nesst-peru.org
- premio.pqs.pe
- 127.0.0.1
- www.gruporural.pucp.edu.pe
- youtu.be

*Figura 52.* Lista de hosts externos.
**Fuente:** Elaboración propia con el software Acunetix.

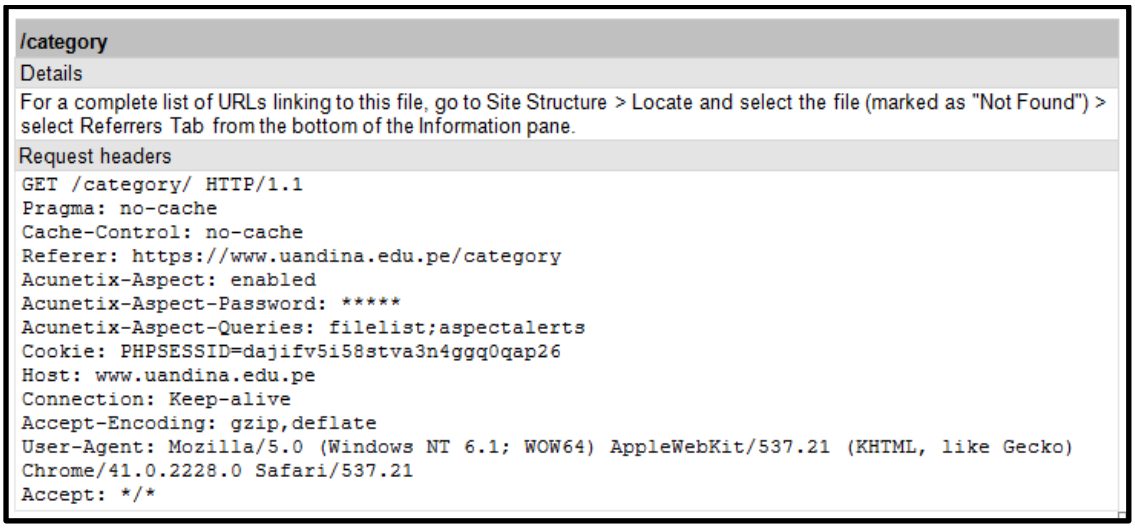
**Comentario:** Estos hosts se vincularon desde este sitio Web, pero no fueron escaneados porque no figuran en la lista de hosts permitidos.

**Enlace roto**


| Classification | |
|---|---|
| *CVSS* | Base Score: 0.0<br><br>- Access Vector: Network<br>- Access Complexity: Low<br>- Authentication: None<br>- Confidentiality Impact: None<br>- Integrity Impact: None<br>- Availability Impact: None |
| *CWE* | CWE-16 |

| Affected items | Variations |
|---|---|
| /category | 1 |

*Figura 53.* Enlaces rotos.
**Fuente:** Elaboración propia con el software Acunetix.



**/category**

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /category/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uandina.edu.pe/category
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=dajifv5i58stva3n4ggq0qap26
Host: www.uandina.edu.pe
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

*Figura 54.* Enlace roto '/category'.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario**: Se encontró un enlace roto cuyo nombre es "/Category", este enlace roto era un sitio Web el cual ya no puede consultar en la Internet; cuyo contenido ya no está disponible en los servidores u otros recursos para siempre.

Un enlace roto tiene referencia a distintos enlaces que debería llevarlo a documentos, imágenes o páginas Web, que en realidad resulta en una falla. Esta página se vinculó desde la Web pero es inaccesible. El impacto '/category' traería contratiempo al navegar por el sitio. Se recomienda eliminar los enlaces a este archivo o hacer que este accesible.

**Entrada de tipo contraseña con autocompletado habilitado**

| Classification | |
|---|---|
| *CVSS* | Base Score: 0.0<br><br>- Access Vector: Network<br>- Access Complexity: Low<br>- Authentication: None<br>- Confidentiality Impact: None<br>- Integrity Impact: None<br>- Availability Impact: None |
| *CVSS3* | Base Score: 7,5<br><br>- Attack Vector: Network<br>- Attack Complexity: Low<br>- Privileges Required: None<br>- User Interaction: None<br>- Scope: Unchanged<br>- Confidentiality Impact: High<br>- Integrity Impact: None<br>- Availability Impact: None |
| *CWE* | CWE-200 |

| Affected items | Variations |
|---|---|
| /wp-login.php | 1 |

*Figura 55.* Autocompletado habilidad.
**Fuente:** Elaboración propia con el software Acunetix.

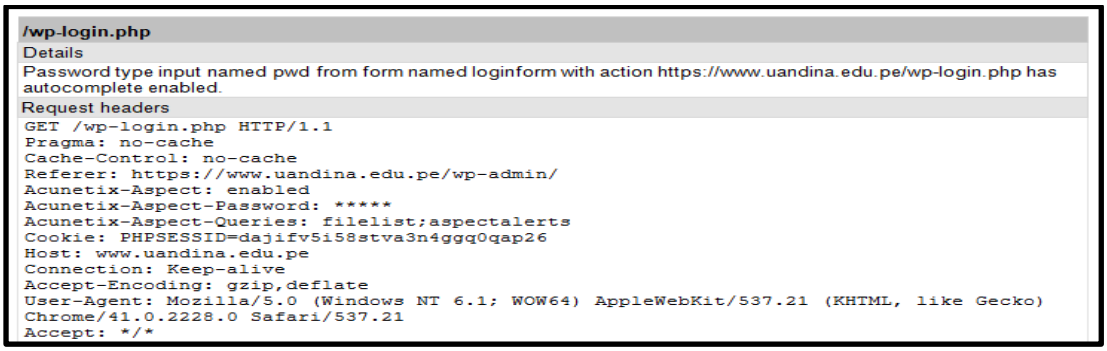



*Figura 56.* Entrada de tipo contraseña con autocompletado habilitado '/wp-login.php'.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** El autocompletado de contraseñas es útil si somos los únicos usuarios del equipo ya que nos ahorra tiempo evitando ingresar una y otra vez pero esto puede llegar a ser un riesgo de seguridad al quedar almacenada la contraseña y en cualquier momento alguien puede acceder a nuestra maquina o algún hacker puede acceder remotamente, obtener nuestra contraseña y perjudicar nuestra información.

Cuando se ingresa un nuevo nombre y contraseña en un formulario y se envía el formulario, el navegador pregunta si se debe guardar la contraseña. A continuación, cuando se muestra el formulario, el nombre y la contraseña se autocompletan o se completan a medida que se ingresa el nombre. Un hacker con acceso local podría obtener la contraseña de texto claro del caché del navegador. Su impacto sería de una posible divulgación de información sensible. Y se recomienda deshabilitar el autocompletado de contraseñas.

**Elementos Escaneados (Informe de Cobertura)**

– 599 URLs escaneadas. 3 vulnerabilidades encontradas.

**Sitios Afectados**

– https://www.uandina.edu.pe/wp-login.php?action=lostpassword

– https://www.uandina.edu.pe/category

– https://www.uandina.edu.pe/wp-admin

**b) Ataque Cross-site Scripting o XSS.**

**Detalles de Escaneo**

Tabla 14.
*Información XSS.*

| **Ataque XSS** | |
|---|---|
| **Fecha de inicio** | 11/02/2018 |
| **Fecha de finalización** | 11/02/2018 |
| **Tiempo de escaneo** | 1 horas, 52 minutos |
| **Perfil** | XSS |
| **Portal Web a Vulnerar** | www.uandina.edu.pe |
| **Número de Pruebas** | 4 |
| **Nivel de Vulnerabilidad** | Medio |
| **Información del servidor** | |
| **Responsive** | True |
| **Server banner** | Apache |
| **Server OS** | Unknown |

**Fuente:** Elaboración propia.

**Selección del Ataque XSS**

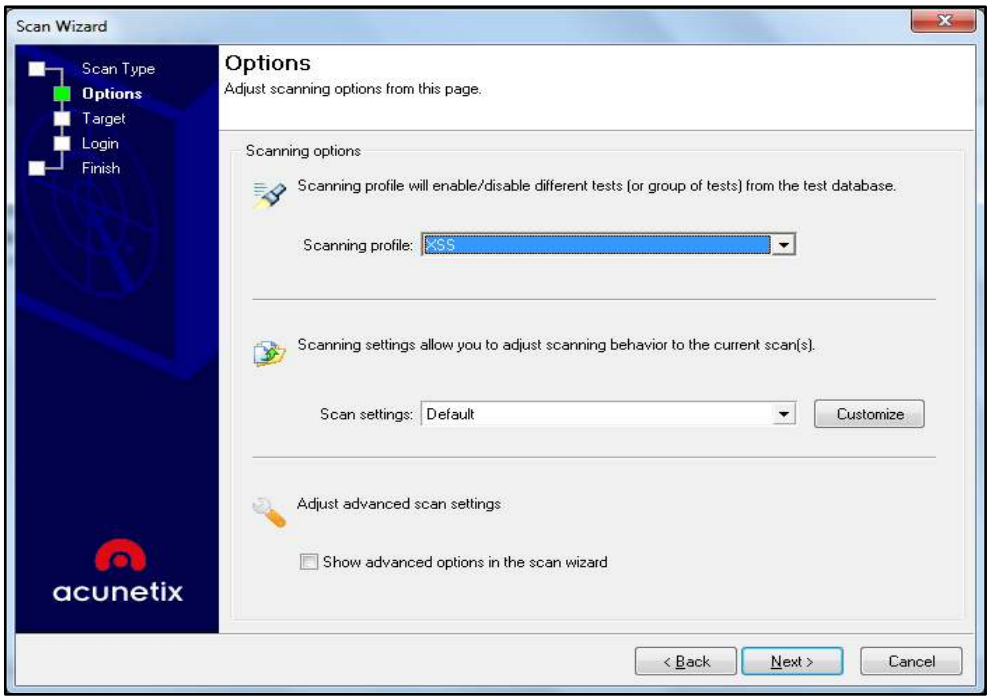



*Figura 57.* Selección del tipo de ataque.
**Fuente:** Elaboración propia con el software Acunetix.

**Configuración de Ataque XSS por defecto**

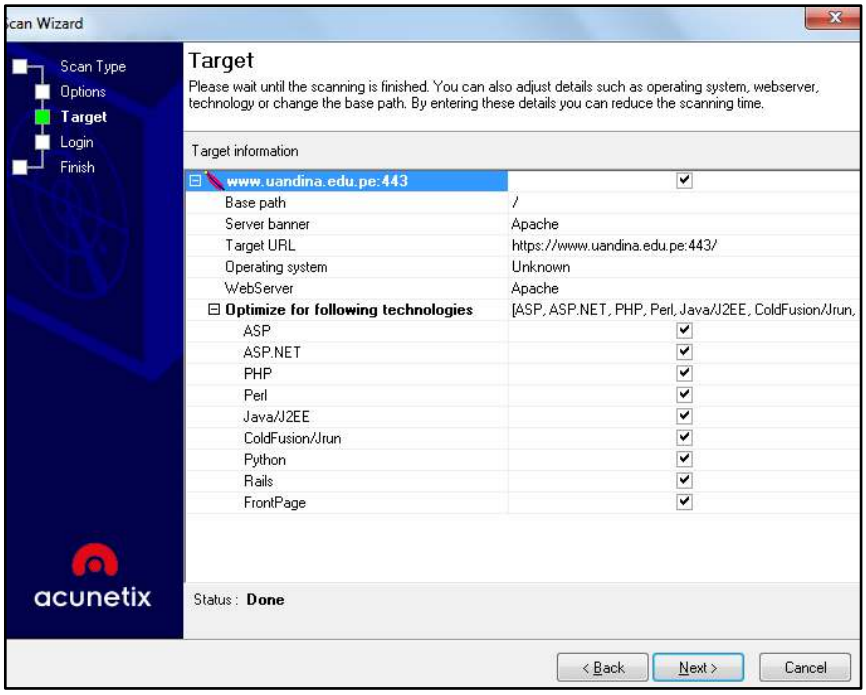



*Figura 58.* Configuración ataque XSS.
**Fuente:** Elaboración propia con el software Acunetix.

**Nivel de Amenaza**

Amenaza Acunetix nivel 2: El escáner descubrió una o más vulnerabilidades de tipo de gravedad media. Debe averiguar cada una de estas vulnerabilidades para garantizar que no pase a problemas severos.


*Figura 59.* Nivel de vulnerabilidad XSS.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** La alerta de riesgo 2 que es de vulnerabilidad media, son causadas por la mala configuración del servidor y defectos de codificación del sitio, que facilitan la interrupción e intrusión del servidor.

**Distribución de Alertas**

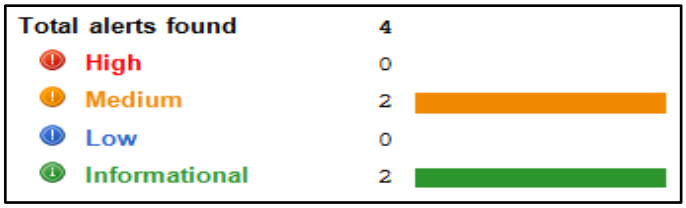



*Figura 60.* Distribución de alertas XSS.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** El escáner Acunetix encontró dos vulnerabilidades medias, dando a conocer que esas vulnerabilidades encontradas son causadas por la mala configuración del servidor y defectos de decodificación del sitio.

**Base de Conocimientos**

**Lista de Scripts de clientes**

- /wp-content/themes/yoo_revista_wp/warp/js/search.js
- /wp-content/plugins/widgetkit/widgets/twitter/twitter.js
- /wp-content/plugins/widgetkit/widgets/gallery/js/lazyloader.js
- /wp-content/plugins/widgetkit/widgets/slideset/js/lazyloader.js
- /wp-content/plugins/widgetkit/widgets/accordion/js/accordion.js
- /wp-content/plugins/widgetkit/widgets/slideshow/js/lazyloader.js
- /wp-content/plugins/widgetkit/widgets/map/js/lazyloader.js
- /wp-content/plugins/widgetkit/js/jquery.plugins.js
- /wp-content/plugins/widgetkit/js/responsive.js
- /wp-content/plugins/google-analytics-for-wordpress/assets/js/frontend.min.js
- /wp-includes/js/jquery/jquery.js
- /wp-includes/js/jquery/jquery-migrate.min.js
- /wp-includes/js/wp-embed.min.js

*Figura 61.* Archivos javascript.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** Estos archivos contienen un código Javascript al que se hace referencia desde el sitio Web.

**Lista de archivos con entradas**

- / - 3 inputs
- /index.php/wp-json/oembed/1.0/embed - 2 inputs
- /xmlrpc.php - 1 inputs
- /wp-content/themes/yoo_revista_wp/cache/gzip.php - 1 inputs
- /wp-admin/load-styles.php - 1 inputs
- /wp-admin/load-scripts.php - 1 inputs
- /wp-login.php - 39 inputs

*Figura 62.* Lista de archivos con entradas GET Y POST.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** Estos archivos tienen al menos una entrada GET o POST. Eso quiere decir que los ataques a los archivos con entradas pueden obtener (GET) y enviar (POST) información al servidor. La cantidad total de entradas de GET y POST encontrados son 48, mediante el ataque de XSS.

**Lista de hosts externo**

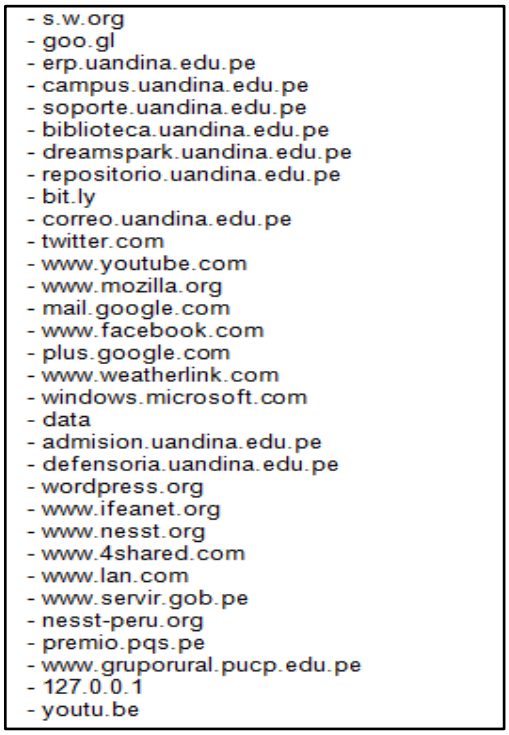

- s.w.org
- goo.gl
- erp.uandina.edu.pe
- campus.uandina.edu.pe
- soporte.uandina.edu.pe
- biblioteca.uandina.edu.pe
- dreamspark.uandina.edu.pe
- repositorio.uandina.edu.pe
- bit.ly
- correo.uandina.edu.pe
- twitter.com
- www.youtube.com
- www.mozilla.org
- mail.google.com
- www.facebook.com
- plus.google.com
- www.weatherlink.com
- windows.microsoft.com
- data
- admision.uandina.edu.pe
- defensoria.uandina.edu.pe
- wordpress.org
- www.ifeanet.org
- www.nesst.org
- www.4shared.com
- www.lan.com
- www.servir.gob.pe
- nesst-peru.org
- premio.pqs.pe
- www.gruporural.pucp.edu.pe
- 127.0.0.1
- youtu.be

*Figura 63.* Lista de hosts externos.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** Estos hosts se vincularon desde este sitio Web, pero no fueron escaneados porque no figuran en la lista de hosts permitidos.

**Enlace Roto**

| Classification | | |
|---|---|---|
| *CVSS* | Base Score: 0.0<br><br>- Access Vector: Network<br>- Access Complexity: Low<br>- Authentication: None<br>- Confidentiality Impact: None<br>- Integrity Impact: None<br>- Availability Impact: None | |
| *CWE* | CWE-16 | |
| Affected items | | Variations |
| /category | | 1 |

*Figura 64.* Enlaces rotos.
**Fuente:** Elaboración propia con el software Acunetix.

**/category**

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /category/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uandina.edu.pe/category
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ivappu44doqove9d26mfd03kr2
Host: www.uandina.edu.pe
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

*Figura 65.* Enlace roto '/category'.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** Se encontró un enlace roto cuyo nombre es "/Category", este enlace roto era un sitio Web el cual ya no puede consultar en la Internet; cuyo contenido ya no está disponible en los servidores u otros recursos para siempre.

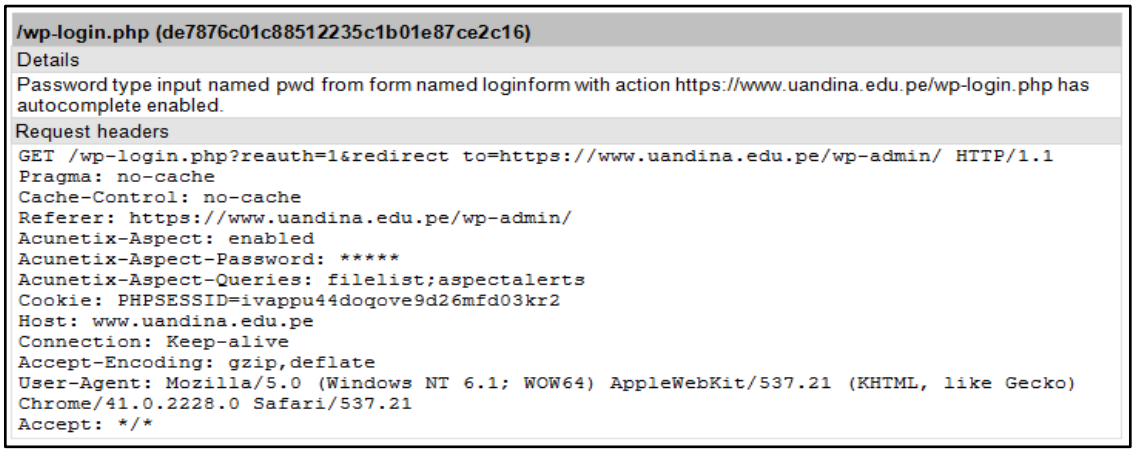
Un enlace roto tiene referencia a distintos enlaces que debería llevarlo a documentos, imágenes o páginas Web, que en realidad resulta en una falla. Esta página se vinculó desde la Web pero es inaccesible. El impacto '/category' traería contratiempo al navegar por el sitio. Se recomienda eliminar los enlaces a este archivo o hacer que este accesible.

**Entrada de tipo contraseña con autocompletado habilitado**

| Classification | |
|---|---|
| *CVSS* | Base Score: 0.0<br><br>- Access Vector: Network<br>- Access Complexity: Low<br>- Authentication: None<br>- Confidentiality Impact: None<br>- Integrity Impact: None<br>- Availability Impact: None |
| *CVSS3* | Base Score: 7,5<br><br>- Attack Vector: Network<br>- Attack Complexity: Low<br>- Privileges Required: None<br>- User Interaction: None<br>- Scope: Unchanged<br>- Confidentiality Impact: High<br>- Integrity Impact: None<br>- Availability Impact: None |
| *CWE* | CWE-200 |

| Affected items | Variations |
|---|---|
| /wp-login.php (de7876c01c88512235c1b01e87ce2c16) | 1 |

*Figura 66.* Autocompletado habilitado.
**Fuente:** Elaboración propia con el software Acunetix.



/wp-login.php (de7876c01c88512235c1b01e87ce2c16)

Details

Password type input named pwd from form named loginform with action https://www.uandina.edu.pe/wp-login.php has autocomplete enabled.

Request headers

```
GET /wp-login.php?reauth=1&redirect to=https://www.uandina.edu.pe/wp-admin/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uandina.edu.pe/wp-admin/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ivappu44doqove9d26mfd03kr2
Host: www.uandina.edu.pe
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

*Figura 67.* Entrada de tipo contraseña con autocompletado habilitado '/wp-login.php'.

**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** El autocompletado de contraseñas es útil si somos los únicos usuarios del equipo ya que nos ahorra tiempo evitando ingresar una y otra vez pero esto puede llegar a ser un riesgo de seguridad al quedar almacenada la contraseña y en cualquier momento alguien puede acceder a nuestra maquina o algún hacker puede acceder remotamente, obtener nuestra contraseña y perjudicar nuestra información.

Cuando se ingresa un nuevo nombre y contraseña en un formulario y se envía el formulario, el navegador pregunta si se debe guardar la contraseña. A continuación, cuando se muestra el formulario, el nombre y la contraseña se completan automáticamente o se completan a medida que se ingresa el nombre. Un hacker con acceso local podría obtener la contraseña de texto claro del caché del navegador. Su impacto sería de una posible divulgación de información sensible. Y se recomienda deshabilitar el autocompletado de contraseñas.

**Elementos Escaneados (Informe de Cobertura)**

– 599 URLs escaneadas. 2 vulnerabilidades encontradas.

**Sitios Afectados**

– https://www.uandina.edu.pe/category

– https://www.uandina.edu.pe/wp-admin

**c) Ataque Cross-site request reference forgery o CSRF.**

**Detalles de Escaneo**

Tabla 15.
*Información CSRF.*

| **Ataque CSRF** | |
|---|---|
| **Fecha de inicio** | 11/02/2018 |
| **Fecha de finalización** | 11/02/2018 |
| **Tiempo de escaneo** | 9 minutos, 2 segundos |
| **Perfil** | CSRF |
| **Portal Web a Vulnerar** | www.uandina.edu.pe |
| **Número de Pruebas** | 4 |
| **Nivel de Vulnerabilidad** | Medio |
| **Información del servidor** | |
| **Responsive** | True |
| **Server banner** | Apache |
| **Server OS** | Unknown |

**Fuente:** Elaboración propia.

**Selección del Ataque CSRF**

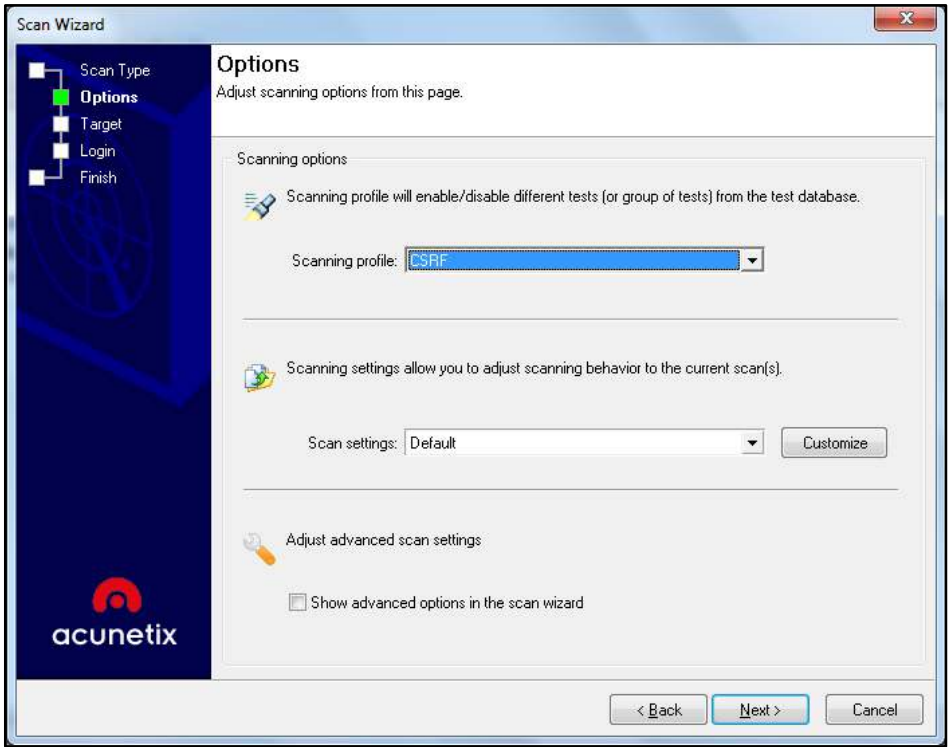



*Figura 68.* Selección del tipo de ataque.
**Fuente:** Elaboración propia con el software Acunetix.

**Configuración de Ataque XSS por defecto**

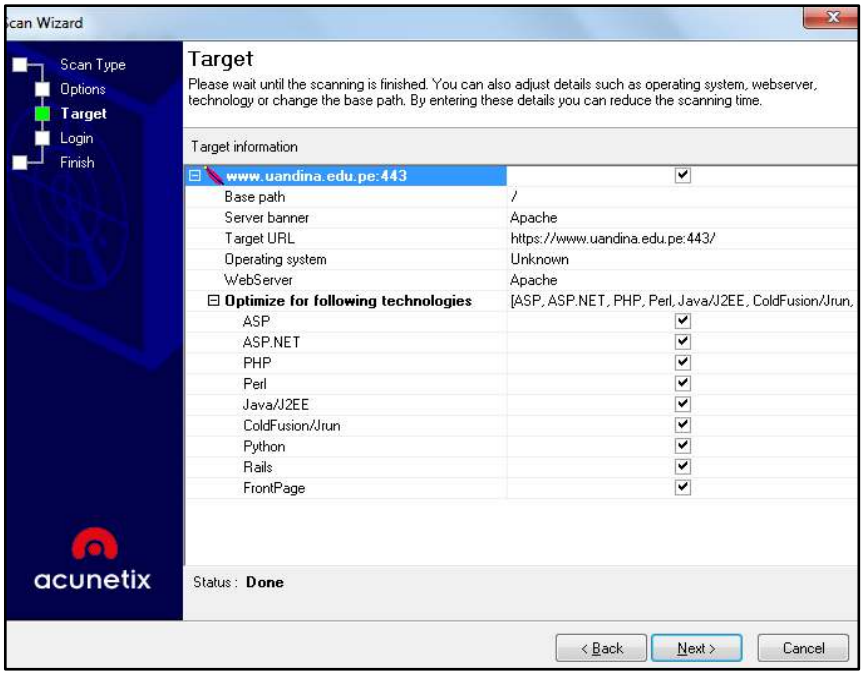



*Figura 69.* Configuración ataque CSRF.
**Fuente:** Elaboración propia con el software Acunetix.

**Nivel de Amenaza**

Amenaza Acunetix nivel 2: El escáner descubrió una o más vulnerabilidades de tipo de gravedad media. Debe averiguar cada una de estas vulnerabilidades para garantizar que no pase a problemas severos.


*Figura 70.* Nivel de vulnerabilidad CSRF.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** La alerta de riesgo 2 que es de vulnerabilidad media, son causadas por la mala configuración del servidor y defectos de codificación del sitio, que facilitan la interrupción e intrusión del servidor.

**Distribución de Alertas**

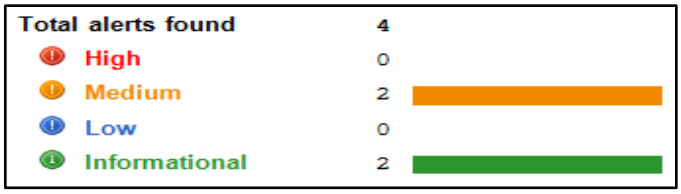



*Figura 71.* Distribución de alertas CSRF.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** El escáner Acunetix encontró dos vulnerabilidades medias, dando a conocer que esas vulnerabilidades encontradas son causadas por la mala configuración del servidor y defectos de decodificación del sitio.

**Base de Conocimientos**

Lista de Scripts de clientes


*Figura 72.* Archivos javascript.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** Estos archivos contienen un código Javascript al que se hace referencia desde el sitio Web.

**Lista de archivos con entradas**

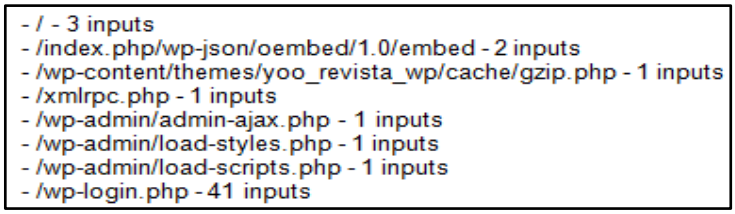



*Figura 73.* Lista de archivos con entradas GET Y POST.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** Estos archivos tienen al menos una entrada GET o POST. Eso quiere decir que los ataques a los archivos con entradas pueden obtener (GET) y enviar (POST) información al servidor. La cantidad total de entradas de GET y POST encontrados son 48, mediante el ataque de XSS.

**Lista de hosts externo**

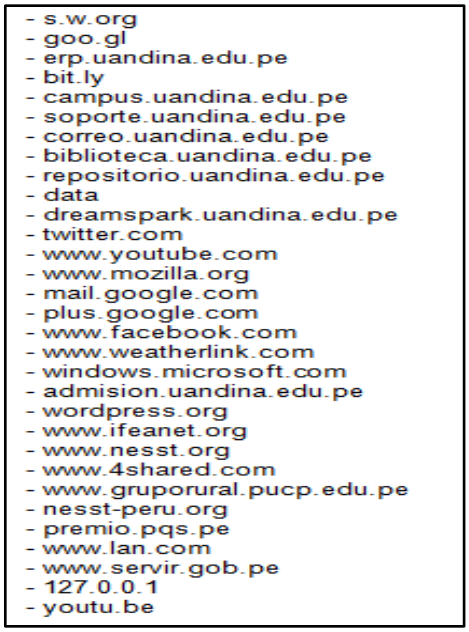



*Figura 74*. Lista de hosts externos.
**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** Estos hosts se vincularon desde este sitio Web, pero no fueron escaneados porque no figuran en la lista de hosts permitidos.

**Enlace Roto**


*Figura 75.* Enlaces rotos.
**Fuente:** Elaboración propia con el software Acunetix.

**/category**

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /category/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uandina.edu.pe/category
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=k6m601cbcf0ii5b094f3ebnn35
Host: www.uandina.edu.pe
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

*Figura 76.* Enlace roto '/category'.

**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** Se encontró un enlace roto cuyo nombre es "/Category", este enlace roto era un sitio Web el cual ya no puede consultar en la Internet; cuyo contenido ya no está disponible en los servidores u otros recursos para siempre.

Un enlace roto tiene referencia a distintos enlaces que debería llevarlo a documentos, imágenes o páginas Web, que en realidad resulta en una falla. Esta página se vinculó desde la Web pero es inaccesible. El impacto '/category' traería contratiempo al navegar por el sitio. Se recomienda eliminar los enlaces a este archivo o hacer que este accesible.

**Entrada de tipo contraseña con autocompletado habilitado**.

| Classification | |
|---|---|
| *CVSS* | Base Score: 0.0<br><br>- Access Vector: Network<br>- Access Complexity: Low<br>- Authentication: None<br>- Confidentiality Impact: None<br>- Integrity Impact: None<br>- Availability Impact: None |
| *CVSS3* | Base Score: 7,5<br><br>- Attack Vector: Network<br>- Attack Complexity: Low<br>- Privileges Required: None<br>- User Interaction: None<br>- Scope: Unchanged<br>- Confidentiality Impact: High<br>- Integrity Impact: None<br>- Availability Impact: None |
| *CWE* | CWE-200 |
| Affected items | Variations |
| /wp-login.php | 1 |

*Figura 77.* Autocompletado habilidad.

**Fuente:** Elaboración propia con el software Acunetix.

/wp-login.php

Details

Password type input named pwd from form named loginform with action https://www.uandina.edu.pe/wp-login.php has autocomplete enabled.

Request headers

```
GET /wp-login.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uandina.edu.pe/wp-admin/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=k6m60lcbcf0ii5b094f3ebnn35
Host: www.uandina.edu.pe
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

*Figura 78.* Entrada de tipo contraseña con autocompletado habilitado '/wp-login.php'.

**Fuente:** Elaboración propia con el software Acunetix.

**Comentario:** El autocompletado de contraseñas es útil si somos los únicos usuarios del equipo ya que nos ahorra tiempo evitando ingresar una y otra vez pero esto puede llegar a ser un riesgo de seguridad al quedar almacenada la contraseña y en cualquier momento alguien puede acceder a nuestra maquina o algún hacker puede acceder remotamente, obtener nuestra contraseña y perjudicar nuestra información.

Cuando se ingresa un nuevo nombre y contraseña en un formulario y se envía el formulario, el navegador pregunta si se debe guardar la contraseña. A continuación, cuando se muestra el formulario, el nombre y la contraseña se completan automáticamente o se completan a medida que se ingresa el nombre. Un hacker con acceso local podría obtener la contraseña de texto claro del caché del navegador. Su impacto sería de una posible divulgación de información sensible. Y se recomienda deshabilitar el autocompletado de contraseñas.

**Elementos Escaneados (Informe de Cobertura)**

– 545 URLs escaneadas. 3 vulnerabilidades encontradas.

**Sitios Afectados**

– https://www.uandina.edu.pe/wp-login.php?action=lostpassword

– https://www.uandina.edu.pe/category

– https://www.uandina.edu.pe/wp-admin

**DISEÑO PARA LA VULNERABILIDAD DE USO**

– En la vulnerabilidad de uso uno de sus ataques es el de Denegación de Servicios (DoS), el formato que se presenta a continuación es para completar los resultados del ataque.

Tabla 16.
*Ataque DoS.*

| **Ataque DoS** | |
|---|---|
| **Software** | Linux |
| **Repositorio a clonar** | Nombre del Repositorio del GitHub clonado. |
| **Archivo del Repositorio Clonado** | Nombre del archivo que contiene el repositorio clonado. |
| **Objetivo** | Definición de lo que hará el ataque. |
| **Portal Web a Vulnerar** | www.uandina.edu.pe |
| **Número de Pruebas** | Cantidad de veces que se aplicó el ataque. |
| **Tiempo de Ejecución** | Tiempo de demora que lleva ejecutar el ataque. |
| **Nivel de Vulnerabilidad** | Nivel de Gravedad en la que se encuentra el ataque. |

**Fuente:** Elaboración propia.

**RESULTADOS DE LA VULNERABILIDAD DE USO**

**Ataque de Denegación de Servicio sobre el protocolo XML-RPC**

Tabla 17.
*Información DoS.*

| **Ataque DoS** | |
|---|---|
| **Software** | Linux |
| **Repositorio a clonar** | CVE-2018-6389 |
| **Archivo del Repositorio Clonado** | CVE-2018-6389.py |
| **Objetivo** | Hacer un ataque de DoS. |
| **Portal Web a Vulnerar** | www.uandina.edu.pe |
| **Número de Pruebas** | 6 |
| **Tiempo de Ejecución** | 30 minutos aprox. |
| **Nivel de Vulnerabilidad** | Alta |

**Fuente:** Elaboración propia.

- Se instaló kali Linux en una máquina virtual: VMware Workstation Pro donde se instaló Kali-Linux-2017.1-vm-amd64.
- Como resultado de las investigaciones el usuario WazeHell subió un repositorio con el nombre CVE-2018-6389 que esta guardada en la plataforma GitHub. El repositorio contiene código en Python el cual sirve para atacar las vulnerabilidades XML- RPC de la plataforma de WordPress, con el repositorio se puedo explotar las vulnerabilidades del portal Web de la Universidad Andina del Cusco.

  Sitio Web: https://github.com/WazeHell/CVE-2018-6389
- Se Clonó el repositorio CVE-2018-6389 de la plataforma GitHub copiando la URL de la página, utilizando la consola de Kali Linux. Comando:root@kali:~#gitclone https://github.com/WazeHell/CVE-2018-6389

```
root@kali:~# git clone https://github.com/WazeHell/CVE-2018-6389
fatal: destination path 'CVE-2018-6389' already exists and is not an empty direc
tory.
```

*Figura 79.* Comando para clonar el repositorio CVE-2018-6389.
**Fuente:** Elaboración propia con el software Kali-Linux.

**Comentario**: En este caso la clonación ya estaba realizada.

- Se accedió al repositorio CVE-2018-6389 clonada (`root@kali:~# cd CVE-2018-6389/`) y se encuentra un archivo llamado CVE-2018-6389.py elaborado en Python. Comando: root@kali:`~# nano CVE-2018-6389.py`

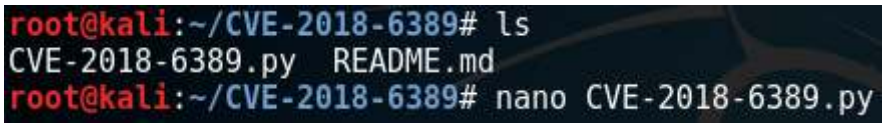



*Figura 80.* Comando para visualizar el archivo CVE-2018-6389.py.
**Fuente:** Elaboración propia con el software Kali-Linux.

- Antes de llamar al repositorio CVE-2018-6389, se ingresó al portal Web de la Universidad Andina del Cusco que utiliza la plataforma WordPress la cual presenta vulnerabilidad. URL: https://www.uandina.edu.pe


*Figura 81.* Portal Web de la Universidad Andina del Cusco.
**Fuente:** Elaboración propia de la página UAC.

- Se verificó la versión de la plataforma de Wordpress que maneja el portal Web de la Universidad Andina del Cusco. Par revisar la versión que lleva.

  Comando: "view-source:https://www.uandina.edu.pe/wp-login.php".


*Figura 82.* Versión de WordPress 4.8.5 del portal Web de la UAC.
**Fuente:** Elaboración propia de la página de WordPress de la UAC.

**Comentario**: Como se aprecia en la imagen, la versión con la que trabaja la plataforma de WordPress de la Universidad Andina del Cusco es la 4.8.5, tomando en cuenta dicha información puedo decir que cuenta con el XML-RPC activo, puesto que a partir de la versión 3.5 de WordPress viene activa por defecto y es vulnerable.

– Se Verificó que el XML-RPC este activo.

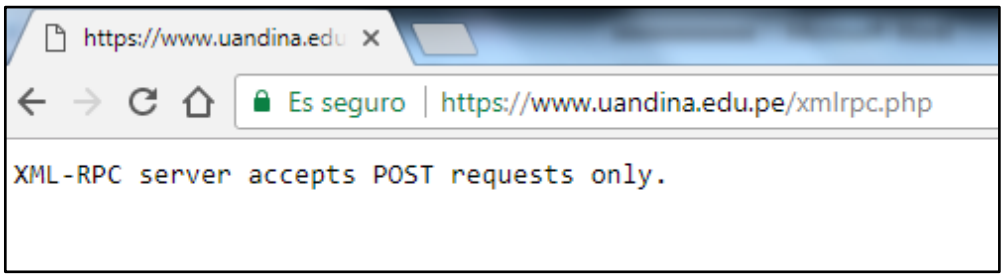



*Figura 83.* Diagnóstico del protocolo XML-RPC en el portal Web de la UAC.
**Fuente:** Elaboración propia de la página XML-RPC de la UAC.

**Comentario:** El comentario de la página Web significa que XML-RPC está activo, por lo tanto la plataforma de WordPress del portal Web de la Universidad Andina del Cusco es vulnerable.

– Se ejecutó el archivo CVE-2018-6389.py, se nombró el sitio Web a vulnerar y se eligió la cantidad de hilos a ejecutar.

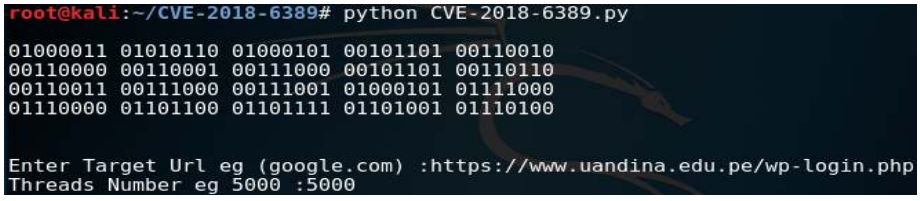



*Figura 84.* Completando el domino y cantidad de hilos.
**Fuente:** Elaboración propia con el software Kali-Linux.

- Se ejecutó el archivo CVE-2018-6389.py.

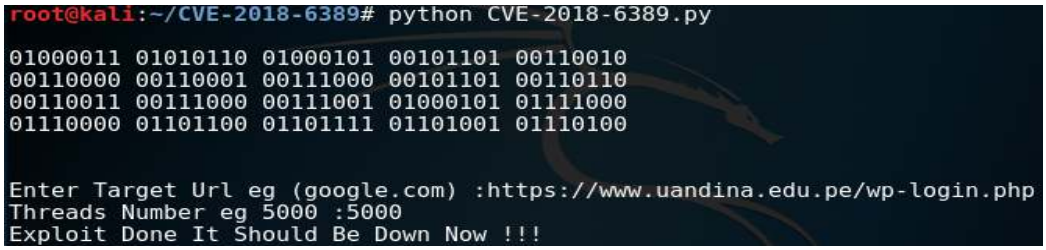



*Figura 85.* Ejecutando el archivo CVE-2018-6289.py.
**Fuente:** Elaboración propia con el software Kali-Linux.

- Portal Web de la Universidad Andina del Cusco.

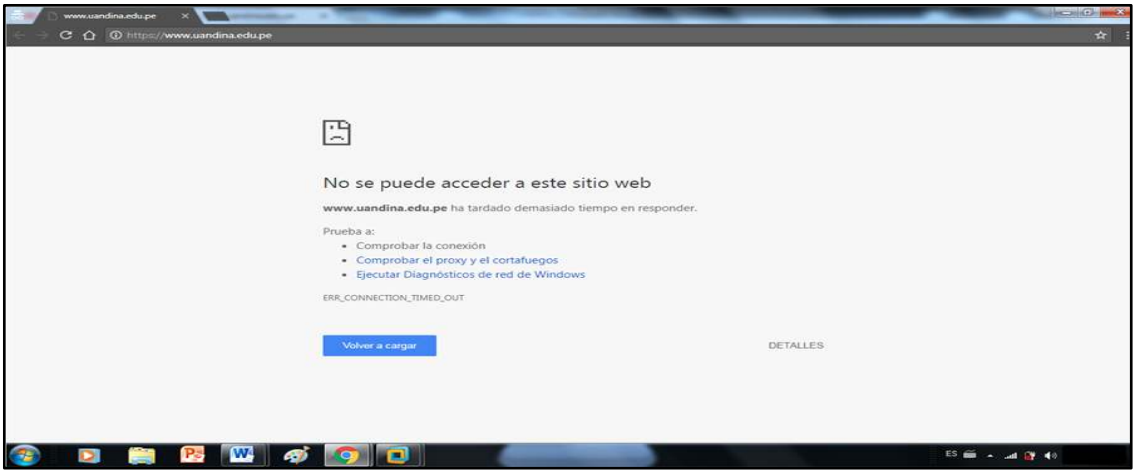



*Figura 86.* Página de la UAC inaccesible debido al ataque de DoS.
**Fuente:** Elaboración propia de la página UAC.

**Comentario:** Como se puede observar, teniendo conexión a internet la plataforma de WordPress en la que corre el portal Web de la Universidad Andina del Cusco ha sido vulnerada y por lo tanto el portal Web de la Universidad Andina del Cusco no responde.

Este ataque si se aplica desde varias computadoras conectadas a la vez y haciendo las mismas consultas, podría dejar inaccesible el portal Web de la Universidad Andina del Cusco.

Ya que el ataque de DoS a la plataforma de WordPress de la Universidad Andina del Cusco funciona, se recomienda corregir la vulnerabilidad de uso, ya que los usuarios que utilicen el portal Web se verán afectados.

## 4.2 Resultados Respecto al Objetivo General

Tabla 18.
*Resultados respecto al objetivo general.*

| Nombre de ataques | Nivel de vulnerabilidad | Cantidad de entradas GET y POST | URL encontradas | Vulnerabilidades encontradas |
|---|---|---|---|---|
| Ataque con Nmap | Media | - | 1 | 5 |
| Ataque SQL injection | Media | 45 | 599 | 3 |
| Ataque XSS | Media | 48 | 599 | 2 |
| Ataque CSRF | Media | 51 | 545 | 3 |
| Ataque de DoS | Alta | - | 1 | 1 |

**Fuente:** Elaboración propia.

En la tabla 18 se presenta un resumen de los resultados de cada uno de los tipos de vulnerabilidades aplicadas al sitio Web www.uandina.edu.pe. Se aprecia que la vulnerabilidad por ataque de DoS es alta, mientras que los ataques por SQL, XSS, CSRF y DoS son de nivel medio. Asimismo, observamos que en los análisis se encontró cinco (5) vulnerabilidades de ataque con Nmap; tres (03) vulnerabilidades de ataque por SQL injection y (03) vulnerabilidades por ataque CSRF. En el ataque por XSS (02) vulnerabilidades y en el ataque por DoS (01) vulnerabilidades.

En consideración al objetivo general que es encontrar las vulnerabilidades informáticas en el portal Web de la Universidad Andina del Cusco, se determinó, que el portal Web de la Universidad Andina del Cusco es vulnerable a un ataque de denegación de servicios o DoS el cual es un tipo de ataque común dentro de las vulnerabilidades online. Cabe resaltar que este tipo de ataque puede generar problemas a nivel de Usuario, donde el afectado no podrá acceder a dicho portal Web.

Asimismo se concluye que el portal www.uandina.edu.pe actualmente requiere de un tratamiento especial con respecto a mejorar la seguridad dentro de las vulnerabilidades de Uso.

# Capítulo V

## Discusión

En el presente capitulo se expone la discusión de los resultados logrados y comparados con diferentes estudios, señalados en el marco teórico.

De los resultados obtenidos en los capítulos anteriores, se pudo determinar que el portal Web de la Universidad Andina del Cusco es vulnerable.

Para la vulnerabilidad de diseño se utilizó el software Kali Linux con la herramienta Nmap para ataques de Sniffer, encontrando deficiencias en cuanto a: nivel de vulnerabilidad (media), dirección IP visible, puertos abiertos, los sistemas operativos y sus versiones, nombres de usuarios, dirección IP del router, servicios y versiones que utilizan los puertos abiertos; al capturar, interpretar y almacenar la información que fluye por la red, un hacker black hat podría hacer mal uso de toda la información encontrada, afectando la confidencialidad del sistema informático.

Para la vulnerabilidad de implementación se utilizó el software Acunetix Web Vulnerability Scanner 10.5 para ataques de Inyección de código SQL, Cross-site Scripting (XSS) y Cross-site request reference forgery (CSRF), se encontró deficiencia en cuanto a: nivel de vulnerabilidad (media), lista de archivos con entradas Get y Post, enlaces rotos y contraseñas con autocompletado habilitado; un hacker black hat, podría eliminar información de la base de datos, inyectar códigos y ejecutar scripts maliciosos, entre muchas cosas más, afectando la integridad del sistema informático.

Para la vulnerabilidad de uso se utilizó el software Kali-Linux-2017.1 para el ataque de Denegación de Servicio sobre el protocolo XML-RPC, se encontró deficiencia en cuando a: nivel de vulnerabilidad (alta), versión de WordPress desactualizada y el protocolo XML-RPC activo por defecto; un hacker black hat al utilizar este ataque podría dejar inaccesible el portal web, afectando la disponibilidad del sistema informático.

## Conclusiones

- A lo largo de este trabajo de investigación se cumple con el objetivo principal que era identificar vulnerabilidades informáticas mediante la aplicación de las herramientas de detección de vulnerabilidades en el portal Web de la Universidad Andina del Cusco.
- Debido a las constantes amenazas en que se encuentran los sistemas informáticos a nivel mundial, es necesario que la Universidad Andina del Cusco tenga un enfoque permanente en los niveles altos de vulnerabilidad, y en las herramientas de seguridad con las que cuenta para prevenir posibles ataques informáticos.
- El portal Web de la Universidad Andina del Cusco es vulnerable a un ataque de denegación de servicios o DoS (Nivel de vulnerabilidad alta) el cual es un tipo de ataque común dentro de las vulnerabilidades online. Cabe resaltar que este tipo como objetivo inhabilitar el uso de un sistema, con el fin de bloquear el servicio para el que está destinado.
- Ningún sistema de seguridad es infalible y, en muchas ocasiones ocurre lo que ya dijo Carbajal en el libro Tecnologías Globales para la Seguridad de la Información "un sistema de información se considera seguro si: se encuentra libre de todo peligro y daño, pero esto es poco probable, porque es imposible dar garantía a la seguridad total de un sistema".
- La única solución posible es la realización de auditorías periódicas y la creación de una cultura de seguridad para concienciar al personal de la unidad de diseño y programación de la Dirección de tecnologías de la información de los riesgos a los que se exponen.

## Recomendaciones

- Implementar, controlar y monitorear las actividades sugeridas en la propuesta de plan de seguridad del presente proyecto, con el fin de eliminar vulnerabilidades encontradas y disminuir la probabilidad de ocurrencia de los riesgos a futuro.
- Capacitar al personal de la unidad de diseño y programación de la Dirección de tecnologías de la información, en temas de seguridad de la información. Concientizando al personal a tener un buen uso de los recursos informativos por la importancia que estos representan para la Universidad Andina del Cusco.
- Realizar evaluaciones periódicas para mejorar la seguridad de los recursos de TI y de la información. Estas evaluaciones resultarían beneficiosas para cumplir las estipulaciones, normativas y requisitos de clientes, socios y fabricantes.
- Revisar periódicamente las políticas y procedimientos, debido a que la tecnología tiene avances constantemente y por ende aparecen diversos ataques que se deben prevenir para evitar problemas futuros.

# Bibliografía

Acunetix Vulnerability Scanner. (15 de Febrero de 2017). *Inyección de SQL*. Obtenido de Inyección de SQL: https://www.acunetix.com/websitesecurity/sql-injection/

bitdegree.org. (6 de Diciembre de 2019). *bitdegree.org*. Obtenido de bitdegree.org: https://es.bitdegree.org/tutoriales/desarrollador-web/

Built With. (20 de Julio de 2008). *Descubra en que esta construido el sitio web*. Obtenido de Descubra en que esta construido el sitio web: https://builtwith.com/

Cabero, J. (1998). Impacto de las nuevas tecnologías de la información y la comunicación en las organizaciones educativas. En J. Cabero, *Impacto de las nuevas tecnologías de la información y la comunicación en las organizaciones educativas* (págs. 1-2). España: Universitario.

Carvajal, A. (2007). Globalteksecurity. En A. Carvajal, *Tecnologías Globales para la Seguridad de la Información* (pág. 5). Colombia: Universidad Incca de Colombia.

Castro Jaime, C. Y., & Hernández Muñoz, T. (2012). *Políticas y buenas prácticas de seguridad en servidores WEB del CDMIT.* Mexico: Universidad Nacional Autonoma de Mexico.

CSIRC. (2016). *Manual básico de Wordpress.* España: Universidad de Granada.

Deymonnaz, P. A. (2012). *Analisis de vulnerabilidades esteganográficas en protocolos de comunicación IP y HTTP.* Buenos Aires: Universidad de Buenos Aires.

Dirección de Planificación y Desarrollo Universitario. (2017). *Anuario Estadístico de la Universidad Andina del Cusco año 2016.* Cusco: Universidad Andina del Cusco.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la Investigación Científica.* México: Mc Graw Hill Education.

Hernández Saucedo, A. L., & Mejia Miranda, J. (2015). *Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web.* Mexico: Universidad Autónoma de Zacatecas.

Herrera, E. A. (2012). *Lineamientos para identificar vulnerabilidades en una red publica que contiene un servidor web.* Guatemala: Universidad de San Carlos Guatemala.

Khalimonenko, A., Kupreev, O., & Ilgan, K. (6 de Febrero de 2018). *Los ataques DDoS en el cuarto trimestre de 2017*. Obtenido de Los ataques DDoS en el cuarto trimestre de 2017: https://securelist.lat/ddos-attacks-in-q4-2017/85956/

Martí Talón, R. M. (2016). Desarrollo e implementacion practica de un pentest. En R. M. Martí Talón, *Desarrollo e implementacion practica de un pentest* (pág. 51). Gandia, España: Universidad Politecnica de Valencia.

Nmap.org. (16 de Agosto de 2007). *Nmap*. Obtenido de Nmap: https://nmap.org/

Pintado Cuji, K. A., & Hurtado Valero, C. L. (2015). *Diagnostico de las vulnerabilidades informaticas en los sistemas de informacion para prponer soluciones de seguridad a la rectificadora Gabriel Mosquera S.A.* Guayaquil: Universidad Politecnica salesiana sede Guayaquil.

Prado Herrera, E. A. (2012). *Lineamientos para identificar vulnerabilidades en una red publica que contiene un servidor web.* Guatemala: Universidad de San Carlos de Guatemala.

Romaniz, S. (S.F.). *Seguridad de Aplicaciones Web: vulnerabilidades en los controles de acceso.* Argentina: Universidad Tecnológica Nacional.

Sampieri Hernandez, R. (1998). Metodología de la Investigación. En H. R. Sampieri , *Metodología de la Investigación* (pág. 60). Jupiter.

Tecnologias paralos negocios. (22 de Marzo de 2016). *Tecnologias paralos negocios*. Obtenido de Tecnologias paralos negocios: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/

Universidad Andina del Cusco. (22 de noviembre de 2017). *www.uandina.edu.pe*. Obtenido de www.uandina.edu.pe: https://www.uandina.edu.pe/index.php/mision-vision-uac/

Universidad Internacional de la Rioja . (2015). *Arquitectura de las aplicaciones web y bases de datos.* España: Universidad Internacional de la Rioja.

webempresa. (12 de Agosto de 2016). *WordPress*. Obtenido de WordPress: https://www.webempresa.com/wordpress/que-es-wordpress.html

WordPress. (3 de Enero de 2013). *Protección WordPress de vulnerabilidades Pingback*. Obtenido de Protección WordPress de vulnerabilidades Pingback: https://ayudawp.com/como-proteger-wordpress-de-la-vulnerabilidad-pingback/

## Glosario

- Pentest: Es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.
- Dominio: Parte de una dirección de Internet que identifica un sitio Web y que describe el tipo de empresa u organización a la que pertenece o bien el país donde está registrado.
- Portal Web: Un portal es una plataforma basada en Web que recopila información de diferentes fuentes en una única interfaz de usuario y presenta a los usuarios la información más relevante para su contexto.
- Servidor Web: Sirven para almacenar contenidos de Internet y facilitar su disponibilidad de forma constante y segura.
- HTTPs (Hypertext Transfer Protocol Secure): Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto.
- PKI (Public Key Infrastructure): es una combinación de hardware, software, y políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital, y el no repudio de transacciones electrónicas.
- SLL (Secure Sockets Layer): Es un protocolo de seguridad permite las comunicaciones cifradas entre servidores y navegadores para garantizar los movimientos de los clientes y visitantes en los portales Web de las Organizaciones.
- TLS (Transport Layer Security): es un protocolo mediante el cual se establece una conexión segura por medio de un canal cifrado entre el cliente y servidor.
- SHH (Secure Shell): Es un protocolo de administración remota que permite a los usuarios controlar y modificar sus servidores remotos a través de Internet.

- Telnet (Telecommunication Network): Es un protocolo de red que se utiliza para acceder a una computadora y manejarla de forma remota.
- IDS (Intrusion Detection System): es un programa de detección de accesos no autorizados a un computador o a una red.
- ICMP (Internet Control Message Protocol): es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).