**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Seguridad de aplicaciones web |
| --- | --- |

| COMPETENCIA | 220501111. Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501111-01 - Clasificar indicadores, métricas y alcance de seguimiento de la seguridad web según normas y estándares. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF05 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Artefactos de seguridad para el monitoreo de seguridad orientada a aplicaciones Web |
| BREVE DESCRIPCIÓN | En esta última década el avance tecnológico impulsó a las empresas a trasladar buena parte de sus actividades y servicios hacia el mundo digital por medio de la sistematización de sus procesos a través de la creación de aplicaciones web. Sin embargo, pese a las ventajas adquiridas, también se contraen sus principales desventajas ligadas a los ataques cibernéticos, virus y demás afectaciones posibles del mundo software.  Es por ello, que el área dedicada a la seguridad web se ha convertido en uno de los temas de mayor interés para los expertos y profesionales de las tecnologías alrededor del planeta. Dentro de esta temática, un proceso importante radica en la detección temprana de vulnerabilidades por monitoreo o sondeo de aplicaciones, tema que será abordado a continuación. |
| PALABRAS CLAVE | Aplicaciones Web, Indicadores, Métricas, OWASP, Seguridad |

| ÁREA OCUPACIONAL | 2 - CIENCIAS NATURALES, APLICADAS Y RELACIONADAS |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS:**

**Introducción**

* + - 1. **Seguridad en Aplicaciones Web**
      2. **Fases para la adopción de un Plan Estratégico de Seguridad en Aplicaciones Web**

2.1 Identificación del estado actual de la Seguridad en Aplicaciones Web.

2.2 Definición de los objetivos de la Seguridad en Aplicaciones Web.

2.3 Determinación del estado deseado de la Seguridad en Aplicaciones Web.

2.4 Definición de los Indicadores en Aplicaciones Web.

2.5 Definición de Métricas de la Seguridad.

**3.** **Ejecución del Plan Estratégico de la Seguridad en Aplicaciones Web.**

* 1. Herramientas de Monitoreo de Seguridad en Aplicaciones Web**.**

3.2 El marco de conocimiento de seguridad (Security Knowledge Framework).

3.3. Medición de tráfico

**B. INTRODUCCIÓN**

Le damos la bienvenida al componente formativo denominado “Artefactos de seguridad para el monitoreo de seguridad orientada a aplicaciones Web”, el cual hace parte del programa de formación Técnico en “Seguridad en aplicaciones web”, para lo cual se invita a observar el siguiente video:



**C. DESARROLLO DE CONTENIDOS:**

1. **Seguridad en Aplicaciones Web**

Las últimas décadas presenciaron la masificación de internet y los dispositivos inteligentes trayendo consigo el estallido de las aplicaciones sociales y la era de la conexión total, esta revolución, generó un sinnúmero de acontecimientos que modificaron la forma como las personas ven los dispositivos o herramientas tecnológicas; puesto que, ahora se le da mayor prioridad a las cuentas, usuarios y contactos por encima del hardware, dado que este, es fácil de cambiar o mejorar por un nuevo dispositivo.

Esto indica que para las personas el activo más importante es su información personal y esta premisa es un común denominador que se extiende a las organizaciones y empresas, puesto que, dicha información es sensible y vital para el buen desarrollo de las actividades diarias, de los procesos pertinentes y en la prestación de sus servicios. Esto claramente indica la innegable dependencia de la tecnología y del activo informático, siendo los soportes claros de los sistemas de una organización. No obstante, no ha sido siempre de esta manera.

Años atrás para las empresas era más sencillo proteger sus activos, ya que las grandes plataformas de datos se encontraban aisladas e independientes de conectividad a la red, usando arquitecturas centralizadas con terminales con capacidades de procesamiento muy limitadas. Empero, actualmente, la diversificación de las redes de telecomunicaciones y la masiva creación de plataformas externas hacen que la información organizacional quede cada vez más expuesta a todas las ciberamenazas y ataques informáticos (V. Mouli and K. P. Jevitha, 2016), en vista de que cualquier dispositivo conectado a internet es un foco sensible al ataque por las latentes vulnerabilidades, como un diseño inicial inadecuado, la ejecución de programas que pueden presentar rutinas de código realizadas con desidia y descuido, escasa implementación de medidas de control de acceso, falta de validación y verificación de datos de ingreso o inclusive el riesgo más latente originado por el error humano que es la ingeniería social (M. Seyyar, F. Çatak and E. Gül, 2018).

En (OWASP. Top Ten, 2022) es posible apreciar con mayor claridad las amenazas y vulnerabilidades más importantes a día de hoy para las organizaciones y sus aplicaciones web; a través del esfuerzo colaborativo global conocido como el ***Proyecto Abierto de Seguridad en Aplicaciones Web*** (**OWASP, Open Web Application Security Project**), que busca concientizar a los equipos de desarrollo y los gerentes de proyectos la importancia de proteger sus activos informáticos con la generación de procesos que estimen el nivel de seguridad de sus sistemas, de manera que sea posible tomar decisiones y medidas preventivas ante una ciberamenaza o una eventualidad.

Es así como:



El área de ciberseguridad, como eje transversal a la empresa debe crear o fortalecer los procesos de control y protección a todas las demás áreas de la organización, a fin de garantizar integridad, confidencialidad y la seguridad de su información y la de sus clientes. (A. Pineda, John A. Bohada y M. L. Pineda, 2018).

* **Plan Estratégico de Seguridad en Aplicaciones Web.**

En (R. Rodriguez, H. Alberto, 2019) se describe el concepto de estrategia corporativa como: “***el patrón de decisiones en una compañía, que determina y revela sus objetivos, propósitos o metas; que genera las principales políticas y planes para alcanzar dichas metas y define el rango de negocio que debe perseguir la compañía, el tipo de organización económica y humana que es o pretende ser y la naturaleza de la contribución tanto económica, como no económica, que pretende hacer a sus accionistas, empleados, clientes y comunidades***”. y en parte esta idea puede ser transferida al contexto de un plan estratégico de seguridad en aplicaciones web.



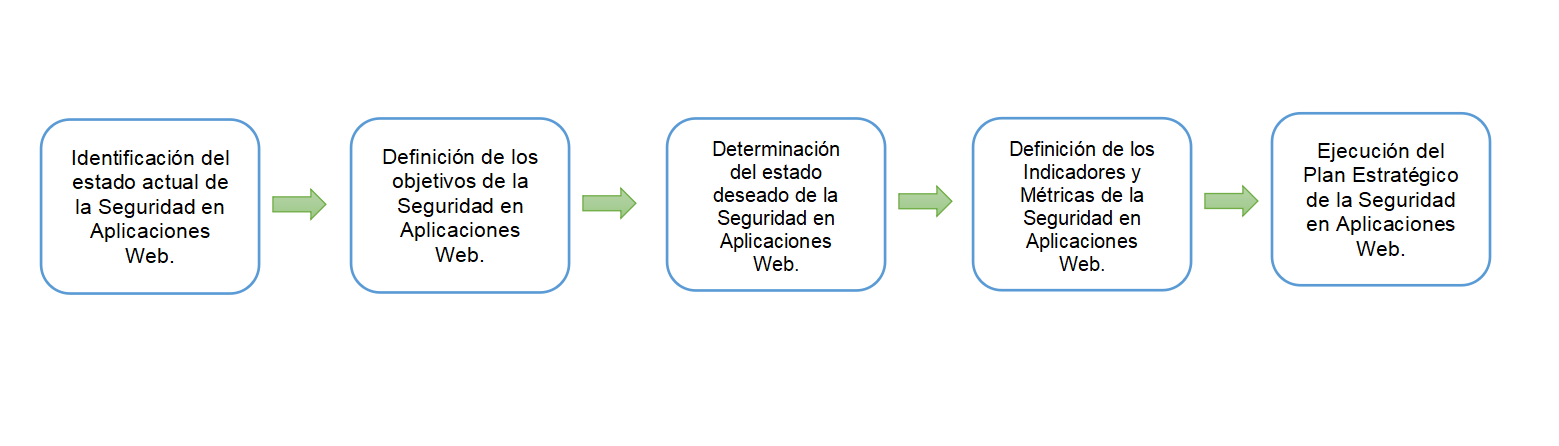
El trazado de una estrategia debe estar definido y alineado a un alto nivel con los objetivos de la organización y la operación del negocio. Por tanto, las pautas que se presentan a continuación son de común acuerdo entre la alta dirección y el equipo TI o los encargados del área de ciberseguridad; determinando el nivel de verificación de seguridad de aplicaciones al que desean llevar el sistema. Para ello, esta estrategia establece la base del plan de acción a ejecutar, permitiendo llevar el proceso de seguridad de las aplicaciones web desde el nivel actual hasta el nivel de madurez deseado. Dentro del plan de acción es apremiante conocer el personal y los recursos hardware y software disponibles, además de identificar las limitaciones existentes a nivel de conocimiento, posibilidad de adquisiciones, alcance y considerando un apartado para los requerimientos legales y regulatorios. Además, el plan estratégico debe establecer mecanismos de monitoreo y métricas bien definidas para determinar al final si el cambio en el nivel de verificación representa un éxito o un fracaso en el proceso.

El plan estratégico de seguridad en aplicaciones web debe establecer como mínimo los siguientes elementos abordados a continuación:

* Un objetivo: Lo que se busca alcanzar a través de la ejecución de la estrategia.
* Acciones: Actividades a ejecutar para cumplir con lo definido en la estrategia.
* Resultados: Lo que se espera obtener de esas acciones que permiten cumplir con el objetivo propuesto.
* Tiempos: Periodo en el cual se debe ejecutar la estrategia.
* Indicadores: Una forma de medir y proporcionar una evaluación a los resultados.
* Métricas: El rendimiento real medido por los datos de manera cuantitativa.
* Niveles: El estado del sistema antes y después de la ejecución de la estrategia.
  + - 1. **Fases para la adopción de un Plan Estratégico de Seguridad en Aplicaciones Web**

**Figura 1**

Fases para la adopción de un Plan Estratégico de Seguridad en Aplicaciones Web



A continuación, se describe el objetivo de cada fase, los artefactos de entrada, de salida y actividades a ejecutar para cumplir cada uno de ellos.

* 1. **Identificación del estado actual de la Seguridad en Aplicaciones Web**

El primer paso para generar un plan estratégico consiste en identificar el estado actual en el que se encuentra la seguridad en aplicaciones web; para ello es posible utilizar dos enfoques: a partir de un modelo de madurez o por los niveles ASVS que verifican la seguridad en sistemas web. El enfoque por madurez requiere de un proyecto base que permita generar el contraste y el punto de partida, por ello el enfoque basado en los niveles permite iniciar el plan a partir del esfuerzo en conjunto de la dirección general y los equipos relacionados con TI siguiendo el marco de referencia ofrecido por el OWASP y sus comunidades. Para ello se tienen los siguientes artefactos de entrada, salida y las actividades en esta fase:



* **Niveles de verificación de seguridad de aplicaciones Web**

El ASVS ha definido tres niveles de verificación en los cuales se aumenta la profundidad de los conceptos con cada nivel superado y estos contienen una lista de requisitos intrínsecos que garantizan la ciberseguridad correspondiendo a una funcionalidad o un grupo de ellas orientadas netamente al tema en cuestión, las cuales deben ser implementadas por los equipos de desarrollo de software. Los niveles son los siguientes:

* **Nivel 1 (Oportunista)**: El nivel base no distingue software puesto que sirve para todos los sistemas.
* **Nivel 2 (Estándar)**: Se encuentra conducido para aplicaciones que dentro de su operación manejan datos sensibles que requieren un nivel de protección.
* **Nivel 3 (Avanzado)**: Este nivel es para sistemas críticos encargados de realizar transacciones de alto valor o dentro de su información existen datos personales sensibles y confidenciales, que son el más alto nivel de confianza.

A continuación se profundiza en qué consiste cada nivel:



* + **Ejemplos en la Industria**

Como se apreció anteriormente las diferentes amenazas son motivadas por distintos factores y propósitos, puesto que existen algunos sectores en la industria con activos de información únicos y valiosos para los atacantes, los cuales podrían causar gran conmoción con su revelación o simplemente a partir de ellos es podrían obtener beneficios de cualquier índole, obligando explícitamente a estas organizaciones a cumplir con regulaciones y normas específicas.

No obstante, es claro que cada sector posee criterios únicos y bien diferenciados en cuanto a las amenazas y vulnerabilidades presentes, es común en todos los segmentos de la industria encontrar ataques oportunistas. En este tipo se busca cualquier sistema que se encuentre en un estado vulnerable para explotar sus debilidades de una manera rápida y sencilla. Por lo que el rango oportunista se recomienda para todas las aplicaciones y debe ser el punto base para manejar las amenazas más habituales de encontrar. A continuación, se identifican algunas recomendaciones para cada nivel en diferentes sectores de la industria:



* 1. **Definición de los objetivos de la Seguridad en Aplicaciones Web**

La segunda fase en el plan estratégico consiste en definir y acordar el alcance a través de unos objetivos claros alineados a los objetivos de la organización. Puesto que, la compañía actúa como *stakeholder* buscando que el plan presentado satisfaga las necesidades establecidas por la gerencia y permitan mejorar sustancialmente sus procesos con un nivel de verificación superior en sus aplicaciones. En seguida se aprecian los artefactos de entrada, salida y las actividades en esta fase:



* 1. **Determinación del estado deseado de la Seguridad en Aplicaciones Web**

En esta fase del plan estratégico se establece el nivel de verificación al que se aspira llegar en cuanto a seguridad de las aplicaciones web. Teniendo presente las listas de chequeo recopiladas en el paso previo, los objetivos definidos plenamente por las partes interesadas, las limitaciones a las que se enfrenta la organización y el análisis del estado actual en materia de seguridad en aplicaciones web. A continuación, se presentan los siguientes artefactos de entrada, salida y las actividades en esta fase:



* 1. **Definición de los Indicadores en Aplicaciones Web**

Esta fase es vital en el plan estratégico de seguridad en aplicaciones web debido a que le proporciona a los interesados la manera correcta de cuantificar el rendimiento real del sistema después de realizar un plan estratégico de seguridad en aplicaciones web; permitiéndole a la gerencia un punto de referencia en la toma de decisiones, en las oportunidades de mejora o en el proceso de pivotar la dirección de los objetivos trazados por la corporación para lograr ventajas competitivas.

Dentro de esta etapa se definen cuatro importantes actividades que al final permiten gestar un paquete de métricas para implementar. Para este paso se establecen los siguientes artefactos de entrada, salida y las actividades:



* + - * 1. **Lista de Chequeo Requisitos de seguridad en Aplicaciones Web**

Para conseguir los indicadores y sus métricas es necesario conocer los requisitos de seguridad que se pretenden verificar en una aplicación web, es por ello que se presenta a continuación una lista de estos, basado en la propuesta del **ASVS** en su versión 4.0. **(**OWASP. 2021)**.**

* 1. **Arquitectura, Diseño y Modelado de amenazas**

Se coloca al inicio de todos los requisitos por analizar debido al papel fundamental que juega el diseño, el modelado y la arquitectura para cualquier sistema software, puesto que, este define la estructuras que componen la aplicación y la forma como se comunican entre ellas, para tener la capacidad de satisfacer los atributos de calidad del sistema. Es por ello que para este elemento se debe asegurar que se cumplan estos requisitos:



* 1. **Autenticación**

El siguiente requisito en ser verificado es el mecanismo de inicio y control del estado de la sesión de un usuario a través del método de autenticación. Este proceso es el punto de entrada a la aplicación en consecuencia asegurar este componente es la principal tarea del equipo de TI. Por este motivo, para la autenticación se debe controlar que:



* 1. **Control de acceso**

Este requisito consiste en el mecanismo que autoriza el acceso y uso de los recursos acorde con los permisos del solicitante. Teniendo en cuenta esto, es obligatorio que se valide que:



* 1. **Manejo de entrada de datos maliciosos**

Otro requisito sensible en la seguridad de las aplicaciones web consiste en la validación de entrada de datos maliciosos al sistema provenientes de ataques oportunistas desde el mismo usuario de la aplicación. Esta debilidad permite la ejecución de distintos ataques al sistema de ficheros, ataques como inyección de intérprete, ***cross-site scripting (XSS),*** ataques ***locale/Unicode,*** inyección de SQL y desbordamientos de búferes. Por lo cual es necesario validar que para este elemento se validan que:



* 1. **Criptografía en el almacenamiento**

Esta verificación hace referencia a la importancia del encriptamiento de los datos más sensible dentro de una aplicación; es por ello que el sistema debe asegurar que se cumplan con:



* 1. **Gestión y registro de errores**

La gestión y registro de errores en log, tiene como objetivo proporcionar un mecanismo reactivo de respuesta a incidentes para los usuarios, administradores y equipos de TI, creando registros de log bastante significativos para los desarrolladores proporcionando datos útiles y sin agregar ruido innecesario. Los datos almacenados en el log deben presentar una cobertura acorde a las reglamentaciones y leyes dispuestas por el país ante los temas de privacidad de la información o directivas similares y se debe garantizar que se gestiona de forma segura. Es por ello que la aplicación debe contar con:



* 1. **Protección de Datos**

Este requisito de verificación se centra en la confidencialidad, integridad y disponibilidad de los datos, teniendo presente que esto se aplica en un servidor de aplicaciones lo que permite asumir que posee protecciones confiables y suficientes. Sin embargo, un sistema debe comprender que todos los dispositivos de los usuarios pueden comprometer la seguridad de alguna forma en el proceso de transmisión de información, por lo que es responsabilidad de la aplicación que los datos persistidos en algún dispositivo esté cifrado y sea complicado o imposible obtenerlo, alterarlo o divulgarlo. A continuación se identifican los por menores que debe cumplir en temas de protección de datos:



* 1. **Seguridad de las Comunicaciones**

Para el elemento de seguridad de las comunicaciones es obligatorio que se cubran los requisitos siguientes:



* 1. **Configuración de seguridad HTTP**

La configuración de seguridad HTTP necesita asegurar lo siguiente:



* 1. **Controles Maliciosos**

El requisito de control malicioso es susceptible de no ser detectado con facilidad, puesto que debe ser revisado minuciosamente el código fuente por un experto en el tema de forma manual para detectar bombas lógicas alojadas en alguna línea indetectable a simple vista. Por ello, En este se deben satisfacer los elementos de alto nivel presentados a continuación:



* 1. **Lógica de negocios**

Para este requisito de verificación se necesita satisfacer las siguientes características:



* 1. **Archivos y recursos**

Para los archivos y recursos se deben remediar los requisitos tales como:



* 1. **Servicios Web.**

Es necesario que la aplicación verifique que al utilizar servicios web **REST** o **SOAP** mantenga:



A partir de los anteriores requisitos el equipo TI puede plantear la selección de ciertos KPI y métricas que luego serán validadas y aprobadas por los interesados; que le permitan posteriormente a la gerencia identificar si el plan estratégico de la seguridad en aplicaciones web ha impactado positivamente los procesos y los sistemas aportando a los objetivos del negocio.

* **Indicadores Claves de Rendimiento** (**KPI, Key Performance Indicator**)

Para afirmar que un proceso, servicio o producto mejora durante la ejecución de un plan, es necesario que existan mediciones que permitan evaluar, comparar y contrastar resultados a fin de respaldar esta declaración (G. V. Ríos, John A. Bohada e I. A. Delgado, 2018). Por esta razón el área de TI durante la fase de “*Definición de los Indicadores y Métricas de la Seguridad en Aplicaciones Web”,* del plan estratégico debe centrar sus esfuerzos en identificar los KPI y las métricas asociadas a ellos para brindar a los ***stakeholders*** un conjunto de herramientas e información puntual que les permitirá tomar decisiones y realizar acciones proactivas/reactivas frente a los objetivos del negocio y el direccionamiento estratégico de la organización.

Ahora bien, antes de identificarlos es importante entender y diferenciar un KPI de una métrica para que el proceso de establecer ambos elementos sea exitoso:



Para establecer los KPI para el plan estratégico de seguridad en aplicaciones web que se van a estar monitoreando se pueden seguir algunos consejos simples que lo facilitan:



* 1. **Definición de Métricas de Seguridad en Aplicaciones Web.**

Como se indicó anteriormente los KPI necesitan de ciertas métricas para su confección y refinamiento; sin embargo, está claro que se puede seleccionar cualquier variable de la gran cantidad que pueden generar una programa sobre el ecosistema de temas en seguridad; por esta razón, es pertinente aclarar cómo se debe establecer si una métrica está acorde a lo que se necesita para el plan estratégico de seguridad de las aplicaciones web. Así, las características más sobresalientes de las métricas son:



Si las métricas seleccionadas poseen estas características, permitirán a la corporación comprender de mejor forma los riesgos a los que se pueden enfrentar, las amenazas y problemas emergentes, identificar y aislar las debilidades y tener una evaluación más acertada del desempeño de los controles implementados en materia de seguridad en aplicaciones web; del mismo modo, se crearán oportunidades de mejora y actualización en procesos, herramientas y tecnologías en comparación a los actuales evidenciando el incremento y evolución de la cultura organizacional en materia de seguridad en sistemas.

Las métricas en la temática de ciberseguridad pueden clasificarse de la siguiente manera:



1. **Ejecución del Plan Estratégico de la Seguridad en Aplicaciones Web.**

La última fase del plan estratégico de la seguridad consiste en su ejecución. Para ello se tiene los siguientes artefactos de entrada, salida y las actividades en esta fase:



A recordar:



El plan estratégico propuesto será para las compañías una herramienta de gran utilidad para prevenir atacantes y vulnerabilidades asociadas a las aplicaciones web, gracias a que la implementación de este plan permitirá a los equipos de desarrollo tomar decisiones oportunas ante eventualidades y de esta forma perfeccionar gradualmente los mecanismos de seguridad y de control de los sistemas de las organizaciones.

En el siguiente capítulo se proponen algunas herramientas que brindan al equipo de desarrollo opciones para el monitoreo automatizado de las aplicaciones en temas de seguridad web.

* 1. **Herramientas de Monitoreo de Seguridad en Aplicaciones Web**

En el capítulo anterior se introdujo el estándar de verificación en seguridad en aplicaciones ASVS, el cual puede convertirse para las organizaciones en una hoja de ruta para la verificación de sus sistemas en conjunto con los proyectos abiertos y sin restricciones aprovechándose de su documentación, su código fuente y el manejo de la autenticación al sistema, particularmente para los niveles de verificación estándar y avanzado.

En la gran mayoría de ejercicios de revisión de código y test de penetración todos los hallazgos presentados en el informe que recibe la dirección general se componen exclusivamente de defectos de seguridad; no obstante es necesario incluir cuál es el alcance de la verificación, el resumen detallado de los resultados del nivel de verificación anexando a éste las pruebas que se completaron, las pruebas exitosas y las fallidas, estableciendo además una posible solución a las erradas.

Es por ello que las organizaciones promueven prácticas que mantengan la documentación asociada a las pruebas en formato electrónico, usando imágenes, videos, registros logs, o scripts entre otros. puesto que, esta serie de archivos sirven de hallazgos para los desarrolladores cuando tengan dudas en sus procesos.



How do you know your apps are secure? | Codebots

En este caso se debe tener presente que la industria software madura a un ritmo acelerado y en materia de seguridad en aplicaciones la diferencia entre pruebas manuales y asistidas por herramientas es significativamente mínima. Es por ello, que es importante aclarar que estas herramientas automatizadas simplemente se adaptan para realidades puntuales y no tienen la capacidad de cubrir todos los requerimientos que a día de hoy existen.

A continuación se presentan algunos proyectos de OWASP que utilizan ASVS y proveen una herramienta para los equipos de desarrollo:

* 1. **El marco de conocimiento de seguridad (Security Knowledge Framework)**

La experiencia de la comunidad de OWASP permite identificar que el nivel de seguridad en las aplicaciones web no es significativamente alto para garantizar tranquilidad a las organizaciones. Esto debido a que muchos equipos de desarrollo no dimensionan el riesgo y las vulnerabilidades que pueden ser explotados por los piratas informáticos. Razón por la cual, se decantan por desarrollar un framework utilizando ASVS como guía para crear un sistema que sirva como hoja de ruta desde el primer paso para el desarrollo de aplicaciones seguras.

El OWASP-SKF es una aplicación web de código abierto escrita en el lenguaje de programación ***python*** usando el framework ***Flask*** que le proporciona a los desarrolladores de software una potente herramienta para que aprendan los principios de codificación segura en múltiples lenguajes de programación; entrenandolos en la escritura de código seguro desde la concepción, diseño e implementación de un sistema. La premisa es plantar la semilla de la seguridad en el desarrollador desde el diseño hasta la última etapa del ciclo de vida, a través de una serie de listas de verificación como por ejemplo OWASP- ASVS, OWASP-MASVS y la ejecución de laboratorios y prácticas que permiten explorar los niveles de verificación de seguridad (Security Knowledge Framework, 2022).

* **OWASP ZAP (Zed Attack Proxy)**

 ZAP es un herramienta de código abierto de fácil uso, flexible, extensible y gratuita mantenida por el esfuerzo conjunto del OWASP, que permite realizar pruebas de penetración para aplicaciones web. La aplicación actúa como un proxy ubicándose entre el navegador y el sistema a testear para la búsqueda de vulnerabilidades; con el fin de interceptar e inspeccionar los mensajes enviados entre estos dos y con la disponibilidad de realizar cambios en el contenido de este y re-enviarlo al destino.

Además ofrecen la opción de escaneo automatizado para una gran variedad de niveles de verificación ASVS y contiene otras herramientas para encontrar vulnerabilidades de seguridad manualmente. Esta aplicación ofrece al público versiones para los distintos sistemas operativos y también se puede usar a través de ***docker*;** otras opciones adicionales y complementos son posible descargarlos gratuitamente desde el **ZAP Marketplace.** Por último, la herramienta permite a los desarrolladores usarla como aplicación independiente o como un proceso que corre en background en el sistema operativo. (OWASP Zed Attack Proxy, 2022).

Otro punto importante que vale la pena resaltar es que este proyecto al ser de código abierto permite a los desarrolladores examinarlo sin inconvenientes; dándoles la posibilidad de identificar cómo se implementa alguna funcionalidad. Además ZAP, brinda la opción de trabajar en su proyecto en la corrección de errores, aditamento de funciones o funcionalidades, o creación de complementos para situaciones especiales requeridas.

* **OWASP Juice Shop**

Este proyecto de OWASP consiste en la exposición de una aplicación web moderna y sofisticadam que usa tecnologías actuales como **Node**.**js**, **Express** y **Angular,** pero que presenta una gran cantidad de vulnerabilidades en materia de seguridad; esto con el fin de realizar capacitación en esta materia, demostraciones de fallos y concientización para la comunidad software en general. Además sirve también como Forma, Icono

Descripción generada automáticamenteejemplo para las otras herramientas como **OWASP ZAP,** entre otras.

**Juice Shop** contiene todas las vulnerabilidades del **OWASP Top Ten,** junto a otro gran número de falencias en temas de seguridad que se basan en todos los hallazgos encontrados en aplicaciones web en la comunidad global. Dentro de ella se pueden descubrir gran variedad de ejemplos y desafíos de piratería informática de dificultad variable que el usuario debe explotar; a medida que se avanza con estas dinámicas el progreso se aprecia en un tablero de puntuación.

Como se mencionó anteriormente esta herramienta le puede ayudar a los expertos en el área de seguridad y a los equipos de software como aplicación para adiestrarse y comprobar qué tan bien sus herramientas se adaptan a las interfaces de aplicaciones con gran cantidad de código **JavaScript** y **API REST**. (OWASP Juice Shop 2022).

* **Demos herramientas Juice Shop y OWASP ZAP:**

A continuación, en el siguiente video se presenta una demostración del uso de estas aplicaciones. Antes de empezar con las herramientas es necesario instalar algunos paquetes en el sistema referenciados en este documento (NodeJs, 2022) y (Git, 2022).



Es importante tener presente que en el mercado existe una gran variedad de estas tanto libres y gratuitas como pagadas y de terceros; todas con características especiales que se adaptan a las necesidades de los expertos y las condiciones de las vulnerabilidades a medir dentro de las aplicaciones web.

* 1. **Medición de tráfico de red**

Actualmente es casi imposible para la sociedad pensar en su día a día sin la conexión al internet. La red mundial creció en las últimas décadas a un ritmo increíblemente rápido, lo que produjo un aumento sustancial en el tráfico de datos e información en la red, proveniente en gran medida de los servicios de transmisión, las redes sociales y las aplicaciones web en general (Pries, R, 2009).

Con este panorama las redes deben soportar un aumento en el promedio de carga de tráfico y un cambio errático en los patrones de los datos. Por tanto, las organizaciones y sus equipos de desarrollo necesitan contar con una supervisión y análisis efectivo de todo el tránsito de datos de información; debido a que detectar eventos externos, cuellos de botella, patrones erráticos, actividades maliciosas y/o procesos poco usuales en la red, permite anticiparse de manera oportuna y efectiva a potenciales problemas cuando ocurren o antes de que sucedan. De modo que, los servicios y/o aplicaciones no presenten interrupciones, indisponibilidad, intermitencia o suspensión durante ráfagas o durante largos periodos de tiempo (Xinyu, X., S. Mishra, 2009).

La medición de tráfico es una técnica que supervisa y notifica de manera constante el flujo de datos de la red al equipo de gestión y administración de las aplicaciones y/o servicios cada vez que ocurre un evento. Para realizar dicho monitoreo es posible encontrar en el mercado distintas herramientas que utilizan múltiples técnicas para analizar el tráfico total.

A continuación, se exponen algunos enfoques de monitoreo de red y se presentan algunas herramientas para dicha tarea:

* **Wireshark**

Este proyecto inició su desarrollo en el año 2007 y continúa aún en vigencia exhibiendo una librería de información amplia y con múltiples protocolos de red, permitiendo su ejecución en diferentes sistemas operativos nativos, tales como linux, MacOs o Windows (Dabir, A., A. Matrawy, 2007).

Wireshark captura todos los paquetes del flujo de la red para luego exponerlos completamente en una interfaz gráfica de usuario con metainformación de cada dato analizado, brindándole a los administradores la oportunidad de identificar qué equipo o dispositivo está tratando de interactuar con otro, ofreciendo, además, corroborar si un paquete tiene una estructura correcta o no (Shaoqiang, W., X. DongSheng, y Y. ShiLiang, 2010).

| Esta herramienta posee una función de línea de comandos que recopila paquetes de transmisión, que posteriormente son archivados en disco para un análisis y presentación en la interfaz mencionada anteriormente. La aplicación debe ser ejecutada con un usuario administrador o en su defecto con privilegios, o en consecuencia no será capaz de visualizar las interfaces de red disponibles para análisis y monitoreo. | **Tomado de (Shaoqiang, W., X. DongSheng, y Y. ShiLiang, 2010)** |
| --- | --- |

| La herramienta en la interfaz provee una opción de filtrado por las distintas columnas que presenta directamente; como por ejemplo fuente, destino, protocolo, etc. Es importante detener la captura de paquetes, puesto que si no se realiza Wireshark seguirá analizando el tráfico en modo silencioso, incurriendo en consumo de memoria del sistema.  Si se hace clic en cualquier paquete, se mostrará información detallada sobre el paquete capturado en la mitad inferior de vista. |
| --- |

* **NTOP**

Esta herramienta ofrece una solución para monitorear el tráfico con un nivel sustancialmente alto de visibilidad de los datos, permitiendo realizar un análisis detallado de los protocolos de red y los paquetes transmitidos.

A continuación, se podrá conocer detalles de esta herramienta:



* **Microsoft Message Analyzer**

Esta herramienta creada para el sistema operativo Microsoft contiene entre sus características principales el rastreo en vivo (***Live Trace***) que logra capturar y rastrear el flujo de tráfico de los dispositivos, HTTPS sin cifrar, el tráfico de la capa de enlace local de NDIS, las interfaces remotas de red, el tráfico IPSEC sin cifrado, VPN y acceso directo a red.



* **Paessler Router Traffic Grapher (PRTG)**

Esta herramienta de análisis y rastreo de red que identifica el tráfico que más congestiona el flujo de datos permite prevenir eventos y problemas que se generen por consecuencia de ello. PRTG provee características avanzadas en el descubrimiento automatizado de la red, con un énfasis en la seguridad ya que alerta al usuario ante eventuales fallos o emergencias a través del envío de correo o mensaje de texto.

La aplicación tiene compatibilidad con navegadores, interfaces de usuario de windows y iphone, permitiendo el acceso en cualquier momento y desde cualquier ubicación. Además, le brinda al usuario el monitoreo del ancho de banda de la red y los clientes conectados a la misma, con el plus de indicar con qué propósito se conectan (PRTG, 2022).

PRTG posee más de 200 tipos de sensores para todos los servicios de red comunes, incluidos HTTP, SMTP/POP3 y FTP; admitiendo diferentes protocolos de red para la recolección de la información, tales como: SNMP y WMI, Packet Sniffing, NetFlow, IPFIX, JFlow y SFlow. A continuación, se podrá conocer las características de esta herramienta:



| En esta sección se presentan algunas herramientas que permiten analizar y monitorear el tráfico y el flujo de red, puesto que la carga en promedio de las redes ha aumentado con el paso del tiempo, convirtiendo sus patrones y comportamiento en impredecibles para los administradores; por lo cual, se hace necesario supervisar y rastrear el tráfico para solucionar y resolver problemas de manera efectiva cuando suceden o antes de que puedan ocurrir, de modo que los servicios y aplicaciones no se detengan por largos períodos de tiempo. |
| --- |

**D. SÍNTESIS**

En el siguiente recurso podrá evidenciar un resumen de este componente formativo:



**E. ACTIVIDADES DIDÁCTICAS**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la actividad | Relacionar conceptos. |
| Objetivo de la actividad | Relación de conceptos de artefactos de seguridad para el monitoreo de seguridad orientada a aplicaciones Web |
| Tipo de actividad sugerida | Relacionar conceptos |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo17\_ActividadDidactica1\_CF05 |

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la actividad | Verdadero y Falso. |
| Objetivo de la actividad | Identificación de conceptos de artefactos de seguridad para el monitoreo de seguridad orientada a aplicaciones Web |
| Tipo de actividad sugerida | Verdadero y Falso. |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo18\_ActividadDidactica2\_CF05 |

**F. MATERIAL COMPLEMENTARIO**

| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del recurso o  archivo del documento o material |
| --- | --- | --- | --- |
| 2.5 Definición de Métricas de Seguridad en Aplicaciones Web | *OWASP Security Qualitative Metrics. (s/f). Owasp.Org. Recuperado de https://owasp.org/www-project-security-qualitative-metrics/SECURITY-QUALITATIVE-METRICS* | enlace | <https://owasp.org/www-project-security-qualitative-metrics/SECURITY-QUALITATIVE-METRICS> |
| * 1. El marco de conocimiento de seguridad (Security Knowledge Framework) | *wstg: The Web Security Testing Guide is a comprehensive Open Source guide to testing the security of web applications and web services*. (s/f). | repositorio | <https://github.com/OWASP/wstg> |
| 3.2 El marco de conocimiento de seguridad (Security Knowledge Framework) | Pereira, C. P. T.-D. [DavidPereira]. (2021, marzo 4).*Curso de Pentesting a Aplicaciones WEB (Video 1) OWASP Juice Shop.* Youtube. https://www.youtube.com/watch?v=6eAJ1dinee0 | enlace | <https://www.youtube.com/watch?v=6eAJ1dinee0&t=690s> |
| * 1. El marco de conocimiento de seguridad (Security Knowledge Framework) | Tech, T. [TaggartTech]. (2021, septiembre 8). *#AttackOnTuesday | OWASP ZAP/Juice Shop*. Youtube. https://www.youtube.com/watch?v=4CNWTkAbT4o | enlace | <https://www.youtube.com/watch?v=4CNWTkAbT4o&t=801s> |
| * 1. El marco de conocimiento de seguridad (Security Knowledge Framework) | UskoKruM [UskoKruM2010]. (2021, agosto 19). *Cómo Descargar e Instalar Node.js en Windows 10 | Explicación Sencilla.* Youtube. https://www.youtube.com/watch?v=ipmhBYqIP44 | enlace | <https://www.youtube.com/watch?v=ipmhBYqIP44&t=4s> |
| * 1. El marco de conocimiento de seguridad (Security Knowledge Framework) | Eber, D. [donEber]. (2021, junio 17). Instalación de Git en Windows paso a paso | [2021| 2022]. Youtube. https://www.youtube.com/watch?v=cYLapo1FFmA | enlace | <https://www.youtube.com/watch?v=cYLapo1FFmA&t=2s> |

**G. GLOSARIO**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| API Endpoints | Son las URLs de un API o un backend que responden a una petición. |
| API REST | Es una arquitectura que permite la interacción con los servicios web de RESTful. |
| Aplicaciones POS | Son un tipo de programas destinados a sistematizar el control de ventas e inventarios del punto físico de un negocio. |
| Ataques Oportunistas | Es un tipo de ataque a un sistema software que aprovecha algún punto vulnerable que no ha sido identificado previamente. |
| Bearer Token | Es un token de acceso seguro que contiene las credenciales de seguridad para la gestión de la sesión e identificación del usuario. |
| Bombas lógicas de tiempo | Es un ataque malicioso programado a una fecha precisa a los sistemas. |
| Cámara de Compensación Automatizada (ACH) | Es un tipo de tecnología que permite procesar transacciones entre bancos y otras instituciones financieras. |
| Indicadores Claves de Rendimiento (KPI) | Es una medida del nivel de rendimiento o desempeño de un proceso. |
| Ingeniería social | Es una práctica ilegal que consiste en obtener información privada o confidencial a través de la manipulación de las personas y sus cuentas de usuario. |
| WYSIWYG | Lo que ves es lo que tienes *(What You See Is What You Get )*, esto se aplica a los procesadores de texto y otros editores de texto con formato que permiten escribir un documento mostrando directamente el resultado final. |

H. **REFERENCIAS BIBLIOGRÁFICAS**

Eber, D. [donEber]. (2021, junio 17). *Instalación de Git en Windows paso a paso | [2021| 2022]*. Youtube. https://www.youtube.com/watch?v=cYLapo1FFmA

G. V. Ríos, John A. Bohada e I. A. Delgado, “Gestión de seguridad de la información en las organizaciones”, en Investigación e Innovación en Ingeniería del Software. Medellín: Tecnológico de Antioquia, vol. 2, 2018, pp. 111-121.

Git. [En línea] 17 de mayo de 2022. [Citado el: 17 de mayo de 2022.]

<https://git-scm.com/download/win>

M. Seyyar, F. Çatak and E. Gül, “Detection of attack-targeted scans from the Apache HTTP Server access logs”, Appl. Comput. Inf., vol. 14, N.º 1, pp. 28-36, 2018.

NodeJs. [En línea] 17 de mayo de 2022. [Citado el: 17 de mayo de 2022.]

<https://nodejs.org/es/download/>

Pereira, C. P. T.-D. [DavidPereira]. (2021, marzo 4). *Curso de Pentesting a Aplicaciones WEB (Video 1) OWASP Juice Shop*. Youtube. https://www.youtube.com/watch?v=6eAJ1dinee0

R. Rodriguez, H. Alberto. “The Concept of Corporate Strategy. Innovar: Revista de Ciencias Administrativas y Sociales”. 19, 2009.

S. A. Pineda, John A. Bohada y M. L. Pineda, “Ingeniería Social en Instituciones de Educación Superior”, Revista Colombiana de Tecnologías de Avanzada, vol. 2, N.º 32, pp. 52-61, 2018.

Security Knowledge Framework. [En línea] 15 de mayo de 2022. [Citado el: 15 de mayo de 2022.] <https://owasp.org/www-project-security-knowledge-framework/>

OWASP. 2021. [En línea] 11 de mayo de 2022. [Citado el: 11 de mayo de 2022.] <https://owasp.org/>

OWASP. Top Ten. [En línea] 10 de mayo de 2022. [Citado el: 10 de mayo de 2022.] <https://owasp.org/www-project-top-ten/>

OWASP Zed Attack Proxy (ZAP). [En línea] 15 de mayo de 2022. [Citado el: 15 de mayo de 2022.]

<https://owasp.org/www-project-zap/>

OWASP Juice Shop. [En línea] 15 de mayo de 2022. [Citado el: 15 de mayo de 2022.]

<https://owasp.org/www-project-juice-shop/>

UskoKruM [UskoKruM2010]. (2021, agosto 19). *Cómo Descargar e Instalar Node.js en Windows 10 | Explicación Sencilla* . Youtube. https://www.youtube.com/watch?v=ipmhBYqIP44

V. Mouli and K. P. Jevitha, “Web Services Attacks and Security- ASystematic Literature Review”, Procedia Comp. Sci., vol. 93, pp. 870-877, 2016.

*wstg: The Web Security Testing Guide is a comprehensive Open Source guide to testing the security of web applications and web services*. (s/f).

Pries, R., et al. Traffic Measurement and Analysis of a Broadband Wireless Internet Access. In Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th. 2009.

Xinyu, X. and S. Mishra. Where is the tight link in a home wireless broadband environment? in Modeling, Analysis & Simulation of Computer and Telecommunication Systems, 2009. MASCOTS '09. IEEE International Symposium on. 2009.

Dabir, A. and A. Matrawy. Bottleneck Analysis of Traffic Monitoring using Wireshark. in Innovations in Information Technology, 2007. IIT '07. 4th International Conference on. 2007.

Shaoqiang, W., X. DongSheng, and Y. ShiLiang. Analysis and application of Wireshark in TCP/IP protocol teaching. in E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010 International Conference on. 2010.

Francesco Fusco, L.D., Joseph Gasparakis. Towards Monitoring Programmability in the Future Internet: challenges and solutions. 2010.

Microsoft. Microsoft Message Analyzer Operating Guide. [En línea] 21 de junio de 2022. [Citado el: 21 de junio de 2022.] <https://technet.microsoft.com/enus/library/jj649776.aspx>

PRTG Network Monitor. [En línea] 21 de junio de 2022. [Citado el: 21 de junio de 2022.]: <https://www.paessler.com/manuals/prtg>

1. **CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Danny Alejandro Solano | Experto temático | Regional Cauca, Centro de teleinformática y Producción Industrial | Mayo 2022 |
| Paula Andrea Taborda Ortiz | Diseñadora Instruccional | Regional Norte de Santander, Centro de la Industria, la Empresa y Los Servicios CIES | Mayo de 2022 |
| Carolina Coca Salazar | Asesora Metodológica | Regional Distrito Capital- Centro de Diseño y Metrología | Junio de 2022 |
| Sandra Patricia Hoyos Sepúlveda | Corrección de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Julio de 2022 |

**J. CONTROL DE CAMBIOS**

|  | Nombre | Cargo | Dependencia | Fecha | Razón del cambio |
| --- | --- | --- | --- | --- | --- |
| Autor (es) |  |  |  |  |  |