ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingenieria en Electricidad y Computación

"ANÁLISIS Y DESARROLLO DE UN ESQUEMA DE SEGURIDAD PARA LA REDUCCIÓN DE VULNERABILIDADES DEL SERVIDOR DE BANCA EN LÍNEA DE LA COOPERATIVA DE AHORRO Y CRÉDITO COMERCIO LTDA."

TRABAJO DE TITULACIÓN

PREVIA A LA OBTENCIÓN DEL TITULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

JAVIER ALEXANDER ZAMBRANO PARRALES

GUAYAQUIL – ECUADOR

2017

AGRADECIEMIENTO

Agradezco sobre todas las cosas a Dios por sus infinitas bendiciones, por las cuales ahora he logrado cumplir una meta más en mi vida en el ámbito profesional.

A mis padres y hermanos por su apoyo constante e incondicional, por siempre estar a mi lado dándome los mejores consejos y valores, inculcándome el amor al estudio, a la academia y así ayudarme a forjar un futuro prometedor y exitoso.

A mi tutor por su tiempo y conocimientos los cuales permitieron guiarme por el camino correcto para la culminación de este proyecto.

DEDICATORIA

A Dios, a mi familia, tutor, maestros, amigos, compañeros y sobre todo a mi sobrina para quien espero ser un ejemplo de disciplina, constancia y superación.

TRIBUNAL DE SUSTENTACION

Ing. Lenin Freire Cobo

DIRECTOR MSIA

Mgs. Albert Espinal

DIRECTOR DEL PROYECTO DE GRADUACIÓN

Mgs. Laura Ureta

MIEMBRO DEL TRIBUNAL

DECLARACIÒN EXPRESA

“Declaro expresamente que la responsabilidad del contenido de esta Tesis de Grado es de mi total propiedad intelectual y responsabilidad, para lo cual doy mi consentimiento que la ESPOL proceda a la publicación de la obra por cualquier medio con el objetivo de promover la investigación y difusión de contenido relacionado a la seguridad tecnológica”

_____

Ing. Javier Alexander Zambrano Parrales

RESUMEN

El objetivo primordial del desarrollo e implementación de este esquema de seguridad es poder garantizar el cumplimiento de los fundamentos básicos de la seguridad de la información tales como confidencialidad, integridad y disponibilidad en el servidor de banca en línea de la Cooperativa Comercio.

Como herramienta principal del escaneo de las vulnerabilidades y posterior implementación de soluciones recomendadas se utilizó el aplicativo licenciado Qualys, el cual permitió generar un reporte antes de la implementación del esquema y posterior al mismo y así poder determinar su efectividad.

Adicional se analizaron aspectos físicos en cuanto al área donde se encuentra alojado el servidor, aplicativos instalados y características de la configuración las cuales influyen directamente en el impacto de las vulnerabilidades encontradas.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

El presente tema de tesis se refiere al análisis de las vulnerabilidades encontradas en el servidor de comercio en línea de la Cooperativa Comercio y el desarrollo de un esquema de seguridad para determinar sus posibles soluciones.

La característica de este tipo de servicio el cual es publicado por internet, si bien acerca a la institución a la tendencia mundial de la globalización y dar a conocer sus prestaciones de una manera más ágil, es la causa también de aparecer en el mapa como un objetivo de ataque de los hackers informáticos.

La investigación de esta problemática se realizó por el interés de conocer que tan vulnerable se encuentra el servidor antes mencionado y que medidas serían las factibles tomar para su remediación o disminución.

En el ámbito profesional, como ingeniero en sistemas informáticos, el interés surgió por profundizar más en el ámbito de la seguridad orientado a las instituciones financieras y sus servicios publicados por internet.

El desarrollo del análisis se basa principalmente en la metodología OSSTMM y OTP (OWASP Testing Project) enfocándose en entornos específicos tales como auditoria de aplicación web, auditoria en sistema operativo, y red interna LAN.

CAPITULO 1

GENERALIDADES

1.1 ANTECEDENTES DE LA INVESTIGACIÓN

La globalización ha permitido que el acceso a la información sea un derecho más de las personas en cualquier parte del mundo, para lo cual todas las instituciones de cualquier índole deben cumplir con ese requerimiento gestionando el acceso a sus datos por medio de una plataforma rápida y amigable al usuario final, pero así mismo que preste las condiciones necesaria de seguridad para que solo pueda ser visualizada por su legítimo dueño.

La Cooperativa Comercio LTDA es una entidad financiera, que brinda servicios de esa índole como créditos, cuenta de ahorros, transferencias, etc. Dicha información se encuentra publicada en el internet con el fin de brindarles a sus socios la posibilidad de acceder a ella desde cualquier

lugar. La capacidad de brindar ese servicio, conlleva también a la responsabilidad de tomar medidas que salvaguarden la disponibilidad, integridad y confidencialidad de la información por medio de un esquema de seguridad y así mitigar posibles accesos no autorizados evitando perjudicar a la institución y al socio.

1.2 DESCRIPCIÓN DEL PROBLEMA

La Cooperativa de Ahorro y Crédito COMERCIO Ltda., es una entidad de intermediación financiera con el público en general, autorizada por la Superintendencia de Bancos y Seguros mediante resolución # 85-027-DC DEL 24 DE Octubre de 1985, iniciando su actividad el 01 de Julio de 1985.

Cuenta con 4 agencias dentro de la provincia de Manabí, haciendo posible el incremento constante de sus socios diariamente dentro de toda la provincia, teniendo como compromiso brindar el mejor servicio en sitio y digitalmente, para lo cual se vio en la necesidad de publicar sus servicios en internet a través de la banca en línea.

La institución cuenta con un centro de cómputo principal que es donde se encuentra alojado físicamente el servidor de banca en línea y un centro alterno en una de sus agencias, si bien el centro de cómputo principal ubicado en la oficina matriz cuenta con todas las especificaciones de seguridad exigidas por el ente regulador, nunca se ha realizado un análisis formal de las vulnerabilidades de dicho servidor.

En dicho servidor se encuentra alojado el sitio web institucional que sirve para que las aplicaciones se encuentren en línea y así los socios puedan hacer uso de los servicios que la institución brinda por este medio. El problema se evidencia si el servidor sufre intrusión por parte de terceros, ya sea para hurtar información o para desactivar los servicios equipo. El primero causaría un daño en la confidencialidad de la información y en la integridad, y el segundo el impacto sería económico, el estar fuera de línea le causaría a la cooperativa $50 de pérdidas por día.

Actualmente, los incidentes informáticos que ha tenido la cooperativa han sido:

- Intrusión por parte de terceros al servidor de intranet publicado en internet, cuyo origen se dio por la versión de Joomla desactualizada.
- Caída del enlace de datos con el proveedor de internet, bloqueando la salida de los servicios publicados por la institución.

Con respecto al servidor en mención los incidentes han sido:

- Transmisión de datos a través de protocolo no seguro HTTP.
- Bloqueo por parte de los navegadores al no contar con Certificado SSL validado por una entidad certificadora.

1.3 OBJETIVO GENERAL

Analizar y desarrollar un esquema de seguridad para reducir las vulnerabilidades existentes en el servidor de banca en línea de la Cooperativa de Ahorro y Crédito Comercio Ltda.

1.4 OBJETIVOS ESPECÍFICOS

- Recabar la información necesaria para poder analizar las posibles vulnerabilidades existentes en un servidor de banca en línea.
- Analizar y diseñar un esquema de seguridad para la reducción de las vulnerabilidades existentes en un servidor de banca en línea.
- Implementar un esquema que cierre vulnerabilidades encontradas.
- Realizar las pruebas y comprobación de resultados del esquema de seguridad implementado en el servidor de banca en línea.

1.5 JUSTIFICACIÓN DE LA INVESTIGACIÓN

Toda las instituciones financieras, bancos o cooperativas cuentan con su propia página web ya que en la actualidad se hace imperativo brindar sus servicios por internet, servicios tales como consulta de saldo, transferencias electrónicas, pagos, etc.; para ello deben prestar las garantías necesaria con el fin de reducir las vulnerabilidades que estos puedan sufrir, evitando así que sean afectadas la seguridad y reputación de la institución.

Según la resolución No. JB-2012-2148 de 26 de abril del 2012 [1] y la No. JB-2014-3066 de 2 de septiembre del 2014 [2], es necesario realizar como mínimo una vez al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica, como parte de una auditoria de seguridad con el fin de mitigar los riesgos que podían afectar a la seguridad de los servicios que se brindan.

Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las instituciones deberán definir y ejecutar planes de acción sobre las vulnerabilidades detectadas.

1.6 SOLUCIÓN PROPUESTA

La solución propuesta consiste en elaborar un esquema de seguridad que cierre las vulnerabilidades encontradas a través de procedimientos y configuraciones preventivas y correctivos que serán evaluadas.

Este esquema de seguridad propuesto está acorde a las necesidades del negocio y sensibilidad de los datos que aquí se publican y así reducir dichas vulnerabilidades, aumentando la seguridad de las transacciones ejecutadas en dicho servidor, salvaguardando la integridad, confiabilidad y disponibilidad de la información bancaria de sus socios.

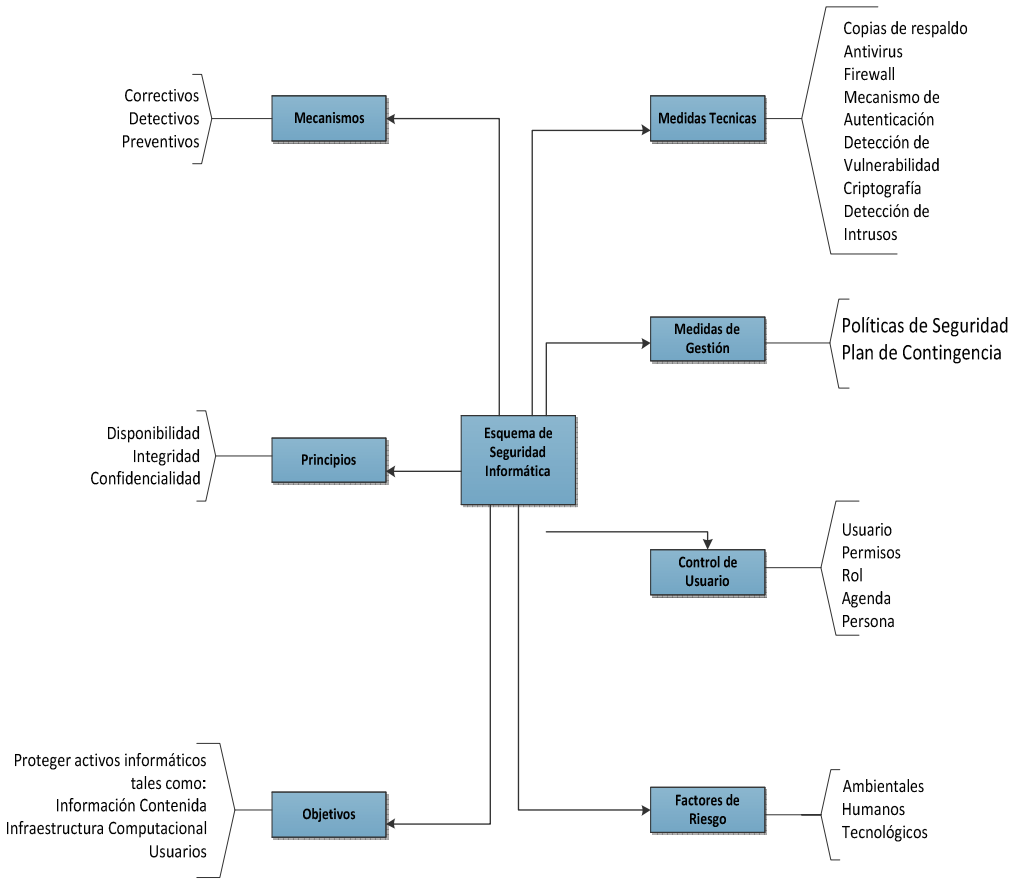

FIGURA 1.1 Esquema de seguridad informática.

1.7 METODOLOGÍA

Para la elaboración del presente trabajo de investigación y cumplimiento de los objetivos planteados, se realizó reuniones y entrevistas con el fin de recopilar datos relevantes y así conocer la situación actual de la institución, para luego analizar y clasificar los datos obtenidos.

- **Diseño metodológico**

  En el desarrollo de esta investigación se aplicó los diferentes métodos, procedimientos y técnicas que ayudarán al cumplimiento de los objetivos propuestos.

- **Tipo de estudio**

  La investigación se realizó como trabajo de campo y de aplicación ya que se elaboró con el área involucrada.

- **Método de investigación**

  La investigación se desarrolló en base a los métodos deductivos e inductivos, estos ayudan a evaluar de mejor manera la investigación. Como parte del proceso se analizaron los problemas suscitados que involucran al servidor de Banca en Línea de la Cooperativa Comercio.

- **Técnicas para recolección de información**

La técnica que se aplicó para el proceso investigativo fue bibliográfica documental, la investigación se realizó con fuentes primarias y secundarias combinada con los métodos inductivo - deductivo. También se utilizó la técnica de la observación, la cual fue de mucha ayuda para identificar y recopilar información para el desarrollo de la investigación en el trabajo de campo y las entrevistas con las personas involucradas en la seguridad y administración del servidor de Banca en Línea de la institución.

1.8 ACTIVIDADES DE LA ORGANIZACIÓN

La Cooperativa Comercio LTDA es una entidad financiera cuyo objetivo principal es captar y dar créditos a sus socios con tasas justas y productos competitivos, promoviendo su desarrollo económico y social, sin descuidar la educación financiera, y como base promoviendo los principios del cooperativismo entre las partes interesadas. La entidad fue constituida a los 29 días del mes de abril de 1985 en el cantón Portoviejo iniciando sus actividades el 1 de julio del mismo año y luego, la Superintendencia de Bancos le otorga la calificación para operar como Institución autorizada el 24 octubre del mismo año.

A partir de mayo de 2011, las cooperativas de ahorro y crédito forman parte de un nuevo régimen el sector financiero popular y solidario esto parte de la aprobación de la ley orgánica de la economía popular y solidaria, pero a su vez conservando los controles que exige la Superintendencia de Bancos y Seguros.

- **Misión**

  “Confiar en el potencial de nuestros socios, brindándoles servicios competitivos de calidad, con tratos justos y condiciones convenientes”.

- **Visión**

  “Tener presencia en los principales cantones de nuestra provincia siendo una Cooperativa de ahorro y crédito líder con amplia cobertura, conformada por un equipo de personas innovadoras, y solidarias, trabajando con profesionalismo”.

1.9 OBJETIVOS ORGANIZACIONALES

La Cooperativa Comercio se tiene planteado los siguientes objetivos:

- Ser la principal institución financiera de la Provincia.
- Tener un equipo de personas integro cumpliendo los valores cooperativos.
- Ofrecer servicios y productos de calidad con tasas justas a clientes y socios.

1.10 ESTRUCTURA ORGANIZACIONAL

La Cooperativa Comercio presenta la siguiente estructura organizacional, partiendo por su máxima autoridad que inicia en la asamblea general.

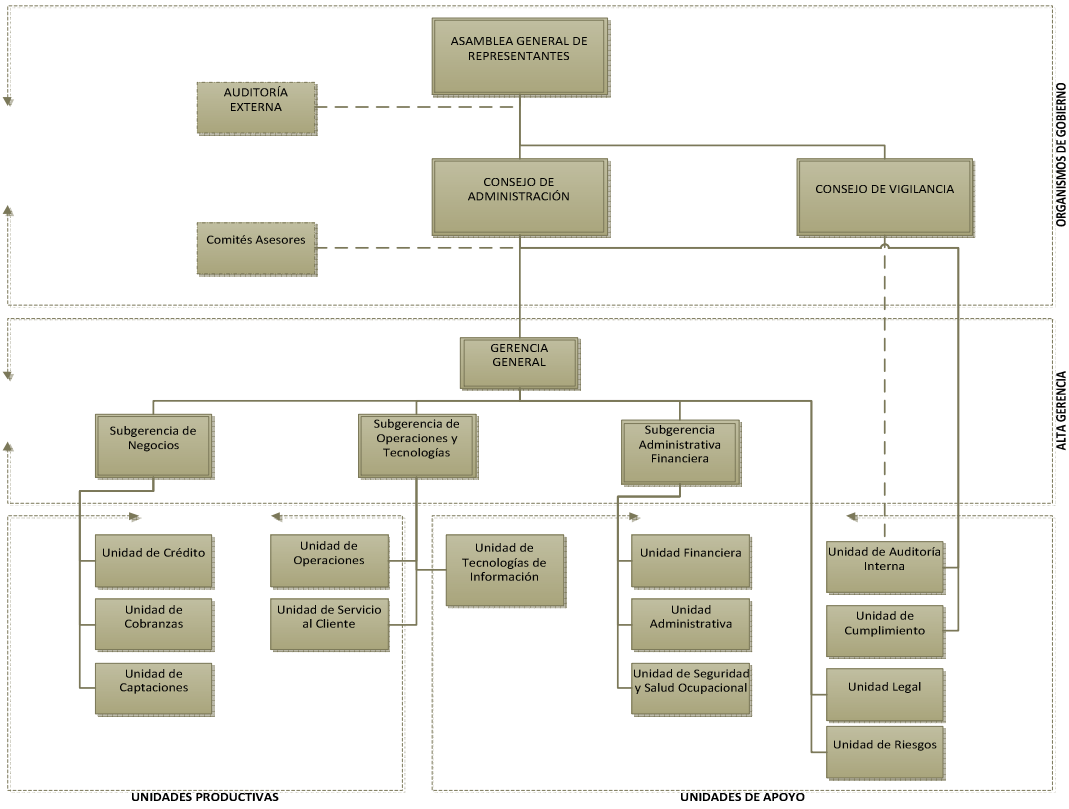

FIGURA 1.2 Estructura Organizacional de la Cooperativa Comercio.

CAPÍTULO 2

MARCO TEORICO

2.1 BANCA ELECTRÓNICA.

"Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de internet en el sitio que corresponda a uno o más dominios de la institución, indistintamente del dispositivo tecnológico a través del cual se acceda" [3].

2.2 PRINCIPIOS DE LA BANCA ELECTRÓNICA.

La banca electrónica es un servicio ofrecido por los bancos que permite a sus clientes efectuar ciertas operaciones bancarias desde una computadora que cuente con acceso a internet.

La banca electrónica también es conocida como Home Banking, Banca Virtual, E-Banking o PC-Banking. En algunos casos, la banca telefónica, la banca móvil y los cajeros automáticos se incluyen dentro de este concepto [4].

Las operaciones bancarias habilitadas difieren según el banco, siendo las más comunes:

- Verificar el saldo y movimientos de las cuentas bancarias.
- Solicitar préstamos.
- Transferir dinero entre cuentas bancarias.
- Contratar depósitos a plazos fijos.
- Comprar moneda extranjera.
- Conocer tasas de interés y tasas de cambio.
- Realizar pagos de servicios (domiciliación de gastos).
- Efectuar inversiones, tales como compras de títulos de deuda (públicos y privados), acciones y participaciones en fondos comunes de inversión.

2.3 MECANISMOS DE SEGURIDAD FÍSICOS Y LÓGICOS DE UN SERVIDOR DE BANCA ELECTRÓNICA.

Según la función que desempeñen los mecanismos de seguridad pueden clasificarse en:

- **Preventivos**. Actúan antes de que se produzca un ataque. Su misión es evitarlo.
- **Detectores**. Actúan cuando el ataque se ha producido y antes de que cause daños en el sistema.
- **Correctores**. Actúan después de que haya habido un ataque y se hayan producido daños. Su misión es la de corregir las consecuencias del daño.

Cada mecanismo ofrece al sistema uno o más servicios de los especificados en el epígrafe anterior.

Existen muchos y variados mecanismos de seguridad. En esta sección se mencionan los más habituales.

La elección de mecanismos de seguridad depende de cada sistema de información, de su función, de las posibilidades económicas de la organización y de cuáles sean los riesgos a los que esté expuesto el sistema.

a) Seguridad lógica

Los mecanismos y herramientas de seguridad lógica tienen como objetivo proteger digitalmente la información de manera directa.

- **Control de acceso** mediante nombres de usuario y contraseñas.
- **Cifrado de datos (encriptación).** Los datos se enmascaran con una clave especial creada mediante un algoritmo de encriptación. Emisor y receptor son conocedores de la clave y a la llegada del

mensaje se produce el descifrado. El cifrado de datos fortalece la confidencialidad.

- **Antivirus**. Detectan e impiden la entrada de virus y otro software malicioso.

  En el caso de infección tienen la capacidad de eliminarlos y de corregir los daños que ocasionan en el sistema. Preventivo, detector y corrector. Protege la integridad de la información.

- **Cortafuegos (firewall).** Se trata de uno o más dispositivos de software, de hardware o mixtos que permiten, deniegan o restringen el acceso al sistema.

- **Firma digital.** Se utiliza para la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos (por ejemplo, gestiones en oficinas virtuales). Su finalidad es identificar de forma segura a la persona o al equipo que se hace responsable del mensaje o del documento. Protege la integridad y la confidencialidad de la información.

- **Certificados digitales.** Son documentos digitales mediante los cuales una entidad autorizada garantiza que una persona o entidad es quien dice ser, avalada por la verificación de su clave pública. Protege la integridad y la confidencialidad de la información.

- **Desarrollo de aplicaciones.** Según resolución No. JB-2012-2148 de 26 de abril del 2012, “Implementar técnicas de seguridad de la información en los procesos de desarrollo de las

aplicaciones que soportan los canales electrónicos, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades [5].

b) Seguridad física

Son tareas y mecanismos físicos cuyo objetivo es proteger al sistema (y, por tanto indirectamente a la información) de peligros físicos y lógicos.

- **Respaldo de datos.** Guardar copias de seguridad de la información del sistema en lugar seguro. Disponibilidad.
- **Dispositivos físicos** de protección, como pararrayos, detectores de humo y extintores, cortafuegos por hardware, alarmas contra intrusos, sistemas de alimentación ininterrumpida (para picos y cortes de corriente eléctrica) o mecanismos de protección contra instalaciones. En cuanto a las personas, acceso restringido a las instalaciones; por ejemplo, mediante vigilantes jurados o cualquier dispositivo que discrimine la entrada de personal a determinadas zonas [6].

2.4 CANALES DE COMUNICACIÓN.

- **Canal.** Un canal es un medio capaz de transmitir un mensaje de una entidad a otra.

  La mayoría de los canales de comunicación, o al menos aquellos que hoy en día despiertan nuestro interés (Internet, WiFi, telefonía, etc.), no son seguros.

- **Canal seguro.** Un canal seguro es un canal sobre el que un atacante no puede realizar operaciones de lectura, escritura, borrado o reordenación.

  La finalidad última de la criptografía, cuya etimología está en la unión de los términos griegos κρυπτός (oculta) y γραφία (escritura), es la creación de canales seguros, es decir, convertir información perfectamente comprensible en un formato completamente ilegible para un observador que carezca de cierta información secreta.

- **Canales electrónicos. "**Se refiere a todas las vías o formas a través de las cuales los clientes o usuarios pueden efectuar transacciones con las instituciones del sistema financiero, mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas. Principalmente son canales electrónicos: los cajeros automáticos (ATM), dispositivos de puntos de venta (POS y PIN Pad), sistemas de audio respuesta (IVR), señal telefónica, celular e internet u otro similares" [7].

- **Criptografía.** La criptografía es el estudio de las técnicas matemáticas relacionadas con aspectos de la seguridad de la información tales como la confidencialidad, integridad, autentificación y no repudio.

  La confidencialidad, secretismo o privacidad, consiste en garantizar que el contenido del mensaje de una comunicación quede limitado únicamente a las entidades autorizadas.

La integridad de los datos consiste en evitar la manipulación o alteración no autorizada de los datos; por autentificación se entiende la correcta identificación de todas las entidades que participan en la comunicación; mientras que el no repudio consiste en evitar que alguna de las entidades de la comunicación niegue haber realizado ciertas acciones [8].

2.5 MÉTODO DE AUTENTICACIÓN.

El método de autenticación es el procedimiento a seguir para poder acceder a cualquier sistema informático tecnológicamente hablando, este procedimiento debe contar con la suficiente seguridad para garantizar que dicha comunicación sea legítima.

Entre dichos métodos podemos citar los siguientes:

a) Biomédico, por huellas dactilares, retina del ojo, etc.
b) Tarjetas inteligentes que guardan información de los certificados de un usuario.
c) Métodos basados en contraseña:
    - Comprobación local o método tradicional en la propia máquina.
    - Comprobación en red o método distribuido, más utilizado actualmente.

2.6 HACKING ÉTICO.

El concepto de ética hacker aparece por vez primera en el libro de Steven Levy publicado en 1984 (Hackers : heroes of the computer revolution), en donde señala que:

a) El acceso a las computadoras debe ser ilimitado y total.
b) Toda la información debe ser libre.
c) Es necesario promover la descentralización.
d) Los hackers deben ser juzgados por su labor, no por su raza, edad o posición. Su labor se centrará en el logro del libre acceso a la información [9].

En la actualidad el hacking ético está mejor conceptualizado refiriéndose a la práctica exclusiva de encontrar vulnerabilidades en sistemas informáticos cuya connotación para el usuario es de suma importancia y ameritan el análisis exhaustivo de su seguridad con métodos de vanguardia.

Este análisis es realizado por el llamado hacker ético en diferentes entornos los cuales citamos a continuación.

- **Caja negra.** En este entorno la información de la entidad o sistema informático al cual intervendrá el hacker, es totalmente aislada de su conocimiento y debe obtenerlo por sí mismo, con el fin de recrear un escenario real en el cual el ataque vendría desde el exterior.

- **Caja blanca.** En este caso el hacker tiene acceso a la información de la entidad a intervenir, esta información está relacionada con aspectos tales como; segmento de red, tecnología de la infraestructura informática, sistemas operativos, servicios publicados por internet, firewall, etc.
- **Caja gris.** Es una mezcla de los dos entornos anteriores, se proporciona información inicial y a partir de ella se obtiene el resto por sí mismo escalando a través de los sistemas internos de la entidad.

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN PARA EL ANALISIS

3.1 CARACTERÍSTICAS FÍSICAS DEL SERVIDOR.

A continuación se presenta la ficha técnica del servidor donde se encuentra alojado el aplicativo web de la Banca en Línea.

Tabla 1 Ficha técnica del servidor de banca en línea

FICHA TECNICA DEL SERVIDOR DE BANCA EN LINEA	
Equipo	IBM SYSTEM X3200
Procesador	INTEL XEON 2.40 GHz.
Memoria RAM	16 GB.
Almacenamiento interno	2 T. Sata Hot Swap

Interfaz de red	Gigabit Ethernet (GbE) dual
Fuente de alimentación	1/1 fija de 401 W

El equipo servidor físico se adquirió analizando las necesidades mínimas y considerando el crecimiento a futuro de los recursos consumidos por este servicio, concluyendo en el hardware con las características mencionadas en la figura anterior.

3.2 SISTEMA OPERATIVO Y SERVIDOR WEB.

El Sistema operativo actualmente instalado en el servidor de Banca en Línea es Windows Server 2008 R2 Standard Service Pack 1, debidamente licenciado con el código de producto 00477-OEM-8420052-70710.

Por motivo de continuidad del negocio y estabilidad de los aplicativos, se encuentran desactivadas las actualizaciones automáticas desde la instalación del sistema operativo.

Como servidor web se encuentra establecido el aplicativo Internet Information Services Versión 7.5.7600.16385, siento este el más apto debido a su compatibilidad con el código de programación del sitio web “asp.net, c# y html”.

3.3 APLICATIVOS DE SEGURIDAD LÓGICA INSTALADA Y CONFIGURADA EN EL SERVIDOR.

Como Aplicativo Antivirus y Firewall se encuentra instalado “Kaspersky Endpoint Security 10 para Windows 10.2.4.674” ejecutándose como agente y se conecta al servidor principal “Kaspersky Security Center” el cual gestiona las debidas actualizaciones de bases de datos de virus y de aplicativo.

Dicho aplicativo centraliza el control de la seguridad del servidor, desplazando en segundo plano a aquellos que vienen por defecto en el sistema operativo tales como Firewall de Windows.

3.4 CARACTERÍSTICAS FÍSICAS DEL CENTRO DE CÓMPUTO DONDE SE ENCUENTRA EL SERVIDOR.

El centro de cómputo cuenta con las siguientes características:

Tabla 2 Características del centro de cómputo.

CARACTERISTICAS DEL CENTRO DE COMPUTO	
Dimensiones	Largo 2,06 m - Ancho 1,77 m - Alto 2,60 m.
Climatización	Aire acondicionado genérico de 12000 btu.
Piso falso	NO.
Techo falso	SI.
Ventanas	NO.

Acceso secundario	NO.
Ubicación de servidores	Rack de 24 ur.
Seguridad de acceso	Puerta metálica con cerradura convencional.

El centro de cómputo matriz donde se encuentra alojado el servidor de página web y banca en línea, presenta las características antes mencionadas ya que es un área improvisada a consecuencia del desastre natural ocurrido el 16 de abril del año 2016.

A pesar de esta situación, se ha procurado cumplir con las exigencias mínimas básicas requeridas para poder garantizar la seguridad a los equipos que aquí se encuentran.

3.5 MÉTODO DE AUTENTICACIÓN.

El método de autenticación para el ingreso al sistema operativo del servidor es el implementado por defecto con solicitud de “Usuario” y “Contraseña” existiendo únicamente el usuario Administrador para dicho cometido.

Se encuentra también habilitado el acceso por escritorio remoto, cabe recalcar que este tipo de acceso solo es permitido desde dentro de red LAN, y bloqueado mediante un firewall desde fuera de ella, es decir INTERNET.

- **Seguridad de red.**

La solución actualmente implementada para la seguridad de la red institucional es un Firewall Appliance de marca DELL-SonicWall Modelo NSA 220.

Los servicios de seguridad licenciados con esta solución se detallan a continuación:

Tabla 3 Características del centro de cómputo.

SERVICIO DE SEGURIDAD	STATUS	CANTIDAD	EXPIRACIÓN
Nodes/Users	Licensed	Unlimited	
App Control	Licensed		07-nov-17
App Visualization	Licensed		07-nov-17
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		07-nov-17
VPN	Licensed		
Global VPN Client	Licensed	22	
VPN SA	Licensed	25	
SSL VPN	Licensed	2 Max: 52	
WAN Acceleration Client	Licensed	1	
Botnet Filter	Licensed		07-nov-17
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		07-nov-17
Premium Content Filtering Service	Licensed		07-nov-17
Analyzer	Licensed		

Dynamic Support 24x7	Licensed		10-sep-17
Software and Firmware Updates	Licensed		10-sep-17
Hardware Warranty	Licensed		10-sep-17

CAPÍTULO 4

ANALISIS DE LAS VULNERABILIDADES

4.1 ANÁLISIS DE VULNERABILIDADES DEL COMPONENTE DE AUTENTICACIÓN DE USUARIOS.

La autenticación para el ingreso a la banca en línea de la Cooperativa Comercio se basa en el ingreso de usuario y contraseña con un código de confirmación temporal que se envía por dos vías, a través de un mensaje de texto al celular del socio y un correo electrónico a su cuenta de e-mail personal.

Como canal de comunicación se utiliza el internet por medio de los protocolos “http” y “https” en la cual en el primer caso, la información viaja totalmente desprotegida haciéndola vulnerable por cualquiera que la pueda intervenir y solo en el segundo caso esta viaja encriptada y validada con un certificado de autenticación emitida por un ente regulador.

En la imagen a continuación se muestran las especificaciones del certificado y el nombre de la entidad que lo emite.

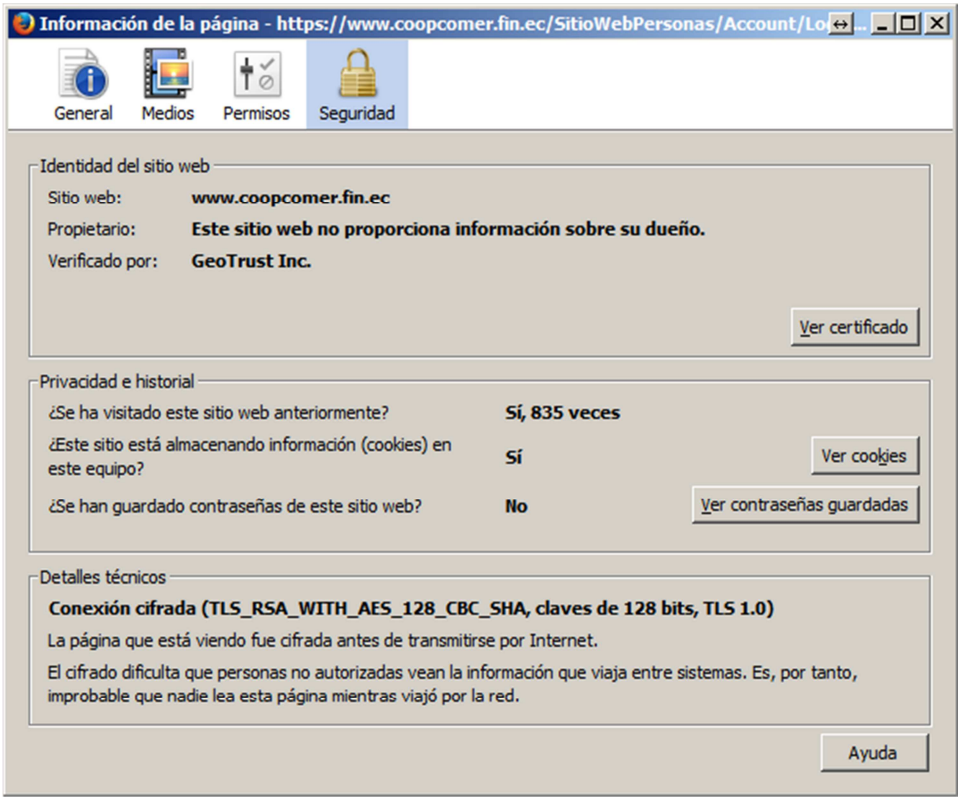

FIGURA 4.1 Información de la página web.

Como vulnerabilidad se puede apreciar que el protocolo utilizado para generar la conexión cifrada es el TLS versión 1.0, sabiendo que en esta versión se han descubierto fallas de seguridad que podrían comprometer la confidencialidad de la comunicación.

Otra vulnerabilidad encontrada puede ser el hecho de que la página permite almacenar la contraseña de usuario en el equipo que se esté ingresando, dándole acceso a otro usuario totalmente ajeno a la cuenta con solo tener al alcance dicho equipo.

4.2 ANÁLISIS DE VULNERABILIDADES DEL SISTEMA OPERATIVO.

Como sistema Operativo se encuentra instalado Windows Server 2008 R2 Standard Service Pack 1 Licenciado. Como vulnerabilidad encontramos que dicho sistema operativo no se encuentra actualizado con sus últimos parches de seguridad ya que según se muestra en la imagen no se ha instalado ninguna actualización:

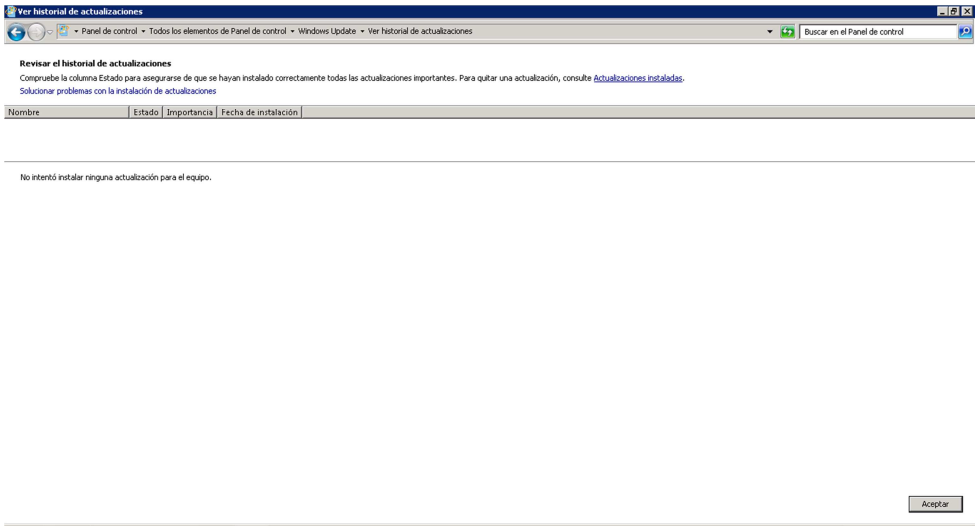

FIGURA 4.2 Historial de actualizaciones.

Como se puede apreciar, las actualizaciones automáticas se encuentran desactualizadas.

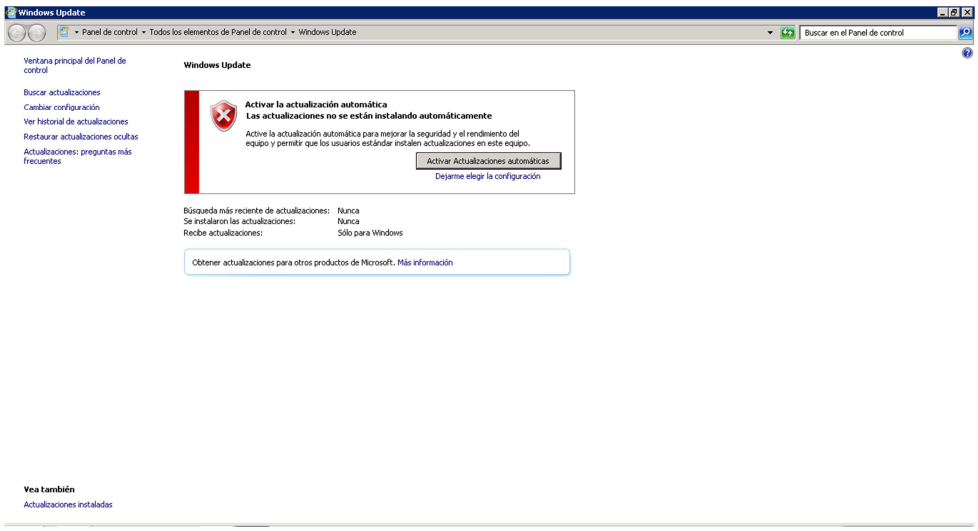

FIGURA 4.3 Windows Update.

Como consecuencia de la falta de actualizaciones, se puede anticipar que el servidor web IIS “Internet Information Services” se encuentra en la misma situación.

4.3 ANÁLISIS DE LOS APLICATIVOS INSTALADOS EN EL SERVIDOR.

A continuación se muestran los aplicativos instalados en el servidor.

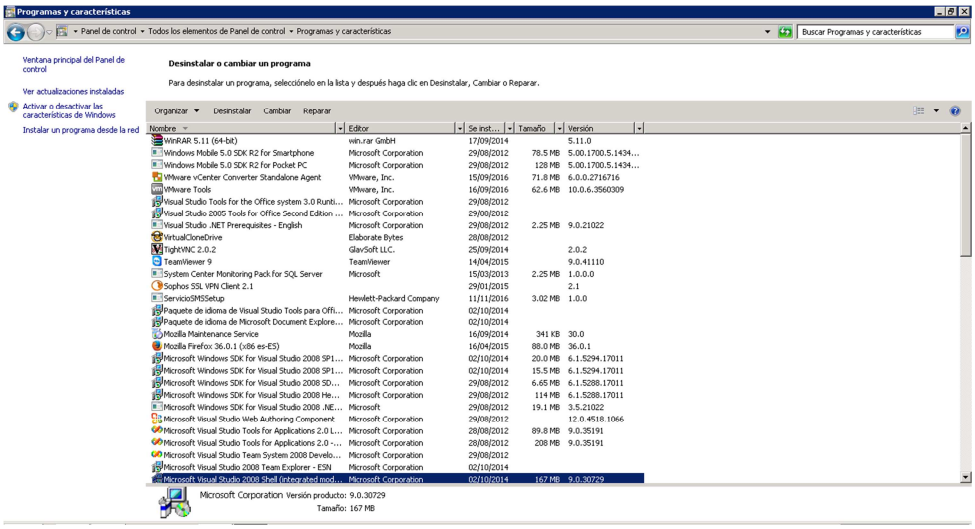

FIGURA 4.4 Programas y características.

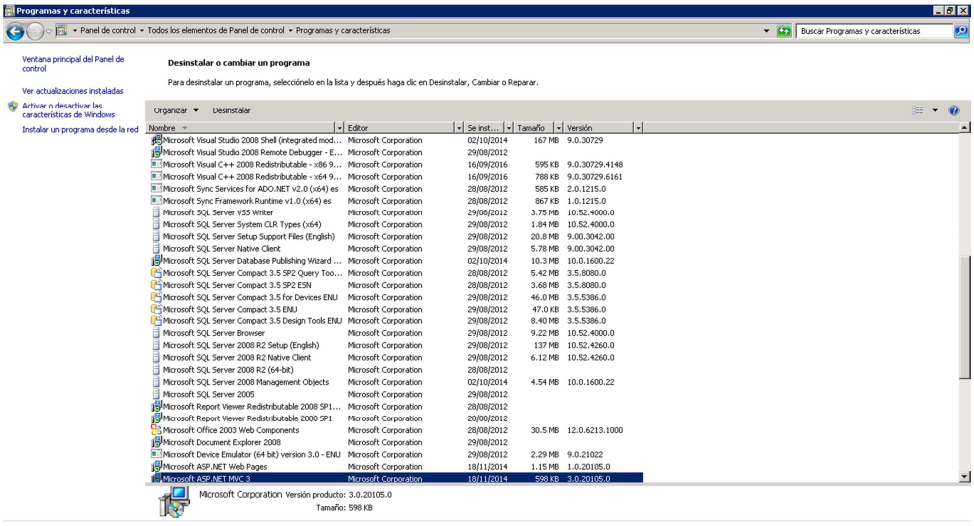

FIGURA 4.5 Programas y características.

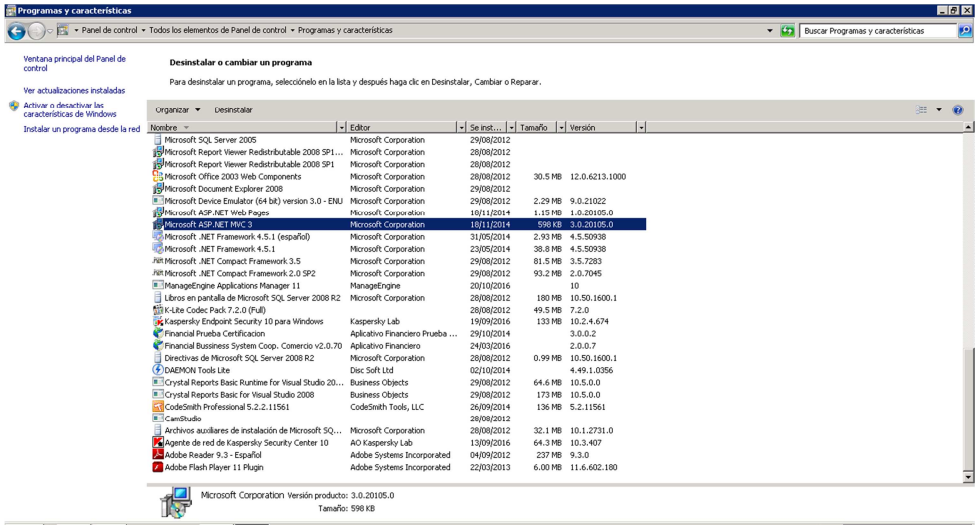

FIGURA 4.6 Programas y características.

En la lista de programas instalados apreciamos que hay varios tipos, entre ellos propios al servicio que presta y otros cuya presencia lo vuelven vulnerable, entre estos nombramos a los siguientes:

- TeamViewer
- TightVNC

Este tipo de programas permiten la conexión remota al servidor con el usuario que actualmente se encuentre activo, incluido el usuario administrador.

4.4 ANÁLISIS DE VULNERABILIDADES EN EL ÁREA FÍSICA DONDE SE ENCUENTRA EL SERVIDOR.

En la actualidad el servidor se encuentra ubicado en el centro de cómputo matriz cuyas características de seguridad se describen a continuación según documentación interna del departamento de TI de la institución.

Tabla 4 Consideraciones de seguridad físicas del CC.

	ASPECTOS DE SEGURIDAD	CUMPLIMIENTO
CONSIDERACIONES DE SEGURIDAD FÍSICAS DEL CENTRO DE COMPUTO	Lugar sin accesos a ventanas, puertas secundarias y paso de personas no autorizadas	Si
	Puerta de seguridad blindada	No
	Acceso biométrico	No
	Cámaras de seguridad	No
	Detectores de humo	Si
	Local con planta eléctrica para contingencias	Si
	Protectores y estabilizadores de voltaje	Si
	Aire acondicionado Split 24 horas	Si
	Techo falso	Si
	Aire acondicionado de precisión	No
	Piso falso	No
	Equipos con sistema de Backup eléctrico	Si
	Tomas eléctricas correctamente aterrizadas	Si
	Cableado estructurado	Si
	Sensores de movimiento	Si

Según se muestra, este centro de cómputo cumple con el 66.6% de las consideraciones físicas ideales para su funcionamiento.

CAPÍTULO 5

DESARROLLO DEL ESQUEMA DE SEGURIDAD PARA REDUCIR LAS VULNERABILIDADES

5.1 CRONOGRAMA DE ACTIVIDADES.

A continuación se presenta el cronograma de las actividades realizadas para el desarrollo del esquema de seguridad.

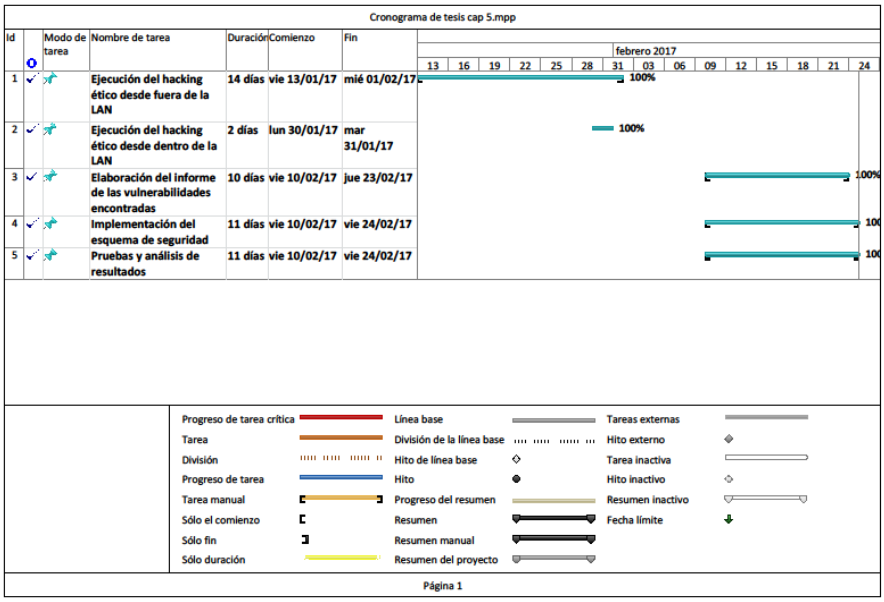

FIGURA 5.1 Cronograma de actividades.

5.2 EJECUCIÓN DEL HACKING ÉTICO DESDE DENTRO Y FUERA DE LA RED LOCAL.

En este capítulo se presentan las pruebas de hacking ético realizadas para encontrar vulnerabilidades desde dentro como fuera de la red, usando como marco de referencia la metodología OSSTMM, trabajando con las principales herramientas de seguridad tanto libres como licenciadas.

5.2.1. RED EXTERNA - INTERNET

Se procederá con las siguientes pruebas externas:

- **Pruebas de enumeración.**

  Esta prueba consiste en descubrir los puertos que se encuentran abiertos y escuchando peticiones, para lo cual se utilizó una máquina virtual con Kali Linux con acceso a internet y como parámetros el comando “nmap” y la ip publica del servidor de página web.

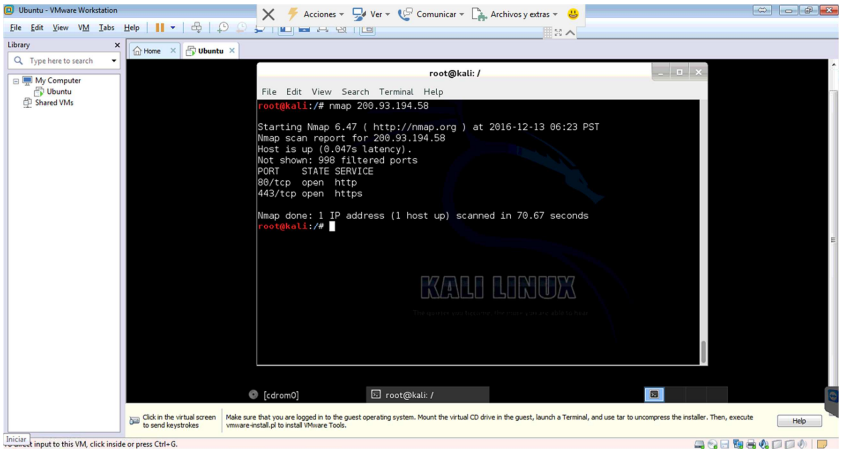

FIGURA 5.2 Prueba de enumeración.

- **Ataque de fuerza bruta.**

  Este procedimiento consiste en atacar un puerto abierto y cuyo servicio permita realizar consultas simultáneas de credenciales de usuario y contraseña por medio de comandos y un diccionario. En este caso encontramos según la imagen anterior que no existen servicios activos a los que les podamos realizar este tipo de ataques.

- **Prueba SQL Injectión.**

  El ataque de Sql Injectión se basa en ingresar código SQL en campos de ingreso de datos en aplicativos web, los cuales no validan dicho ingreso y son vulnerables de tal manera que permiten la extracción de información sensible de la base de datos con la cual se conectan.

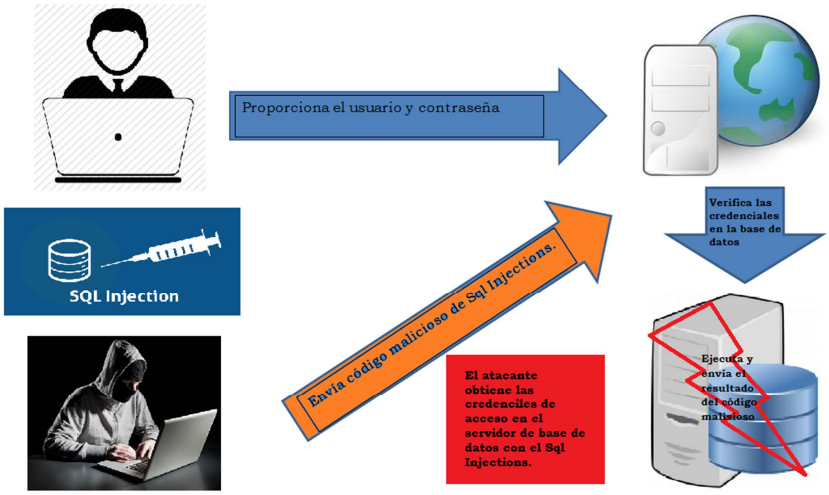

FIGURA 5.3 Proceso de SQL Injectión.

En primer lugar se verificó si se valida la entrada en los campos de ingreso de datos.

Esto se logró probando con bypasses tales como el ya conocido ' or '1'='1.

FIGURA 5.4 Prueba de SQL Injectión.

Una vez hecho el ingreso, visualizamos el mensaje de error que lanzó la página, confirmando que no permite el ingreso de este tipo de código.

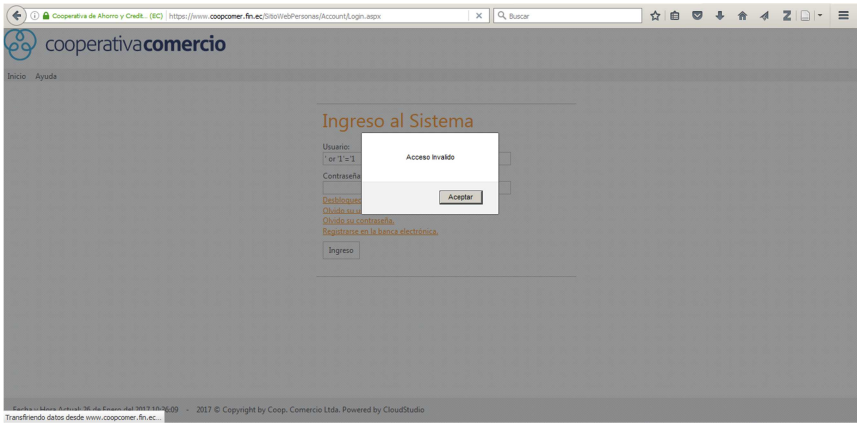

FIGURA 5.5 Resultado SQL Injectión.

A continuación se procedió a probar si el LOGIN tiene algún otro tipo de vulnerabilidad, se regresó al formulario y dejando en blanco el usuario y clave, se dio click en el botón “Ingreso”, para lo cual el servidor nos mostró los mensajes de error “Usuario Requerido” y “Password Requerido”.

FIGURA 5.6 Prueba de verificación de campos de ingreso.

Otra prueba realizada fue con la herramienta “sqlmap” de Kali Linux.

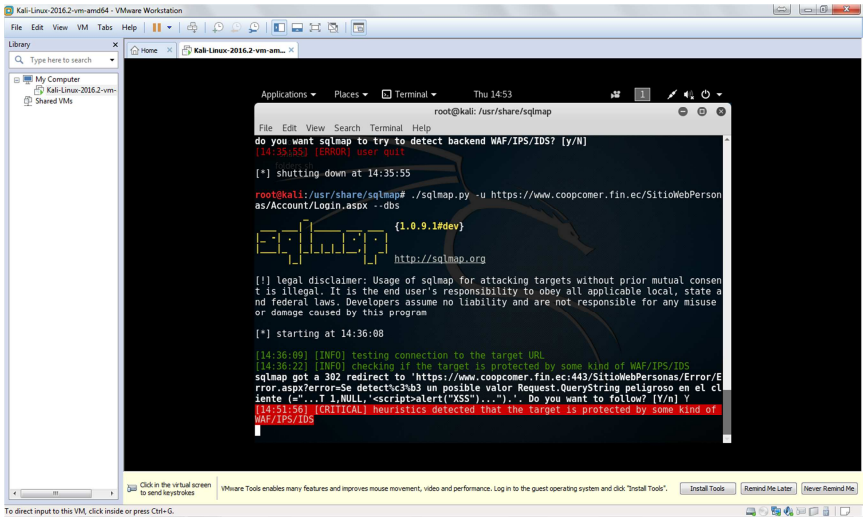

FIGURA 5.7 Prueba de sqlmap con herramienta Kali Linux.

Según se muestra en el resultado que arrojó la herramienta, el objetivo se encontraba protegido por un WAF/IPS/IDS y no puedo continuar con el proceso.

- **Hacker Google.**

  Este método de análisis de vulnerabilidades se realiza mediante palabras claves utilizadas en el motor de búsqueda de Google, permitiendo recopilar información relevante y sensible la cual en muchos casos no debería estar publicada o de libre acceso.

  A continuación se muestran los resultados de las búsquedas realizadas a la página de la institución comprendida en esta tesis.

  (info:"sitio web").- Utilizada para buscar información general de la página.

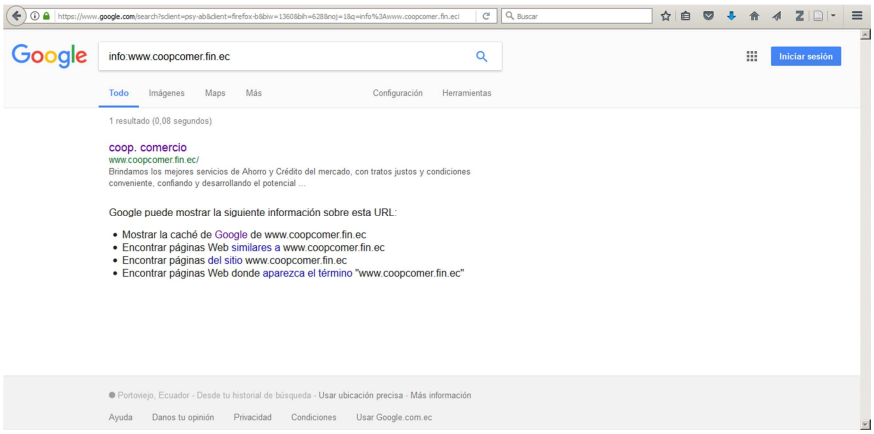

FIGURA 5.8 Prueba con la palabra clave "info".

(site:"sitio web" filetype:sql).- Permite la búsqueda de bases de datos publicados en un sitio web.

Según se observa, no arrojó ningún resultado.

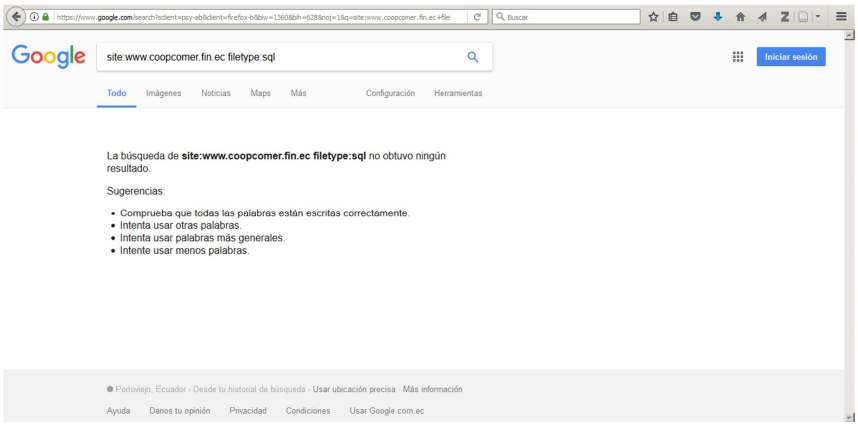

FIGURA 5.9 Prueba con palabra clave “site”.

(allinurl:”sitio web/subsitio”).- Este palabra clave permita buscar coincidencia con un enlace si es que existe en un sitio web.

En nuestro caso se utilizó con el objetivo de encontrar consolas de administración publicadas con la pagina tales como “phpmyadmin” y posterior a esto verificar otras vulnerabilidades, entre ellas credenciales de acceso por defecto como “admin” o “root”.

Según se muestra en la imagen, tampoco arrojó ningún resultado.

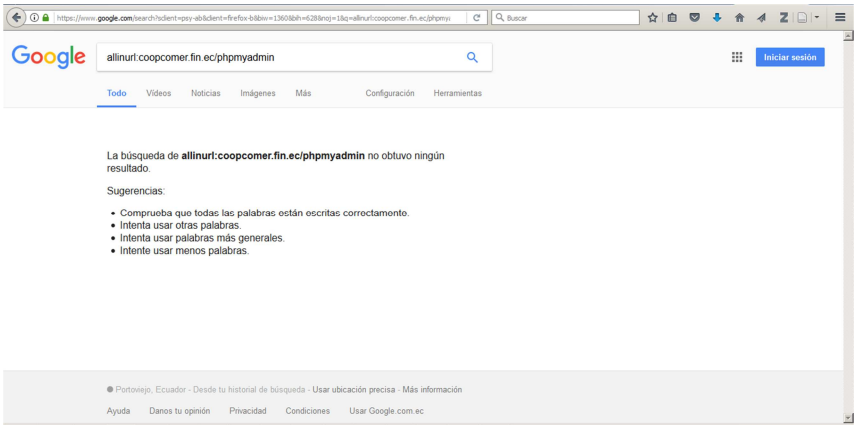

FIGURA 5.10 Prueba con la palabra clave "allinurl".

(site:"sitio web" filetype:inc).- En este caso la búsqueda fue a archivos "inc" (utilizados en php para realizar referencias a las conexiones de bases de datos).

En la caso de nuestra página, no arrojó ningún resultado.

FIGURA 5.11 Prueba 2 con palabra clave "site".

(site:"sitio web" index.of).- Como particularidad, la palabra "index.of" es incluida para buscar archivos indexados en el sitio web.

Tampoco encontró ningún resultado.

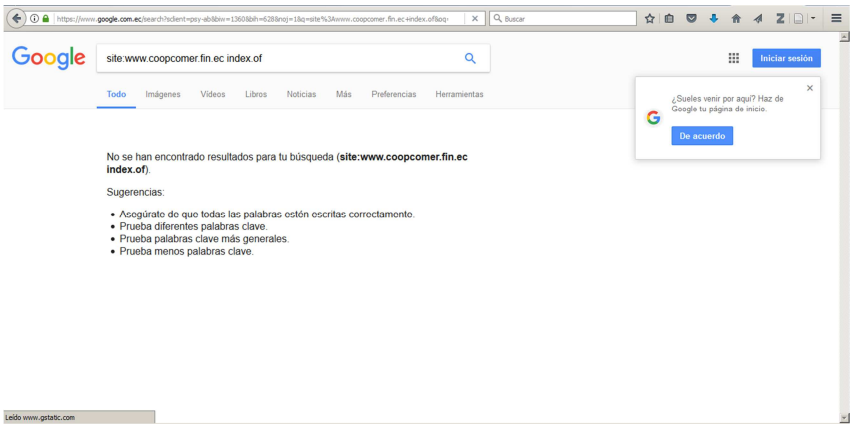

FIGURA 5.12 Prueba 3 con palabra clave "site".

5.2.2. Auditoria de Aplicación Web.

En este caso se utilizaron dos herramientas, "Owasp-zap" de Kali Linux y Qualys, ambas basándose en la metodología Owasp.

- **Owasp-Zap.-** En esta herramienta fue necesario ingresar la página que deseamos analizar y posterior a esto una vez transcurrido el tiempo necesario obtendremos los resultados de dicho análisis.

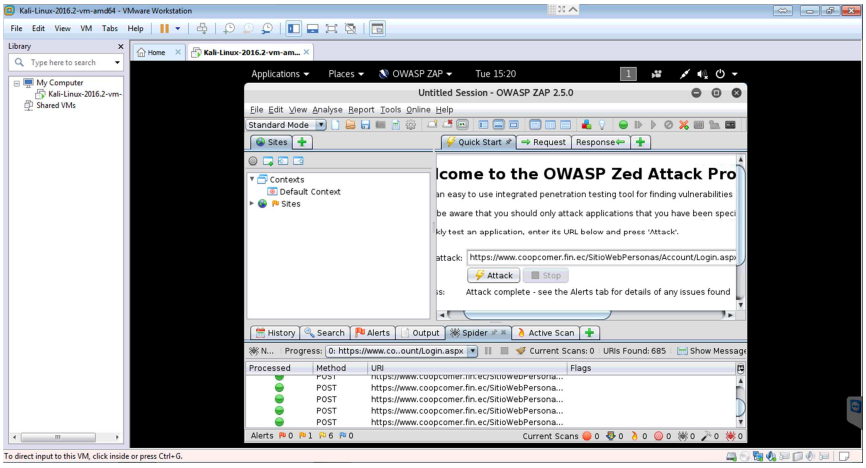

FIGURA 5.13 Prueba con herramienta Owasp-Zap.

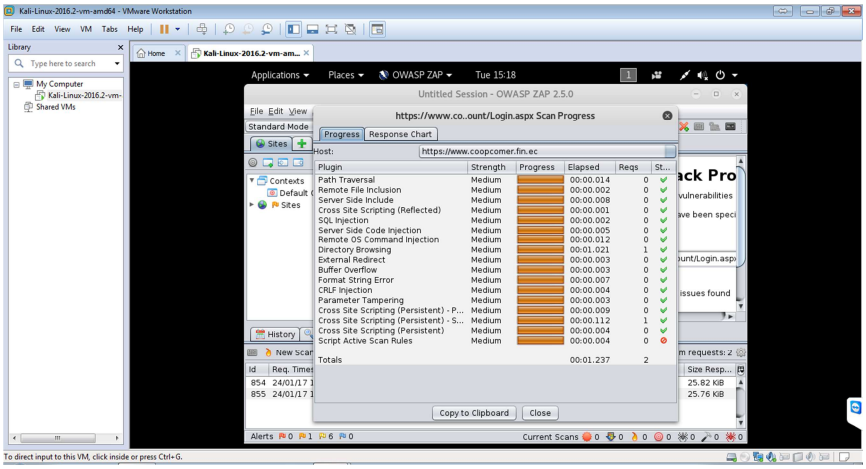

FIGURA 5.14 Resultado de prueba con herramienta Owasp-Zap.

Los resultados se presentan mediante un reporte el cual mostramos a continuación.

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	6
Informational	0

Alert Detail

Tabla 5 Reporte de escaneo ZAP

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx
URL	https://www.coopcomer.fin.ec/robots.txt
URL	https://www.coopcomer.fin.ec/sitemap.xml
URL	https://www.coopcomer.fin.ec/nuevos-servicios.html
URL	https://www.coopcomer.fin.ec/mis-finanzas-mi-futuro.html
URL	https://www.coopcomer.fin.ec/cosede.html
URL	https://www.coopcomer.fin.ec/seguridad-financiera.html
URL	https://www.coopcomer.fin.ec/seguridad-tarjetas.html
URL	https://www.coopcomer.fin.ec/los-lopez-y-su-dinero.html

URL	https://www.coopcomer.fin.ec/educacion-financiera.html
URL	https://www.coopcomer.fin.ec/videoteca.html
URL	https://www.coopcomer.fin.ec/seguridad-cajeros-automaticos.html
URL	https://www.coopcomer.fin.ec/seguridad-p%C3%A1ginas-web.html
URL	https://www.coopcomer.fin.ec/educacion-y-seguridad-financiera.html
URL	https://www.coopcomer.fin.ec/seguridad-correos.html
URL	https://www.coopcomer.fin.ec/consumo-reactivacion.html
URL	https://www.coopcomer.fin.ec/reactivacion.html
URL	https://www.coopcomer.fin.ec/planeas-un-proyecto.html
URL	https://www.coopcomer.fin.ec/microcredito-reactivaci%C3%B3n.html
URL	https://www.coopcomer.fin.ec/cta-de-ahorros-a-la-vista.html
Instances	155
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Other information	At "High" threshold this scanner will not alert on client or server error responses.

Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15

Low (Medium)	**Incomplete or No Cache-control and Pragma HTTP Header Set**
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx
URL	https://www.coopcomer.fin.ec/robots.txt
URL	https://www.coopcomer.fin.ec/sitemap.xml
URL	https://www.coopcomer.fin.ec/nuevos-servicios.html
URL	https://www.coopcomer.fin.ec/mis-finanzas-mi-futuro.html
URL	https://www.coopcomer.fin.ec/cosede.html
URL	https://www.coopcomer.fin.ec/seguridad-financiera.html
URL	https://www.coopcomer.fin.ec/seguridad-tarjetas.html
URL	https://www.coopcomer.fin.ec/los-lopez-y-su-dinero.html
URL	https://www.coopcomer.fin.ec/educacion-financiera.html
URL	https://www.coopcomer.fin.ec/videoteca.html
URL	https://www.coopcomer.fin.ec/seguridad-cajeros-automaticos.html

URL	https://www.coopcomer.fin.ec/seguridad-p%C3%A1ginas-web.html
URL	https://www.coopcomer.fin.ec/educacion-y-seguridad-financiera.html
URL	https://www.coopcomer.fin.ec/seguridad-correos.html
URL	https://www.coopcomer.fin.ec/consumo-reactivacion.html
URL	https://www.coopcomer.fin.ec/reactivacion.html
URL	https://www.coopcomer.fin.ec/planeas-un-proyecto.html
URL	https://www.coopcomer.fin.ec/microcredito-reactivaci%C3%B3n.html
URL	https://www.coopcomer.fin.ec/cta-de-ahorros-a-la-vista.html
Instances	151
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate, private; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
Low (Medium)	**Cookie Without Secure Flag**
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx
Parameter	ASP.NET_SessionId=1rj1vkvne4l11iesspbox5ak; path=/; HttpOnly
Evidence	ASP.NET_SessionId=1rj1vkvne4l11iesspbox5ak; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx
Parameter	ASP.NET_SessionId=aagxx305i3b1h5u1xkbtzf54; path=/; HttpOnly
Evidence	ASP.NET_SessionId=aagxx305i3b1h5u1xkbtzf54; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/DesbloqueoCuenta.aspx
Parameter	ASP.NET_SessionId=ltd0coba5ozysqpj0wp3snwe; path=/; HttpOnly
Evidence	ASP.NET_SessionId=ltd0coba5ozysqpj0wp3snwe; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/UsuarioOlvidado.aspx
Parameter	ASP.NET_SessionId=r03ervcxupd4wrnkrhtx3o3e; path=/; HttpOnly
Evidence	ASP.NET_SessionId=r03ervcxupd4wrnkrhtx3o3e; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/ClaveOlvidada.aspx
Parameter	ASP.NET_SessionId=fh2nyppeylcpbrc5v3s203p1; path=/; HttpOnly
Evidence	ASP.NET_SessionId=fh2nyppeylcpbrc5v3s203p1; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Registrarse.aspx

Parameter	ASP.NET_SessionId=2uv4tjuub52hvmheztt01z1x; path=/; HttpOnly
Evidence	ASP.NET_SessionId=2uv4tjuub52hvmheztt01z1x; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx
Parameter	ASP.NET_SessionId=xysznfomoe4pktc2ckkmhjvi; path=/; HttpOnly
Evidence	ASP.NET_SessionId=xysznfomoe4pktc2ckkmhjvi; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx?ReturnUrl=%2fSitioWebPersonas%2fDefault.aspx
Parameter	ASP.NET_SessionId=ja4fjmjgtimrs5u0ukryls5s; path=/; HttpOnly
Evidence	ASP.NET_SessionId=ja4fjmjgtimrs5u0ukryls5s; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx?ReturnUrl=%2fSitioWebPersonas%2fAyuda.aspx
Parameter	ASP.NET_SessionId=agr1udu3cdu5hnju1hoyhcqd; path=/; HttpOnly
Evidence	ASP.NET_SessionId=agr1udu3cdu5hnju1hoyhcqd; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/DesbloqueoCuenta.aspx
Parameter	ASP.NET_SessionId=cpu2lwi2vsgehnfwh4rxonia; path=/; HttpOnly
Evidence	ASP.NET_SessionId=cpu2lwi2vsgehnfwh4rxonia; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/UsuarioOlvidado.aspx

Parameter	ASP.NET_SessionId=oxqc42wgfv5cot2bntpyghin; path=/; HttpOnly
Evidence	ASP.NET_SessionId=oxqc42wgfv5cot2bntpyghin; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/ClaveOlvidada.aspx
Parameter	ASP.NET_SessionId=dqav0psfahnidsykqkwq1k20; path=/; HttpOnly
Evidence	ASP.NET_SessionId=dqav0psfahnidsykqkwq1k20; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Registrarse.aspx
Parameter	ASP.NET_SessionId=f0w0wyfa40h5v55qdyzcdqid; path=/; HttpOnly
Evidence	ASP.NET_SessionId=f0w0wyfa40h5v55qdyzcdqid; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx
Parameter	ASP.NET_SessionId=ib4rjx4uxeuqzs224fmnn213; path=/; HttpOnly
Evidence	ASP.NET_SessionId=ib4rjx4uxeuqzs224fmnn213; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx?ReturnUrl=%2fSitioWebPersonas%2fDefault.aspx
Parameter	ASP.NET_SessionId=ukqubhgqof2ubxadxuwaj1ys; path=/; HttpOnly
Evidence	ASP.NET_SessionId=ukqubhgqof2ubxadxuwaj1ys; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx?ReturnUrl=%2fSitioWebPersonas%2fAyuda.aspx

Parameter	ASP.NET_SessionId=em1qyi5sfqtacjqskuuksmzb; path=/; HttpOnly
Evidence	ASP.NET_SessionId=em1qyi5sfqtacjqskuuksmzb; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/DesbloqueoCuenta.aspx
Parameter	ASP.NET_SessionId=frei5bgwpnbz12ipdsdv0ryg; path=/; HttpOnly
Evidence	ASP.NET_SessionId=frei5bgwpnbz12ipdsdv0ryg; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/UsuarioOlvidado.aspx
Parameter	ASP.NET_SessionId=nzp1mdyc1negcdfyfyfigvry; path=/; HttpOnly
Evidence	ASP.NET_SessionId=nzp1mdyc1negcdfyfyfigvry; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/ClaveOlvidada.aspx
Parameter	ASP.NET_SessionId=ilfqqamw52dmyol3z4cxejmd; path=/; HttpOnly
Evidence	ASP.NET_SessionId=ilfqqamw52dmyol3z4cxejmd; path=/; HttpOnly
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx
Parameter	ASP.NET_SessionId=umb1ntfz3gtc44uhkoxcxk0z; path=/; HttpOnly
Evidence	ASP.NET_SessionId=umb1ntfz3gtc44uhkoxcxk0z; path=/; HttpOnly
Instances	37
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using

	an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614
WASC Id	13

Low (Medium)	**Web Browser XSS Protection Not Enabled**
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx
URL	https://www.coopcomer.fin.ec/robots.txt
URL	https://www.coopcomer.fin.ec/sitemap.xml
URL	https://www.coopcomer.fin.ec/nuevos-servicios.html
URL	https://www.coopcomer.fin.ec/mis-finanzas-mi-futuro.html
URL	https://www.coopcomer.fin.ec/cosede.html
URL	https://www.coopcomer.fin.ec/seguridad-financiera.html
URL	https://www.coopcomer.fin.ec/seguridad-tarjetas.html
URL	https://www.coopcomer.fin.ec/los-lopez-y-su-dinero.html
URL	https://www.coopcomer.fin.ec/educacion-financiera.html
URL	https://www.coopcomer.fin.ec/videoteca.html

URL	https://www.coopcomer.fin.ec/seguridad-cajeros-automaticos.html
URL	https://www.coopcomer.fin.ec/seguridad-p%C3%A1ginas-web.html
URL	https://www.coopcomer.fin.ec/educacion-y-seguridad-financiera.html
URL	https://www.coopcomer.fin.ec/seguridad-correos.html
URL	https://www.coopcomer.fin.ec/consumo-reactivacion.html
URL	https://www.coopcomer.fin.ec/reactivacion.html
URL	https://www.coopcomer.fin.ec/planeas-un-proyecto.html
URL	https://www.coopcomer.fin.ec/microcredito-reactivaci%C3%B3n.html
URL	https://www.coopcomer.fin.ec/cta-de-ahorros-a-la-vista.html
Instances	155
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and

	Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Low (Medium)	**Password Autocomplete in Browser**
Description	The AUTOCOMPLETE attribute is not disabled on an HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx
Parameter	input
Evidence	<input class="dxeEditArea_Metropolis dxeEditAreaSys" name="ctl00$ctl00$ASPxSplitter1$Content$MainContent$ASPxRoundPanel1$Password" onkeyup="aspxEKeyUp('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password', event)" id="ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password_I" onchange="aspxEValueChanged('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onblur="aspxELostFocus('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onfocus="aspxEGotFocus('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" type="password"

	onkeydown="aspxEKeyDown('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password', event)" />
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx
Parameter	Input
Evidence	<input class="dxeEditArea_Metropolis dxeEditAreaSys" id="ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password_I" name="ctl00$ctl00$ASPxSplitter1$Content$MainContent$ASPxRoundPanel1$Password" onfocus="aspxEGotFocus('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onblur="aspxELostFocus('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onchange="aspxEValueChanged('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onkeyup="aspxEKeyUp('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password', event)" type="password" />
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx?ReturnUrl=%2fSitioWebPersonas%2fDefault.aspx
Parameter	Input
Evidence	<input class="dxeEditArea_Metropolis dxeEditAreaSys" id="ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password_I" name="ctl00$ctl00$ASPxSplitter1$Content$MainContent$ASPxRoundPanel1$Password" onfocus="aspxEGotFocus('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onblur="aspxELostFocus('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onchange="aspxEValueChanged('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onkeyup="aspxEKeyUp('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password',

	event)" type="password" />
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx?ReturnUrl=%2fSitioWebPersonas%2fAyuda.aspx
Parameter	Input
Evidence	<input class="dxeEditArea_Metropolis dxeEditAreaSys" id="ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password_I" name="ctl00$ctl00$ASPxSplitter1$Content$MainContent$ASPxRoundPanel1$Password" onfocus="aspxEGotFocus('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onblur="aspxELostFocus('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onchange="aspxEValueChanged('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onkeyup="aspxEKeyUp('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password', event)" type="password" />
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx?ReturnUrl=%2fSitioWebPersonas%2fstyle11217.css
Parameter	Input
Evidence	<input class="dxeEditArea_Metropolis dxeEditAreaSys" id="ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password_I" name="ctl00$ctl00$ASPxSplitter1$Content$MainContent$ASPxRoundPanel1$Password" onfocus="aspxEGotFocus('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onblur="aspxELostFocus('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onchange="aspxEValueChanged('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password')" onkeyup="aspxEKeyUp('ASPxSplitter1_Content_MainContent_ASPxRoundPanel1_Password', event)" type="password" />

Instances	5
Solution	Turn off the AUTOCOMPLETE attribute in forms or individual input elements containing password inputs by using AUTOCOMPLETE='OFF'.
Reference	http://www.w3schools.com/tags/att_input_autocomplete.asp https://msdn.microsoft.com/en-us/library/ms533486%28v=vs.85%29.aspx
CWE Id	525
WASC Id	15

Low (Medium)	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://www.coopcomer.fin.ec/SitioWebPersonas/Account/Login.aspx
URL	https://www.coopcomer.fin.ec/robots.txt
URL	https://www.coopcomer.fin.ec/sitemap.xml
URL	https://www.coopcomer.fin.ec/nuevos-servicios.html
URL	https://www.coopcomer.fin.ec/mis-finanzas-mi-futuro.html
URL	https://www.coopcomer.fin.ec/cosede.html

URL	https://www.coopcomer.fin.ec/seguridad-financiera.html
URL	https://www.coopcomer.fin.ec/seguridad-tarjetas.html
URL	https://www.coopcomer.fin.ec/los-lopez-y-su-dinero.html
URL	https://www.coopcomer.fin.ec/educacion-financiera.html
URL	https://www.coopcomer.fin.ec/videoteca.html
URL	https://www.coopcomer.fin.ec/seguridad-cajeros-automaticos.html
URL	https://www.coopcomer.fin.ec/seguridad-p%C3%A1ginas-web.html
URL	https://www.coopcomer.fin.ec/educacion-y-seguridad-financiera.html
URL	https://www.coopcomer.fin.ec/seguridad-correos.html
URL	https://www.coopcomer.fin.ec/consumo-reactivacion.html
URL	https://www.coopcomer.fin.ec/reactivacion.html
URL	https://www.coopcomer.fin.ec/planeas-un-proyecto.html
URL	https://www.coopcomer.fin.ec/microcredito-reactivaci%C3%B3n.html
URL	https://www.coopcomer.fin.ec/cta-de-ahorros-a-la-vista.html
Instances	155
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a

	standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15

Low (Medium)	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://www.coopcomer.fin.ec/nuevos-servicios.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/mis-finanzas-mi-futuro.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js

URL	https://www.coopcomer.fin.ec/cosede.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/seguridad-financiera.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/seguridad-tarjetas.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/los-lopez-y-su-dinero.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/educacion-financiera.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/videoteca.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-

	35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/seguridad-cajeros-automaticos.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/seguridad-p%C3%A1ginas-web.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/educacion-y-seguridad-financiera.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/seguridad-correos.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/consumo-reactivacion.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js

Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/reactivacion.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/planeas-un-proyecto.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/microcredito-reactivaci%C3%B3n.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/cta-de-ahorros-a-la-vista.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/tramsparencia-de-informacion.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js

URL	https://www.coopcomer.fin.ec/contactenos.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
URL	https://www.coopcomer.fin.ec/seguro-de-desgravamen.html
Parameter	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Evidence	//seal.globalsign.com/SiteSeal/gmogs_image_90-35_en_blue.js
Instances	43
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15

- **Qualys.-** Los resultados del análisis por medio de esta herramienta se presentan en el anexo # 001.

5.2.3. Auditoria en Sistema Operativo.

Este procedimiento se realizó con la herramienta licenciada Qualys, los resultados se presentan en el anexo # 002.

5.2.4. Análisis de certificado.

Para el análisis del certificado de la página web se hizo uso de la herramienta Qualys SSL LABS, como resultado se obtuvo una calificación tipo “C” según se muestra en la imagen a continuación.

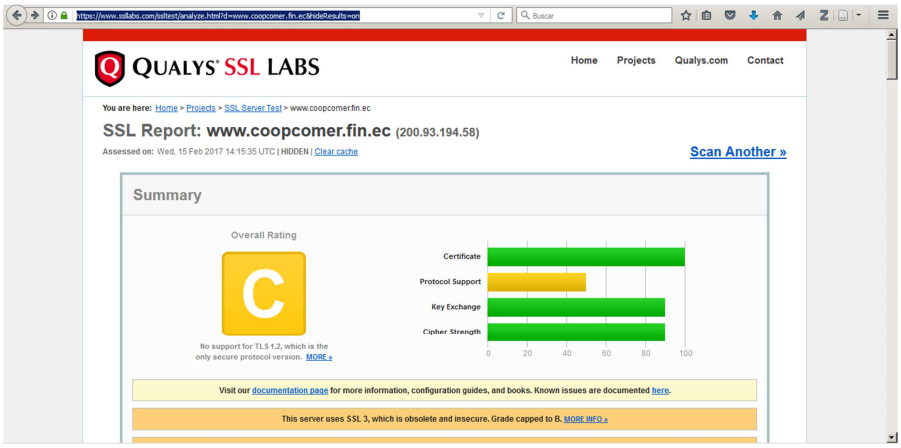

FIGURA 5.15 Análisis de certificado del sitio web.

El reporte completo del análisis se puede visualizar en el anexo # 003.

5.2.5. RED INTERNA - LAN

Los resultados del análisis a la red LAN se ejecutaron con la herramienta Qualys, dicha información se presentan en el anexo # 004.

5.3 INFORME DE LAS VULNERABILIDADES ENCONTRADAS.

5.3.1. AUDITORIA DE APLICACIÓN WEB

- **Cross-Site Scripting:** Según lo indicado en el informe, no se encontró riesgo de explotación.

  Detalles:

  Amenaza.

  La aplicación web refleja caracteres potencialmente peligrosos como comillas simples, comillas dobles y corchetes angulares. Estos caracteres se usan comúnmente para ataques de inyección de HTML, tales como secuencias de comandos entre sitios (XSS).

  Impacto.

  No se determinó ningún exploit para estos caracteres reflejados. El parámetro de entrada se debe analizar manualmente para verificar que no se pueden inyectar otros caracteres que conducirían a una vulnerabilidad de la inyección HTML (XSS).

  Solución.

  Revise los caracteres reflejados para asegurarse de que se manejan correctamente según lo definido por la práctica de codificación de la aplicación web. Las soluciones típicas son

aplicar codificación HTML o codificación porcentual a los caracteres dependiendo de dónde se colocan en el HTML. Por ejemplo, una comilla doble podría ser codificada como "cuando se muestra en un nodo de texto, pero como % 22 cuando se coloca en el valor de un atributo “href”.

- **Path Disclosure:** Se determinó como una vulnerabilidad latente.

  Detalles:

  Amenaza.

  Se descubrió en el servidor Web una lista de archivos, directorios o directorios potencialmente confidenciales.

  Impacto.

  El contenido de este archivo o directorio puede revelar información confidencial.

  Solución.

  Compruebe que no se permite el acceso a este archivo o directorio. Si es necesario, quítelo o aplique controles de acceso.

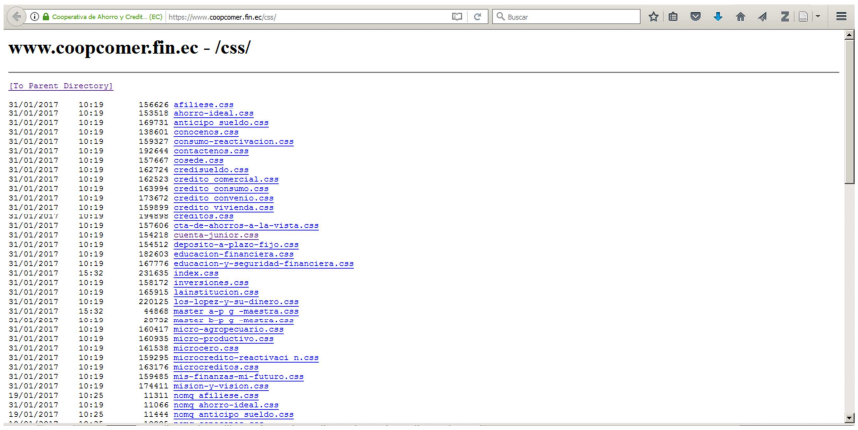

FIGURA 5.16 Listado de directorios.

- **Clickjacking - Framable Page:** Se determinó como una vulnerabilidad real.

  Detalles:

  Amenaza.

  El encabezado X-Frame-Options no está establecido, y eso puede conducir a un posible enmarcado de la página. Un atacante puede engañar al usuario para que haga clic en el enlace encuadrando la página original y mostrando una capa encima de ella con botones ficticios.

  Impacto.

  Pueden realizarse ataques como Clickjacking y Cross-Site Request Forgery (CSRF).

  Solución.

Establezca las opciones de X-Frame: Esta cabecera funciona con navegadores modernos y se puede utilizar para evitar el enmarcado de la página. Tenga en cuenta que debe ser una cabecera HTTP, la configuración se ignora si se crea como un elemento meta "http-equiv" dentro de la página.

- **Session Cookie Does Not Contain the "Secure" Attribute:** Se determinó como una vulnerabilidad latente.

  Detalles:

  Amenaza.

  La cookie de sesión no contiene el atributo "seguro"

  Impacto.

  Las cookies de sesión con el atributo "seguro" sólo se permiten ser enviadas a través de HTTPS. Las cookies de sesión enviadas a través de HTTP exponen a los usuarios a recibir ataques que podrían llevar a la suplantación de usuarios o a compromisos de cuentas

  Solución.

  Aplique el atributo "seguro" a las cookies de sesión para asegurarse de que se enviarán sólo a través de HTTPS.

- **Sensitive form field has not disabled autocomplete:** Se determinó como una vulnerabilidad latente.

  Detalles:

  Amenaza.

  Un formulario HTML que recopila información confidencial (como un campo de contraseña) no impide que el navegador solicite al usuario que guarde los valores rellenados para su posterior reutilización. Las credenciales almacenadas no deben estar disponibles para nadie, excepto para su propietario.

  Impacto.

  Si el navegador se utiliza en un entorno informático compartido en el que más de una persona puede utilizar el navegador, los valores de "autocompletar" pueden ser enviados por un usuario no autorizado. Por ejemplo, si un navegador guarda el nombre de inicio de sesión y la contraseña de un formulario, cualquiera con acceso al navegador puede enviar el formulario y autenticarse en el sitio sin tener que saber la contraseña de la víctima.

  Solución.

  Agregue el siguiente atributo al elemento de formulario o entrada: autocomplete = "off" Este atributo impide que el navegador solicite al usuario que guarde los valores de formulario rellenados para su posterior reutilización.

- **Active Mixed Content Vulnerability:** Se determinó como una vulnerabilidad latente.

  Detalles:

  Amenaza.

  Se ha descubierto una vulnerabilidad de contenido mixto activo al cargar la página web. En aplicaciones web de contenido mixto, la página web se entrega al navegador a través de un canal seguro, pero el contenido adicional se entrega a través de un canal no seguro. Clasificamos el contenido mixto en contenido mixto activo con referencia al comportamiento del navegador Mozilla Firefox. Vulnerabilidad de contenido mixto activo se informa si se descubre cualquiera de los siguientes contenidos al cargar la página web para entregarla en un canal no seguro. Script, enlace, iframe, solicitudes XMLHttpRequest, objeto, applet

  Impacto.

  Los canales no seguros (HTTP) no están cifrados y por lo tanto son vulnerables a los ataques de olfatear. Estos canales no seguros pueden ser explotados para obtener acceso a un amplio conjunto de capacidades tales como solicitudes de forja, robo de cookies o fuga de datos DOM.

  Solución.

La solución a la vulnerabilidad de contenido mixto es simplemente cargar sub-recursos de la página web a través de HTTPS. Además de cargar el sub-recurso a través de HTTPS, puede mitigarse utilizando las siguientes dos opciones: 1. HTTP Strict Transport Security (HSTS) 2. Política de seguridad de contenido (CSP)

FIGURA 5.17 Sitio web con contenido mixto.

- **Clickjacking - X-Frame-Options header is not set:** Esta vulnerabilidad ya fue evaluada en el punto 3.

5.3.2. Auditoria en Sistema Operativo

- **Microsoft Windows HTTP.sys Remote Code Execution Vulnerability.**

  Detalle:

  Amenaza.

  Windows es propenso a una ejecución de código remoto que afecta a la pila de protocolo HTTP (HTTP.sys).

  La vulnerabilidad se produce cuando la pila de protocolo HTTP (HTTP.sys) analiza de forma incorrecta peticiones HTTP creadas.

  Microsoft ha publicado una actualización de seguridad que corrige la vulnerabilidad al corregir la forma en que HTTP.sys gestiona las solicitudes.

  Esta actualización de seguridad se considera crítica para las ediciones compatibles de Windows 7, Windows 8, Windows 2008 R2 y Windows Server 2012.

  Impacto.

  La vulnerabilidad podría permitir la ejecución remota de código si un atacante envía con éxito peticiones HTTP creadas a un sistema Windows afectado.

  Solución.

Consulte MS15-034 (https://technet.microsoft.com/library/security/MS15-034) para obtener más información.

Parche:

A continuación encontrará enlaces para descargar parches para solucionar las vulnerabilidades:

MS15-034: Windows 7 para sistemas de 32 bits Service Pack 1 (https://www.microsoft.com/downloads/details.aspx?Familyid=5e2fda5f-60ba-4769-81b6-2b3206f25831)

MS15-034: Windows 7 para sistemas basados en x64 Service Pack 1 (https://www.microsoft.com/downloads/details.aspx?familyid=b0a6edc3-f693-4328-Aebc-001bf96bf1b2)

MS15-034: Windows Server 2008 R2 para sistemas basados en x64 Service Pack 1 (https://www.microsoft.com/downloads/details.aspx?Familyid=70ec42c6-588c-4d32-9ec0-bcc39085fbe7)

MS15-034: Windows Server 2008 R2 para sistemas basados en Itanium Service Pack 1 (https://www.microsoft.com/downloads/details.aspx?Familyid=7d485942-c4af-49e0-aa0d-ed338de82196)

MS15-034: Windows 8 para sistemas de 32 bits (https://www.microsoft.com/downloads/details.aspx?familyid=6791bb93-3925-406c-87a1-1f44a7133db0)

MS15-034: Windows 8 para sistemas basados en x64 (https://www.microsoft.com/downloads/details.aspx?familyid=428768eb-d99d-464b-b546-B04dab5d6476)

MS15-034: Windows 8.1 para sistemas de 32 bits (https://www.microsoft.com/downloads/details.aspx?familyid=9a4c4c1d-87ed-49fb-bc55-adc011eb1207)

MS15-034: Windows 8.1 para sistemas basados en x64 (https://www.microsoft.com/downloads/details.aspx?familyid=3d9475fa-3255-4f80-Aad0-1ebf692b0bea)

MS15-034: Windows Server 2012 (https://www.microsoft.com/downloads/details.aspx?familyid=66fc9a93-28ce-4d50-9a11-fa8254390a6f)

MS15-034: Windows Server 2012 R2 (https://www.microsoft.com/downloads/details.aspx?familyid=3c995a85-6068-4cf0-a54d-220c2f061b95)

MS15-034: Windows Server 2008 R2 para sistemas basados en x64 Service Pack 1 (https://www.microsoft.com/downloads/details.aspx?Familyid=70ec42c6-588c-4d32-9ec0-bcc39085fbe7)

MS15-034: Windows Server 2012 (https://www.microsoft.com/downloads/details.aspx?familyid=66fc9a93-28ce-4d50-9a11-fa8254390a6f)

MS15-034: Windows Server 2012 R2 (https://www.microsoft.com/downloads/details.aspx?familyid=3c995a85-6068-4cf0-a54d-220c2f061b95)

- **SSL/TLS use of weak RC4 cipher.**

Detalles:

Amenaza.

Los protocolos Secure Sockets Layer (SSL v2 / v3) y TLS (Transport Layer Security) proporcionan servicios de integridad, confidencialidad y autenticidad a otros protocolos que carezcan de estas características.

Los protocolos SSL / TLS usan cifras como AES, DES, 3DES y RC4 para cifrar el contenido de los protocolos de capa superior y así proveer el servicio de confidencialidad. Normalmente, la salida de un proceso de cifrado es una secuencia de bytes de aspecto aleatorio. Se sabía que la salida RC4 tiene algún sesgo en la salida. Recientemente un grupo de investigadores ha descubierto que hay un sesgo más fuerte en RC4, lo que hace que el análisis estadístico del texto cifrado sea más práctico.

El ataque descrito es inyectar un javascript malicioso en el navegador de la víctima que garantice que hay múltiples conexiones que se establecen con un sitio web de destino y la

misma cookie HTTP se envía varias veces al sitio web en forma cifrada. Esto proporciona al atacante un gran conjunto de muestras de texto cifrado, que se pueden utilizar para el análisis estadístico.

NOTA: El 3/12/15 NVD cambió la complicidad de acceso CVSS v2 de alto a medio. Como resultado, Qualys revisó el puntaje CVSS a 4.3 inmediatamente. El 5/4/15 Qualys también está revisando la gravedad al nivel 3.

Impacto.

Si se realiza este ataque y se recupera una cookie HTTP, el atacante puede utilizar la cookie para suplantar al usuario cuya cookie se recuperó.

Este ataque no es muy práctico ya que requiere que el atacante tenga acceso a millones de muestras de texto cifrado, pero hay ciertos supuestos que un atacante puede hacer para mejorar las posibilidades de recuperar el texto claro de cihpertext. Por ejemplo, las cookies HTTP están codificadas en base64 o en dígitos hexadecimales. Esta información puede ayudar al atacante en sus esfuerzos por recuperar la cookie.

Solución.

RC4 no debe usarse donde sea posible. Una de las razones por las que RC4 todavía estaba siendo utilizada fue BEAST y

Lucky13 ataques contra codificaciones de modo CBC en SSL y TLS. Sin embargo, TLSv 1.2 o posterior trata estos problemas.

- **SSLv3 Padding Oracle Attack Information Disclosure Vulnerability.**

  Detalles:

  Amenaza.

  El error de diseño del protocolo SSL 3.0, utiliza relleno de CBC no determinista, lo que hace más fácil para los ataques man-in-the-middle.

  El destino admite SSLv3, lo que lo hace vulnerable a POODLE (Padding Oracle On Encryption Legacy Downgraded), aunque también admita versiones más recientes de TLS. Está sujeto a un ataque de downgrade, en el que el atacante engaña al navegador para que se conecte con SSLv3.

  Impacto.

  Un atacante que puede tomar una posición de hombre en el medio (MitM) puede explotar esta vulnerabilidad y tener acceso a la comunicación cifrada entre un cliente y un servidor.

  Solución.

Deshabilite el soporte SSLv3 para evitar esta vulnerabilidad.

Ejemplos para deshabilitar SSLv3.

Nginx: lista de protocolos permitidos específicos en la línea "ssl_protocols". Asegúrese de que SSLv2 y SSLv3 no aparezcan en la lista. Por ejemplo: ssl_protocols TLSv2 TLSv1.1 TLSv1.2;

Apache: Agregue -SSLv3 a la línea "SSLProtocol".

Cómo deshabilitar SSL 3.0 en Microsoft IIS (https://support.microsoft.com/kb/187498/en-us).

Para PCI, consulte el artículo de la comunidad Qualys (https://community.qualys.com/thread/15280).

- **SSL Server Has SSLv3 Enabled Vulnerability.**

Detalles:

Amenaza.

SSL 3.0 es un protocolo obsoleto e inseguro.

El cifrado en SSL 3.0 utiliza la cifra de flujo RC4 o un cifrado de bloque en modo CBC.

RC4 es conocido por tener sesgos, y el cifrado de bloque en modo CBC es vulnerable al ataque de POODLE.

El protocolo SSLv3 es inseguro debido al ataque de POODLE y a la debilidad del cifrado RC4.

Nota: En abril de 2015, PCI lanzó PCI DSS v3.1 (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf) anunciando que el NIST ya no considera el protocolo Secure Socket Layers (SSL) v3.0 como aceptable para proteger los datos y que todas las versiones del SSL no cumplen con la definición PCI de "criptografía fuerte".

Impacto.

Un atacante puede aprovechar esta vulnerabilidad para leer comunicaciones seguras o modificar mensajes maliciosos.

Solución.

Deshabilite el protocolo SSL 3.0 en el cliente y en el servidor, consulte Cómo deshabilitar SSLv3: Deshabilitar SSLv3 (http://disablessl3.com/)

- **SSL/TLS Server supports TLSv1.0.**

Detalle:

Amenaza.

TLS es capaz de utilizar una multitud de cifrados (algoritmos) para crear los pares de claves públicas y privadas.

Por ejemplo, TLSv1.0 podría utilizar el cifrado de flujo RC4 o un cifrado de bloque en modo CBC.

RC4 es conocido por tener sesgos y el cifrado de bloque en modo CBC es vulnerable al ataque de POODLE.

TLSv1.0, si está configurado para usar los mismos conjuntos de cifrado que SSLv3, incluye un medio por el cual una implementación TLS puede degradar la conexión a SSL v3.0, debilitando así la seguridad.

Un ataque tipo POODLE (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) también podría iniciarse directamente en TLS sin negociar una degradación.

Este QID será marcado como un fallo para PCI a partir del 1 de noviembre de 2016 de acuerdo con las nuevas normas. Para las implementaciones existentes, los comerciantes podrán presentar una Solicitud de Falso Positivo / Excepción de PCI y proporcionar prueba de su Plan de Mitigación de Riesgo y Migración, lo cual resultará en un pase para PCI hasta el 30 de junio de 2018.

Se pueden encontrar más detalles en: NUEVO PCI DSS v3.2 y migración desde SSL y TLS temprano v1.1 (https://community.qualys.com/message/34120)

Impacto.

Un atacante puede explotar fallas criptográficas para realizar ataques de tipo man-in-the-middle o comunicaciones de descifrado.

Por ejemplo: Un atacante podría forzar una degradación del protocolo TLS al antiguo protocolo SSLv3.0 y explotar la vulnerabilidad POODLE, leer comunicaciones seguras o modificar mensajes maliciosos.

Un ataque tipo POODLE (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) también podría iniciarse directamente en TLS sin negociar una degradación.

Solución.

Deshabilite el uso del protocolo TLSv1.0 en favor de un protocolo criptográfico más fuerte como TLSv1.2.

- **Listing of Scripts in the scripts Directory.**

Detalle:

Amenaza.

Se permite el listado de archivos en el directorio de scripts.

Impacto.

Al explorar el directorio de scripts, los usuarios no autorizados pueden obtener una lista de los scripts CGI presentes en su servidor. Con esta información pueden implementar ataques adicionales en secuencias de comandos CGI vulnerables.

Solución.

Establezca una regla más restrictiva en su servidor para evitar el listado del directorio de scripts.

- **Web Server Internal IP Address/Internal Network Name Disclosure Vulnerability.**

Detalle:

Amenaza.

Algunos servidores Web contienen una vulnerabilidad que proporciona a los atacantes remotos la capacidad de obtener su dirección IP interna o su nombre de red interna.

Un atacante conectado a un host en su red utilizando HTTPS (normalmente en el puerto 443) podría elaborar una solicitud GET especialmente formada desde el servidor Web, resultando en un mensaje de error de Movimiento de Objetos 3XX que contiene la dirección IP interna o el nombre de red interna del servidor Web.

Un host de destino que utiliza HTTP también puede ser vulnerable a este problema.

Impacto.

La explotación exitosa de esta vulnerabilidad resulta en la divulgación de su dirección IP interna o nombre de red interna, que podría utilizarse en ataques adicionales contra el host de destino.

Solución.

No hay parches disponibles en este momento.

Opciones:

Para IIS Web Server 6.x y anterior:

Consulte el artículo de Microsoft sobre cómo establecer el nombre de host en lugar de la dirección IP interna de IIS (https://support.microsoft.com/en-us/kb/218180).

Para IIS 7.0

La versión de lanzamiento de IIS7 por defecto incluye la funcionalidad de enmascarar la dirección IP. Consulte Eliminación de la dirección IP de un servidor IIS de las respuestas HTTP (http://blogs.msdn.com/b/webtopics/archive/2008/11/18/removing-an-iis-server-s-ip-address-from-http-responses.aspx).

Para el servidor web de Apache:

Modifique el archivo de configuración de Apache de la siguiente manera:

- Establezca "ServerName" en un FQDN adecuado.

- Utilice el módulo mod_rewrite para modificar el mensaje de error 3xx devuelto por el servidor.

No hay información de solución disponible para otros servidores Web en este momento.

- **Web Directories Listable Vulnerability.**

Detalle:

Amenaza.

El servidor Web tiene algunos directorios listables. Se puede obtener información muy sensible de los listados de directorios.

Impacto.

Un usuario remoto puede explotar esta vulnerabilidad para obtener información muy sensible sobre el host. La información obtenida puede ayudar en nuevos ataques contra el huésped.

Solución.

Desactive la exploración de directorios o la lista de todos los directorios.

- **Microsoft ASP.NET ValidateRequest Filters Bypass Cross-Site Scripting Vulnerability.**

  Detalle:

  Amenaza.

  ASP.NET es un framework de aplicaciones Web desarrollado por Microsoft. ValidateRequest filters, es una característica de ASP.NET que evita que el servidor acepte contenido que contenga HTML no codificado. Esta función está diseñada para ayudar a prevenir algunos ataques de inyección de secuencias de comandos en los que el código de script del cliente o el HTML pueden enviarse sin saberlo a un servidor, almacenarse y luego presentarse a otros usuarios.

  Los filtros de validateRequest de Microsoft ASP.NET podrían permitir a un atacante remoto evitar sus filtros y realizar ataques de secuencias de comandos entre sitios utilizando una secuencia de caracteres tales como (</) y (<~ /). Estas vulnerabilidades se describen en CVE-2008-3842 y CVE-2008-3843.

  Este QID no busca activamente el XSS en la aplicación web, sino que se basa en la versión de banner ASP.NET.

  Para confirmar la vulnerabilidad, ejecute una exploración de aplicaciones web.

Versiones afectadas:

Microsoft ASP.NET CLR versión 1.1.4322.2407 y 2.0.50727 que se utiliza en ASP.NET versión 1.0 a 3.5.

Para obtener una descripción detallada de las versiones de CLR y la versión ASP.NET, consulte .NET framework (http://msdn.microsoft.com/en-us/library/w4atty68.aspx)

Impacto.

Los atacantes pueden lanzar ataques XSS contra aplicaciones vulnerables que dependen únicamente de los filtros ASP.NET ValidateRequest. Este tipo de ataque puede resultar en la degradación del sitio de destino o en el reenvío de información confidencial (por ejemplo: ID de sesión o contraseñas) a terceros no autorizados.

Solución.

El problema descrito en CVE-2008-3842 se corrige mediante la actualización MS07-040. No hay parches disponibles para CVE-2008-3843. La vulnerabilidad se puede mitigar al no confiar en los filtros ValidateRequest entregados con ASP.NET, utilizando filtros de entrada personalizados y prácticas de codificación segura.

Por favor, actualice el último marco NET Framework .NET (http://msdn.microsoft.com/en-us/subscriptions/downloads/

5.3.3. RED INTERNA LAN

- **SSL/TLS Server Factoring RSA Export Keys (FREAK) vulnerability.**

  Detalle:

  Amenaza.

  El servidor SSL/TLS remoto es vulnerable al ataque FREAK cuando:

  1. Las cifras "RSA + EXPORT" son compatibles.

  2. El tamaño de la clave pública RSA en el certificado no es superior a 1024.

  3. El tamaño temporal de la clave RSA es inferior a 1024.

  4.La clave temporal de RSA es estable (usada varias veces).

  Sólo SSLv3 y TLSv1 son potencialmente vulnerables

  Impacto.

  La explotación permite a un atacante evitar las restricciones de seguridad en el host de destino.

  Solución.

  Deshabilite los conjuntos de cifrado RSA_EXPORT.

  No utilice la clave RSA temporal varias veces

- **SSL Server Has SSLv2 Enabled Vulnerability.**

Detalle:

Amenaza.

El protocolo Secure Socket Layer (SSL) permite una comunicación segura entre un cliente y un servidor.

Hay defectos conocidos en el protocolo SSLv2. Un ataque de tipo man-in-the-middle puede forzar la comunicación a un nivel menos seguro y luego tratar de romper el cifrado débil. El atacante también puede truncar los mensajes cifrados.

Los servidores SSL que admiten SSLv2 y utilizan las mismas claves privadas también son vulnerables al ataque de DROWN.

Estos defectos se han corregido en SSLv3 (o TLSv1). La mayoría de los servidores (incluidos todos los servidores Web, servidores de correo, etc.) y clientes (incluidos Webclients como IE, Netscape Navigator, Mozilla y clientes de correo) admiten SSLv2 y SSLv3. Sin embargo, SSLv2 está habilitado de forma predeterminada para la compatibilidad con versiones anteriores.

El siguiente enlace proporciona más información sobre esta vulnerabilidad:

Análisis del protocolo SSL 3.0 (http://www.schneier.com/paper-ssl.html)

Ataque de DROWN (https://drownattack.com/)

Impacto.

Un atacante puede aprovechar esta vulnerabilidad para leer comunicaciones seguras o modificar mensajes maliciosos.

Solución.

Deshabilitar SSLv2.

Normalmente, para Apache /mod_ssl, httpd.conf o ssl.conf deberían tener las siguientes líneas:

SSLProtocol -ALL + SSLv3 + TLSv1

SSLCipherSuite TODOS:! ANULL:! ADH:! ENULL:! LOW:! EXP: RC4 + RSA: + ALTO: + MEDIO

Para Apache /apache_ssl, httpd.conf o ssl.conf debería tener la siguiente línea:

SSLNoV2

Cómo deshabilitar SSLv2 en IIS: Microsoft

Artículo de Knowledge Base - 187498 (https://support.microsoft.com/en-us/kb/187498)

Cómo restringir el uso de ciertos algoritmos y protocolos criptográficos en Schannel.dll:

Artículo de Microsoft Knowledge Base - 245030 (http://support.microsoft.com/kb/245030/es/)

Para IIS 7, consulte el artículo Cómo deshabilitar SSL 2.0 en IIS 7 (http://www.sslshopper.com/article-how-to-disable-ssl-2.0-in-iis-7.html) para obtener más información.

- **SSL/TLS use of weak RC4 cipher.**

Detalles:

Amenaza.

Los protocolos Secure Sockets Layer (SSL v2 / v3) y TLS (Transport Layer Security) proporcionan servicios de integridad, confidencialidad y autenticidad a otros protocolos que carezcan de estas características.

Los protocolos SSL/TLS usan cifras como AES, DES, 3DES y RC4 para cifrar el contenido de los protocolos de capa superior y así proporcionar el servicio de confidencialidad. Normalmente, la salida de un proceso de cifrado es una secuencia de bytes de aspecto aleatorio. Se sabía que la salida RC4 tiene algún sesgo en la salida. Recientemente un grupo de investigadores ha descubierto que hay un sesgo más fuerte en RC4, lo que hace que el análisis estadístico del texto cifrado sea más práctico.

El ataque descrito es inyectar un javascript malicioso en el navegador de la víctima que garantice que hay múltiples conexiones que se establecen con un sitio web de destino y la

misma cookie HTTP se envía varias veces al sitio web en forma cifrada. Esto proporciona al atacante un gran conjunto de muestras de texto cifrado, que se pueden utilizar para el análisis estadístico.

NOTA: El 3/12/15 NVD cambió la complicidad de acceso CVSS v2 de alto a medio. Como resultado, Qualys revisó el puntaje CVSS a 4.3 inmediatamente. El 5/4/15 Qualys también está revisando la gravedad al nivel 3.

Impacto.

Si se realiza este ataque y se recupera una cookie HTTP, el atacante puede utilizar la cookie para suplantar al usuario cuya cookie se recuperó.

Este ataque no es muy práctico ya que requiere que el atacante tenga acceso a millones de muestras de texto cifrado, pero hay ciertos supuestos que un atacante puede hacer para mejorar las posibilidades de recuperar el texto claro de cihpertext. Por ejemplo, las cookies HTTP están codificadas en base64 o en dígitos hexadecimales. Esta información puede ayudar al atacante en sus esfuerzos por recuperar la cookie.

Solución.

RC4 no debe usarse donde sea posible. Una de las razones por las que RC4 todavía estaba siendo utilizada fue BEAST y

Lucky13 ataques contra codificaciones de modo CBC en SSL y TLS. Sin embargo, TLSv 1.2 o posterior trata estos problemas.

- **SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE).**

  Detalles:

  Amenaza.

  El error de diseño del protocolo SSL 3.0, utiliza relleno de CBC no determinista, lo que hace más fácil para los ataques man-in-the-middle.

  El destino admite SSLv3, lo que lo hace vulnerable a POODLE (Padding Oracle On Encryption Legacy Downgraded), aunque también admita versiones más recientes de TLS. Está sujeto a un ataque de downgrade, en el que el atacante engaña al navegador para que se conecte con SSLv3.

  Impacto.

  Un atacante que puede tomar una posición de hombre en el medio (MitM) puede explotar esta vulnerabilidad y tener acceso a la comunicación cifrada entre un

  Cliente y servidor.

Solución.

Deshabilite el soporte SSLv3 para evitar esta vulnerabilidad.

Ejemplos para deshabilitar SSLv3.

Nginx: lista de protocolos permitidos específicos en la línea "ssl_protocols". Asegúrese de que SSLv2 y SSLv3 no aparezcan en la lista. Por ejemplo: ssl_protocols TLSv2 TLSv1.1 TLSv1.2;

Apache: Agregue -SSLv3 a la línea "SSLProtocol".

Cómo deshabilitar SSL 3.0 en Microsoft IIS (https://support.microsoft.com/kb/187498/en-us).

Para PCI, consulte el artículo de la comunidad Qualys (https://community.qualys.com/thread/15280).

- **SSL/TLS Server supports TLSv1.0.**

Detalle:

Amenaza.

TLS es capaz de utilizar una multitud de cifrados (algoritmos) para crear los pares de claves públicas y privadas.

Por ejemplo, TLSv1.0 utiliza el cifrado de flujo RC4 o un cifrado de bloque en modo CBC.

RC4 es conocido por tener sesgos y el cifrado de bloque en modo CBC es vulnerable al ataque de la POODLE.

TLSv1.0, si está configurado para usar los mismos conjuntos de cifrado que SSLv3, incluye un medio por el cual una implementación TLS puede degradar la conexión a SSL v3.0, debilitando así la seguridad.

Este QID será marcado como un fallo para PCI a partir del 1 de noviembre de 2016 de acuerdo con las nuevas normas. Para las implementaciones existentes, los Comerciantes podrán presentar una Solicitud de Falso-Positivo/Excepción de PCI y proporcionar prueba de su Plan de Mitigación de Riesgo y Migración, lo cual resultará en un pase para PCI hasta el 30 de junio de 2018.

Se pueden encontrar más detalles en: NUEVO PCI DSS v3.2 y migración desde SSL y TLS temprano v1.1 (https://community.qualys.com/message/34120)

Impacto.

Un atacante puede explotar fallas criptográficas para realizar ataques de tipo man-in-the-middle o comunicaciones de descifrado.

Por ejemplo: Un atacante podría forzar una degradación del protocolo TLS al antiguo protocolo SSLv3.0 y explotar la vulnerabilidad POODLE, leer comunicaciones seguras o modificar mensajes maliciosos.

Un ataque tipo POODLE (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls)

también podría iniciarse directamente en TLS sin negociar una degradación.

Solución.

Deshabilite el uso del protocolo TLSv1.0 en favor de un protocolo criptográfico más fuerte como TLSv1.2.

- **SSL Server Supports Weak Encryption Vulnerability.**

Detalle:

Amenaza.

El protocolo Secure Socket Layer (SSL) permite una comunicación segura entre un cliente y un servidor.

Los cifrados SSL se clasifican según la longitud de clave de cifrado de la siguiente manera:

HIGH-Longitud de clave de más de 128 bits

MEDIUM-Longitud de clave igual a 128 bits

LOW-Longitud de clave menor a 128 bits

Los mensajes cifrados de tipo LOW son fáciles de descifrar. Los servidores SSL comerciales sólo deben admitir cifras MEDIUM o HIGH para garantizar la seguridad de las transacciones.

El siguiente enlace proporciona más información sobre esta vulnerabilidad:

Análisis del protocolo SSL 3.0 (http://www.schneier.com/paper-ssl-revised.pdf)

Tenga en cuenta que esta detección sólo comprueba el soporte de cifrado débil en la capa SSL. Algunos servidores pueden implementar protección adicional en la capa de datos. Por ejemplo, algunos servidores SSL y proxies SSL (como los aceleradores SSL) permiten completar la negociación de cifrado, pero devuelven un mensaje de error y abortan la comunicación en el canal seguro. Esta vulnerabilidad puede no ser explotable para tales configuraciones.

Impacto.

Un atacante puede aprovechar esta vulnerabilidad para descifrar las comunicaciones seguras sin autorización.

Solución.

Deshabilite la compatibilidad con cifrado de tipo LOW.

Apache

Si TLSv1.1 o TLSv1.2 están disponibles, entonces esos protocolos deben ser utilizados:

SSLProtocol TLSv1.1 TLSv1.2

Si TLSv1.1 y TLSv1.2 no están disponibles, sólo debe utilizarse TLS1.0:

SSLProtocol TLSv1

Normalmente, para Apache /mod_ssl, httpd.conf o ssl.conf deberían tener las siguientes líneas:

SSLCipherSuite
ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDI
UM

Para Apache / apache_ssl, incluya la siguiente línea en el archivo de configuración (httpsd.conf):

SSLRequireCipher
ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDI
UM

Tomcat

sslProtocol = "SSLv3"

ciphers = "SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, SSL_DHE_RSA_W
ITH_3DES_EDE_CBC_SHA"

IIS

Cómo restringir el uso de ciertos algoritmos y protocolos criptográficos en Schannel.dll (http://support.microsoft.com/default.aspx?scid=kb;ENUS;245030) (Requiere reiniciar Windows)

Cómo deshabilitar PCT 1.0, SSL 2.0, SSL 3.0 o TLS 1.0 en IIS (http://support.microsoft.com/default.aspx?scid=kb;enus;187498)

Guía de seguridad para IIS (http://www.microsoft.com/technet/security/prodtech/IIS.mspx)

Para Novell Netware 6.5, consulte el siguiente documento

SSL Permite el uso de cifras débiles. -TID10100633 (http://support.novell.com/cgi-bin/search/searchtid.cgi?10100633.htm)

- **SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST).**

  Detalle:

  Amenaza.

  Los protocolos SSLv 3.0 y TLS v1.0 se utilizan para proporcionar integridad, autenticidad y privacidad a otros protocolos como HTTP y LDAP. Proporcionan estos servicios usando el cifrado para el aislamiento, los certificados x509 para la autenticidad y las funciones hash unidireccionales para la integridad. Para cifrar los datos, SSL y TLS pueden utilizar cifrados de bloque, que son algoritmos de cifrado que sólo pueden cifrar un bloque fijo de datos originales en un bloque cifrado del mismo tamaño. Tenga en cuenta que estas cifras siempre obtendrá el mismo bloque resultante para el mismo bloque original de datos. Para conseguir la diferencia en la salida, la salida del cifrado es XOR con otro bloque del mismo tamaño denominado vectores de inicialización (IV). Un modo especial de operación para los cifrados de bloques

conocidos como CBC (encadenamiento de bloques de cifrado) utiliza una IV para el bloque inicial y el resultado del bloque anterior para cada bloque subsiguiente para obtener la diferencia en la salida del cifrado de bloques.

En la implementación de SSLv3.0 y TLSv1.0 el uso de modo de CBC de elección era pobre porque todo el tráfico comparte una sesión de CBC con un solo conjunto de IV iniciales. El resto de la IV es como se mencionó anteriormente los resultados de la encriptación de los bloques anteriores. Los IV subsiguientes están disponibles para los espías. Esto permite que un atacante con la capacidad de inyectar tráfico arbitrario en el flujo de texto sin formato (para ser cifrado por el cliente) para verificar su conjetura del texto normal que precede al bloque inyectado. Si los atacantes suponen que es correcto, la salida del cifrado será la misma para dos bloques.

Para datos de entropía baja es posible adivinar el bloque de texto sin formato con relativamente pocos intentos. Por ejemplo, para datos que tienen 1000 posibilidades el número de intentos puede ser 500.

Para obtener más información, consulte un artículo de Gregory V. Bard. (Http://eprint.iacr.org/2006/136.pdf)

NOTA:

La complejidad de acceso CVSS asignada por NIST a la CVE-2011-3389 es 'Medium', lo que la hace de puntuación base 4.3.

Pero Qualys ha asignado la complejidad de acceso a 'High' para el lado del servidor, porque Javascipt inyección y capacidades MiTM y un cliente vulnerable son necesarios para explotar esta vulnerabilidad.

Por lo tanto, la calificación CVS de Qualys es 2.6.

Impacto.

Recientemente se han descrito ataques contra las cookies de autenticación web que utilizaron esta vulnerabilidad. Si el atacante entiende la cookie de autenticación, el atacante puede suplantar al usuario legítimo en el sitio Web que acepta la cookie de autenticación.

Solución.

Este ataque fue identificado en 2004 y posterior a esto se realizaron revisiones del protocolo TLS que contienen una corrección para esto. Si es posible, actualice a TLSv1.1 o TLSv1.2. Si no es posible actualizar a TLSv1.1 o TLSv1.2, deshabilitar cifras de modo CBC eliminará la vulnerabilidad.

Configurar su servidor SSL para dar prioridad a las cifras RC4 mitiga esta vulnerabilidad. Microsoft ha publicado información incluida las soluciones provisionales para IIS en:

KB2588513 (http://technet.microsoft.com/en-us/security/advisory/2588513).

El uso de la siguiente configuración de SSL en Apache mitiga esta vulnerabilidad:

SSLHonorCipherOrder On

SSLCipherSuite RC4-SHA:HIGH:!ADH

Las mejores prácticas de implementación de SSL / TLS de Qualys se pueden encontrar aquí (https://www.ssllabs.com/projects/best-practices/).

Nota: La recomendación de RC4 sólo se aplica a situaciones en las que no es posible actualizar a TLSv1.2.

RC4 en TLS v1.0 tiene un problema de sesgo de salida como se describe en QID 38601. por lo tanto se recomienda actualizar a TLS v1.2 o posterior.

- **Listing of Scripts in the scripts Directory.**

Detalle:

Amenaza.

Se permite el listado de archivos en el directorio de scripts.

Impacto.

Al explorar el directorio de scripts, los usuarios no autorizados pueden obtener una lista de los scripts CGI presentes en su

servidor. Con esta información pueden implementar ataques adicionales en secuencias de comandos CGI vulnerables.

Solución.

Establezca una regla más restrictiva en su servidor para evitar la lista de directorios del directorio de secuencias de comandos.

- **TCP Test-Services.**

Detalles:

Amenaza.

Este sistema está ejecutando servicios TCP, que generalmente se usan sólo para propósitos de pruebas de red (7 echo, 9 discard, 13 daytime, 17 quote of the day, 19 chargen, 37 time). Recomendamos que no se revele información (incluso el tiempo actual del servidor). Además, le aconsejamos que no ejecute servicios superfluos.

Impacto.

Al explotar esta vulnerabilidad, los usuarios no autorizados pueden recopilar información sobre el servidor.

Solución.

Deshabilite todos los servicios TCP no necesarios en el servidor.

- **SSL Certificate - Signature Verification Failed Vulnerability.**

Detalles:

Amenaza.

Un certificado SSL asocia una entidad (persona, organización, host, etc.) con una clave pública. En una conexión SSL, el cliente autentica el servidor remoto utilizando el certificado del servidor y extrae la clave pública en el certificado para establecer la conexión segura. La autenticación se realiza verificando que la clave pública en el certificado está firmada por una entidad emisora de certificados de terceros de confianza.

Si un cliente no puede verificar el certificado, puede interrumpir la comunicación o pedir al usuario que continúe la comunicación sin autenticación.

Impacto.

Al explotar esta vulnerabilidad, pueden ocurrir ataques de man-in-the-middle en tándem con el envenenamiento de caché DNS.

Excepción:

Si el servidor se comunica sólo con un grupo restringido de clientes que tienen el certificado de servidor o el certificado de CA

de confianza, es posible que el certificado de servidor o de CA no esté disponible públicamente y la exploración no pueda verificar la firma.

Solución.

Instale un certificado de servidor firmado por una entidad emisora de certificados de terceros de confianza.

- **SSL Certificate - Self-Signed Certificate.**

Detalles:

Amenaza.

Un certificado SSL asocia una entidad (persona, organización, host, etc.) con una clave pública. En una conexión SSL, el cliente autentica el servidor remoto utilizando el certificado del servidor y extrae la clave pública en el certificado para establecer la conexión segura.

El cliente puede confiar en que el certificado de servidor pertenece al servidor sólo si está firmado por una entidad emisora de certificados (CA) de tercero de confianza mutua. Los certificados auto-firmados se crean generalmente para propósitos de prueba o para evitar el pago de CA de terceros. Éstos no se deben utilizar en ninguna producción o servidores críticos.

Al explotar esta vulnerabilidad, un atacante puede suplantar al servidor presentando un falso certificado autofirmado. Si el cliente sabe que el servidor no tiene un certificado de confianza, aceptará este certificado falsificado y se comunicará con el servidor remoto.

Impacto.

Al explotar esta vulnerabilidad, un atacante puede lanzar un ataque man-in-the-middle.

SOLUCIÓN:

Instale un certificado de servidor firmado por una entidad emisora de certificados de terceros de confianza.

- **SSL Certificate - Subject Common Name Does Not Match Server FQDN:**

  Detalle:

  Amenaza.

  Un certificado SSL asocia una entidad (persona, organización, host, etc.) con una clave pública. En una conexión SSL, el cliente autentica el servidor remoto utilizando el certificado del servidor y extrae la clave pública en el certificado para establecer la conexión segura.

Un certificado cuyo SubjectName común o subjectAltName no coincide con el FQDN de servidor sólo ofrece cifrado sin autenticación.

Tenga en cuenta que un informe falsamente positivo de esta vulnerabilidad es posible en el siguiente caso:

Si el nombre común del certificado utiliza un comodín como * .somedomainname.com y la resolución DNS inversa de la dirección IP de destino no está configurada. En este caso, no es posible que Qualys asocie el nombre común de comodín a la IP. La adición de una entrada de búsqueda DNS inversa al IP de destino resolverá este problema.

Impacto.

Un atacante en el medio puede explotar esta vulnerabilidad en tándem con un ataque de envenenamiento de caché DNS para atraer al cliente a otro servidor y luego robar toda la comunicación de cifrado.

Solución.

Instale un certificado de servidor cuyo Subject commonName o subjectAltName coincida con el FQDN del servidor.

- **X.509 Certificate MD5 Signature Collision Vulnerability.**

Detalle:

Amenaza.

Los algoritmos de hash se utilizan para generar un valor de hash para un mensaje (un bloque arbitrario de datos) de tal manera que una serie de propiedades criptográficas se mantienen.

En particular, se espera que sea resistente a las colisiones, es decir, dado un mensaje m, es difícil calcular un segundo mensaje m 'tal que ambos tengan el mismo valor de hash.

Los algoritmos de hash se utilizan en muchas aplicaciones criptográficas. En particular, se utilizan para firmar certificados X.509 utilizados para verificar la identidad en una variedad de aplicaciones, incluidas las comunicaciones SSL.

El algoritmo hash MD5 ha visto con el paso del tiempo la mejora gradual de los ataques contra la propiedad de colisión. En particular, en los últimos años ha sido posible crear mensajes de colisión con prefijos y sufijos arbitrarios, especificados por atacantes. Recientes mejoras han extendido estas técnicas de tal manera que es posible crear mensajes de colisión que también son diferentes pero válidos certificados SSL.

Impacto.

Un atacante puede crear un par de certificados X.509 con información diferente que comparten la misma firma. Si uno de

los certificados está firmado, la firma también se puede utilizar para el segundo certificado. Es posible explotar este problema para obtener un certificado firmado para una identidad que el atacante no controla o para obtener un certificado firmado como autoridad de firma intermediaria. En el segundo caso, el atacante podrá firmar certificados arbitrarios adicionales que serán confiados por cualquier parte que confíe en la autoridad legítima original.

Un atacante es más probable que explote este problema para realizar ataques de phishing o para suplantar sitios web legítimos aprovechando los certificados maliciosos. Es probable que otros ataques sean posibles.

Solución:

Si el certificado está firmado usando la función de hash MD5, entonces se debe obtener un nuevo certificado que use un algoritmo de hash de prueba más de colisión como SHA. Si se firma la CA del certificado con MD5, debe utilizarse una CA diferente que no tenga esta vulnerabilidad.

Solución Cisco ASA appliance -

Las instrucciones para cambiar el hash de firma para los certificados auto-firmados de Cisco ASA están disponibles en la página Web de Cisco Security Response MD5

Los hash pueden permitir la falsificación de certificados (http://www.cisco.com/en/US/products/products_security_response09186a0080a5d24a.html).

- **Web Directories Listable Vulnerability.**

  Detalle:

  Amenaza.

  El servidor Web tiene algunos directorios listable. Se puede obtener información muy sensible de los listados de directorios.

  Impacto.

  Un usuario remoto puede explotar esta vulnerabilidad para obtener información muy sensible sobre el host. La información obtenida puede ayudar en nuevos ataques contra el huésped.

  Solución.

  Desactive la exploración de directorios o la lista de todos los directorios.

- **EOL/Obsolete Software: Microsoft SQL Server 2008 R2 Service Pack 2 Detected.**

Detalle:

Amenaza.

Microsoft SQL Server 2008 es un sistema de gestión de datos que ofrece un conjunto fijo de características, protección de datos y rendimiento para aplicaciones integradas, sitios Web ligeros y aplicaciones y almacenes de datos locales.

El soporte técnico y el soporte del Service Pack para el Service Pack 2 finalizaron el 13 de octubre de 2015.

Impacto.

El sistema está en alto riesgo de ser expuesto a vulnerabilidades de seguridad. Dado que el proveedor ya no proporciona actualizaciones, el software obsoleto es más propenso a vulnerabilidades.

Solución.

Se recomienda a los usuarios que obtengan el Service Pack 3 para SQL Server 2008 R2 a través de SQL Server 2008 R2 SP3 (Https://www.microsoft.com/en-us/download/details.aspx?id=44271).

- **TLS Protocol Session Renegotiation Security Vulnerability.**

Detalle:

Amenaza.

Transport Layer Security (TLS) es un protocolo criptográfico que proporciona seguridad para las comunicaciones a través de redes en la capa de transporte.

TLS protocolo es propenso a una vulnerabilidad de seguridad que permite ataques man-in-the-middle. Tenga en cuenta que este problema no permite a los atacantes descifrar datos cifrados

específicamente, el problema existe en una forma en que las aplicaciones manejan el proceso de renegociación de sesión y pueden permitir que los atacantes inyecten texto sin formato arbitrario en el inicio del flujo del protocolo de aplicación. El ataque ha sido confirmado para trabajar con HTTP como protocolo de aplicación, pero se cree que también es posible con otros protocolos que están en capas en TLS.

Impacto.

En el caso del protocolo HTTP utilizado con la implementación TLS vulnerable, este ataque se lleva a cabo interceptando las solicitudes de 'Client Hello' y forzando la renegociación de la sesión. Un atacante no autorizado puede hacer que el servidor web procese peticiones arbitrarias que de otra forma requerirían un certificado válido del lado del cliente para su autorización.

Tenga en cuenta que el atacante no podrá obtener acceso directo a la respuesta del servidor.

Se ha demostrado una prueba de concepto de ataques donde se extrajeron las credenciales de usuario utilizando esta vulnerabilidad.

Factores atenuantes:

Para explotar esta vulnerabilidad con éxito, se requiere un control completo de la conexión TCP en el medio. El atacante debe aceptar la conexión TCP desde el cliente y establecer una nueva conexión con el servidor.

Solución.

Para Microsoft Windows, consulte MS10-049 (http://technet.microsoft.com/en-us/security/bulletin/MS10-049) para obtener más información.

Inhabilitar la renegociación completamente.

Solución:

OpenSSL ha proporcionado una versión (0.9.8l) que tiene una solución. Consulte el Registro de cambios OpenSSL (Cambios entre las secciones 0.9.8k y 0.9.8l) (http://www.openssl.org/news/changelog.html) para obtener detalles adicionales.

Microsoft ha proporcionado la solución siguiente:

- Habilitar SSLAlwaysNegoClientCert en IIS 6 o superior: Los servidores web que ejecutan IIS 6 y posteriores que se ven afectados porque requieren autenticación mutua al solicitar un certificado de cliente, pueden endurecerse al activar la configuración SSLAlwaysNegoClientCert. Esto hará que IIS solicite al cliente un certificado en la conexión inicial y no requiere una renegociación iniciada por el servidor.

Impacto de la solución provisional: la configuración de este indicador requerirá que el cliente se autentique antes de cargar cualquier elemento del sitio web protegido por SSL. Esto hará que el navegador siempre solicite al usuario un certificado de cliente al conectarse al sitio Web protegido por SSL.

Consulte el Asesoramiento de seguridad de Microsoft 977377 (http://www.microsoft.com/technet/security/advisory/977377.mspx) para obtener más detalles sobre cómo aplicar las soluciones. Información adicional también está disponible en KB977377 (http://support.microsoft.com/kb/977377).

Parche:

A continuación encontrará enlaces para descargar parches para solucionar las vulnerabilidades:

Renegociación de sesión de TLS: Windows (http://technet.microsoft.com/en-us/security/bulletin/MS10-049)

- **Microsoft SQL Server Remote Code Execution Vulnerability (MS15-058).**

  Detalles:

  Amenaza.

  Existe una vulnerabilidad de elevación de privilegios en Microsoft SQL Server cuando imprime incorrectamente punteros a una clase incorrecta. Un atacante podría explotar la vulnerabilidad si sus credenciales permiten el acceso a una base de datos de SQL Server afectada (CVE-2015-1761).

  Existe una vulnerabilidad de ejecución remota de código en Microsoft SQL Server cuando maneja incorrectamente las llamadas de función internas a la memoria no inicializada (CVE-2015-1762).

  Existe una vulnerabilidad de ejecución remota de código autenticada en Microsoft SQL Server cuando incorrectamente trata las llamadas de función internas a la memoria no inicializada (CVE-2015-1763).

  Esta actualización de seguridad está clasificada como Importante para las ediciones compatibles de Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012 y Microsoft SQL Server 2014.

Impacto.

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante ejecutar código arbitrario.

SOLUCIÓN:

Consulte el Boletín de seguridad de Microsoft MS15-058 (https://technet.microsoft.com/library/security/ms15-058) para obtener más información.

Parche:

A continuación encontrará enlaces para descargar parches para solucionar las vulnerabilidades:

MS15-058: Microsoft SQL Server 2008 para sistemas de 32 bits Service Pack 3 (https://www.microsoft.com/downloads/details.aspx?Familyid=0f30cfef-9fc0-4701-ab54-16fe4a3f449e)

MS15-058: Microsoft SQL Server 2008 para sistemas x64 Service Pack 3 (https://www.microsoft.com/downloads/details.aspx?Familyid=0f30cfef-9fc0-4701-ab54-16fe4a3f449e)

MS15-058: Microsoft SQL Server 2008 para sistemas basados en Itanium Service Pack 3 (https://www.microsoft.com/downloads/details.aspx?Familyid=0f30cfef-9fc0-4701-ab54-16fe4a3f449e)

MS15-058: Microsoft SQL Server 2008 para sistemas de 32 bits Service Pack 4 (https://www.microsoft.com/downloads/details.aspx?

Familyid=40328565-3067-4e36 - 96ba - 26ade333d715)

MS15-058: Microsoft SQL Server 2008 para sistemas de x 64 Service Pack 4 (https://www.microsoft.com/downloads/details.aspx? Familyid=40328565-3067-4e36 - 96ba - 26ade333d715)

MS15-058: Microsoft SQL Server 2008 R2 para sistemas de 32 bits Service Pack 2 (https://www.microsoft.com/downloads/details.aspx?familyid= B9e90a50 - 2258 - 45ad - aad6 - 1403987a84e4)

MS15-058: Microsoft SQL Server 2008 R2 para sistemas x64 Service Pack 2 (https://www.microsoft.com/downloads/details.aspx?familyid= B9e90a50 - 2258 - 45ad - aad6 - 1403987a84e4)

MS15-058: Microsoft SQL Server 2008 R2 para sistemas basados en Itanium Service Pack 2 (https://www.microsoft.com/downloads/details.aspx?familyid= B9e90a50 - 2258 - 45ad - aad6 - 1403987a84e4)

MS15-058: Microsoft SQL Server 2008 R2 para sistemas de 32 bits Service Pack 3 (https://www.microsoft.com/downloads/details.aspx? Familyid=7af16cb8 - c944 - 41cb - a897 - c6fc373869cd)

MS15-058: Microsoft SQL Server 2008 R2 para sistemas basados en x64 Service Pack 3 (https://www.microsoft.com/downloads/details.aspx?

Familyid=7af16cb8 - c944 - 41cb - a897 - c6fc373869cd)

MS15-058: Microsoft SQL Server 2012 para sistemas de 32 bits Service Pack 1 (https://www.microsoft.com/downloads/details.aspx?Familyid=469ce2b3-1065 - 46d6 - aaeb - 1a3c5ba5525a)

MS15-058: Microsoft SQL Server 2012 para sistemas x64 Service Pack 1 (https://www.microsoft.com/downloads/details.aspx?Familyid=469ce2b3-1065 - 46d6 - aaeb - 1a3c5ba5525a)

MS15-058: Microsoft SQL Server 2012 para sistemas de 32 bits Service Pack 2 (https://www.microsoft.com/downloads/details.aspx?familyid=71770059-A4d6-499c-b4c7-53dbaee3de62)

MS15-058: Microsoft SQL Server 2012 para sistemas x 64 Service Pack 2 (https://www.microsoft.com/downloads/details.aspx?Familyid = 71770059-a4d6-499c-b4c7-53dbaee3de62)

MS15-058: Microsoft SQL Server 2014 para sistemas de 32 bits (https://www.microsoft.com/downloads/details.aspx?familyid=f269a099-66eb-4ee1-a1eef792dd410b72)

MS15-058: Microsoft SQL Server 2014 para sistemas basados en x64 (https://www.microsoft.com/downloads/details.aspx?familyid=f269a099-66eb-4ee1-

A1ee-f792dd410b72)

- **Microsoft SQL Server 2008 R2 Service Pack 3 Not Installed.**

Detalles:

Amenaza.

Microsoft SQL Server es un sistema de gestión de bases de datos relacional desarrollado por Microsoft.

Qualys ha detectado que no se ha instalado el Service Pack 2 de Microsoft SQL Server 2008 R2 en el sistema operativo.

La versión de RTM de SQL Server 2008 R2 (versión para fabricación) es 10.50.1600.1

La versión de SQL Server 2008 R2 SP2 es 2009.100.4000

La versión de SQL Server 2008 R2 SP3 es 2009.100.6000

Impacto.

SQL Server 2008 R2 Service Pack 3 corrige muchos problemas que afectan la confidencialidad, integridad y disponibilidad de la base de datos.

Solución.

Se recomienda a los administradores que instalen Microsoft SQL Server 2008 R2 Service Pack 3 que se puede obtener de este

enlace (https://www.microsoft.com/enin/downloads/details.aspx?Id=44271).

Parche:

A continuación encontrará enlaces para descargar parches para solucionar las vulnerabilidades:

Microsoft SQL Server 2008 R2 SP3: Windows (https://www.microsoft.com/en-in/download/details.aspx?id=44271)

- **SMB Signing Disabled or SMB Signing Not Required.**

Detalles:

Amenaza.

Este host no parece estar utilizando firma SMB (Server Message Block). La firma SMB es un mecanismo de seguridad en el protocolo SMB y también se conoce como firmas de seguridad. La firma SMB está diseñada para ayudar a mejorar la seguridad del protocolo SMB.

La firma SMB agrega seguridad a una red utilizando NetBIOS, evitando ataques de man-in-the-middle.

Cuando se habilita la firma SMB tanto en el cliente como en el servidor, las sesiones SMB se autentican entre las máquinas en un paquete por paquete.

Impacto.

Los usuarios no autorizados que escanean la red pueden atrapar muchos intercambios de challenge/response y reproducir todo para tomar claves de sesión particulares y luego autenticarse en el controlador de dominio.

Solución.

Sin la firma de SMB, un dispositivo podría interceptar paquetes de red SMB de un equipo de origen, alterar su contenido y transmitirlos al equipo de destino. Dado que, la firma digital de los paquetes permite al destinatario de los paquetes para confirmar su punto de origen y su autenticidad, se recomienda que la firma SMB esté habilitada y requerida.

Consulte el artículo 887429 de Microsoft (http://support.microsoft.com/kb/887429) para obtener información sobre cómo habilitar la firma SMB.

Para Windows Server 2008 R2, Windows Server 2012, consulte el artículo de Microsoft Requerir firmas de seguridad SMB (http://technet.microsoft.com/en-us/library/cc731957.aspx) para obtener información sobre cómo habilitar la firma SMB.

- **Microsoft SQL Server Elevation of Privilege and Denial of Service Vulnerability (MS14-044).**

  Detalles:

  Amenaza.:

  Esta actualización de seguridad resuelve dos vulnerabilidades reportadas de forma privada en Microsoft SQL Server, una en los Servicios de datos maestros de SQL Server y la otra en el sistema de administración de bases de datos relacionales de SQL Server.

  Existe una vulnerabilidad XSS en los Servicios de datos maestros de SQL (MDS) que podría permitir a un atacante inyectar una secuencia de comandos del cliente en la instancia del usuario de Internet Explorer. El guión podría falsificar contenido, revelar información o tomar cualquier acción que el usuario pudiera tomar en el sitio en nombre del usuario (CVE-2014-1820).

  Existe una vulnerabilidad de denegación de servicio en SQL Server. Un atacante que explote esta vulnerabilidad con éxito podría hacer que el servidor dejara de responder hasta que se inicie un reinicio manual.

Esta actualización de seguridad está clasificada como Importante para las ediciones compatibles de Microsoft SQL Server 2008 Service Pack 3, Microsoft SQL Server 2008 R2 Service Pack 2 y Microsoft SQL Server 2012 Service Pack 1; También se considera importante para Microsoft SQL Server 2014 para sistemas basados en x64.

Impacto.

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto obtener privilegios escalonados o provocar la denegación de servicio.

Solución.

Consulte MS14-044 (https://technet.microsoft.com/en-us/security/bulletin/MS14-044).

Parche:

A continuación encontrará enlaces para descargar parches para solucionar las vulnerabilidades:

MS14-044: Microsoft SQL Server 2008 for 32-bit Systems Service Pack 3 (http://www.microsoft.com/downloads/details.aspx?familyid=a66b4bc8-e2ec-4283-a38f-060dd483f816)

MS14-044: Microsoft SQL Server 2008 for x64-based Systems Service Pack 3 (http://www.microsoft.com/downloads/details.aspx?familyid= a66b4bc8-e2ec-4283-a38f-060dd483f816)

MS14-044: Microsoft SQL Server 2008 for Itanium-based Systems Service Pack 3 (http://www.microsoft.com/downloads/details.aspx?familyid= a66b4bc8-e2ec-4283-a38f-060dd483f816)

MS14-044: Microsoft SQL Server 2008 R2 for 32-bit Systems Service Pack 2 (http://www.microsoft.com/downloads/details.aspx?familyid=a2b4 9e80- d124-4fc5-9862-412991094edc)

MS14-044: Microsoft SQL Server 2008 R2 for x64-based Systems Service Pack 2 (http://www.microsoft.com/downloads/details.aspx?familyid= a2b49e80-d124-4fc5-9862-412991094edc)

Scan Results page 28

MS14-044: Microsoft SQL Server 2008 R2 for Itanium-based Systems Service Pack 2 (http://www.microsoft.com/downloads/details.aspx?familyid= a2b49e80-d124-4fc5-9862-412991094edc)

MS14-044: Microsoft SQL Server 2012 for 32-bit Systems Service Pack 1 (http://www.microsoft.com/downloads/details.aspx?

familyid=6c318774-3f0f-4775-9a20-e52719aded5f)

MS14-044: Microsoft SQL Server 2012 for x64-based Systems Service Pack 1 (http://www.microsoft.com/downloads/details.aspx?familyid=6c318774-3f0f-4775-9a20-e52719aded5f)

MS14-044: Microsoft SQL Server 2014 for x64-based Systems (http://www.microsoft.com/downloads/details.aspx?familyid=54e8b816-4396-41a8-8c55-cba2322adc11)

- **Microsoft SQL Server Database Link Crawling Command Execution.**

  Detalles:

  Amenaza.

  Microsoft SQL Server está expuesto a una vulnerabilidad de ejecución de comandos remotos.

  Versiones afectadas:

  Microsoft SQL Server 2005, 2008, 2008 R2, 2012 están afectados.

  Impacto.

  Una explotación exitosa podría permitir a los atacantes obtener información confidencial y ejecutar código arbitrario.

Solución.

No hay soluciones disponibles en este momento.

- **Service Stopped Responding.**

Detalles:

Amenaza.

El servicio/demonio que escucha en el puerto mostrado dejó de responder a los intentos de conexión TCP durante la exploración.

Impacto.

El servicio / daemon es vulnerable a un ataque de denegación de servicio.

Solución.

Este QID se puede contabilizar por una serie de razones (por ejemplo, fallo de servicio, utilización de ancho de banda o un dispositivo con comportamiento similar al IPS).

Si el servicio se ha estrellado, comunique el incidente al servicio de atención al cliente o al vendedor de QualysGuard y deje de escanear el puerto de escucha del servicio hasta que se resuelva el problema.

Si el problema está relacionado con el ancho de banda, modifique la configuración de rendimiento de Qualys para reducir el impacto del análisis.

Si no encuentra ningún servicio / demonio escuchando en este puerto, puede ser un puerto dinámico y puede omitir este informe. Esto se registra como un fallo de PCI ya que el servicio dejó de responder. No se lanzaron más controles para ese servicio y, por lo tanto, la evaluación del PCI fue incompleta.

- **Microsoft ASP.NET ValidateRequest Filters Bypass Cross-Site Scripting Vulnerability.**

  Detalle:

  Amenaza.

  ASP.NET es un framework de aplicaciones Web desarrollado por Microsoft. ValidateRequest filters, es una característica de ASP.NET que evita que el servidor acepte contenido que contenga HTML no codificado. Esta función está diseñada para ayudar a prevenir algunos ataques de inyección de secuencias de comandos en los que el código de script del cliente o el HTML pueden enviarse sin saberlo a un servidor, almacenarse y luego presentarse a otros usuarios.

Los filtros de validateRequest de Microsoft ASP.NET podrían permitir a un atacante remoto evitar sus filtros y realizar ataques de secuencias de comandos entre sitios utilizando una secuencia de caracteres (</) (<~ /). Estas vulnerabilidades se describen en CVE-2008-3842 y CVE-2008-3843.

Este QID no busca activamente el XSS en la aplicación web, sino que se basa en la versión de banner ASP.NET. Para confirmar la vulnerabilidad, ejecute una exploración de aplicaciones web.

Versiones afectadas:

Microsoft ASP.NET CLR versión 1.1.4322.2407 y 2.0.50727 que se utiliza en ASP.NET versión 1.0 a 3.5 se ve afectada.

Para obtener una descripción detallada de las versiones de CLR y la versión ASP.NET, consulte .NET framework (http://msdn.microsoft.com/en-us/library/w4atty68.aspx)

Impacto.

Los atacantes pueden lanzar ataques XSS contra aplicaciones vulnerables que dependen únicamente de los filtros ASP.NET ValidateRequest. Este tipo de ataque puede resultar en la degradación del sitio de destino o en el reenvío de información confidencial (por ejemplo: ID de sesión o contraseñas) a terceros no autorizados.

Solución.

El problema descrito en CVE-2008-3842 se corrige mediante la actualización MS07-040. No hay parches disponibles para CVE-2008-3843. La vulnerabilidad se puede mitigar al no confiar en los filtros ValidateRequest entregados con ASP.NET, utilizando filtros de entrada personalizados y prácticas de codificación segura.

Por favor, actualice el último .Net framework (http://msdn.microsoft.com/en-us/subscriptions/downloads/)

- **UDP Test-Services.**

Detalles:

Amenaza.

Este sistema está ejecutando servicios UDP, que generalmente se usan sólo para pruebas de redes (7 echo, 9 discard, 13 daytime, 17 quote of the day, 19 chargen, 37 time). Recomendamos que no se revele información (ni siquiera la hora actual del servidor).

Además, en sistemas operativos antiguos, Echo y chargen, u otras combinaciones de servicios UDP, se pueden utilizar en tándem para inundar el servidor. Esto se puede lograr con ataques como bombas UDP o tormentas de paquetes UDP.

IMPACTO:

Al explotar esta vulnerabilidad, los usuarios no autorizados pueden recopilar información sobre el servidor o provocar una denegación de servicio, dependiendo de la pila TCP/IP que se esté ejecutando.

SOLUCIÓN:

Deshabilite todos los servicios UDP que no se requieren en el servidor.

- **Deprecated Public Key Length.**

Detalles:

Amenaza.

NIST tiene una publicación especial SP800-131A (http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf) en la que tiene varias recomendaciones con respecto al algoritmo criptográfico y el uso de la longitud de clave. La recomendación para la longitud de clave es:

- longitudes de clave inferiores a 1024 bits

Son rechazados, lo que significa que se consideran débiles y no deben utilizarse.

- las longitudes de clave entre 1024 bits y 2047 bits están obsoletas.

- las longitudes de llave 2048 y más están aprobadas y son seguras de usar.

Impacto.

Una clave debe ser lo suficientemente grande como para que un ataque de fuerza bruta sea imposible, es decir, tomaría demasiado tiempo para ejecutarse.

Solución.

Obtenga un certificado de longitud de clave pública de 2048 o más de su Autoridad de certificación.

5.4 IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD PARA DISMINUIR LAS VULNERABILIDADES.

Una vez obtenido el informe de las vulnerabilidades presentadas en el escaneo de seguridad del servidor de página web de la institución, se procedió a ejecutar el esquema de seguridad el cual consiste en una serie de procedimientos implementados y alineados a resolver en conjunto, las brechas de seguridad descubiertas en el informe anterior.

5.4.1. AUDITORIA DE APLICACIÓN WEB

- **Path Disclosure:**

  Ubicándonos en el aplicativo IIS del servidor, accedemos a las propiedades del sitio principal y damos doble click en la opción "Examen de directorio".

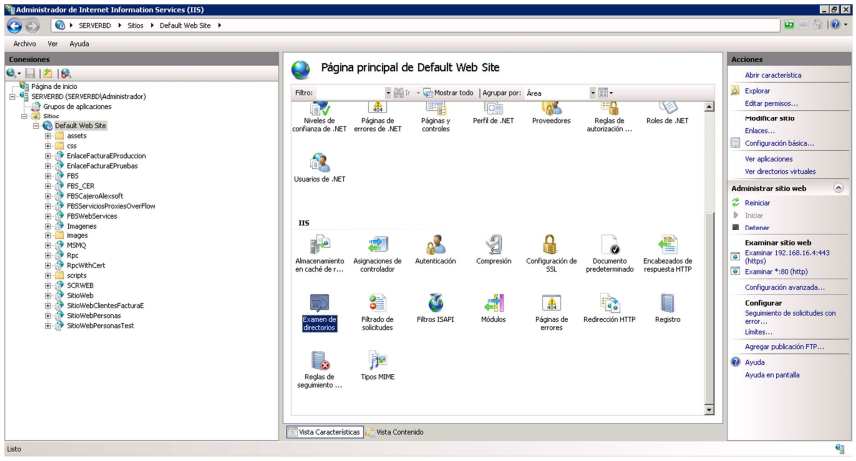

FIGURA 5.18 Solución del listado de directorios 1.

Una vez dentro, deshabilitamos la opción en el menú “Acciones” en la parte derecha.

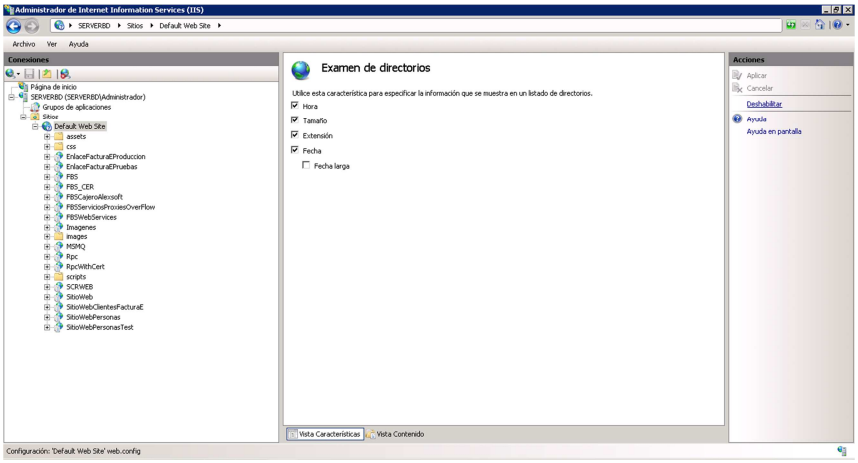

FIGURA 5.19 Solución del listado de directorios 2.

- **Session Cookie Does Not Contain the "Secure" Attribute:**

  Se procedió a agregar el atributo (<httpCookies requireSSL="true" />) en el archivo “Web.config” del dominio y subdominio, también se modificó la configuración de las cookies en IIS poniendo en modo “Usar URI” según se muestra en la imagen a continuación.

  Antes

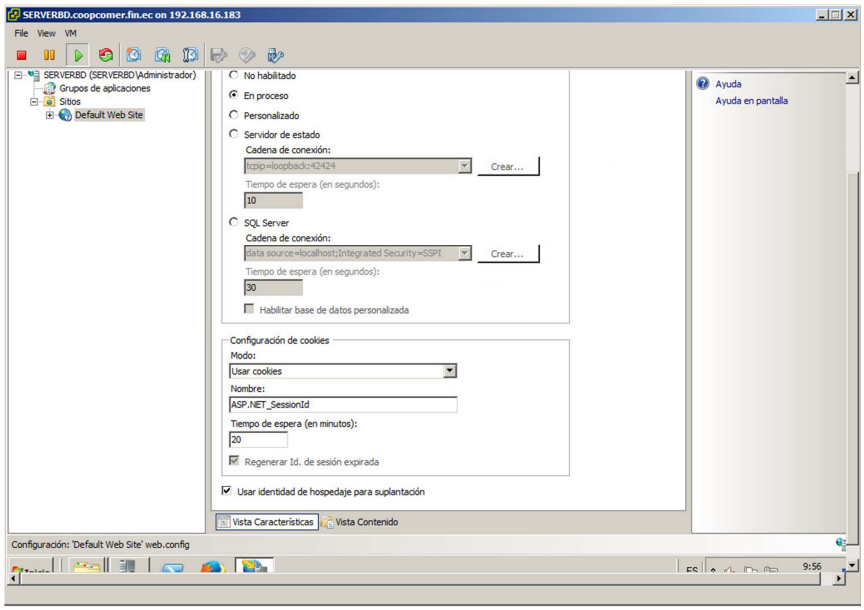

FIGURA 5.20 Solución Session Cookie 1.

Después

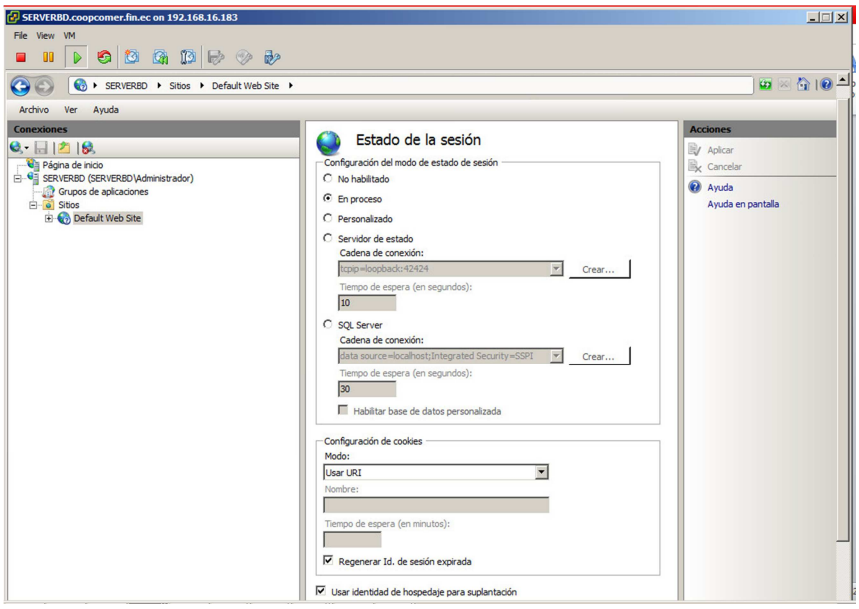

FIGURA 5.21 Solución Session Cookie 2.

Adicional se verificó que el sitio solo se puede visualizar mediante “https” controlando que la información sea enviando de manera cifrada.

Según se muestre en un nuevo escaneo, verificamos si se solucionó la alarma.

- **Active Mixed Content Vulnerability:**

Se hizo una revisión completa la codificación del sitio para que solo acepte contenido de tipo “https” y así evitar el contenido mixto.

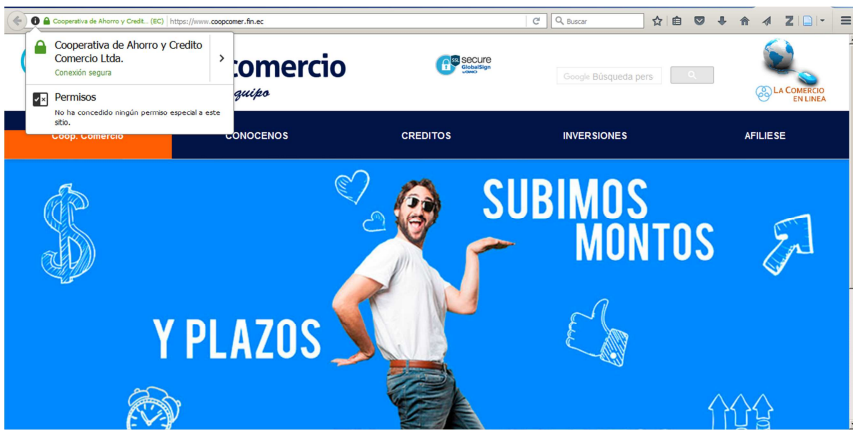

FIGURA 5.22 Solución contenido mixto.

Se realizó una prueba en la página principal verificando la solución implementada, como podemos observar efectivamente se solventó el problema del contenido mixto.

Cabe recalcar que dicha solución no se aplicó a todo el sitio ya que algunas de las páginas hacen referencia a links externos donde solo se puede acceder por medio del protocolo “http”, esto se refleja en el nuevo escaneo, verificando que aún sigue apareciendo la alarma en el reporte automático generado por la herramienta Qualys.

- **Clickjacking - Framable Page:**

  Para solventar esta alarma, se agregó el encabezado “X-Frame”.

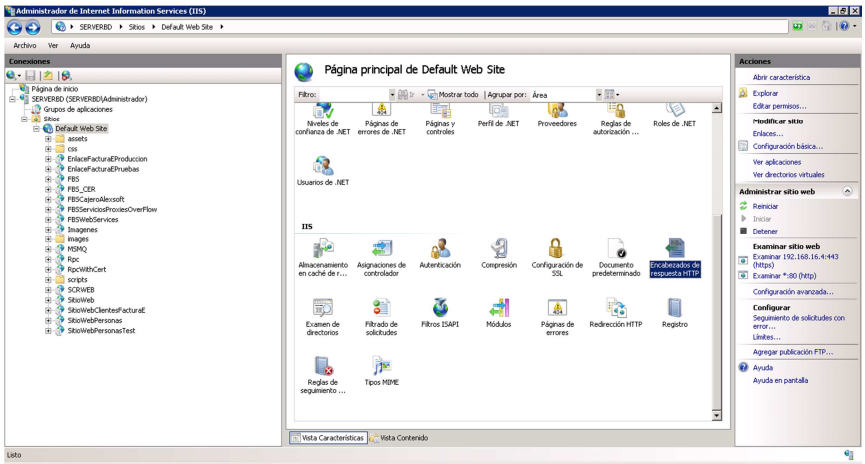

FIGURA 5.23 Agregando encabezado X-Frame 1.

Dentro de la opción “Encabezado de respuesta HTTP” agregamos un nuevo encabezado.

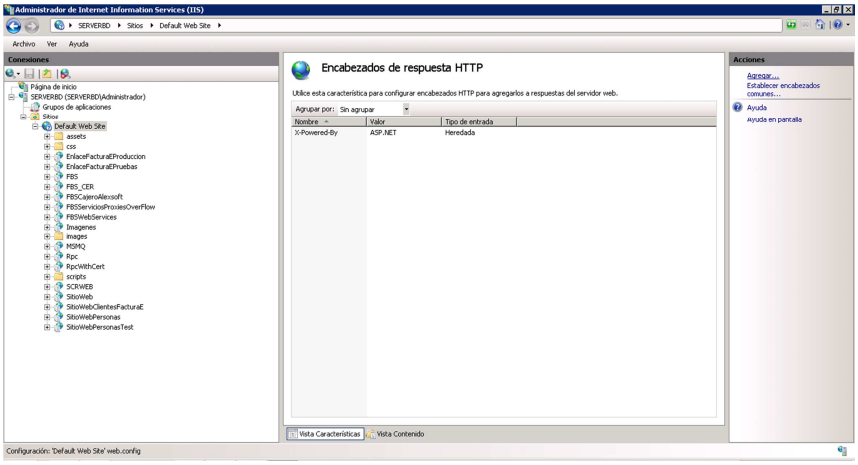

FIGURA 5.24 Agregando encabezado X-Frame 2.

Se especificó como nombre “X-Frame-Options” y como valor “SAMEORIGIN”

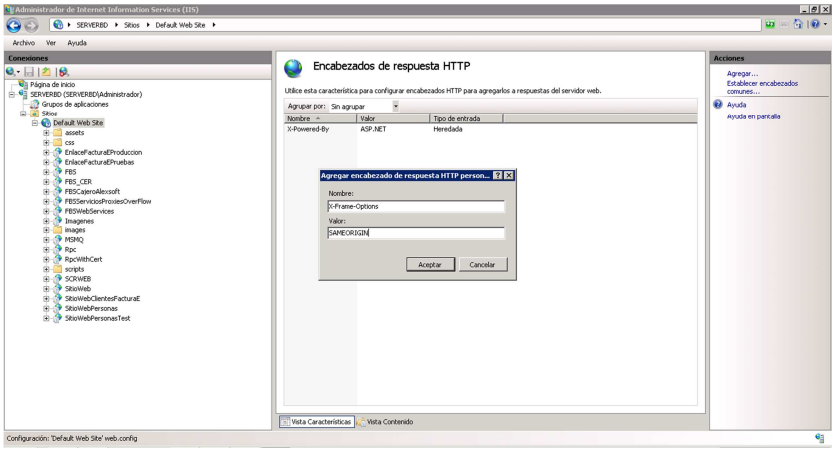

FIGURA 5.25 Agregando encabezado X-Frame 3.

- **Sensitive form field has not disabled autocomplete:**

  Se procedió a agregar el atributo (autocomplete="off") en la codificación de las páginas que presentaron la alarma.

  Según se muestre en un nuevo escaneo, verificamos si se solucionó la alarma.

5.4.2. AUDITORIA DE SISTEMA OPERATIVO

- **Microsoft Windows HTTP.sys Remote Code Execution Vulnerability:**

  Se optó por la solución recomendada en el reporte de análisis, descargamos el parche y lo instalamos.

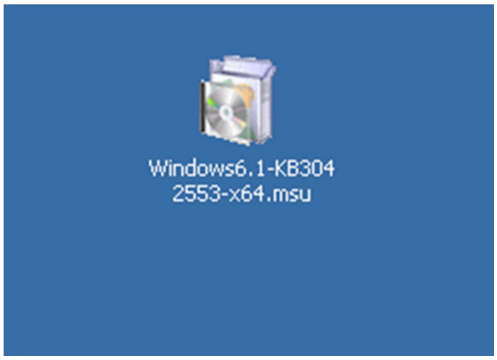

FIGURA 5.26 Instalación de parche 1.

- **SSL/TLS use of weak RC4 cipher:**

  Se optó por la solución recomendada en el reporte de análisis, descargamos el parche con el TLSv 1.2 y lo instalamos.

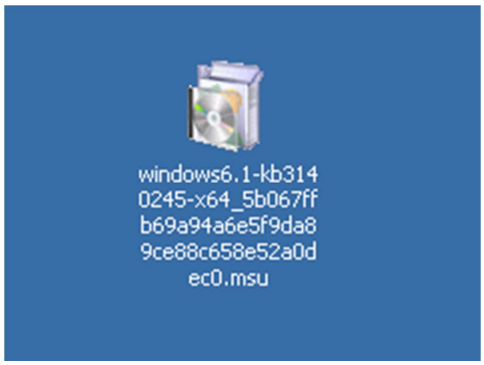

FIGURA 5.27 Instalación de parche 2.

Adicionalmente se modificó el registro para deshabilitar el RC4.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]

"Enabled"=dword:00000000

- **SSLv3 Padding Oracle Attack Information Disclosure Vulnerability:**

  Se procedió a modificar el registro para deshabilitar el SSLv 3.0

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]

  "Enabled"=dword:00000000

- **SSL Server Has SSLv3 Enabled Vulnerability:**

  Solventado por la solución del punto anterior (modificar el registro para deshabilitar el SSLv 3.0)

- **SSL/TLS Server supports TLSv1.0:**

  Se procedió a modificar el registro para deshabilitar TLSv1.0 TLSv1.1, adicional se habilito TLSv1.2.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
"DisabledByDefault"=dword:00000000

- **Listing of Scripts in the scripts Directory:**

  Solventado con la solución implementada en el punto 1 de "Auditoria de Aplicación Web".

- **Web Server Internal IP Address/Internal Network Name Disclosure Vulnerability:**

  Se solucionó ejecutando en la ventana de comandos el comando "(appcmd.exe set config -section:system.webServer/serverRuntime /alternateHostName:"myServer" /commit:apphost)" para modificar la propiedad alternateHostName de IIS y evitar que se publique la ip del servidor en una respuesta http.

- **Web Directories Listable Vulnerability:**

  Solventado con la solución implementada en el punto 1 de "Auditoria de Aplicación Web".

- **Microsoft ASP.NET ValidateRequest Filters Bypass Cross-Site Scripting Vulnerability:**

  En este caso no se procedió a modificar el .Net Framework ya que todas las versiones instaladas son necesarias para el funcionamiento de algunos aplicativos.

5.4.3. RED INTERNA LAN

- **SSL/TLS Server Factoring RSA Export Keys (FREAK) vulnerability:**
  Resuelto en los punto anteriores.
- **SSL Server Has SSLv2 Enabled Vulnerability:**
  Resuelto en los puntos anteriores.
- **SSL/TLS use of weak RC4 cipher:**
  Resuelto en los puntos anteriores.
- **SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE):**
  Resuelto en los puntos anteriores.
- **SSL/TLS Server supports TLSv1.0:**
  Resuelto en los puntos anteriores.
- **SSL Server Supports Weak Encryption Vulnerability:**
  Resuelto en los puntos anteriores.

- **SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST):**
  Resuelto en los puntos anteriores.

- **Listing of Scripts in the scripts Directory:**
  Resuelto en los puntos anteriores.

- **TCP Test-Services:**
  Resuelto en los puntos anteriores.

- **SSL Certificate - Signature Verification Failed Vulnerability:**
  Existe un certificado firmado para la ip y dominio público, pero no existe certificado para la ip y dominio privado.

- **SSL Certificate - Subject Common Name Does Not Match Server FQDN:**
  Existe certificado firmado para la ip y dominio público, pero no existe certificado para la ip y dominio privado.

- **X.509 Certificate MD5 Signature Collision Vulnerability:**
  Resuelto en los puntos anteriores.

- **Web Directories Listable Vulnerability:**
  Resuelto en los puntos anteriores.

- **EOL/Obsolete Software: Microsoft SQL Server 2008 R2 Service Pack 2 Detected:**
  Se sugirió la solución pero no se la pudo implementar por motivos de licencia.

- **TLS Protocol Session Renegotiation Security Vulnerability:**
  Se procedió a implementar la solución recomendada por el reporte, obteniendo como resultado un mensaje de error indicando que no es aplicable al equipo.

- **Microsoft SQL Server Remote Code Execution Vulnerability (MS15-058):**
  Se procedió a implementar la solución recomendada por el reporte, obteniendo como resultado un mensaje de error indicando que no es aplicable al equipo.

- **Microsoft SQL Server 2008 R2 Service Pack 3 Not Installed:**
  Se sugirió la solución pero no se la pudo implementar por motivos de licencia.

- **SMB Signing Disabled or SMB Signing Not Required:**
  Se sugirió la solución pero no fue autorizada su implementación ya que podría causar problemas con las conexiones.

- **Microsoft SQL Server Elevation of Privilege and Denial of Service Vulnerability (MS14-044):**
  Se sugirió la solución pero no se la pudo implementar por motivos de licencia.

- **Microsoft SQL Server Database Link Crawling Command Execution:**
  No hay solución específica.

- **Microsoft ASP.NET ValidateRequest Filters Bypass Cross-Site Scripting Vulnerability:**
  Resuelto en los puntos anteriores.

- **UDP Test-Services:**
  Resuelto en los puntos anteriores.

- **Deprecated Public Key Length:**
  Se omite ya que no existe un certificado para el nombre de host o ip en la red local.

CAPÍTULO 6

PRUEBAS Y ANALISIS DE RESULTADOS.

6.1 PRUEBAS DE HACKING ÉTICO CON EL ESQUEMA DE SEGURIDAD IMPLEMENTADO.

A continuación se presentan los resultados de las pruebas realizadas una vez implementado el esquema de seguridad, debido al extenso análisis, se optó por mostrarlo en anexos los cuales están enumerados de acuerdo al entrono analizado.

6.1.1. PRUEBAS DE APLICACIÓN WEB

- **Eliminación del listado de directorios.**

  En la imagen a continuación se muestra el bloquedo gereado por el sitio web a cualquier tipo de visalización de listado de directorio.

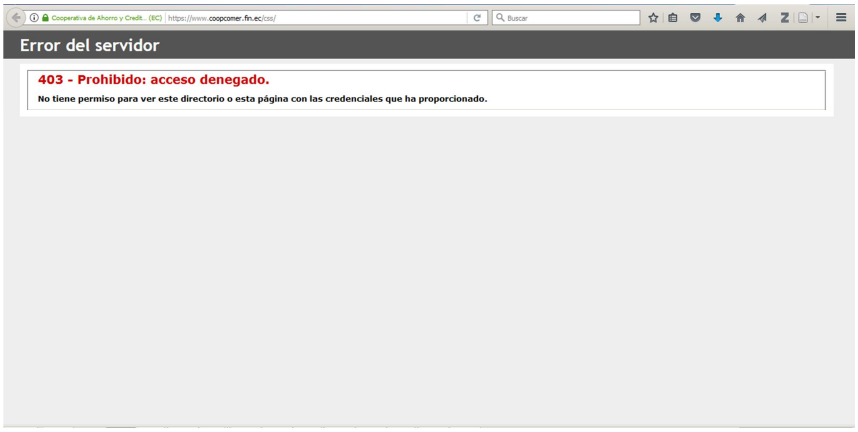

FIGURA 6.1 Prueba de listado de directorio.

- **Sensitive form field has not disabled autocomplete:**

  La solución implementada según lo recomendado por la herramienta Qualys, solo es aplicable a campos de tipo texto, en nuestro caso y según la codificación de la página, el campo es de tipo password de tal manera que no surge efecto alguno y mantiene la propiedad de autocompletado solicitado por el explorador web

  Para verificar el resultado de las soluciones implementadas en las demás vulnerabilidades ver anexo # 005.

6.1.2. PRUEBAS DE SISTEMA OPERATIVO

Para verificar el resultado de las soluciones implementadas en las vulnerabilidades de sistema operativo ver anexo # 006.

6.1.3. PRUEBA DE CERTIFICADO

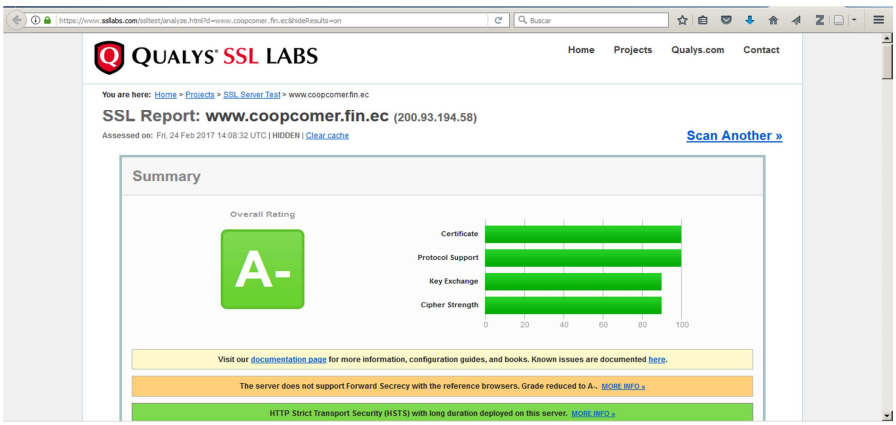

FIGURA 6.2 Certificado de página con calificación A-.

El reporte completo de la prueba se puede visualizar en el anexo # 007.

6.1.4. PRUEBAS DE RED LAN

Para verificar el resultado de las soluciones implementadas en las vulnerabilidades de red LAN ver anexo # 008.

6.2 PRUEBAS DE CONECTIVIDAD SEGURA Y TRANSACCIONALIDAD CON EL CORE FINANCIERO PRINCIPAL.

Para este fin, se verificó el tipo de certificado utilizado por el servidor para establecer la conexión entre la información solicitada, alojada en la base de datos del core financiero principal y el usuario final.

Según muestra la imagen a continuación, el protocolo utilizado en la comunicación cliente-servidor es el “https”.

FIGURA 6.3 Conexión a la página con protocolo https.

Posterior a esto visualizamos que el navegador identifica que dicha página tiene un certificado firmado por una entidad de confianza reconocida.

FIGURA 6.4 Certificado firmado por una entidad de confianza reconocida.

A continuación analizaremos el certificado y sus características.

Cabe recalcar con anticipación que el certificado fue reemplazado por uno nuevo y mejorado e incluso emitido por una entidad certificadora diferente, solventando así la vulnerabilidad referente al protocolo TLS versión 1.0.

Según los detalles técnicos, la clave del certificado es de tipo (TLS_RSA_WITH_AES_128_CBC_SHA, clave de 128 bits, tls 1.2) con una longitud de 128 bits, es decir un nivel medio.

En la pestaña general se visualiza información tal como el tipo de uso del certificado, emitido para y emitido por, periodo de validez y las huellas digitales.

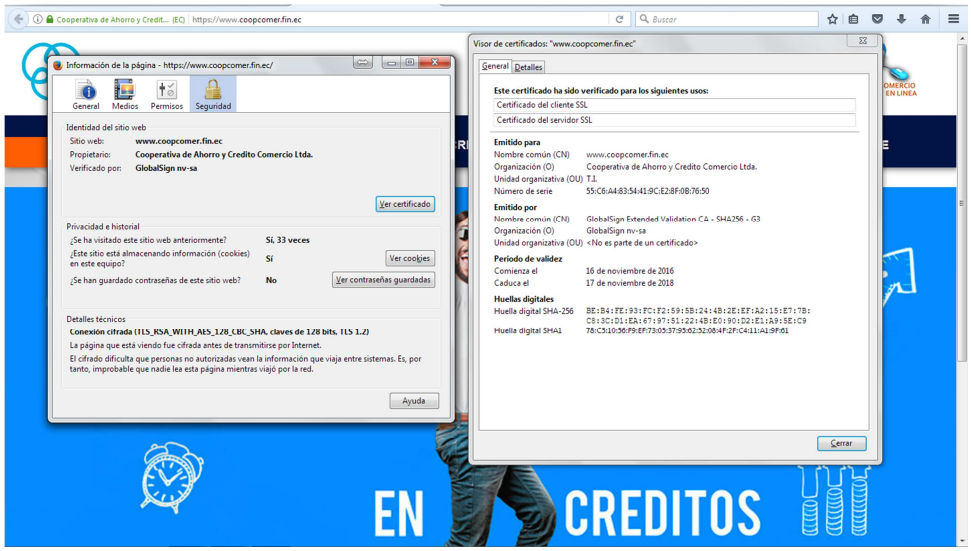

FIGURA 6.5 Análisis del certificado.

En la pestaña detalles encontramos datos referentes a:

- **Versión:**

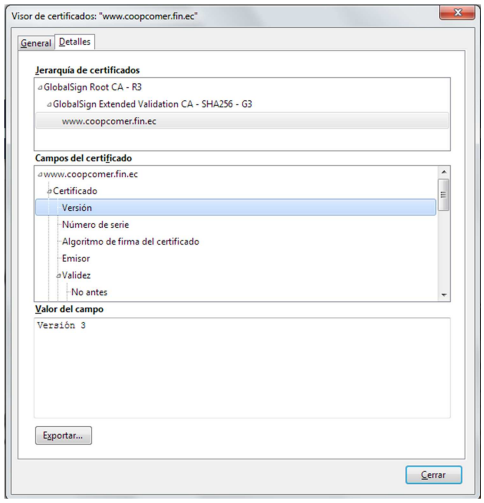

FIGURA 6.6 Detalles del certificado 1.

- **Algoritmo de firma del certificado**

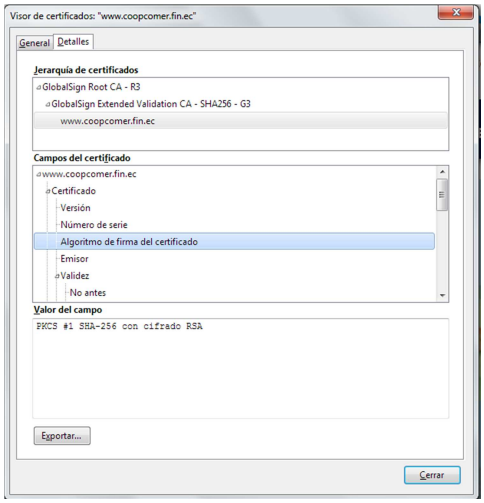

FIGURA 6.7 Detalles del certificado 2.

- **Emisor**

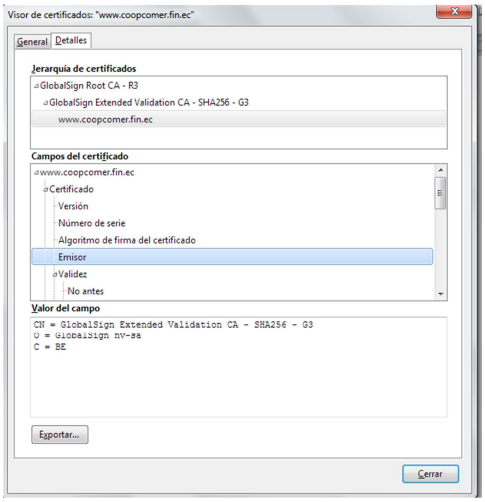

FIGURA 6.8 Detalles del certificado 3.

- **Algoritmo de la clave pública.**

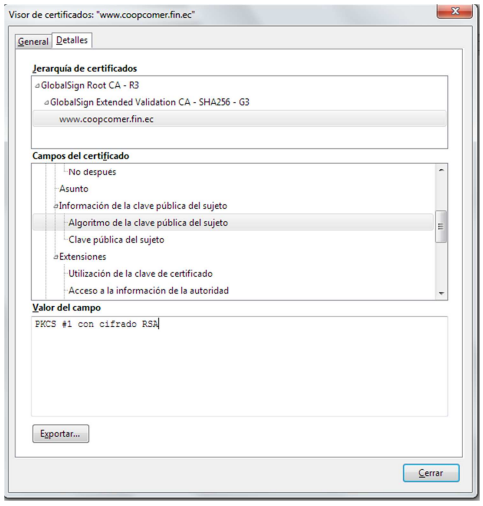

FIGURA 6.9 Detalles del certificado 4.

- **Clave publica**

  La cual es de 2048 bits siendo este de nivel alto.

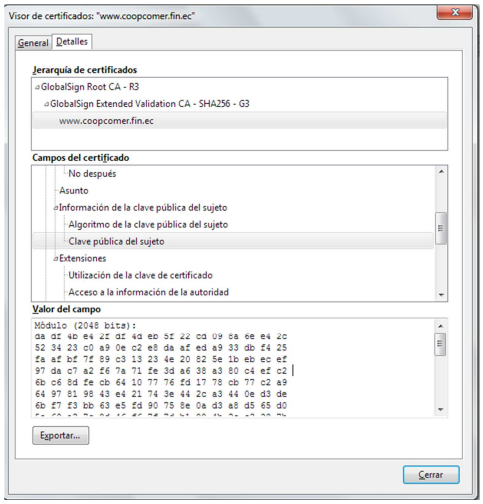

FIGURA 6.10 Detalles del certificado 5.

- **Valor de la firma del certificado.**

  La cual es de 2048 bits siendo este de nivel alto.

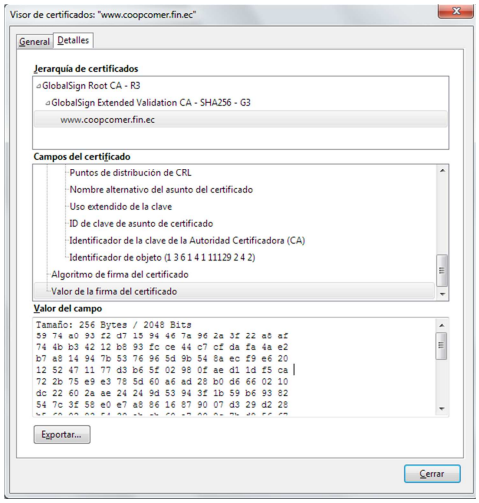

FIGURA 6.11 Detalles del certificado 6.

COCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. El desarrollo de esta tesis logró verificar el grado de vulnerabilidad en el que se encontraba el servidor analizado, siendo de gran importancia para el cumplimiento de los fundamentos básicos de la seguridad de la información, confidencialidad, integridad y disponibilidad.
2. La implementación del esquema solventa en gran medida los vacíos de seguridad existentes, garantizando un entorno adecuado para el tipo de servicios brindado por una institución financiera.
3. El esquema de seguridad se enfoca e implementa en el servidor de banca en línea ya que es quien presta el principal servicio transaccional publicado por internet a los socios de la institución.
4. Si bien el esquema de seguridad fue desarrollado en base a un servidor en específico, es probable la factibilidad de ser replicado en los demás servidores obteniendo los mismos resultados concluyentes para la disminución de vulnerabilidades.

5. Al concluir con este trabajo de tesis se comprobó el cumplimiento de los objetivos planteados los cuales se indican a continuación:
6. Analizar y desarrollar un esquema de seguridad para reducir las vulnerabilidades existentes en el servidor de banca en línea de la Cooperativa de Ahorro y Crédito Comercio Ltda.
7. Recabar la información necesaria para poder analizar las posibles vulnerabilidades existentes en un servidor de banca en línea.
8. Analizar y diseñar esquema de seguridad para la reducción de las vulnerabilidades existentes en un servidor de banca en línea.
9. Realizar las pruebas y comprobación de resultados del esquema de seguridad implementado en el servidor de banca en línea.

RECOMENDACIONES.

1. Implementar una campaña informativa orientada al usuario final con el cual se oriente de las mejores prácticas en cuanto al resguardo de sus credenciales de ingreso a páginas sensibles tales como a las de las instituciones financieras y así mitigar las vulnerabilidades expuestas por ingeniería social.
2. Proponer a la alta gerencia un proyecto de migración de la plataforma actual donde se encuentra el servidor de banca en línea a un entorno virtualizado para mejorar la tolerancia a fallos y robustecer el sistema de contingencia con respaldos diarios íntegros de la máquina virtual.
3. Gestionar la adquisición de las licencias respectivas de todos los aplicativos utilizados para el correcto funcionamiento de los sistemas de la institución.
4. Implementar una política de gestión de actualizaciones de los sistemas operativos, bases de datos y demás herramientas con el objetivo de contar con las últimas versiones incluyendo los parches de seguridad que solventaran el adecuado resguardo de la información que estos contengan.

5. Implementar el esquema de seguridad a los demás servidores y mediantes políticas estandarizar su uso prolongado a cada nuevo agregado.
6. Sugerir a la alta gerencia la creación de un departamento de seguridad de la información, que se dedique exclusivamente a atender los aspectos de seguridad implícitos al tipo de servicio que presta la institución.
7. Bloquear el usuario “Administrador”, siendo de uso exclusivo para la administración del sistema operativo del servidor y crear un usuario adicional con las características necesarias para la administración del servicio prestado.
8. Desinstalar los programas que no estén acorde al servicio prestado por el servidor de banca en línea y que puedan comprometer su seguridad.

BIBLIOGRAFÍA

[1] Junta Bancaria del Ecuador, RESOLUCIÓN JB-2012-2148, http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf, (2012), p. 9.

[2] Junta Bancaria del Ecuador, RESOLUCIÓN JB-2014-3066, http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/2014/resol_JB-2014-3066.pdf, (2014), p. 13.

[3] Junta Bancaria del Ecuador, RESOLUCIÓN JB-2012-2148, http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf, (2012), p. 3.

[4] S. S. M. Antonio, B. F. J. del Consuelo & S. P. L. Alberto, BANCA ELECTRÓNICA, http://www.asba-supervision.org/PEF/pdf/educacion-financiera-asba-medios-de-pago.pdf, fecha de consulta Marzo 2016.

[5] Superintendencia De Bancos y Seguros, LIBRO 1.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO, http://www.wikiriesgo.com/images/b/bd/Riesgo_operativo_ec.pdf , (2005), p. 640.

[6] López, P. A., Seguridad informática. Editex, (2010).

[7] Junta Bancaria del Ecuador, RESOLUCIÓN JB-2012-2148, http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf, (2012), p. 4.

[8] Martínez Pérez, F. M., Criptosistemas de Cifrado en Flujo Basados en Matrices Triangulares con Múltiples Bloques, https://rua.ua.es/dspace/bitstream/10045/54318/1/tesis_francisco_miguel_martinez_perez.pdf, (2016).

[9] Mondo 2000 : a user’s guide to the new edge. Harper Collins, New York,1992. p. 132.