**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

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

| **COMPETENCIA** | 220501099 - Probar la solución del *software* de acuerdo con parámetros técnicos y modelos de referencia. | **RESULTADOS DE APRENDIZAJE** | 220501099-02 - Ejecutar pruebas de seguridad digital en aplicaciones web con base en lo establecido, marcos de referencia y estándares |
| --- | --- | --- | --- |

| **NÚMERO DEL COMPONENTE FORMATIVO** | CF004 |
| --- | --- |
| **NOMBRE DEL COMPONENTE FORMATIVO** | Pruebas de seguridad orientadas a aplicaciones web con Owasp |
| **BREVE DESCRIPCIÓN** | Este componente formativo pretende enseñar a cómo realizar pruebas de seguridad a las aplicaciones web utilizando Owasp, los niveles de seguridad, tipos de pruebas, métodos, metodologías y confidencialidad; además escanear las vulnerabilidades y el tipo de ataques orientados a estas aplicaciones y, por último, documentar los hallazgos de las pruebas realizadas. |
| **PALABRAS CLAVE** | Ciberseguridad, configuración, diagnóstico, Owasp, seguridad |

| **ÁREA OCUPACIONAL** | 2 - Ciencias naturales, aplicadas y relacionadas |
| --- | --- |
| **IDIOMA** | Español |

1. **TABLA DE CONTENIDOS:**

**Introducción**

1. Tipología de ataques web
2. Clasificación de ataques
3. Prueba de seguridad orientada a aplicaciones web
4. Documentación de hallazgos
5. **INTRODUCCIÓN**

Le damos la bienvenida al componente formativo denominado **“Pruebas de seguridad Orientadas a aplicaciones web con Owasp”**. Este componente enseñará cómo realizar las pruebas a las aplicaciones web de las organizaciones teniendo en cuenta un Plan de pruebas diseñado anteriormente, siguiendo el *top ten* (10) del Owasp, para lo cual se invita a observar el siguiente video introductorio.



1. **DESARROLLO DE CONTENIDOS:**
2. **Tipología de ataques web**

Para las organizaciones en la actualidad es indispensable adquirir aplicaciones web como base tecnológica para darse a conocer, por esta razón muchas empresas y negocios apuestan a incluir estas tecnologías como estrategia para competir en el mercado; estas plataformas son importantes para una empresa, porque automatizan los procesos, simplifican las tareas volviéndose más eficientes al momento de prestar sus servicios al cliente y, lo mejor de todo, es que funcionan solo desde un navegador, por lo que no hace falta instalar paquetes al computador y su acceso es desde cualquier dispositivo con una previa autenticación.

| **Figura 1**  *Seguridad de datos globales*  Interfaz de usuario gráfica, Aplicación  Descripción generada automáticamente | La principal función actualmente de las aplicaciones web es que el usuario o cliente realice una tarea, como comprar, realizar pagos a la empresa, realizar una transacción bancaria, editar textos, fotos y muchas más acciones y prestar un sinfín de servicios, por esta razón se han vuelto tan populares.  Entre muchas de sus ventajas, se presenta una desventaja con la que hay que tener mucho cuidado y son las brechas de seguridad y vulnerabilidades. |
| --- | --- |

Según el informe *Automated Code Analysis: web Application Vulnerabilities in 2017,* 94% de las aplicaciones web contienen una vulnerabilidad muy grave y 85% una vulnerabilidad explotable, por ello, hoy día es esencial utilizar una herramienta de escaneo de vulnerabilidades en aplicaciones web, pues de lo contrario, una empresa podría ser blanco de ciberdelincuentes (gbadvisors,TechBlog, s. f.).

Para escanear las vulnerabilidades hay que conocer cuáles son, por eso, se muestran y se describen los riesgos más identificados de seguridad a las aplicaciones web, a saber:



1. **Clasificación de ataques**

En la actualidad la amenaza más grande a la que se deben enfrentar las empresas son los ciberataques, teniendo en cuenta que no solo afecta a las empresas, sino también a los individuos particulares e incluso Estados y sociedades.

Por lo tanto, las medidas que se toman en la seguridad informática se han vuelto prioritarias, sobre todo para las organizaciones que dependen casi en su totalidad para funcionar de internet. Las vulnerabilidades en estas aplicaciones y los métodos utilizados para que los atacantes no sean detectados se han convertido en pan de cada día y la práctica de buscar cómo infiltrarse sigue aumentando a diario. Por eso, es necesario mostrar qué clase de ataques existen para ser detectados e identificar su impacto.

A continuación, en el siguiente video se exponen los ataques más comunes.





Por lo anterior, en adelante se encontrará en este componente formativo una prueba a un sitio web, en la que se utilizará una herramienta de detección de vulnerabilidades a una aplicación.



1. **Prueba de seguridad orientada a aplicaciones web**

Con miras a la ejecución de una prueba de seguridad es necesario observar el video tutorial que se presenta a continuación, el cual brinda los elementos para utilizar la herramienta Owasp ZAP, de manera correcta.



A continuación, se muestra una forma práctica de identificar vulnerabilidades, que, aunque no se sepa cómo explotarlas, es seguro que hay quien sí lo haga en perjuicio de una persona, o cliente y sus reputaciones. Por razones de seguridad con las empresas testeadas, los ejemplos que se presentarán han sido tomados de alguna página web de una entidad del Estado, de la cual se reservará el nombre y sus datos, además que la imagen gráfica será editada para no comprometer la reputación de la entidad.

Para iniciar, se debe instalar la aplicación Owasp ZAP, en un sistema Windows 10, este aplicativo tiene como propósito hacer pruebas de vulnerabilidad en aplicaciones y tiene como prerrequisito la instalación de JDK de JAVA, por tanto, para realizar estas instalaciones, debe recurrir al material complementario de este componente formativo, específicamente al denominado **“Owasp ZAP, audita la seguridad de webs y evita vulnerabilidades”** (De Luz, 2021), allí se encuentran los enlaces de los manuales, en caso de que no se tengan estas dos aplicaciones en el computador.

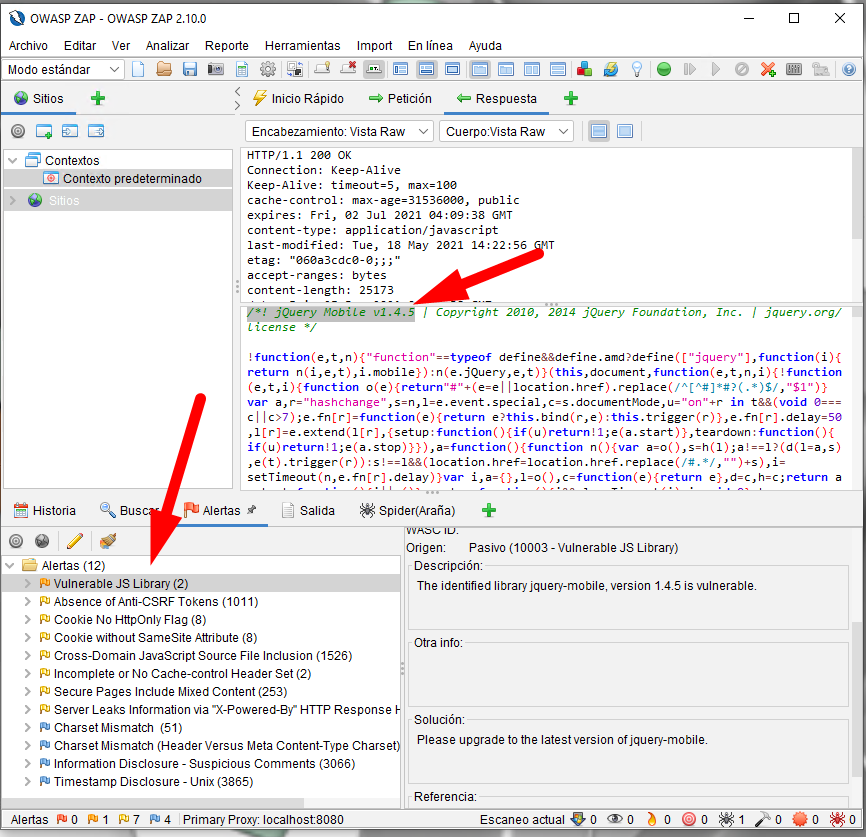


En el anterior ejercicio práctico de identificación de vulnerabilidades, se hallaron dos vulnerabilidades, que a continuación se detallarán:



Para conocer cómo resolver los dos anteriores hallazgos, se debe remitir al material complementario de este componente formativo.

El siguiente es otro ejemplo de un caso también crítico y fácilmente explotable.



Este sitio web está usando una librería jQuery Mobile en su versión 1.4.5, pero esa versión de esta librería tiene vulnerabilidades detectadas por la comunidad JQuery y seguramente en los foros de la comunidad jQuery se detectó y es un indicio de cómo vulnerar este sistema, pero en la imagen se propone una solución y es que se actualice la librería.

Si se observa en el resultado de las pruebas, los ataques que hace la herramienta a los sitios web que se van a probar son los mencionados uno a uno en el primer tema de este componente formativo.

1. **Documentación de hallazgos**

La documentación de hallazgos es el resultado del ejercicio realizado durante la ejecución del proceso de auditoría, que las entidades de fiscalización generan sobre la gestión de todos los procesos de los auditados (personas, instituciones, empresas, etc.) y que servirá para evaluar si se cumple o no con lo que se está auditando. En el siguiente tutorial se brinda información sobre cómo realizar un reporte.



La documentación y saber mostrar los resultados de las pruebas a los clientes u organizaciones es muy importante, además, aprender a interpretarlos ayudará a darle una visión al trabajo posterior de las pruebas, ofreciendo unas recomendaciones para corregir esas vulnerabilidades.

Por lo anterior, en el siguiente video se mostrará cómo se genera el reporte de los hallazgos y cómo se debe interpretar. Esta herramienta permite exportar un reporte en PDF y uno en HTML y se va a mostrar cada uno de ellos explicando *grosso modo* cómo deben interpretarse.



Luego de tener el listado del reporte, se describen los siguientes pasos cada una de las secciones de este para tener una mejor comprensión de este.



Es preciso recordar que estas pruebas deben realizarse con previa autorización de los dueños de las aplicaciones y que este tipo de informes son netamente confidenciales.

1. **Síntesis**

En el siguiente mapa conceptual se resumen los conceptos vistos en este componente formativo.



1. **ACTIVIDADES DIDÁCTICAS**

| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA** | |
| --- | --- |
| **Nombre de la Actividad** | Características representativas de ataques y *malwares*. |
| **Objetivo de la actividad** | Afianzar las características más importantes de algunos conceptos de ataques y *malware* para las pruebas utilizando Owasp ZAP. |
| **Tipo de actividad sugerida** | Falso o verdadero. |
| **Archivo de la actividad (Anexo donde se describe la actividad propuesta)** | Anexos / Anexo4\_ ActividadDidactica1\_CF04 |

1. **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 |
| --- | --- | --- | --- |
| 1. Tipología de ataques web. | Belcic, I. (2020).*¿Qué es la inyección de SQL y cómo funciona?*Avast*.* <https://www.avast.com/es-es/c-sql-injection> | Página web | <https://www.avast.com/es-es/c-sql-injection> |
| 1. Tipología de ataques web. | Quanti Media Group [QuantiSolutions]. (2019). *Las 10 Vulnerabilidades más peligrosas usadas por aplicaciones web (Owasp 10) - 4K*. [Video]. YouTube. <https://www.youtube.com/embed/kNo9fZC1Isw> | Video | <https://www.youtube.com/embed/kNo9fZC1Isw> |
| 1. Tipología de ataques web. | Roelcode. (2021*). Cómo Descargar e Instalar Java JDK 16 en Windows 10 - 2021.* [Video]. YouTube. <https://youtu.be/hCBEavs08as> | Video | <https://youtu.be/hCBEavs08as> |
| 1. Tipología de ataques web. | WeLiveSecurity. (2015). *¿En qué consiste la vulnerabilidad Cross Site Request Forgery (CSRF)?* We Live Security. <https://www.welivesecurity.com/la-es/2015/04/21/vulnerabilidad-cross-site-request-forgery-csrf/> | Página web | <https://www.welivesecurity.com/la-es/2015/04/21/vulnerabilidad-cross-site-request-forgery-csrf/> |
| 1. Tipología de ataques web. | Kumar, C. (2015). *Cookie segura con HttpOnly y bandera segura en Apache*. Geekflare. <https://geekflare.com/es/httponly-secure-cookie-apache/> | Página web | <https://geekflare.com/es/httponly-secure-cookie-apache/> |
| 2. Clasificación de ataques. | GioCode [giova50000]. (2020). *Los tipos de malware | GioCode* [Video]. YouTube. <https://www.youtube.com/embed/A6FAqk2QDjM> | Video | <https://www.youtube.com/embed/A6FAqk2QDjM> |
| 3. Prueba de seguridad orientada a aplicaciones web. | De Luz, S. (2021). *Owasp ZAP, audita la seguridad de webs y evita vulnerabilidades*. RedesZone. <https://www.redeszone.net/tutoriales/seguridad/owasp-zap-auditar-seguridad-web/> | página web | <https://www.redeszone.net/tutoriales/seguridad/owasp-zap-auditar-seguridad-web/> |

1. **GLOSARIO:**

| **TÉRMINO** | **SIGNIFICADO** |
| --- | --- |
| **Amenaza** | cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas. |
| **Aplicación** | programa informático diseñado como una herramienta para realizar operaciones o funciones específicas. Generalmente, son diseñadas para facilitar ciertas tareas complejas y hacer más sencilla la experiencia informática de las personas. |
| **Base de datos** | recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático. |
| ***Browser*** | es el término inglés que se utiliza para identificar a un navegador web o navegador de internet, consiste en un *software*, programa o incluso aplicación, que ofrece al usuario el acceso a la red |
| **Delegar** | dar (a una persona u organización) un poder, una función o una responsabilidad a alguien para que los ejerza en su lugar o para obrar en representación suya. |
| **Implementación** | poner en funcionamiento o aplicar métodos, medidas, etc., para realizar algo. |
| **Interfaz** | en informática, es la conexión física y funcional que se establece entre dos aparatos, dispositivos o sistemas que funcionan independientemente uno del otro, en este sentido, la comunicación entre un ser humano y una computadora se realiza por medio de una interfaz. |
| **Owasp** | *Open web Application Security.* |
| **Riesgo** | posibilidad de que una amenaza se produzca, dando lugar a un ataque sobre un recurso o servicio tecnológico; esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza. |
| **Servidor** | conjunto de computadoras capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

Calder, A. (2018). *NIST Cybersecurity Framework: Una guía de bolsillo*. IT Governance Publishing Ltd.

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *Sistemas (Asociación Colombiana de Ingenieros de Sistemas)*, 119, 4-7.

Dongee. (2018). *Las 7 vulnerabilidades más comunes de sitios web que no puedes pasar por alto.* Dongee. <https://blog.dongee.com/las-7-vulnerabilidades-m%C3%A1s-comunes-de-sitios-web-que-no-puedes-pasar-por-alto-59f29c1c3aea>

Firma-e. (2021). *¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información?* Firma-e. <https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion>

Gómez, M., J. (2017). *Gestión de la ciberseguridad según el ISO/IEC 27032:2012*. <https://www.linkedin.com/pulse/gesti%C3%B3n-de-la-ciberseguridad-seg%C3%BAn-el-isoiec-gianncarlo-g%C3%B3mez-morales>

ISO/IEC. (2020). *Tecnologías de la información. Técnicas de seguridad. Directrices para ciberseguridad.* <https://tienda.icontec.org/gp-tecnologias-de-la-informacion-tecnicas-de-seguridad-directrices-para-ciberseguridad-gtc-iso-iec27032-2020.html>

Portal de la Administración Electrónica - PAE (s. f.). *Magerit v.3: Metodología de análisis y gestión de riesgos de los sistemas de información.* <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html>

Presupuesto Online. (2021). *ISO 27001 - Certificado ISO 27001 punto por punto.* [https://normaiso27001.es](https://normaiso27001.es/)

Seguridad 7”A”. (s. f.). *Metodología NIST SP 800-30.* National Institute of Standards and Technology. <http://seguridades7a.blogspot.com/p/nist-sp-800-30.html>

Soriano, M. (2014). *Seguridad en redes y seguridad de la información*. Improvet.

1. **CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| --- | --- | --- | --- | --- |
| **Autor (es)** | David Eduardo Lozada Cerón | Experto Temático | Regional Cauca - Centro de Tele informática y Producción Industrial | Junio de 2022 |
| Paula Andrea Taborda Ortiz | Diseñadora Instruccional | Regional Norte de Santander, Centro de la Industria, la Empresa y Los Servicios CIES | Julio de 2022 |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Regional Distrito Capital – Centro de Diseño y Metrología | Julio de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo de Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Julio 2022 |
|  | José Gabriel Ortiz Abella | Corrector de estilo | Regional Distrito Capital – Centro de Diseño y Metrología. | Julio del 2022. |

1. **CONTROL DE CAMBIOS**

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