USO DE TECNOLOGÍAS DE PRUEBAS DE PENETRACIÓN PARA VALIDACIÓN DE SEGURIDAD DE APLICACIONES WEB BASADO EN EL TOP 10 DE VULNERABILIDADES DE OWASP

JULIANA ZAPATA GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

SABANETA

2018

USO DE TECNOLOGÍAS DE PRUEBAS DE PENETRACIÓN PARA VALIDACIÓN DE SEGURIDAD DE APLICACIONES WEB BASADO EN EL TOP 10 DE VULNERABILIDADES DE OWASP

JULIANA ZAPATA GARCÍA

Trabajo de Grado de tipo Monografía para optar por el título de Especialista en Seguridad Informática

Director:

SONIA XIMENA MORENO MOLANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

SABANETA

2018

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Ciudad y fecha (día, mes y año)

AGRADECIMIENTOS

Existen muchas personas a las que quisiera mencionar en estos agradecimientos, muchas personas que han aportado de una forma u otra a mi crecimiento personal y profesional, pero mencionarlas a todas haría de los agradecimientos la mayor porción de la monografía. Por ello, he decidido agradecer a las personas que m han acompañado durante el último año, el año en que realicé mi especialización.

A la primera persona que quiero agradecer es a mi esposo Guillermo Andrés Cubillos Rojas, gracias a su paciencia y a sus palabras en los momentos de estrés y de ansiedad entre lo laboral, profesional y familiar, su apoyo ha sido de enorme ayuda en todo este proceso.

También quiero agradecer a mis padres, no sería quién soy hoy en día si no fuera por ellos, por su forma de enfrentar la vida, por sus ganas de progreso y por el esfuerzo que siempre dedicaron en convertirme en una profesional, en enviarme a la universidad en busca de un título de pregrado y de las posibilidades de un futuro mejor.

Finalmente quiero agradecer a los tutores que me acompañaron y guiaron durante todo el proceso de la especialización, al director de grado por sus correcciones y su apoyo constante y la Universidad Nacional Abierta y a Distancia por facilitarme el acceso a la educación en metodología virtual, la cual se adapta perfectamente a mis necesidades de aprendizaje y de estilo de vida.

CONTENIDO

Pág.

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

GLOSARIO

Amenaza: Posibilidad de que una vulnerabilidad de un sistema operativo o aplicación sea explotada.

Aplicación Web: Herramienta o servicio alojado en un servidor al que se puede acceder a través de un navegador web.

Ciberdelincuente: Hacker informático que accede a un sistema sin la debida autorización con el fin de afectar el normal funcionamiento del mismo.

Confidencialidad: La confidencialidad garantiza que la información solo está disponibilidad para quienes tengan autorización sobre la misma.

Disponibilidad: La disponibilidad garantiza que la información siempre estará disponible para quienes requieran acceso.

DoS: Ataque informático cuya finalidad es la denegación de servicios o indisponibilidad de la aplicación o sistema operativo víctima.

Exploit: Software que permite ejecutar una serie de comandos o instrucciones para aprovechar una vulnerabilidad de un sistema operativo o aplicación.

Hacker: Persona con una gran variedad de conocimientos informáticos que le permiten acceder a aplicaciones y sistemas operativos con o sin autorización.

Integridad: La integridad garantiza que la información no ha sido alterada en ningún punto del proceso de comunicación.

Malware: Programa de software o grupo de ordenes que busca afectar o degradar el funcionamiento de una aplicación o sistema operativo.

Pentesting: Prueba de penetración a sistemas informáticos que determina el estado de seguridad de estos.

Phishing: Ataque informático donde se realiza suplantación de una persona, aplicación o entidad de confianza para la víctima con el fin de robar información.

Seguridad de la Información: La seguridad de la información son los procesos que se enfocan en proteger la información de una compañía.

Seguridad Informática: La seguridad informática se enfoca en proteger los equipos de cómputo de una organización.

Sistema Operativo: Conjunto de programas y órdenes que controlan la interfaz y los periféricos de una computadora.

Vulnerabilidad: Error o falla en el sistema operativo o en el código de programación de una aplicación.

RESUMEN

El crecimiento de la tecnología, los servicios ofrecidos en internet y la cantidad de activos tecnológicos de las compañías han llevado a un incremento exponencial de las amenazas informáticas y de los ciberataques a los servicios internos y externos de las compañías.

Por ello, es de vital importancia que los servicios expuestos en internet, que no solo ofrecen transaccionalidad online para la compañía, sino que además son la imagen y el buen nombre de la misma, estén asegurados desde su desarrollo con metodologías claras frente a la creación y el testeo de las aplicaciones antes de su salida a producción y con pruebas periódicas en busca de vulnerabilidades o fallas que puedan representar riesgo para el correcto funcionamiento de las operaciones del negocio.

La seguridad del software debe controlarse desde el nacimiento de la aplicación, es decir, desde la fase de creación del código. La falta de una metodología clara que facilite una guía para el desarrollo y una etapa concisa de pruebas sobre las aplicaciones antes de salir a producción permite que estas aplicaciones presenten fallos y vulnerabilidades que representan altos riesgos para la compañía cuando ya están en producción.

Palabras clave: Prueba de penetración, OWASP, seguridad en servicios Web, vulnerabilidades, aplicaciones web

ABSTRACT

The growth of technology, the services offered on the Internet and the amount of technological assets of companies have led to an exponential increase in cyber threats and cyber-attacks to the internal and external services of companies.

Therefore, it is vitally important that the services displayed on the Internet, which not only offer online trans actionality for the company, but are also the image and the good name of it, are assured from its development with clear methodologies against the creation and the testing of the applications before their production on the internet and with periodic tests in search of vulnerabilities or failures that may represent a risk for the correct operation of the business operations.

The security of the software must be controlled from the very beginning of the application, that is, from the creation phase of the code, the lack of a clear methodology that provides a guide for the development and a concise stage of tests on the applications before leaving a production allows these applications to present failures and vulnerabilities that represent high risks for the company when they are already in production within it.

Keywords: Pentest, OWASP, web server’s security, vulnerabilities, web application

INTRODUCCIÓN

El conocimiento del riesgo para una organización contribuye a tener un panorama claro respecto a lo que podría suceder con los sistemas de información y al nivel de exposición que se tiene.

Un análisis del riesgo agrupa una serie de conceptos de seguridad como vulnerabilidades y amenazas que al ser cuantificadas aportan un valor específico de impacto y de riesgo para el negocio, lo que permite a la compañía actuar de manera oportuna y proactiva ante el riesgo, buscando la mitigación de este o la reducción máxima posible del impacto que puede generar la materialización de un riesgo específico en la compañía.

El crecimiento de la tecnología, de los servicios ofrecidos en internet y de la cantidad de activos tecnológicos de las organizaciones han llevado a un incremento exponencial de las amenazas informáticas y de los ciberataques a los servicios internos y externos de las empresas.

Por ello, es de vital importancia que los servicios y aplicaciones que ofrecen transaccionalidad online para la compañía, que además son la imagen y el buen nombre de esta, estén asegurados desde su desarrollo con metodologías claras frente a la creación y el testeo de las aplicaciones antes de su salida a producción y con pruebas periódicas en busca de vulnerabilidades o fallas que puedan representar riesgo para el correcto funcionamiento de las operaciones del negocio.

La seguridad en las aplicaciones debe controlarse desde la etapa de desarrollo, la falta de una metodología clara que facilite una guía para el desarrollo y una etapa concisa de pruebas sobre las aplicaciones antes de salir a producción permite que estas aplicaciones presenten fallos y vulnerabilidades que representan altos riesgos para la compañía.

1. TÍTULO

Uso de tecnologías de pruebas de penetración para validación de seguridad de aplicaciones web basado en el top 10 de vulnerabilidades de OWASP

2. DEFINICIÓN DEL PROBLEMA

2.1. ANTECEDENTES

Un ataque de seguridad siempre es generado a partir del aprovechamiento de una vulnerabilidad o fallo en un sistema informático, estas vulnerabilidades se producen debido a que el software es desarrollado por personas, por lo tanto, se comenten errores que en algunos casos pueden llegar a ser intencionales durante el proceso de creación. Muchos de estos errores pueden ser mitigados durante el proceso de desarrollo y testeo de las aplicaciones, sin embargo, algunas vulnerabilidades no son evidenciadas hasta después de que el software está en producción, o la aplicación está publicada en la web. [1]

2.2. FORMULACIÓN

¿Cómo pueden las diferentes tecnologías de pruebas de penetración comprobar el estado de la seguridad de las aplicaciones web de una compañía basados en el top 10 de vulnerabilidades de OWASP?

2.3. DESCRIPCIÓN

La tecnología avanza a pasos agigantados, los sistemas informáticos son cada vez más indispensables y las compañías ven en los servicios ofrecidos en línea, el futuro de las transacciones del negocio. Esto ha convertido los sistemas informáticos empresariales en el foco para los delincuentes informáticos, que van al mismo paso

---

[1] OWASP Fundation. Guía de Pruebas OWASP. {En línea}. 2008. {Revisado en marzo 2018}. Disponible en https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf

que la tecnología y que son cada vez más recursivos a la hora de atacar y generar impacto negativo dentro de las operaciones de una organización. [2]

El internet es la red de datos más grande del mundo, por lo tanto, no es fácil para las compañías tener un control de quién, cuando y como se están visualizando o usando sus servicios online. En general los portales web de las empresas son publicados para todo el mundo y esto incluye personas con intensiones maliciosas que son un riesgo potencial para la seguridad de la empresa. No es posible controlar el origen de las conexiones, por lo tanto, las empresas deben controlar y asegurar el destino de las comunicaciones, es decir, sus servicios web. [3]

Las organizaciones deben concentrarse en mitigar las vulnerabilidades y en seguir las mejores prácticas durante el desarrollo, las pruebas y el análisis de riesgos, con el fin de reducir el máximo posible el impacto que puede llegar a generar en la compañía la materialización de un riesgo a través de la explotación de una vulnerabilidad de un servicio web. [4]

Las aplicaciones web deben ser seguras, confiables y deben brindar tranquilidad a las personas que hacen uso de ellas ya que hacen parte no solo de la imagen y el buen nombre de la empresa, si no también, de la productividad y de las transacciones sobre los servicios que estas ofrecen a sus clientes.

---

[2] Informática para tu Negocio. La Evolución de la Informática en la Gestión Empresarial. {En línea} 2016. {Revisado marzo 2018} Disponible en: https://www.informaticaparatunegocio.com/blog/la-evolucion-la-informatica-la-gestion-empresarial/

[3] INC Web Hosting. Riesgos y Amenazas en la Seguridad Web. {En línea}. 2018. {Revisado en marzo 2018} Disponible en: https://www.inc.cl/blog/sitio-web/riesgos-y-amenazas-en-la-seguridad-web

[4] UNITEL Soluciones e Infraestructuras Tecnológicas. Amenazas Informáticas de Seguridad: Seguridad ante Amenazas, más que un servicio, una solución. {En línea} 2017. {Revisado en febrero de 2018}. Disponible en: https://unitel-tc.com/amenazas/

3. JUSTIFICACIÓN

En un mundo cada vez más digital, las compañías se esfuerzan por estar al día con la tecnología, por ofrecer servicios online que les permiten llegar a más personas, en más lugares y de una forma más eficiente. Una oficina virtual puede accederse desde cualquier sitio con una conexión a internet, por lo que es innecesario el desplazamiento de los usuarios y la creación de nuevas sucursales físicas de la compañía. [5] Adicional a la mejora en la prestación de servicios, también es un aporte ambiental, cada vez más empresas están apostando a la telepresencia de sus empleados, esto descongestiona las oficinas y las vías, reduce la contaminación y mejora el medio ambiente. [6]

Todo lo anterior es posible con las tecnologías actuales, sin embargo, la virtualización de las organizaciones no solo trae beneficios, también trae riesgos que pueden materializarse e impactar de forma negativa el correcto funcionamiento de las empresas.

Las aplicaciones web y el software son es diseñados por personas, por lo tanto, presentan errores o fallos que pueden ser aprovechados por un atacante para generar problemas de integridad, confidencialidad o disponibilidad de la información, comprometiendo así la seguridad, la operación y el buen nombre de cualquier empresa. [7]

---

[5] FORBES. 7 beneficios del e-commerce en las empresas. {En línea}. 2014. {Revisado en febrero 2018} Disponible en: https://www.forbes.com.mx/7-ventajas-que-tu-empresa-debe-saber-sobre-el-e-commerce/

[6] BALANTA Heidy. El Teletrabajo y su impacto en el medio ambiente. {En línea}. 2012. {Revisado en abril 2018} Disponible en: https://colombiadigital.net/actualidad/articulos-informativos/item/1938-el-teletrabajo-y-su-impacto-en-el-medio-ambiente.html

[7] GOBIERNO de España. Vulnerabilidades de un sistema Informático. {En línea} 2016. {Revisado en febrero 2018} Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

Todo lo que se publica en internet está expuesto, millones de personas con buenas y malas intenciones puedan visualizarlo o usarlo, de igual manera las aplicaciones oficiales de las compañías deben ser monitoreadas y controladas, con el fin de bloquear intentos de personas maliciosas que puedan hacer daños reales a la compañía y además asegurar que los usuarios internos les den el uso adecuado a los servicios.

La seguridad en las aplicaciones web es fundamental para mitigar o minimizar al máximo posible el riesgo de ocurrencia de cualquier tipo de incidente de seguridad, es necesario que las empresas que ofrecen servicios web puedan brindar tranquilidad a los usuarios respecto a la fiabilidad, estabilidad y disponibilidad del servicio que están ofreciendo, esta tranquilidad de los usuarios se ve reflejada no solo en la transaccionalidad de la empresa, sino también en su buen nombre.

Muchos de los errores o fallos de las aplicaciones web son generados desde el desarrollo, por ello, es necesario implementar metodologías que permitan cerrar estos fallos mientras se avanza con el desarrollo, cuando se realizan las pruebas de funcionalidad de la aplicación, antes de salir a producción e incluso realizar mantenimientos preventivos cuando la aplicación ya está en producción. [8] Toda medida de seguridad es poca, deben tomarse todas las precauciones posibles, cerrar todos los fallos que presente la aplicación. Una vulnerabilidad es una puerta abierta y una invitación a un atacante a afectar la compañía.

Las amenazas en la web han crecido al mismo ritmo que ha avanzado la tecnología [9] y por ello la seguridad en los procesos informáticos debe mantenerse al día, actualizada, supervisada y en constante evolución. Las aplicaciones web son la

---

[8] TALENS-OLIAG Sergio. Seguridad en el Desarrollo de aplicaciones. {En línea}. 2004.{Revisado en febrero 2018} Disponible en: https://www.uv.es/sto/charlas/SDA/SDA.pdf

[9] TECNÓSFERA. A diario se bloquean más de 20.000 aplicaciones móviles maliciosas. {En línea}. 2018. {Revisado en marzo 2018} Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-de-amenazas-informaticas-en-2017-208618

compañía misma expuesta a internet, por lo tanto, así como se cuida el acceso físico a las oficinas, también se debe cuidar con la misma precaución el estado y el uso de los recursos digitales. [10]

Es de gran importancia que las empresas de todos los sectores implementen metodologías para el desarrollo de las aplicaciones y las pruebas que se realizan antes de salir a producción. La implementación de una metodología para pruebas de penetración complementada con el top 10 de vulnerabilidades publicado por OWASP facilita todos estos procesos y realiza grandes aportes a la seguridad de las aplicaciones para una salida a producción de la forma más segura posible.

OWASP es una serie de buenas prácticas y recomendaciones que buscan ser una guía de trabajo enfocada a las aplicaciones desde el clico de desarrollo de software, esta metodología provee soluciones flexibles que mejoran, estandarizan y aseguran el proceso de desarrollo de una aplicación dando prioridad a la seguridad dentro del proceso de ingeniería del Software. Es importante mencionar que las vulnerabilidades pueden estar en cualquiera de los componentes de una aplicación, incluyendo los sistemas operativos de los equipos que las alojan, estos también presentan fallas que pueden afectar sólo el sistema o en ocasiones las aplicaciones que corren sobre el mismo, por lo tanto, un ética hacking desde cualquier metodología, debe buscar vulnerabilidades en ambas partes, sistema operativo y aplicación, con el fin de exponer y reportar todos los puntos de falla por los cuales se pueda aumentar el riesgo en la compañía y finalmente generar cualquier tipo de afectación. [11]

---

[10] DASWANI Deepak. Ciberseguridad en 2018: Tendencias y Amenazas. {En línea}. 2018. {Revisado en abril 2018} Disponible en: https://www.imf-formacion.com/blog/tecnologia/ciberseguridad-2018-tendencias-amenazas-201801/

[11] ASCENCIO MENDOZA Martha y MORENO PATIÑO Pedro Julian. Desarrollo de una propuesta Metodológica para Determinar la Seguridad en una Aplicación Web. {En línea}. 2011. {Revisado en abril 2018} Disponnible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2511/0058A811.pdf?sequence=1.

Con respecto al proyecto OWASP, cabe destacar que al tratarse de una organización que no tiene ningún vínculo directo ni indirecto con ninguna empresa de servicios informáticos o de software, sus publicaciones e investigaciones son una fuente de información independiente y confiable. Fundamentalmente, el proyecto OWASP se basa en tres productos principales que son: Guía de Desarrollo, de Pruebas de aplicaciones y de revisión de código. De igual manera, la compañía publica anualmente un ranking con las vulnerabilidades más activas, este ranking es base fundamental para muchos de los análisis de vulnerabilidades y de riesgos que se realizan en las empresas. [12]

[12] RODRIGUEZ Nacho. OWASP: Creando aplicaciones seguras. {En línea}. 2011. {Revisado en febrero 2018} Disponible en: https://www.genbetadev.com/seguridad-informatica/owasp-creando-aplicaciones-seguras

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Realizar un estudio monográfico que permita analizar y evaluar la efectividad de las metodologías para pruebas de penetración a sitios web respecto al top 10 de vulnerabilidades de OWASP en las organizaciones.

4.2. OBJETIVOS ESPECÍFICOS

1. Analizar las diferentes metodologías para pruebas de penetración y los marcos referenciales de vulnerabilidades.
2. Realizar una comparación entre el marco de referencia de vulnerabilidades de OWASP y otros proyectos de seguridad con marcos de referencia para el análisis de vulnerabilidades de aplicaciones web.
3. Diseñar un ambiente controlado para realizar pruebas de penetración y demostrar la efectividad del marco de referencia para vulnerabilidades de OWASP
4. Recopilar todos los resultados encontrados y las conclusiones de la investigación en un estudio monográfico

5. MARCO REFERENCIAL

5.1. MARCO TEÓRICO

5.1.1. Aplicaciones Web.

Las aplicaciones Web son una plataforma con una serie de funcionalidades a las cuales se accede a través de un navegador, existen en el mercado una gran variedad de navegadores web, que poseen diferentes características en su funcionamiento particular, ejemplo de ellos son Chrome, Firefox, Internet Explorer, Safari, entre otros. Las aplicaciones web son desarrolladas en una serie de lenguajes de programación para posteriormente ser publicadas ya sea en internet y que el acceso pueda hacerse desde cualquier lugar del mundo o simplemente pueden publicarse para la infraestructura interna de una compañía, es decir, que solo los equipos conectados a la red LAN puedan acceder a dicha aplicación. [13]

El funcionamiento interno de las aplicaciones web se basa en una arquitectura tipo Cliente/Servidor donde un equipo a través del navegador web realiza una petición a un servidor web, esta comunicación es trasmitida a través del protocolo HTTP (puerto 80) o de la evolución de este protocolo HTTPS (puerto 443), generalmente detrás del servidor web se tiene una base de datos que tiene comunicación directa con la aplicación o los formularios publicados a través del servicio web. [14]

5.1.2. Lenguajes Web.

Los lenguajes de programación son básicamente un conjunto de símbolos que estructurados de forma correcta se transforman en una serie de instrucciones que ejecutan una tarea específica dentro de un sistema informático, para el desarrollo

---

[13] NEOSOFT. ¿Qué es una aplicación Web? {En línea}. 2018. {Revisado en abril 2018} Disponible en: https://www.neosoft.es/blog/que-es-una-aplicacion-web/

[14] ECURED. Arquitectura Cliente Servidor. {En línea}. 2018. {Revisado en marzo 2018} Disponible en: https://www.ecured.cu/Arquitectura_Cliente_Servidor

web, existen muchos lenguajes de programación que permiten diseñar y desarrollar aplicaciones a medida que cumplan con los requisitos funcionales solicitados por una organización. [15]

Los lenguajes de programación más usados hoy en día por los desarrolladores web son: [16]

- JavaScript**:** Este lenguaje de scripting considerado seguro y confiable posee una cantidad de scripts con capacidades ilimitadas, generalmente es usado del lado del cliente, pero también es posible usarlo en el lado del servidor con nuevas tecnologías como AJAX.

- PHP**:** Es un compendio de una gran variedad de otros lenguajes, es usado principalmente para crear aplicaciones web dinámicas y sus scripts generan código HTML. Este lenguaje requiere Apache o IIS y hereda su sintaxis de C, Java y Perl.

- Python**:** Al igual que JavaScript el código en Python no es compilado, es interpretado. Este lenguaje es considerado en la comunidad de desarrolladores como uno de los más limpios para programar.

- Ruby: Es un lenguaje orientado a objetos que heredó su sintaxis de Python y Perl. Es considerado un lenguaje portátil y tiene la capacidad de cargar librerías de extensiones dinámicas.

---

[15] MORALES Ricardo. Lenguajes de programación: ¿Qué son y para qué sirven?. {En línea}. 2014. {Revisado en abril 2018} Disponible en: https://colombiadigital.net/actualidad/articulos-informativos/item/7669-lenguajes-de-programacion-que-son-y-para-que-sirven.html

[16] PIENSA Solutions. Principales lenguajes de programación para el desarrollo web. {En línea} 2017. {Revisado en mayo 2018} Disponible en: https://www.piensasolutions.com/blog/principales-lenguajes-programacion-web/

5.1.3. Vulnerabilidades en aplicaciones Web.

El informe de 2017 del Top 10 de riesgos críticos en las aplicaciones web de OWASP habla de inyección como el mayor riesgo de las aplicaciones web, [17] estos riesgos pueden ser prevenidos, mitigados o minimizados a través de procesos implementados en todas las fases desde el desarrollo hasta el mantenimiento en producción de las aplicaciones Web.

El siguiente es el listado oficial de las vulnerabilidades que más afectaron a las aplicaciones web durante el 2017 según el Informe de OWASP Top10-2017:

- Inyección
- Pérdida de autenticación
- Exposición de datos sensibles
- Entidades Externas XML (XXE)
- Pérdida de Control de Acceso
- Configuración de Seguridad Incorrecta
- Secuencia de Comandos en Sitios Cruzados (XSS)
- Deserialización Insegura
- Componentes con vulnerabilidades conocidas
- Registro y Monitoreo Insuficientes

[17] OWASP. OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks. {En línea} 2017 {Revisado en febrero 2018} Disponible en https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Mitigar las vulnerabilidades de las aplicaciones web ayuda a reducir el riesgo de que una amenaza pueda explotar los fallos de los desarrollos web para generar un incidente que genere interrupción de la normal operación de la compañía. Mejorar los procesos y generar conciencia de seguridad son los primeros pasos que conllevan a seguir las mejores prácticas para mejorar la seguridad y generar mayor tranquilidad no solo al interior de la compañía, sino también en los clientes que a diario interactúan con las aplicaciones web.

5.1.4. Prueba de penetración (Ethical Hacking).

¿Qué es el Ethical Hacking? Partiendo del precepto que los computadores de todo el mundo son vulnerables, las compañías necesitan conocer que tan vulnerables son sus bases de datos, servidores, aplicaciones web, redes de datos, etc. Por lo tanto, el objetivo fundamental de un Ethical Hacking es descubrir estas vulnerabilidades, realizar pruebas de penetración a la compañía y simular un ataque controlado con el fin de demostrar que un servicio es vulnerable.

¿Por qué hacer un Ethical Hacking? Evaluar las medidas de seguridad de la compañía es clave a la hora de realizar un análisis de riesgos y de prevenir la materialización de una amenaza, para ello, el Ethical Hacking brinda a la compañía visibilidad ante las vulnerabilidades, la posible explotación de las mimas y el impacto que tendría en para el negocio. Hacer un Ethical Hacking permite a las compañías tomar medidas proactivas ante amenazas e incluso distribuir los recursos económicos en las medidas de seguridad necesarias para solventar el riesgo que presentan las vulnerabilidades reportadas.

5.1.5. Herramientas de intrusión

Conocer las vulnerabilidades que poseen los sistemas operativos dentro de la organización ayuda a la compañía a enfocar los esfuerzos en mitigar todos estos fallos con el fin de minimizar el riesgo de explotación y así evitar un incidente de seguridad que pueda afectar el normal funcionamiento de todos los procesos

Las siguientes son las herramientas de Software más reconocidas del mercado para realizar Hacking Ético en las organizaciones y descubrir estas vulnerabilidades.

- Nmap: Esta es la herramienta de código abierto más usada por los administradores que quieren comprobar de manera remota que tan seguros son los componentes de su red. Una de las características principales de Nmap es la exploración de puertos abiertos, el control del host, de la actividad en la red y la identificación de las configuraciones de un ordenador (sistema operativo, firewall, etc.)

- Metasploit: Los exploits son programas diseñados para aprovechar o explotar una vulnerabilidad de un sistema. Metasploit es uno de los paquetes o kit de sploit más completos de la red, con este paquete puede comprobarse la seguridad del sistema o su capacidad de resistir ataques informáticos. Aunque Metasploit no es de código abierto, es uno de los más usados por los ingenieros de seguridad para hacer pruebas de penetración.

- Angry IP Scanner: Esta herramienta al igual que Nmap es de código abierto, es conocida como IPScan y se utiliza para realizar escaneo de las redes. Es sumamente sencilla de usar y esto ayuda a que en el análisis de direcciones IP y de los servicios sea posible encontrar puertas traseras sin códigos complejos.

- Caín y Abel: Esta es quizá la herramienta más completa a la hora de romper contraseñas. Con esta herramienta es posible realizar captura del tráfico de la red con el fin de buscar debilidades en las contraseñas o si pueden ser "adivinadas" con técnicas de explotación como fuerza bruta, diccionario o criptoanálisis.

- John the Ripper: Esta también es una herramienta especializada en contraseñas, es ampliamente utilizada para generar ataques comunes (diccionario y fuerza bruta). Con esta herramienta también pueden buscarse grietas en las contraseñas por medio de análisis de hashes.

5.1.6. Sistemas operativos para pruebas de intrusión

Existen hoy en día una gran variedad de sistemas operativos especializados para pruebas de intrusión, los siguientes son algunos de los más comunes:

- Kali Linux: es una distribución del sistema operativo Linux dedicada para pruebas de penetración y para realizar auditorías de seguridad. Anteriormente llamado BackTrack Linux y contiene los estándares de

desarrollo de Debian. También incluye una serie de herramientas nativas del sistema operativo para cumplir a cabalidad con todas sus finalidades. [18]

- OpenVass: Es un software de código abierto. Esta herramienta fue desarrollada con el fin de escanear y gestionar vulnerabilidades de seguridad. Es utilizado generalmente para pruebas de penetración. Esta herramienta es de gran ayuda y una de las principales utilizadas por el área de seguridad informática. Esta herramienta fue generada a partir de Nessus.

- Nessus: Es una herramienta que cumple la función de escanear vulnerabilidades. Esta herramienta basada en fallas ya conocidas realiza un escáner a un sistema, programa o red y luego identifica las vulnerabilidades a las cuales se encuentra expuesto. Su utilidad está enfocada en el área de seguridad informática, donde se pueden identificar a que vulnerabilidades está expuesto el sistema y además comprobar la seguridad en este. [19]

5.2. MARCO CONCEPTUAL

5.2.1. Seguridad informática

La información es uno de los activos más importantes para una empresa, es posible recuperar casi cualquier elemento físico (computadoras, servidores) pero el costo de la perdida de información puede ser fatal para una compañía. Por lo tanto, en un mundo que avanza a pasos agigantados y donde cada vez la vida es más “online” (adquirir productos online, gestionar certificados, acceder a cursos, entre otros) y por ello, la seguridad informática se ha convertido en un ítem indispensable dentro de cualquier compañía.

---

[18] DOJO Kali Linux, RELEASES Kali Linux. Kali Linux 2.0 Release. Our Next Generation Penetration {En línea}. 2015. {Revisado en abril 2018} Disponible en: https://www.kali.org/releases/kali-linux-20-released/

[19] NESSUS Professional. Whit Vulnerabilities, Seeing is believing. {En línea} 2015. {Revisado en abril 2018}. Disponible en: https://www.tenable.com/products/nessus/nessus-professional

Mantener la integridad, disponibilidad y confidencialidad de la información es el objetivo principal de la ciberseguridad, para esto se han desarrollado modelos, estándares y normas como la ISO27001 que guían a las compañías en la construcción de un modelo para gestionar la seguridad de la información de una manera más eficiente, en constante evolución, corrección y mejoramiento, con el fin de acaparar las necesidades de aseguramiento de datos y transacciones de la empresa. [20]

La seguridad de la información realiza una evaluación de incidentes, estos son eventos que afectan uno o más pilares de la seguridad informática, son eventos no deseados dentro de los sistemas informáticos de la compañía. Estos eventos deben ser registrados y analizados por expertos en seguridad, con el fin de determinar la causa raíz del incidente, poder clasificarlo y tomar las acciones correctivas correspondientes para evitar una nueva ocurrencia.

Controlar o prevenir al cien por ciento los incidentes de seguridad no es factible, ya que la seguridad a la par con la tecnología es dinámica y cambiante, los hackers están desarrollando todo el tiempo nuevas técnicas de ataque, nuevos malware y nuevas formas de infiltrarse en los sistemas informáticos de las compañías con el fin de extraer, modificar o eliminar información. [21]

La mejor forma de protegerse implica tener un sistema para la gestión de la información afinado con un análisis de riesgo efectivo que permita a la compañía conocer los principales patrones de ataque, los activos que son objetivos de estos ataques y el impacto que tendría en la compañía la materialización del riesgo en uno de estos activos. El conocimiento de los incidentes más comunes permite realizar los ajustes en las medidas de seguridad y orientar las inversiones de

---

[20] EQUIPO Editorial. Infografía: Seguridad Digital ¿Cómo aprovecharla en las organizaciones? {En línea}. 2015. {Revisado en mayo 2018} Disponible en: http://reportedigital.com/seguridad/infografia-seguridad-digital-como-aprovecharla-organizaciones/

[21] ESPITIA Diego Samuel. Los beneficios y la importancia de gestionar la seguridad de la información. {En línea}. 2015. {Revisado en abril 2018} Disponible en: https://reportedigital.com/seguridad/importancia-gestionar-seguridad-informacion/

seguridad a la protección de los activos o mitigación del riesgo que más impacto puede generar.

5.2.2. Normal ISO27001

Es una norma internacional que busca estandarizar el cómo se gestiona la seguridad de la información en una compañía. El nombre completo de la norma es ISO/IEC 27001:2013, esto después de la revisión realizada en el 2013. Esta norma puede ser implementada en cualquier empresa, independiente de su tamaño o razón social, la norma ofrece una metodología para realizar la implementación de un SGSI con miras a la certificación de la compañía. [22]

La norma ISO 27001:2013 facilita un formato y un conjunto de alienación para el desarrollo documental del sistema de gestión de la información independientemente del enfoque empresarial. La estructura es la siguiente: [23]

- Introducción: Uno de los cambios más significativos en la revisión de 2013 de la norma es la eliminación del "enfoque del proceso" de la versión de 2005 donde se describía el modelo PHVA (planificar, hacer, verificar y actuar) que era considerado fundamental dentro del SGSI.

- Alcance: La norma establece como obligatoria la definición del alcance, esto con el fin de poder obtener una conformidad de cumplimiento que puedan llevar a la compañía a una exitosa certificación.

- Referencias Normativas: El estándar ISO27002 ya no es una referencia normativa dentro de la nueva versión de ISO27001, esta norma (ISO27002) se convierte en necesaria dentro del desarrollo de la declaración de

[22] SGSI. ISO 27001: ¿Qué beneficios nos aporta implantar esta norma? {En línea}. 2016. {Revisado en mayo 2018} Disponible en: https://www.pmg-ssi.com/2016/07/iso-27001-beneficios-aporta-implantar-esta-norma/

[23] SGSI. La norma ISO 27001:2013 ¿Cuál es su estructura?. SGSI {En línea} 2015. {Revisado en mayo 2018} Disponible en: https://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/

aplicabilidad. Esto convierte a la ISO27001:2013 en una referencia que contiene los nuevos términos y definiciones.

- Términos y Definiciones: Los términos y definiciones de la norma original ISO27001:2005 fueron trasladados y agrupados dentro de una sesión de la revisión 2013 "Fundamento y Vocabulario" esto con el fin de tener en una sola guía los términos y definiciones para que sea más consistente.

- Contexto de la Organización: Esta cláusula identifica todos los problemas externos e internos de la compañía, incluye requisitos para obtener el contexto del SGSI independientemente del tipo de empresa o del alcance, introduce una figura indispensable para definir el alcance del SGSI y prioriza la identificación y definición de necesidades y expectativas del área de seguridad de TI y el sistema de gestión, lo que terminará en la generación de políticas de seguridad y la definición de los objetivos para la Gestión de Riesgos.

- Liderazgo: La relación y responsabilidad de la gerencia con el SGSI, esto garantiza los objetivos y la política de seguridad, la disponibilidad de recursos para implementación de esta y los roles y responsabilidades que serán asignados y comunicados de forma adecuada.

- Planeación: Este apartado se enfoca en la definición de los objetivos que deben estar claros y tener planes específicos para conseguirlos. Esto presenta cambios durante la evaluación del riesgo. El nivel de riesgo es determinado con la medición del impacto de la materialización de una amenaza por la probabilidad de que ocurra, esto lleva a que cada riesgo sea asignado a un propietario.

- Soporte: Este ítem habla de requisitos para la implementación y mejora del SGSI, estos requisitos incluyen los recursos, el personal competente y la concientización y comunicación a las partes interesadas. Además, con el nuevo término "Información Documentada" se establece un proceso donde se debe documentar, mantener, controlar y conservar todos los documentos que pertenecen al SGSI.

- Operación: Este apartado indica cómo realizar la medición del funcionamiento del SGSI, el cumplimiento de las expectativas de la gerencia (definidas en el Contexto de la organización) y que se cumpla a cabalidad la norma ISO27001:2013. La base de este proceso está en la periodicidad y efectividad de la gestión de riesgos. Los activos, las vulnerabilidades y las

amenazas solo se requieren para la identificación de riesgos asociados a la perdida de Confidencialidad, Integridad y Disponibilidad de la información.

- Evaluación de Desempeño**:** Las auditorías internas del SGSI son base para la identificación, medición de la eficiencia y desempeño del SGSI. Dentro de la evaluación de las No Conformidades, debe tenerse en cuenta el estado de los planes de acción definidos, se debe determinar quién y cuándo realiza las evaluaciones y quien sería el responsable de analizar la información.

- Mejora: Las No Conformidades identificadas dentro del proceso de "Evaluación de desempeño" son el elemento estrella del proceso de Mejora. Estas No Conformidades son enumeradas y comparadas con las acciones correctivas buscando que no se presenten nuevamente e identificar la efectividad de las acciones correctivas que se han tomado a partir de las No Conformidades declaradas.

5.3. ESTADO ACTUAL

5.3.1. Amenazas de seguridad informática

Una de las mayores preocupaciones informáticas de las empresas en Latinoamérica es el Malware, debido al grado de sofisticación de este tipo de ataque y a las remuneraciones económicas cada vez más grandes que representan para los delincuentes informáticos. Un ejemplo de ello es el troyano BlackEnergy capaz de infectar los sistemas de control energético SCADA y que logró la interrupción del servicio energético en la región de Ivano-Frankovsk en Ucrania. [24]

En 2017 la mayor causa de incidentes de seguridad para las compañías de Latinoamérica fue el Malware, seguido por el Ransomware que apareció durante el año y que desplazó de su segundo lugar al Phishing. Lo que concuerda con las principales preocupaciones de los empresarios respecto a la Ciberseguridad. Los

[24] ESET Enjoy Safer Tecnology. ESET Security {En línea} 2017. {Revisado en agosto 2018}. Disponible en https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

ataques con Malware han venido en ascenso, esto se debe en gran medida a la gran variedad de código malicioso del mercado, a los diversos métodos de propagación y a la remuneración económica para quienes lo desarrollan o financian. [25] El mayor porcentaje de empresas de Latinoamérica infectadas con Malware se presentó en Nicaragua con un 53% seguido por Panamá con el 50.3% y por Colombia con el 46.7%

5.3.2. Ley 1273 de 2009

La ley 1273 de 2009 de protección de la información y de los datos en Colombia modificó el código penal con el fin de incluir lo relacionado con el delito informático. Los artículos que componen dicha ley hablan sobre las penalidades que puedan tener quienes atenten contra diferentes aspectos informáticos como:

- Acceso abusivo a sistemas informático.
- Obstaculización ilegitima de sistema informático o de red de comunicación.
- Interceptación de datos informáticos.
- Daño informático.
- Uso de Software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.
- Circunstancias de agravación punitiva.
- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos

[25] ESET Enjoy Safer Tecnology. {En línea} 2017. {Revisado en agosto 2018}. Disponible en https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

Las sanciones por la violación de cualquiera de los artículos que componen la ley van desde varios meses de prisión y multas hasta 1.000 salarios mínimos. [26]

Según el balance del Cibercrimen en Colombia durante el 2017 entregado por la Policía Nacional en su Dirección de Investigación Criminal e INTERPOL el Cibercrimen reportó un incremento del 28.30% respecto al año anterior. [27]

Los cibercrímenes que se mantienen en la lista respecto al año anterior son la oferta de malware, venta de datos personales, comercialización de productos ilegales, bienes hurtados y documentos fraudulentos, estos se han visto favorecidos por el uso de las criptomonedas como medio de pago anónimo.

Así mismo el uso de las redes sociales y la temprana edad de los usuarios de estas ayudó con el incremento de delitos como el Gromming y el Sextortion. Las siguientes son las nuevas amenazas que fueron denunciadas por los ciudadanos a la policía Nacional.

- Ciberinducción al daño físico: la viralización de los retos en internet que incitan a la auto lesión, se presentaron 6.498.746 usuarios impactados.
- Estafa por suplantación de Sim Card: se obtiene una sim card nueva a partir de la suplantación del titular con el fin de sincronizar cuentas asociadas al número telefónico, las perdidas ascendieron a los $7.690.000.000

---

[26] BOGOTÁ D.C. Alcaldía Mayor. Ley 1273 de 2009 Nivel Nacional. {En línea}. 2009. {Revisado en junio 2018} Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

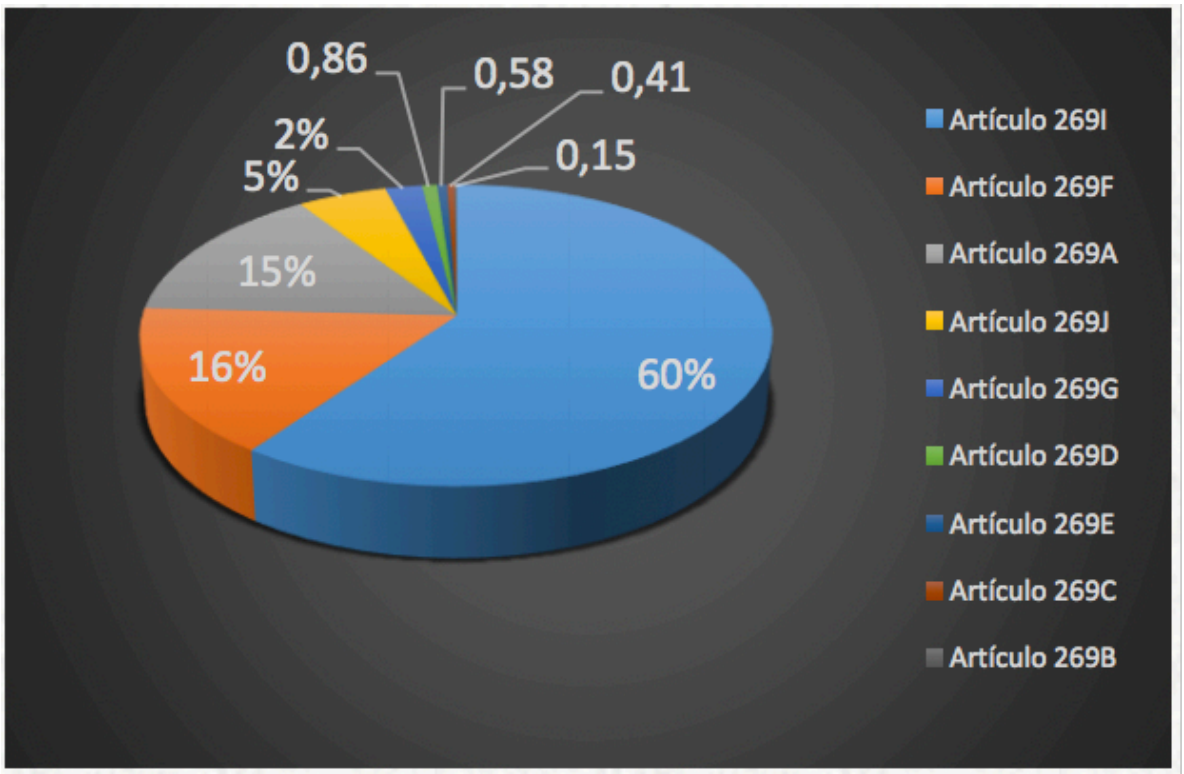
[27] POLICIA Nacional. Informe: Balance de Cibercrimen en Colombia 2017. {En línea}. 2017. {Revisado en agosto 2018} Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

- Vishing - Tráfico de datos financieros personales: técnicas de ingeniería social vía telefónica que permite a los ciberdelincuentes acceder a información personal y financiera, los casos de vishing presentan cifras cercanas a los $2.132.000.000

- Fraude por falso Whatsapp: creación de falsas conversaciones con datos públicos como fotos de perfil y número de celular con el fin de enviar pantallazos y dañar la reputación de las personas, fueron reportados 381 casos.

- Ciberpirámides: aprovechando la incertidumbre respecto a las criptomonedas, los delincuentes captan la atención de inversionistas que compran dichas monedas en internet. Estafas de 1.500 millones de pesos se reportaron en 2017.

Ilustración 1. Tipología criminal más frecuente respecto a los artículos de la ley 1273 de 2009



Controles de Seguridad: Dentro de los controles de seguridad más usados por las compañías se encuentra el Antivirus en primer lugar, seguido por Firewalls, Backups, Antispam, Autenticación, IPS, Cifrado y soluciones de doble autenticación. [28] La mayoría de estas herramientas de seguridad son reactivas, el aseguramiento de las aplicaciones web con la metodología OWASP busca implementar la seguridad desde la prevención.

[28] ESET Enjoy Safer Tecnology. ESET {En líena} 2017. {Revisado en agosto 2018}. Disponible en https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

6. ESQUEMA TEMÁTICO

6.1. CAPITULO 1: METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN Y VENTAJAS Y DESVENTAJAS DE LOS MARCOS REFERENCIALES DE VULNERABILIDADES COMO EL TOP 10 DE OWASP

6.1.1. Metodología OWASP

OWASP es una metodología usada por desarrolladores de software quiénes necesitan cerciorarse de que el código de una aplicación es seguro y que no posee vulnerabilidades; tester de software, estos necesitan una guía base para realizar las diferentes pruebas necesarias en un desarrollo antes de asegurar que es confiable; y por especialistas de seguridad, quiénes tienen la responsabilidad de asegurar que una aplicación es confiable antes de ser publicada por la organización.

Como ya se hizo mención, en este documento, la metodología OWASP cuenta con tres módulos que son la base de la metodología: [29]

- Guía para el Desarrollo**:** Es una recopilación de buenas prácticas y de pasos a seguir para asegurar el proceso de desarrollo del código de las aplicaciones de la compañía, esto con el fin de generar aplicaciones con los estándares de calidad actuales para la seguridad informática. Estas normas evitan los posibles malos hábitos de los programadores indicando cuál es la forma correcta de codificar diferentes patrones teniendo siempre presente que la aplicación puede enfrentarse en algún punto a un ataque informático de alta calidad técnica.

- Guía de Revisión de Código**:** Este módulo es utilizado para realizar de forma correcta la revisión del código que ya está generado, es decir, el código con

[29] RODRIGUEZ Nacho. OWASP: Creando aplicaciones seguras. {En línea} 2011. {Revisado en febrero 2018} Disponible en: https://www.genbetadev.com/seguridad-informatica/owasp-creando-aplicaciones-seguras

el que la compañía contaba antes de implementar la metodología OWASP, aplicaciones que ya están en producción o que no se desarrollaron siguiendo las buenas prácticas de la Guía para el Desarrollo. En muchas ocasiones las organizaciones tienen subcontratado el desarrollo de sus aplicaciones, por lo tanto, esta Guía ofrece las herramientas necesarias para realizar una evaluación del producto de software que entrega un tercero o del que no se tiene control.

- Guía de Pruebas: Esta guía, considerada la más interesante dentro del conjunto documental de la metodología OWASP, resume y evidencia las vulnerabilidades o fallas de seguridad en las aplicaciones y cómo puede un intruso explotar estos puntos de entrada. La guía posee ejemplos gráficos y contundentes que están perfectamente explicados, con el fin de concientizar a las organizaciones o a quién usa la guía de que el peligro es real, de que las aplicaciones mal desarrolladas son un riesgo inminente que podría traer una serie de consecuencias negativas afectando la funcionalidad normal de la organización.

Estructuralmente, las fases de la metodología OWASP son las siguientes: [30]

1. Antes de empezar el desarrollo
    a. Revisión de estándares y políticas
    b. Desarrollo de métricas y criterios de revisión
2. Durante el diseño y la definición.
    a. Revisión de los requisitos de seguridad
    b. Revisión de diseño de arquitectura

[30] OWASP. Análisis de Riesgos Aplicando la Metodología OWASP. {En línea} 2017. {Revisado en septiembre 2018]. Disponible en: https://www.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf

c. Creación y revisión de modelos UML

d. Creación y revisión de modelos de amenaza

3. Durante el desarrollo

    a. Inspección de códigos por fases

    b. Revisiones de Código

4. Durante la implementación

    a. Pruebas de intrusión en aplicaciones

    b. Comprobación y gestión de configuraciones

5. Mantenimiento y operaciones

    a. Ejecución de revisión de la administración operativa

    b. Ejecución de comprobaciones periódicas de mantenimiento

    c. Asegurar la verificación de cambios

Sin embargo, cualquier metodología de Ethical Hacking se debe componer de cuatro fases básicas: planeación, descubrimiento, ataque y reporte. A continuación, se describe cada una de estas fases y los procesos que deben realizarse en cada una de ellas.

Fase de Planeación

Dentro de la fase de planeación o planificación según OWASP, etapa inicial de un Ethical Hacking, se definirá que es lo que se pretende con la prueba, cual es el alcance de esta, como se realizará exactamente el Ethical entre otros.

- Alcance: Dentro del alcance se debe definir qué es lo que espera exactamente la empresa del Ethical Hacking, si se realizará a una subred específica o a toda la compañía. Se deben definir los segmentos que tienen

prioridad (generalmente los segmentos de servidores), si se incluirán redes inalámbricas y usuarios dentro de la prueba.

- Duración: Se debe definir exactamente cuándo se dará inicio y final a la prueba, esto con el fin de informar al personal pertinente y estar en estado de alerta en caso de que se presente alguna afectación en los servicios de la compañía.

- Autorización: Para que la prueba de penetración sea ética, debe estar específicamente autorizada, las pruebas que se realizarán y hasta donde se va a llegar con las mismas, igualmente deben compartirse los contactos de los responsables de parte y parte y el esquema para escalar los casos que se consideren de mayor criticidad.

- Objetivos: Aquí se especifican los equipos, servicios, aplicaciones, usuarios o redes que serán los objetivos principales de la prueba de penetración, el objetivo o victima debe ser definido por la compañía y generalmente son los activos que contiene las aplicaciones más críticas o de mayor importancia para la organización. También puede realizarse una prueba sin objetivo, donde la organización no entregue esta información al encargado de realizar la prueba.

- Metodología: Existe una gran variedad de metodologías para la realización de Ethical Hacking, en esta parte de la fase uno no solo se define OWASP como la metodología base, sino que además debe determinarse si la prueba se realizará con el enfoque de caja negra o caja blanca.

- Tipo de Pruebas**:** También es importante definir qué tan intrusivas son las pruebas que plantea el test de penetración, que son exactamente, como pueden afectar los sistemas y cuánto tiempo puede durar cada una de ellas, esto también debe ser tomado en cuenta para las autorizaciones de la prueba.

- Security Tools: Es importante para la compañía tener claridad y conocer el listado de herramientas que usará el auditor para cada una de las pruebas que se plantean dentro del Ethical hacking.

- Recursos: Aquí se debe definir cuáles son los recursos que el auditor posee y cuáles son los que necesita por parte de la compañía, por ejemplo, si la prueba es caja blanca y con objetivo, se debe proporcionar un punto de acceso a red, una dirección IP estática, entre otros.

Los tipos de pruebas según la metodología OWASP son los siguientes: [31]

- Recopilación de Información
- Pruebas de Gestión de la Configuración
- Pruebas de la Lógica del Negocio
- Pruebas de Autenticación
- Pruebas de Autorización
- Pruebas de Gestión de Sesiones
- Pruebas de Validación de Datos
- Pruebas de Denegación de Servicio
- Pruebas de Servicios Web
- Pruebas de AJAX

Fase de Descubrimiento

La fase de descubrimiento o fase de obtención de información como es nombrada según la metodología OWASP, en esta etapa se realiza el footprinting de la organización. Un footprinting es el proceso de recolección de información acerca de la compañía, la principal fuente de información para esta tarea es Internet, donde puede obtenerse información que bien filtrada puede resultar muy útil para el auditor y la prueba de penetración. [32]

---

[31] SALAZAR T Edgar D. Pruebas de Seguridad en Aplicaciones web según OWASP. ¿Dónde estamos… Hacía dónde vamos? {En línea} 2016. {Revisado en agosto 2018} Disponible en: https://www.owasp.org/images/2/2f/OWASP_SUSCERTE.pdf

[32] PONFERRADA LÓPEZ Javier. ¿Qué es footpirinting y fingerprinting? {En línea}. 2015. {Revisado en mayo 2018} Disponible en: http://www.ticarte.com/contenido/que-es-footprinting-y-fingerprinting

La información principal que debe investigarse acerca de la compañía puede categorizarse de la siguiente manera:

Información de Red:

- Nombre de Dominio
- Direcciones IP
- Servicios TCP/UDP
- Autenticación

Información de Sistema:

- Banners
- SNMP
- Arquitectura
- Passwords

Información de la Organización:

- Portal Web
- Información de Empleados
- Políticas de Seguridad
- Teléfonos

Pasos para la obtención de Información: OWASP recomienda una serie de pasos a seguir para la obtención de toda la información que se necesita para poder iniciar la prueba en sí, los pasos son los siguientes:

- Websites
- Email
- Google
- Who is DNS Network
- Ingeniería Social
- Redes Sociales

Herramientas para la obtención de información: Existen muchas herramientas y métodos para obtener la información necesaria para iniciar una prueba de Ethical Hacking, algunas de las herramientas recomendadas por la metodología OWASP son:

- Google Hacking
- Kali Linux
- Pipl
- Maltego
- Netcraft

Fase de Ataque

Para la metodología OWASP la fase de ataque se compone de dos subfases: Fase de Enumeración y Exploración de Servicios/Vulnerabilidades y Fase de Elevación de Privilegios. [33]

Iniciando con la fase de Enumeración y Exploración de Servicios/Vulnerabilidades, esta a su vez tiene varias etapas:

- Identificación de Host Vivos**:** Dentro de esta etapa el auditor debe utilizar herramientas como Nmap y pruebas como el ICMP Sweep para enviar ICMP ECHO Request a múltiples host dentro de la red, esto con el fin de identificar y numerar a los equipos que retornan un ICMP Replay al Request. La finalidad de esta prueba es identificar cuáles son los hosts "vivos" es decir, las direcciones IP activas dentro del sistema.

- Banner Grabbing: En esta etapa se busca identificar los sistemas operativos de los hosts vivos, es posible realizar la identificación del sistema operativo en un host remoto o también es posible identificar las aplicaciones detrás de los servicios activos.

- Escaneo de Puertos TCP/UDP: En esta etapa el auditor debe identificar los puertos que están "escuchando" para cada servidor, con la herramienta Nmap, por ejemplo, es posible incluso realizar evasión de IDS o Firewall de Red para identificar todos los puertos posibles y su estado.

- Enumeración**:** Existen algunos puertos conocidos más "peligrosos" que otros, es decir, que son más fáciles de explotar o que se puede hacer mayor daño a través de ellos. Por lo tanto, en esta etapa se busca enumerar los puertos abiertos que se encontraron para identificar cuáles podrían representar vulnerabilidades críticas para la organización y cuáles no. Adicionalmente, partiendo del servicio (puerto) que se identificó como abierto, también deben enumerarse las características o información adicional que pueda obtenerse de cada puerto.

---

[33] OWASP Latam Tour 2015. Hacking Ético: Cacería de Vulnerabilidades. {En línea}. 2015. {Revisado en octubre 2018} Disponible en: http://docplayer.es/3407409-Hacking-etico-caceria-de-vulnerabilidades-owasp-latam-tour-2015.html

- Escaneo de Vulnerabilidades: Finalmente teniendo un mapa completo de los hosts activos dentro de la red, de los sistemas operativos, los puertos o servicios activos y la información que puede obtenerse de cada uno de ellos, se realizan pruebas de vulnerabilidades partiendo de toda esta información previa.

- Explotación de vulnerabilidades**:** Es la etapa final de la primera sub-fase, como su nombre lo indica, después de realizar todas las etapas anteriores, ya se tiene un listado de las vulnerabilidades de la compañía, la idea de explotarlas es cerciorarse al 100% que las vulnerabilidades existen, están activas y es posible explotarlas, además de tomar evidencia de los hallazgos para el informe final.

OWASP recomienda una serie de pruebas que apuntan a procesos específicos de la organización, las pruebas son las siguientes:

- Recopilación de Información: Lo primero que se debe realizar es buscar la mayor cantidad de información posible acerca de la aplicación, servicio o sistema operativo víctima del escaneo de vulnerabilidades.

- Pruebas de Gestión de la Configuración: Consta de un análisis de la arquitectura que puede revelar información importante como: código fuente de una aplicación, métodos HTTP permitidos, métodos de autenticación, entre otros.

- Pruebas de la Lógica del Negocio: Saltarse la lógica del negocio implica conocer cómo funcionan los procesos, es decir, si el proceso de autenticación requiera 3 pasos (1,2 y 3) deben realizarse pruebas omitiendo alguno de estos pasos e identificar el comportamiento del sistema o de la aplicación al respecto.

- Pruebas de Autenticación: La finalidad de estas pruebas es probar la verificación de los métodos de autenticación en sistemas operativos o aplicaciones de la compañía. Por ejemplo, las pruebas de fuerza bruta entrarían en esta categoría.

- Pruebas de Autorización: El auditor debe entender cómo funcionan los mecanismos de autorización de la compañía para luego intentar saltarse los mismos y acceder a recursos o ejecutar tareas no autorizadas.

- Pruebas de Gestión de Sesiones: La gestión de las sesiones cubre los controles que se realizan sobre un usuario iniciando en la autenticación hasta finalmente la salida de la aplicación o sistema.

- Pruebas de Validación de Datos: Una debilidad muy común en aplicaciones web es la falta de validaciones adecuadas de la información procedente del cliente o del retorno de la aplicación, en estas pruebas se valida la respuesta de los sistemas ante inyecciones de información con data corrupta.

- Pruebas de Denegación de Servicio: La base de un ataque de DoS es realizar una gran cantidad de peticiones a un sistema, haciéndolo incapaz de sostener el volumen de las peticiones recibidas. En este tipo de pruebas se busca analizar que tanto resisten los equipos o aplicaciones antes de empezar a rechazar peticiones.

- Pruebas de Servicios Web: Los servicios web en general se exponen a internet con protocolos como HTTP, FTP o SMTP, en estas pruebas se busca obtener información confidencial de las aplicaciones, realizar ataques similares al SQL Inyección y/o encontrar vulnerabilidades de XML

- Pruebas de AJAX: Las aplicaciones de AJAX tienen una superficie de ataque mayor que las aplicaciones convencionales, estas aplicaciones se caracterizan por realizar el procesamiento tanto del lado del cliente como del lado del servidor, en esta parte de las pruebas, se deben identificar las vulnerabilidades de este tipo de aplicaciones si existen dentro de la compañía.

La siguiente sub-fase dentro de la Fase de Ataque es la Elevación de Privilegios donde se busca romper la seguridad de protección de contraseñas, identificar y probar las contraseñas encontradas e intentar elevar los privilegios de los usuarios de estas contraseñas, con el fin de tener acceso a sistemas o partes del sistema que no se debería tener.

Técnicas para encontrar contraseñas:

- Ataque de Diccionario

- Ataque de Fuerza Bruta

- Ataque Hibrido
- Ataque basado en reglas

Tipos de ataques para encontrar contraseñas:

- Ataques Pasivos
- Ataques Activos
- Ataques Offline

Elevación de Privilegios:

- Vertical: Escalar privilegios de forma vertical consiste en acceder a privilegios o zonas superiores a los establecidos por el administrador.
- Horizontal: Escalar privilegios de forma horizontal consiste en acceder a zonas o recursos de usuarios con privilegios similares.

Fase de Reporte

Después de realizar todo el test de penetración, se deben recopilar todos los hallazgos en informes, de forma que la compañía que contrató la prueba de vulnerabilidades tenga claridad de la actividad que se realizó y de las vulnerabilidades que se encontraron durante la prueba.

Informe Gerencial: Es un informe muy resumido, se debe evitar al máximo el uso de terminología técnica, la idea es que la gerencia de la organización pueda comprender el riesgo que significan los hallazgos del Ethical Hacking. Los puntos claves que deben documentarse en el informe gerencial son:

- Nivel de exposición de la plataforma.
- Nivel de riesgo

- Plan de remediación sugerido.

Informe Técnico: En este informe se presentan todos los detalles de las pruebas realizadas, los hallazgos y vulnerabilidades encontradas y de la explotación, al igual que las conclusiones y recomendaciones técnicas para la remediación de las vulnerabilidades. Este informe es para el personal de Ciberseguridad de la compañía, por lo tanto, puede contener toda la terminología técnica necesaria para exponer la realidad a nivel de seguridad de la compañía. Los ítems que mas importantes de este informe son:

- Hallazgos
- Detalle de las Vulnerabilidades
- Procedimiento de Explotación
- Evidencias
- Contramedidas

6.1.2. Ventajas de la metodología OWASP

El mayor beneficio de la implementación de una metodología como OWASP es el buen modelamiento de las amenazas de una compañía, lo que proporciona una línea base de seguridad acertada. Este modelamiento permite que todas las decisiones referentes a la seguridad de la compañía se realicen partiendo de un panorama completo del estado de seguridad, es decir, con toda la información sobre la mesa. Sin la implementación de una metodología para el modelamiento de vulnerabilidades, las decisiones de seguridad de la compañía se harían sin apoyo, solo con suposiciones, lo que puede enfocar los esfuerzos de seguridad erróneamente y llevar a una pérdida económica y de información confidencial. El

proceso de modelado de amenazas produce los argumentos de seguridad necesarios para explicar y defender la seguridad de una aplicación. [34]

OWASP como organización tiene la misión de brindar una mayor visibilidad a la seguridad de las aplicaciones web, con la finalidad de que las organizaciones tengan la confianza de tomar decisiones respecto a la seguridad de compañía partiendo de información concisa y de un panorama claro del estado de la seguridad. Es importante destacar que todos los proyectos documentales o de software involucrados en OWASP son gratuitos. Por lo tanto, OWASP busca ser un reconocido referente principalmente en la seguridad enfocada a las aplicaciones web. Todo esto con el fin de ayudar a los creadores de software durante el camino de desarrollo, buscando que estas sean aplicaciones más seguras.[35]

Existe una metáfora llamada “deuda técnica” aplicada al desarrollo de software de la que se habló por primera vez hace dos décadas.[36] Esta explica la necesidad de volver a calcular los costos de un software mal diseñado, de un software mal asegurado. Este concepto se ha venido utilizando en el medio de la seguridad informática para describir deudas referentes al mal desarrollo del software, incluso el concepto es aplicado a los esfuerzos innecesarios que son generados por el software mal desarrollado o a los impedimentos que el software adquiere para actualizarse, evolucionar o integrarse con otro software adicional.

La deuda técnica se refiere al costo y además a los intereses que se deben pagar por realizar las cosas de manera incorrecta. En muchas ocasiones las compañías evitan los costos que representan la implementación y gestión de una metodología de aseguramiento de las aplicaciones como OWASP, en otras ocasiones las

---

[34] GIOINO Mauro y BORGHELLO Christian. Modelado de Amenazas. 1.5 Beneficios. {En línea} 2014. {Revisado en octubre 2018} Disponible en: https://www.owasp.org/index.php/Modelado_de_Amenazas#Beneficios

[35] VINDEL AMOR Rafael. Introducción a OWASP. {En línea} 2016. {Revisado en agosto 2018} Disponible en: https://www.adictosaltrabajo.com/tutoriales/introduccion-a-owasp/

[36] CUNNINGHAM Ward. The WyCash Portfolio Management system. {En línea} 1992. {Revisado en noviembre de 2018} Disponible en: http://c2.com/doc/oopsla92.html

compañías deciden asimilar las vulnerabilidades suponiendo que estas no serán explotadas en ningún punto. La deuda técnica hace referencia al costo que tiene no asegurar el software, a todos los costos que puede generar para la compañía la explotación de una vulnerabilidad asociada a una aplicación. [37]

6.1.3. OSSTMM

Esta metodología propone la evaluación de las diferentes áreas que componen los niveles de seguridad de una compañía comúnmente denominados “Dimensiones de Seguridad”, generalmente hace referencia a la visibilidad, acceso, autenticación, confianza, autorización, privacidad, confidencialidad, integridad entre otros. Esta metodología además de los temas técnicos también abarca aspectos como los responsables de la prueba. [38]

Esta metodología se enfoca en la seguridad de los siguientes ítems:

- Información
- Procesos
- Tecnologías de Internet
- Comunicaciones
- Seguridad Inalámbrica
- Seguridad Física

---

[37] GARZAS Javier. La deuda técnica. Todo el mundo debería saber que la mala calidad software al final se paga. {En línea}. 2012. {Revisado en agosto 2018} Disponible en: http://www.javiergarzas.com/2012/11/deuda-tecnica-2.html

[38] HERZOG Pete. Open Source Security Testing Methodology Manual (OSSTMM). {En línea} 2016. {Revisado en noviembre 2018} Disponible en: http://www.isecom.org/research/osstmm.html

6.1.4. ISSAF

Esta metodología desarrollada por OISSG se enfoca en la clasificación de la información de la prueba, separándola en diferentes dominios y partiendo de pruebas con diferentes criterios. Está principalmente enfocada en los procesos de seguridad y en evaluarlos para encontrar las vulnerabilidades existentes en estos. [39]

6.1.5. CEH (Ethical Hacking Certificado)

Esta es una certificación otorgada por EC-Council y en la que se verifican las capacidades de un profesional para realizar un correcto hacking ético.

6.1.6. Offensive Security (Seguridad Ofensiva)

Este es uno de los conjuntos de certificaciones y cursos más robustas y, por lo tanto, uno de las más exigentes, lo que lo hace líder en las pruebas de penetración y estudios de seguridad.

6.1.7. Top 10 de vulnerabilidades de OWASP

Una de las principales características de OWASP es su top 10 de las vulnerabilidades más críticas de una organización, las vulnerabilidades a las que se le debe dar tratamiento inmediato debido al riesgo que representan para la seguridad de la información de la compañía.

El OWASP Top 10 – 2017 esta basado en los datos enviados por más de 40 organizaciones especializadas en seguridad de aplicaciones además de una

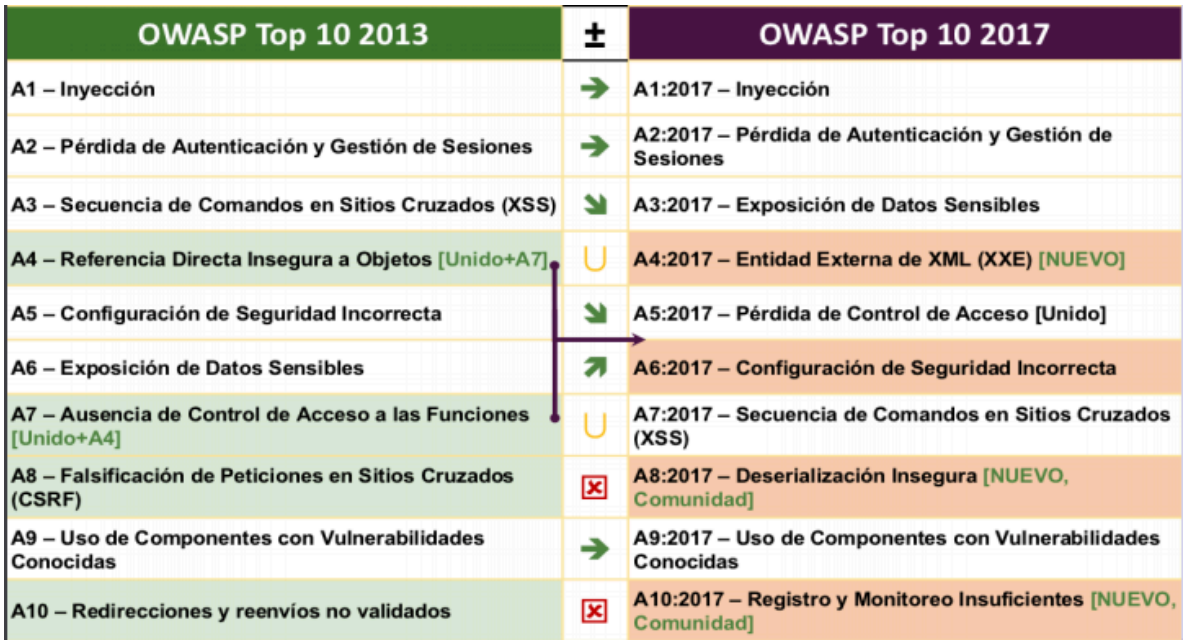
---

[39] OISSG. Information Systems Security Assessment Framework (ISSAF). {En línea} 2016. {Revisado en octubre 2018} Disponible en: http://www.oissg.org/issaf.html

encuesta que se realiza a personas de la industria. La información recopilada contiene vulnerabilidades de una gran cantidad de organizaciones. [40]

La seguridad no es estática, las vulnerabilidades y las técnicas de explotación son cambiantes y se actualizan constantemente, por ello el Top 10 de OWASP también debe actualizarse para mantenerse vigente con el estado global de seguridad en aplicaciones web. Por ello, existen algunos cambios notables entre el Top 10 OWASP de 2013 y el Top 10 de OWASP de 2017.

Ilustración 2 Comparación entre el Top 10 de OWASP 2013 y 2017



Algunas de las vulnerabilidades permanecen en su posición anterior, pero otras han subido o bajado dependiendo de su criticidad, algunas han desaparecido ya que no

[40] OWASP. OWASP Top 10 – 2017 Los diez riesgos más críticos en Aplicaciones Web. {En línea} 2017. {Revisado en noviembre 2018} Disponible en: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

son el foco actual de los atacantes o ya no se presentan de forma constante o reiterativa en las aplicaciones web y han aparecido nuevas vulnerabilidades, descubiertas hace poco o explotadas de forma constante. Cabe resaltar que la posición de una vulnerabilidad dentro del Top 10 de OWASP depende del riesgo que implica para una organización la posible explotación de esta.

Adicional a la categorización de las vulnerabilidades, el Top 10 de OWASP incluye una descripción de cada una de las vulnerabilidades incluidas en el Top, el vector de ataque, ejemplos de escenarios de ataque y recomendaciones para prevenir la explotación de la vulnerabilidad. También incluye recomendaciones para los desarrolladores, tester, administradores de aplicaciones web y para las organizaciones, todo esto enfocado a proteger las aplicaciones web y evitar o mitigar las vulnerabilidades que puedan presentarse en las mismas.

6.1.8. Top 25 de SANS/CWE

Con una filosofía similar a OWASP, SANS tiene un listado con los 25 errores de programación que pueden generar vulnerabilidades peligrosas y fáciles de encontrar y de explotar, donde los atacantes pueden tener control total del software, robar datos importantes o perjudicar el normal funcionamiento de las aplicaciones. [41]

La versión más actual de este marco de referencia de vulnerabilidades es la 2010, donde los 25 errores de software están divididos en tres categorías diferentes: [42]

- Interacción insegura entre los componentes (6 errores)
- Gestión de recursos riesgosos (8 errores)

---

[41] IBM. Informe SANS/CWE Top 25 Most Dangerous Programming Errors v1.03. IBM {En línea} 2017. {Revisado en noviembre 2018} Disponible en: https://www.ibm.com/support/knowledgecenter/es/SSW2NF_9.0.1/com.ibm.ase.help.doc/topics/r_sans_cwe_top25_report.html

[42] SANS. CWE/SANS Top 25 Most Dangerous Software Errors. {En línea} 2017. {Revisado en noviembre 2018} Disponible en: https://www.sans.org/top25-software-errors

- Defensas porosas (11 errores)

En la primera categoría se encuentran relacionadas las seis debilidades o errores relacionados con métodos inseguros para el envío o la recepción de los datos entre los componentes, módulos, programas, procesos, subprocesos o sistemas separados.

Ilustración 3 Errores de Interacción Insegura entre los Componentes

CWE ID	Name
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')

En la segunda categoría se encuentran los ocho errores relacionados con la gestión de recursos riesgosa, estos errores están relacionados con la manera en que el software no presenta una administración correcta de la creación, uso, transferencia o destrucción de recursos importantes del sistema.

Ilustración 4 Errores de Gestión de recursos riesgosa

CWE ID	Name
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-494	Download of Code Without Integrity Check
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-676	Use of Potentially Dangerous Function
CWE-131	Incorrect Calculation of Buffer Size
CWE-134	Uncontrolled Format String
CWE-190	Integer Overflow or Wraparound

En la tercera y última categoría del Top 25 de SANS se encuentran los once errores relacionados con defensas porosas, es decir, los errores relacionados con las técnicas de defensa que están siendo usadas de forma incorrecta, sea porque se abusan o simplemente por que se ignoran.

Ilustración 5 Errores de Defensas Porosas

CWE ID	Name
CWE-306	Missing Authentication for Critical Function
CWE-862	Missing Authorization
CWE-798	Use of Hard-coded Credentials
CWE-311	Missing Encryption of Sensitive Data
CWE-807	Reliance on Untrusted Inputs in a Security Decision
CWE-250	Execution with Unnecessary Privileges
CWE-863	Incorrect Authorization
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-307	Improper Restriction of Excessive Authentication Attempts
CWE-759	Use of a One-Way Hash without a Salt

Adicional a los 25 errores citados por SANS, el proyecto también cuenta con una serie de pasos que pueden ayudar con la eliminación o mitigación de estos errores de software.

6.1.9. Ventajas del Top 10 de OWASP sobre el Top 25 de SANS

Luego de comprender ambos marcos de referencia de vulnerabilidades, queda claro que SANS abarca una gran cantidad de errores en el Software y que la clasificación de estos 25 errores en tres categorías hace que sea mas sencillo comprender cada uno de ellos y realizar planes de trabajo basados en estas categorías que ayuden con la mitigación de las vulnerabilidades y que se enfoque en cada categoría de forma independiente.

También es claro que SANS plantea una serie de recursos que pueden ayudar a la eliminación de estos errores, que pueden incluirse dentro del plan de trabajo de gestión de vulnerabilidades y enfocar los esfuerzos a los que realmente son un riesgo para la compañía. Sin embargo, la mayoría de los recursos planteados por SANS hacen referencia a desarrollos también de SANS, lo que limita el espectro de trabajo a la hora de generar planes de mitigación y hace necesario realizar investigaciones adicionales que expliquen la mejor manera de mitigar cada uno de los errores encontrados en las pruebas de penetración que usan como marco de referencia este top.

Por otro lado, el proyecto OWASP plantea solo 10 vulnerabilidades, las 10 vulnerabilidades con mayor relevancia en el mercado, con mayores índices de explotación, que pueden ser descubiertas con facilidad y que tendrían un impacto importante en la seguridad de la información si se presenta explotación de alguna de ellas. Esto genera información más concisa, planes de trabajo de gestión de vulnerabilidades a corto plazo y con un enfoque realista partiendo de lo que realmente es un riesgo para la organización y de donde se deben iniciar e incrementar los esfuerzos de mitigación.

Adicionalmente, el Top 10 de OWASP incluye la información completa de cada una de las vulnerabilidades que se encuentran dentro de su top, lo que facilita los planes de acción, los pasos a seguir, incluso las recomendaciones luego de mitigar las vulnerabilidades para mejorar las aplicaciones web desde todos los puntos, desarrollo, tester y administración de estas. Lo que nos asegura una gestión de vulnerabilidades más efectiva y con mitigación o prevención de vulnerabilidades desde todas las etapas de las aplicaciones web.

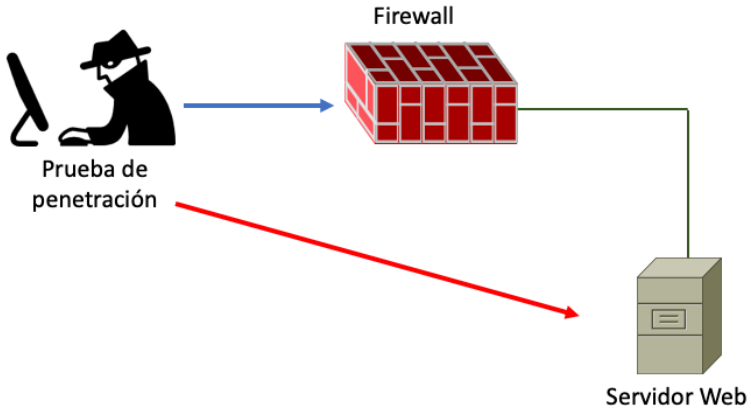
6.2. CAPITULO 2: DISEÑAR UN AMBIETE CONTROLADO PARA REALIZAR PRUEBAS DE PENETRACIÓN Y DEMOSTRAR LA EFECTIVIDAD DEL MARCO DE REFERENCIA PARA VULNERABILIDADES DE OWASP

6.2.1. Arquitectura de la prueba

Para realizar la prueba de penetración se utilizó una arquitectura básica con un servidor web y solo un firewall con reglas de acceso básicas para proteger dicho

servidor. En la ilustración 8 se muestra el esquema específico con el que se realizó la prueba de penetración.

Ilustración 6 Arquitectura de la prueba



6.2.2. Vectores de la prueba

Para la prueba se utilizó el método de caja negra (cuando el consultor de seguridad no tiene conocimiento de la infraestructura, ni de los dispositivos a evaluar); la prueba se realiza bajo el siguiente rol de usuario: Tipo visitante con poco o ningún privilegio, con los controles de seguridad que disponen la compañía, bajo un escenario controlado.

Además, se utilizó la metodología OWASP donde se realiza la identificación del equipo en la prueba con la herramienta Nmap, el escaneo de vulnerabilidades con Kali Linux, la enumeración de las vulnerabilidades y finalmente el análisis de esta información para el informe técnico y el informe ejecutivo. La ilustración 9 muestra en resumen la metodología a usar para la prueba de penetración.

Ilustración 7 Metodología de la prueba

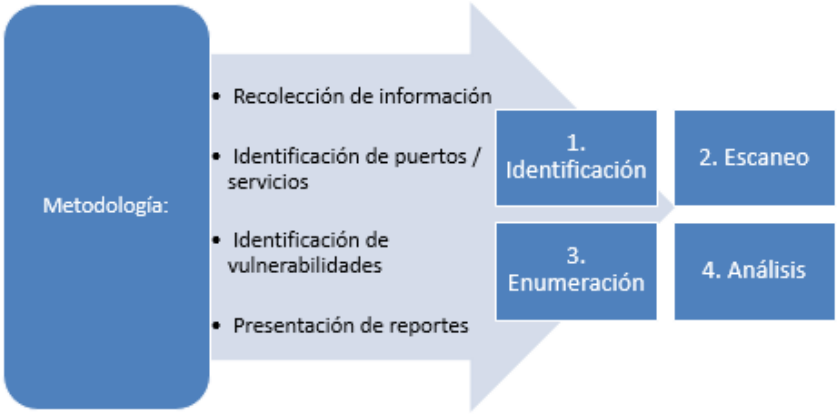


Tabla 1 Mapa de severidad o exposición del objetivo

Crítico / Critical	Vulnerabilidades cuya explotación exitosa puede comprometer un sistema
Alto / High	Vulnerabilidades cuya explotación exitosa puede otorgar privilegios a un atacante sobre el sistema.
Medio / Medium	Vulnerabilidades cuya explotación exitosa puede generar consecuencias con algún impacto para la Compañía al combinarse con otros ataques podría elevar el nivel de exposición a Alto o Crítico
Bajo / Low	Vulnerabilidades que suministran información y no generan un riesgo para la integridad, confidencialidad o disponibilidad del sistema.

6.2.3. Actividades realizadas dentro de la prueba de penetración

Los pasos realizados durante el análisis de vulnerabilidades fueron los siguientes:

- Análisis de la información obtenida sobre el dispositivo objetivo
- Evaluación de la magnitud de las vulnerabilidades del dispositivo evaluado para identificar hasta qué punto potencial un atacante tendría capacidad de ingresar al dispositivo.

Dentro del la prueba de penetración como tal también se cumplió con una serie de actividades:

- Análisis de la información obtenida sobre el dispositivo objetivo
- Exploración del dispositivo objetivo, selección de los exploits
- Ejecución de los exploits seleccionados para el análisis de su impacto
- Verificación y análisis si se obtiene acceso no autorizado al dispositivo o servicio.

Dentro del marco metodológico de las actividades de análisis de vulnerabilidades y pruebas de penetración, se describen las siguientes actividades o dominios a desarrollar de acuerdo con la metodología planteada en la ejecución de las pruebas.

- Escaneo de vulnerabilidades: Se desarrolla la etapa de análisis de vulnerabilidades a través de la herramienta Nessus
- Prueba de penetración: Se desarrolla la etapa de prueba de penetración a través de las herramientas Metasploit y OWASP ZAP

6.2.4. Resultados de la prueba

Se determina que el dispositivo evaluado presenta vulnerabilidades que permiten a un atacante recolectar información para utilizar como insumo para un ataque más elaborado y el uso de comunicaciones sin cifrar o con cifrado débil pueden derivar o facilitar la fuga de información al interceptar o capturar la información transmitida o diligenciada en los formularios.

A continuación, se relacionan las vulnerabilidades encontradas en la evaluación del dispositivo basándose en los niveles de criticidad planteados por el top 10 de OWASP.

Vulnerabilidades Críticas:

- PHP Unsupported Version Detection
- OpenSSL Unsupported

Vulnerabilidades Altas:

- Unsupported Web Server Detection
- IBM WebSphere Application Server 8.0 < Fix Pack 10 Multiple Vulnerabilities (POODLE)
- PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities
- OpenSSL 1.0.1 < 1.0.1h Multiple Vulnerabilities

Vulnerabilidades Medias

- IBM WebSphere snoopservlet Path Disclosure
- IBM WebSphere Application Server 7.0 < 7.0.0.43 / 8.0 < 8.0.0.13 / 8.5 < 8.5.5.10 / Liberty 16.0 < 16.0.0.2 CRLF Sequences http Response Splitting
- HTTP TRACE / TRACK Methods Alloweb
- Apache 2.2.x < 2.2.27 Multiple Vulnerabilities
- Open SSL < 1.0.2i Default Weak 64-bit Block Cipher (SWEET32)

De acuerdo con las vulnerabilidades identificadas se realizan pruebas de Ethical Hacking sobre el objetivo y se intenta explotar las vulnerabilidades Cross-Site Scripting XSS, Clickjacking y referencias a objetos directos inseguros.

Se identifica que el sitio permite visualización de información a través de mensajes de error inseguros que permiten a un atacante conocer la programación del sitio, su funcionamiento, versiones, puertos activos, vislumbrar las aplicaciones que se ejecutan y distinguir posibles vulnerabilidades a explotar.

Al intentar explotar esta vulnerabilidad se obtiene una respuesta satisfactoria, en consecuencia, la vulnerabilidad se logró explotar y se visualizan librerías, manuales de ayuda, configuraciones, versiones de software y archivos.

6.2.5. Conclusiones de la prueba

Las pruebas de vulnerabilidades pueden realizarse de una forma más organizada siguiendo los pasos planteados en la metodología OWASP, con estos pasos se logra identificar correctamente los objetivos, las vulnerabilidades, la explotación de las vulnerabilidades y el análisis de la información.

Adicionalmente, en la fase de documentación planteada por OWASP, es posible entregar a la compañía un informe técnico que contenga todo el paso a paso realizado dentro de la prueba de penetración, información técnica sobre las vulnerabilidades encontradas y las recomendaciones para la mitigación de estas. Sin embargo, la fase de documentación de OWASP también plantea un informe ejecutivo donde se presenta el estado general de seguridad de la organización basándose en los hallazgos encontrados y en la clasificación de las vulnerabilidades según el Top 10 de OWASP

Una prueba de penetración genera bastantes vulnerabilidades de la aplicación web objetivo, con el top 10 de vulnerabilidades de OWASP es posible dar relevancia a los hallazgos realmente críticos que generarían un gran impacto en caso de explotación y que, por lo tanto, representan un gran riesgo para la compañía. De esta manera, la gestión de vulnerabilidades tiene un enfoque más eficaz, donde la mitigación parte de los componentes mas críticos de la organización y de las vulnerabilidades que representan un mayor riesgo para la operación del negocio.

7. RESULTADOS E IMPACTO ESPERADO

La seguridad completa no es posible, la finalidad de la ciberseguridad es acercarse lo máximo posible al ideal de seguridad, esto implica entre muchas cosas que las aplicaciones web de compañía sean seguras, confiables y que difícilmente puedan ser víctimas de ataques que puedan afectar cualquiera de los tres pilares de la seguridad de la información. Y para esto existen una serie de metodologías que incluyen guías para la ejecución de pruebas de vulnerabilidades y de penetración de manera controlada con el fin de tener un panorama completo del estado de seguridad de las aplicaciones o activos de la organización.

En el mercado existen muchas metodologías diferentes que pueden ser usadas como guía para pruebas de tipo Ethical hacking, sin embargo, la metodología OWASP incluye no solo la guía para la ejecución de la prueba, sino que además presenta una serie de recomendaciones donde se involucran todas las fases de una aplicación web, desde el desarrollo, las pruebas y la administración de estas. Además, OWASP presenta su Top 10 de vulnerabilidades, uno de los marcos de referencia más utilizados y conocidos mundialmente en cuanto a vulnerabilidades se refiere, con este marco es posible focalizar los esfuerzos de gestión de vulnerabilidades y parchado de software en los errores que realmente son una amenaza para la compañía, que presentarían un impacto importante en caso de explotación y que representan un gran riesgo para el normal funcionamiento de la organización.

La ejecución de pruebas de vulnerabilidades y el uso de herramientas de exploración de la red se hace mucho más efectiva cuando se utiliza un marco de referencia como OWASP donde se presenta la información de manera ordenada y concreta, con una determinación precisa del alcance, las herramientas y la metodología que se debe usar durante la prueba y con la construcción de informes que permiten tener el detalle técnico de la información para la posterior construcción de un plan de trabajo enfocado en la mitigación de las vulnerabilidades críticas determinadas por el Top 10 de OWASP y adicionalmente la construcción de un informe ejecutivo que permite exponer los puntos críticos encontrados a la gerencia para una mayor comprensión del estado de seguridad que permita justificar los esfuerzos estratégicos y económicos de la compañía en la mitigación de los riesgos potenciales de seguridad encontrados.

8. CONCLUSIONES

La planeación de una prueba de penetración juega un papel vital para el éxito de esta, es en la fase de planeación donde se consideran todas las variables y donde se generan las autorizaciones de la compañía que hacen de la prueba de penetración una prueba ética, donde se exploran las vulnerabilidades de forma legal y se realiza una explotación controlada.

Realizar pruebas de vulnerabilidades periódicamente es una herramienta potente respecto a la posición de seguridad de los sistemas informáticos de la compañía, esto ayuda a identificar las vulnerabilidades y a determinar el riesgo al que estas vulnerabilidades exponen los sistemas. La informática es dinámica, cambiante y evoluciona día a día, por lo tanto, el esfuerzo para asegurar los sistemas debe ser constante y permanente.

Los marcos de referencia y las metodologías para realización de pruebas de penetración son una guía que ayudan a que el desarrollo de la prueba desde la planeación hasta la entrega de resultados se realice de manera eficiente, con el fin de atacar todos los frentes posibles o los que son de mayor interés para la organización que se está analizando.

El top 10 de OWASP es una guía clara con el listado de las vulnerabilidades que según sus encuestas anuales afectan a más compañías o pueden ser explotadas fácilmente, por lo que generan riesgos importantes para las organizaciones. Este top 10 ayuda a enfocar los esfuerzos y los planes de mitigación de vulnerabilidades en los hallazgos con mayor probabilidad de ocurrencia o mayor impacto para el correcto funcionamiento de los procesos vitales de la compañía.

9. CRONOGRAMA

El siguiente es el cronograma del desarrollo de la presente monografía.

Tabla 2 Cronograma de la monografía

Actividades	Mes1				Mes2				Mes3				Mes4			
Semanas	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Analizar las ventajas y desventajas de las diferentes metodologías para pruebas de penetración para diagnosticar vulnerabilidades																
• Investigar sobre metodologías para pruebas de penetración																
• Analizar las metodologías investigadas																
• Comparar las metodologías encontradas.																
• Plantear las ventajas y desventajas de OWASP																

Realizar una comparación entre el marco de referencia de vulnerabilidades de OWASP y otros proyectos de seguridad con marcos de referencia para el análisis de vulnerabilidades de aplicaciones web.																
• Investigar sobre el Top 10 de OWASP																
• Investigar sobre el Top 25 de SANS																
• Identificar las ventajas de cada marco de referencia.																
Diseñar un ambiente controlado para realizar pruebas de penetración y demostrar la efectividad del marco de referencia para vulnerabilidades de OWASP																
• Configurar un servidor con una aplicación Web básica																
• Montar una máquina virtual con Kali Linux para exploración de vulnerabilidades																

• Realizar prueba de penetración con las herramientas de Kali																
• Analizar y recopilar los resultados encontrados																
Recopilar todos los resultados encontrados y las conclusiones de la investigación en un estudio monográfico																
• Organizar la información recopilada																
• Crear documento en Word con toda la información																
• Asesoría con director de proyecto																
• Ajuste de normas NTC al documento																
• Correcciones al documento final																
• Verificación de Derechos de autor en Turnitin																

• Asesoría con director de proyecto																
• Ajuste de cronograma y creación de conclusiones																
• Aval de proyecto																

10. BIBLIOGRAFÍA

ASCENCIO MENDOZA Martha y MORENO PATIÑO Pedro Julian. Desarrollo de una propuesta Metodológica para Determinar la Seguridad en una Aplicación Web. {En línea}. 2011. {Revisado en abril 2018} Disponible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2511/0058A811.pdf?sequence=1.

BALANTA Heidy. El Teletrabajo y su impacto en el medio ambiente. {En línea}. 2012. {Revisado en abril 2018} Disponible en: https://colombiadigital.net/actualidad/articulos-informativos/item/1938-el-teletrabajo-y-su-impacto-en-el-medio-ambiente.html

BOGOTÁ D.C. Alcaldía Mayor. Ley 1273 de 2009 Nivel Nacional. {En línea}. 2009. {Revisado en junio 2018} Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

CUNNINGHAM Ward. The WyCash Portfolio Management system. {En línea} 1992. {Revisado en noviembre de 2018} Disponible en: http://c2.com/doc/oopsla92.html

DASWANI Deepak. Ciberseguridad en 2018: Tendencias y Amenazas. {En línea}. 2018. {Revisado en abril 2018} Disponible en: https://www.imf-formacion.com/blog/tecnologia/ciberseguridad-2018-tendencias-amenazas-201801/

DOJO Kali Linux, RELEASES Kali Linux. Kali Linux 2.0 Release. Our Next Generation Penetration {En línea}. 2015. {Revisado en abril 2018} Disponible en: https://www.kali.org/releases/kali-linux-20-released/

EC-Council. Certified Ethical Hacker Certification. {En línea} 2015. {Revisado en octubre 2018} Disponible en: https://www.eccouncil.org/programs/certified-ethical-%20hacker-ceh/

ECURED. Arquitectura Cliente Servidor. {En línea}. 2018. {Revisado en marzo 2018} Disponible en: https://www.ecured.cu/Arquitectura_Cliente_Servidor

EQUIPO Editorial. Infografía: Seguridad Digital ¿Cómo aprovecharla en las organizaciones? {En línea}. 2015. {Revisado en mayo 2018} Disponible en: http://reportedigital.com/seguridad/infografia-seguridad-digital-como-aprovecharla-organizaciones/

ESET Enjoy Safer Technology. {En línea} 2017. {Revisado en agosto 2018}. Disponible en https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

ESPITIA Diego Samuel. Los beneficios y la importancia de gestionar la seguridad de la información. {En línea}. 2015. {Revisado en abril 2018} Disponible en: https://reportedigital.com/seguridad/importancia-gestionar-seguridad-informacion/

FORBES. 7 beneficios del e-comarca en las empresas. {En línea}. 2014. {Revisado en febrero 2018} Disponible en: https://www.forbes.com.mx/7-ventajas-que-tu-empresa-debe-saber-sobre-el-e-commerce/

GARZAS Javier. La deuda técnica. Todo el mundo debería saber que la mala calidad software al final se paga. {En línea}. 2012. {Revisado en agosto 2018} Disponible en: http://www.javiergarzas.com/2012/11/deuda-tecnica-2.html

GIOINO Mauro y BORGHELLO Christian. Modelado de Amenazas. 1.5 Beneficios. {En línea} 2014. {Revisado en octubre 2018} Disponible en: https://www.owasp.org/index.php/Modelado_de_Amenazas#Beneficios

GOBIERNO de España. Vulnerabilidades de un sistema Informático. {En línea} 2016. {Revisado en febrero 2018} Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

HERZOG Pete. Open Source Security Testing Methodology Manual (OSSTMM). {En línea} 2016. {Revisado en noviembre 2018} Disponible en: http://www.isecom.org/research/osstmm.html

IBM. Informe SANS/CWE Top 25 Most Dangerous Programming Errors v1.03. IBM {En línea} 2017. {Revisado en noviembre 2018} Disponible en: https://www.ibm.com/support/knowledgecenter/es/SSW2NF_9.0.1/com.ibm.ase.help.doc/topics/r_sans_cwe_top25_report.html

INC Web Hosting. Riesgos y Amenazas en la Seguridad Web. {En línea}. 2018. {Revisado en marzo 2018} Disponible en: https://www.inc.cl/blog/sitio-web/riesgos-y-amenazas-en-la-seguridad-web

Informática para tu Negocio. La Evolución de la Informática en la Gestión Empresarial. {En línea} 2016. {Revisado marzo 2018} Disponible en: https://www.informaticaparatunegocio.com/blog/la-evolucion-la-informatica-la-gestion-empresarial/

MORALES Ricardo. Lenguajes de programación: ¿Qué son y para qué sirven? {En línea}. 2014. {Revisado en abril 2018} Disponible en: https://colombiadigital.net/actualidad/articulos-informativos/item/7669-lenguajes-de-programacion-que-son-y-para-que-sirven.html

NEOSOFT. ¿Qué es una aplicación Web? {En línea}. 2018. {Revisado en abril 2018} Disponible en: https://www.neosoft.es/blog/que-es-una-aplicacion-web/

NESSUS Professional. Whit Vulnerabilities, Seeing is believing. {En línea} 2015. {Revisado en abril 2018}. Disponible en: https://www.tenable.com/products/nessus/nessus-professional

OFFENSIVE Security. Offensive Security Training, Certifications and Services. {En línea} 2015. {Revisado en septiembre 2018} Disponible en: https://www.offensive-security.com/

OISSG. Information Systems Security Assessment Framework (ISSAF). {En línea} 2016. {Revisado en octubre 2018} Disponible en: http://www.oissg.org/issaf.html

[1] OWASP Fundation. Guía de Pruebas OWASP {En línea}. 2008 {Revisado en marzo 2018}. Disponible en https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf

OWASP Latam Tour 2015. Hacking Ético: Cacería de Vulnerabilidades. {En línea}. 2015. {Revisado en octubre 2018} Disponible en: http://docplayer.es/3407409-Hacking-etico-caceria-de-vulnerabilidades-owasp-latam-tour-2015.html

OWASP. Análisis de Riesgos Aplicando la Metodología OWASP. {En línea} 2017. {Revisado en septiembre 2018]. Disponible en: https://www.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf

OWASP. OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks. {En línea} 2017 {Revisado en febrero 2018} Disponible en https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

OWASP. OWASP Top 10 – 2017 Los diez riesgos más críticos en Aplicaciones Web. {En línea} 2017. {Revisado en noviembre 2018} Disponible en: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

PIENSA Solutions. Principales lenguajes de programación para el desarrollo web. {En línea} 2017. {Revisado en mayo 2018} Disponible en: https://www.piensasolutions.com/blog/principales-lenguajes-programacion-web/

POLICIA Nacional. Informe: Balance de Cibercrimen en Colombia 2017. {En línea}. 2017. {Revisado en agosto 2018} Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

PONFERRADA LÓPEZ Javier. ¿Qué es footpirinting y fingerprinting? {En línea}. 2015. {Revisado en mayo 2018} Disponible en: http://www.ticarte.com/contenido/que-es-footprinting-y-fingerprinting

RODRIGUEZ Nacho. OWASP: Creando aplicaciones seguras. {En línea}. 2011. {Revisado en febrero 2018} Disponible en: https://www.genbetadev.com/seguridad-informatica/owasp-creando-aplicaciones-seguras

SALAZAR T Edgar D. Pruebas de Seguridad en Aplicaciones web según OWASP. ¿Dónde estamos… Hacía dónde vamos? {En línea} 2016. {Revisado en agosto 2018} Disponible en: https://www.owasp.org/images/2/2f/OWASP_SUSCERTE.pdf

SANS. CWE/SANS Top 25 Most Dangerous Software Errors. {En línea} 2017. {Revisado en noviembre 2018} Disponible en: https://www.sans.org/top25-software-errors

SGSI. ISO 27001: ¿Qué beneficios nos aporta implantar esta norma? {En línea}. 2016. {Revisado en mayo 2018} Disponible en: https://www.pmg-ssi.com/2016/07/iso-27001-beneficios-aporta-implantar-esta-norma/

SGSI. La norma ISO 27001:2013 ¿Cuál es su estructura? SGSI {En línea} 2015. {Revisado en mayo 2018} Disponible en: https://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/

TALENS-OLIAG Sergio. Seguridad en el Desarrollo de aplicaciones. {En línea}. 2004.{Revisado en febrero 2018} Disponible en: https://www.uv.es/sto/charlas/SDA/SDA.pdf

TECNÓSFERA. A diario se bloquean más de 20.000 aplicaciones móviles maliciosas. {En línea}. 2018. {Revisado en marzo 2018} Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-de-amenazas-informaticas-en-2017-208618

UNITEL Soluciones e Infraestructuras Tecnológicas. Amenazas Informáticas de Seguridad: Seguridad ante Amenazas, más que un servicio, una solución. {En línea} 2017. {Revisado en febrero de 2018}. Disponible en: https://unitel-tc.com/amenazas/

VINDEL AMOR Rafael. Introducción a OWASP. {En línea} 2016. {Revisado en agosto 2018} Disponible en: https://www.adictosaltrabajo.com/tutoriales/introduccion-a-owasp/