

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.

Octubre 2023

Tabla de contenido

Introducción.....	1
1. Tipología de ataques web.....	3
2. Clasificación de ataques	6
3. Prueba de seguridad orientada a aplicaciones web.....	9
4. Documentación de hallazgos.....	18
Síntesis.....	27
Material complementario.....	28
Glosario.....	29
Referencias bibliográficas	31
Créditos.....	33

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.

Video 1. Pruebas de seguridad orientadas a aplicaciones web con OWASP



[Enlace de reproducción del video](#)

Síntesis del video: Pruebas de seguridad orientadas a aplicaciones web con OWASP

Se construye este componente formativo como material de apoyo que enseña a realizar pruebas de aplicaciones web, utilizando el “top ten” de OWASP. Es por ello

que se debe entender para el procedimiento qué se quiere probar, para qué y contra qué hay que enfrentarse o defenderse. Sumado a esto, también se explicará los tipos de ataques más frecuentes y los “malwares” que pueden hacer daños a estas aplicaciones.

También, se enseñará cómo generar un reporte en esta herramienta y qué información contiene para mostrar, de la mejor forma, el diagnóstico realizado, la magnitud y la gravedad en la que se encuentra.

1. 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 y se vuelven más eficientes al momento de prestar sus servicios al cliente. Además, lo mejor de todo es que funcionan solo desde un navegador, por lo que no es necesario instalar paquetes en el computador y su acceso es desde cualquier dispositivo con previa autenticación.

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 cosas y prestar un sinnúmero 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. De lo contrario, tu 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:

- **“Clickjacking”**. Estos ataques son muy comunes para atacar y capturar datos confidenciales en páginas como Facebook y Twitter. Suplanta funcionalidades de la página principal y redirecciona al usuario a diferentes dominios, especialmente al diligenciar formularios como el “login” y “password”, enviando la información a un correo electrónico del pirata informático.
- **“Cross Site Scripting” (XSS)**. Es una vulnerabilidad muy común y bastante utilizada, se encuentra en muchas de las aplicaciones web. Esta vulnerabilidad le permite al pirata informático insertar un código malicioso dentro de las aplicaciones que frecuentan los cibernautas, evitando el acceso al sitio y también es utilizado para la práctica del “phishing”.
- **Falsificación de solicitudes entre sitios / CSRF**. Este ataque consiste en engañar al usuario al momento de autenticarse en un sitio web de confianza, se conoce también como ataque con un solo clic y se abrevia CSRF, utiliza comandos por debajo de las aplicaciones no autorizadas.
- **Ejecución remota de código**. La ejecución remota de código es utilizada por los piratas cibernéticos, para implantar “malware” y ejecutar código aprovechando las vulnerabilidades de la aplicación web y así poder tomar el control de toda la aplicación.
- **Inclusión de archivos locales (LFI) e inclusión de archivos remotos (RFI)**. Es una vulnerabilidad que afecta a los servidores web. Permite adquirir, ubicar, obtener y modificar archivos que se encuentran en el directorio raíz de la aplicación web. También permite realizar ataques para adquirir los

usuarios del servidor y obtener todos los privilegios para realizar operaciones maliciosas dentro del servidor.

- **Ataque de inyección SQL.** Este ataque modifica las sentencias SQL y afecta a los datos de toda la aplicación, permitiéndole al atacante suplantar identificación, manipular información de la base de datos, afectar saldos y transacciones, destruir información o datos, obtener los privilegios del administrador y hasta divulgar la información de la organización, entre muchos otros aspectos.
- **Redirección de URL.** Este ataque engaña al usuario, redireccionándolo de un sitio a otro, tomando el control de toda la información que se quiera introducir; es muy común en la suplantación de sitios web en donde se hacen transacciones de dinero, como bancos, entre otros.

2. 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 por los atacantes para no ser detectados se han convertido en algo habitual. La práctica de buscar cómo infiltrarse sigue aumentando a diario. Por eso, es necesario mostrar qué tipos de ataques existen para poder detectarlos e identificar su impacto.

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

Video 2. Ataques de seguridad en la red



[Enlace de reproducción del video](#)

Síntesis del video: Ataques de seguridad en la red

Se da cuando se saca provecho de una vulnerabilidad de un sistema de información para ocasionar daños por parte terceros y con intenciones desconocidas para el administrador del sistema.

Existen numerosos tipos de ciberataques. A continuación, se describen los más conocidos.

- **“Malware”**. Se denomina también “software” malicioso, por la traducción del inglés “malicious software”. Al ingresar en un equipo, tiene como función dañarlo de diferentes maneras.
- **Virus**. Tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo, propagarse de un equipo a otro e infectar las aplicaciones del mismo.
- **“Worms” - Gusanos**. Programas de “software” malintencionado, el cual se propaga sin intervención de usuario. Se activa de forma automática y sin ser visto, extendiéndose a otros sistemas informáticos por medio de las redes.
- **Trojanos**. Tiene la apariencia de un programa confiable pero esconden otro tipo de “malware”, que se instala automáticamente, para asumir el control total del equipo.
- **“Keyloggers”**. Registran y captan todas las pulsaciones del teclado y esta información se emplea para conseguir contraseñas y datos de la víctimas.
- **“Spyware”**. El objetivo principal de este “malware” es el robo de información.

- **“Adware”**. Muestra publicidad al usuario a través de “banners”, “pop ups” y nuevas ventanas en el explorados. En muchos casos, el objetivo secundario también es obtener información sobre la actividad del usuario en la red.
- **“Ransomware”**. Es el tipo de ataque más común en la actualidad. Se basa en el cifrado de los datos, restringiendo el acceso de los archivos del equipo para pedir un pago por el rescate de estos. En la mayoría de los casos, en “bitcoins”.

Importante: para hacer las pruebas es necesario conocer las anteriores terminologías, pues existen diversas técnicas que son utilizadas para atacar una aplicación web y qué datos son sensibles a vulnerabilidades; por ello, es necesario contar con una herramienta adecuada para hacer diagnósticos y detectar cada vulnerabilidad.

Por lo anterior y 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.

Nota: en caso de hacer la práctica, deben tener una autorización previa para no llegar a tener problemas legales, dado que se estará ingresando a zonas de datos privados.

3. 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.

Video 3. Instalación OWASP ZAP



[Enlace de reproducción del video](#)

Síntesis del video: Instalación OWASP ZAP

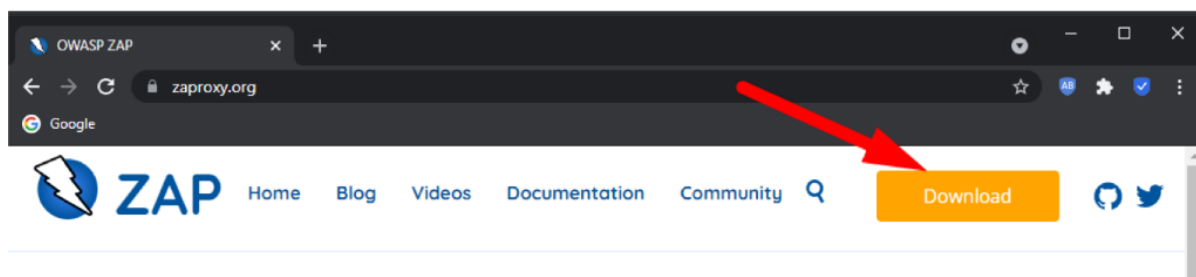
Videotutorial en el que se describe el proceso para la instalación de la herramienta OWASP ZAP a través del sitio oficial en el que se encuentran distintas versiones y de acuerdo al tipo de sistema operativo que se tenga. Esta herramienta permite realizar diagnósticos a los sitios web para identificar vulnerabilidades y fallas

de seguridad. Es video cierra mostrando un ejemplo de cómo realizar este proceso de análisis.

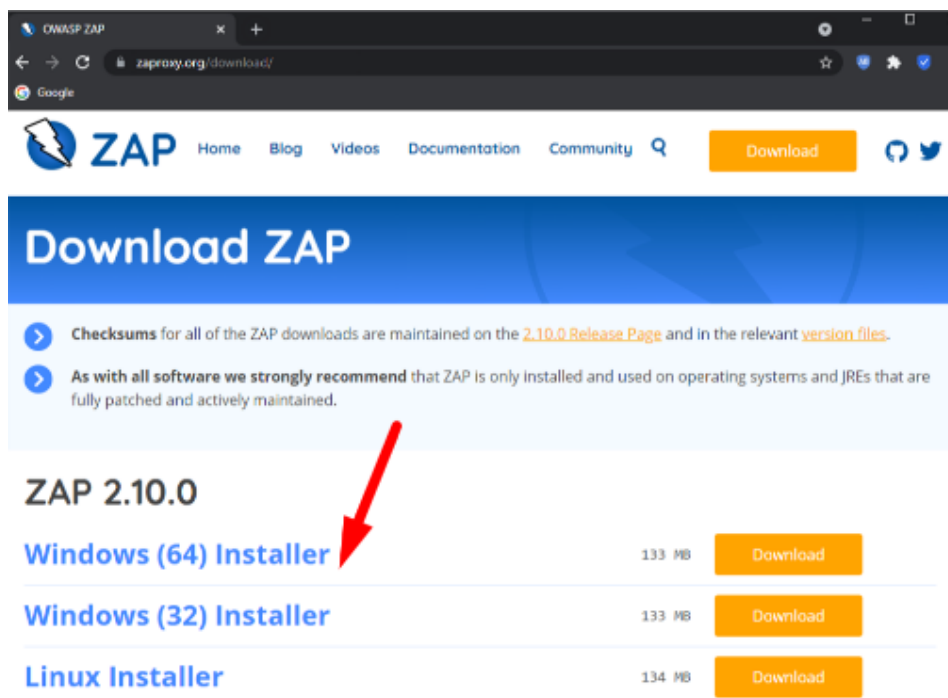
A continuación, se muestra una forma práctica de identificar vulnerabilidades. Aunque no se sepa cómo explotarlas, es seguro que hay quien sí lo hará, en perjuicio de una persona, un cliente o sus reputaciones. Por razones de seguridad con las empresas testeadas, los ejemplos que se presentarán han sido tomados de alguna página web de una entidad del Estado, de la cual se reservará el nombre y sus datos. Además, 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 requiere la instalación de JDK de JAVA como prerequisite. Para realizar estas instalaciones, se 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.

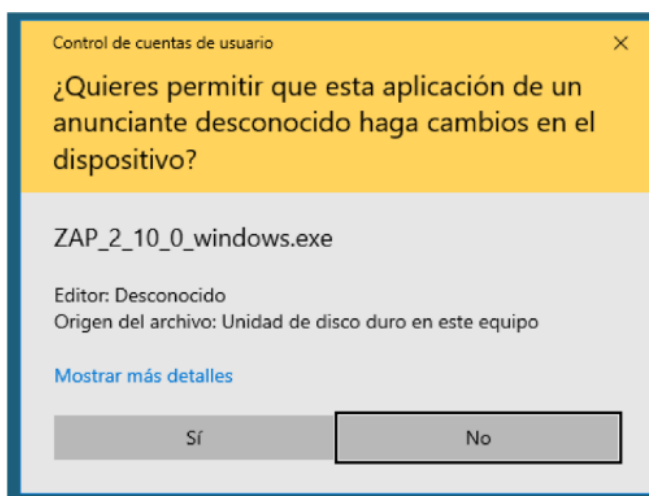
- a. Una vez instalado el JDK puede continuar. Diríjase a la página principal de Zaproxy.org y busque el botón de descarga.



- b. Descargue la versión compatible con su sistema operativo, si no está seguro use la de 32 “bits”, ya que sirve en sistemas operativos de 32 “bits” y 64 “bits”.



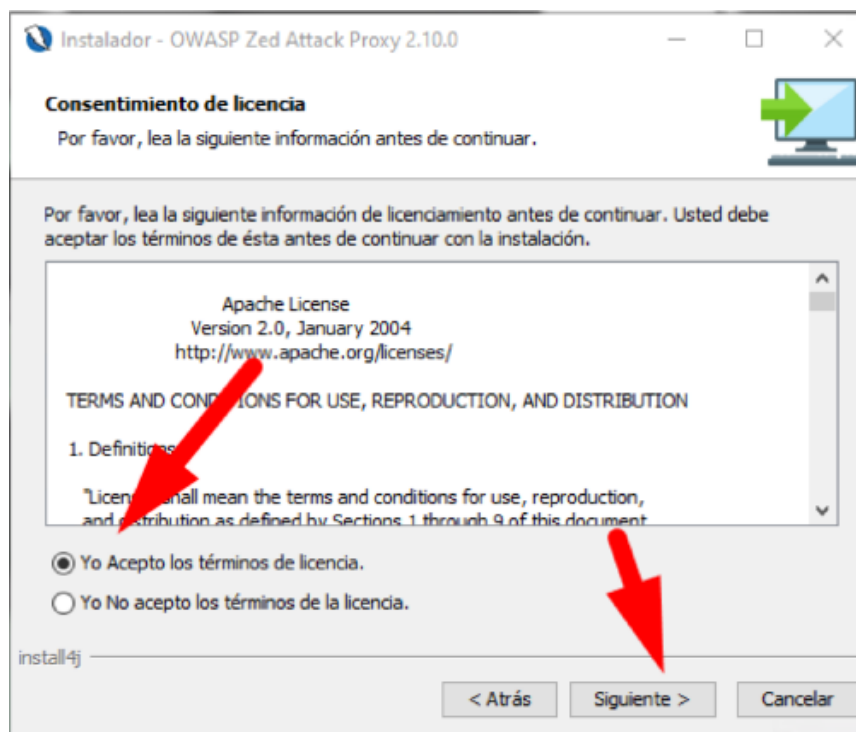
- c. Una vez lo descargue, debe proceder a instalarlo, seguramente le pedirá permisos para realizar la instalación en su sistema, tenga confianza y de clic en Sí.



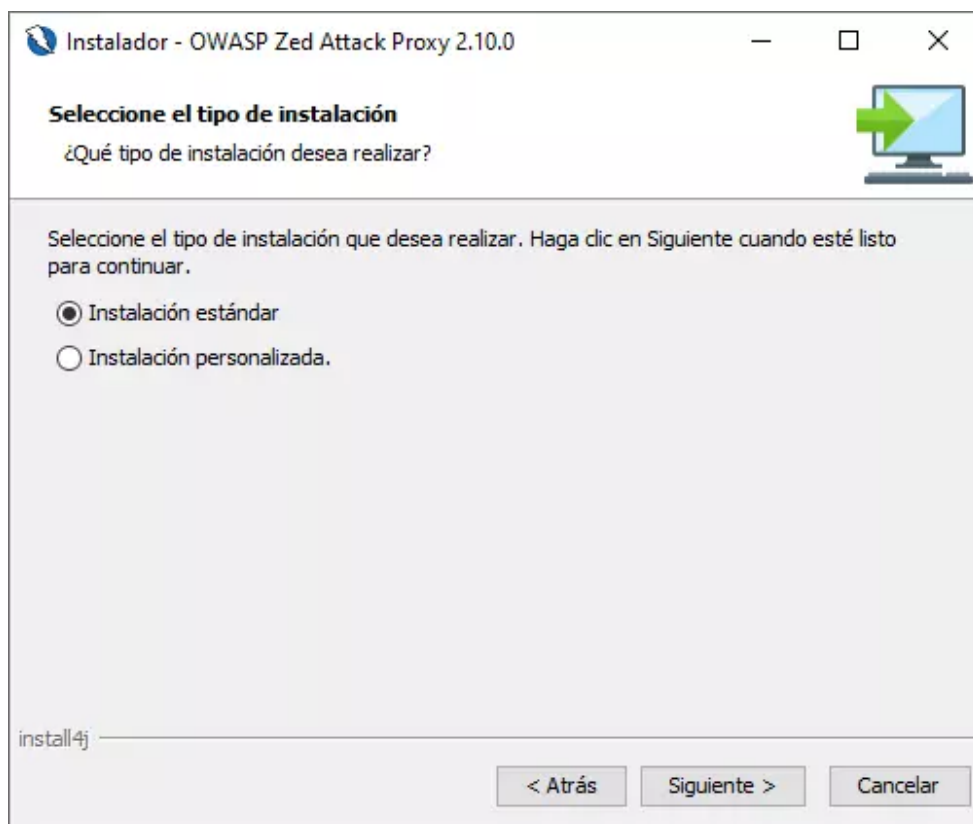
d. Dé clic en Siguiente.



e. Acepte los términos y dé clic en Siguiente.



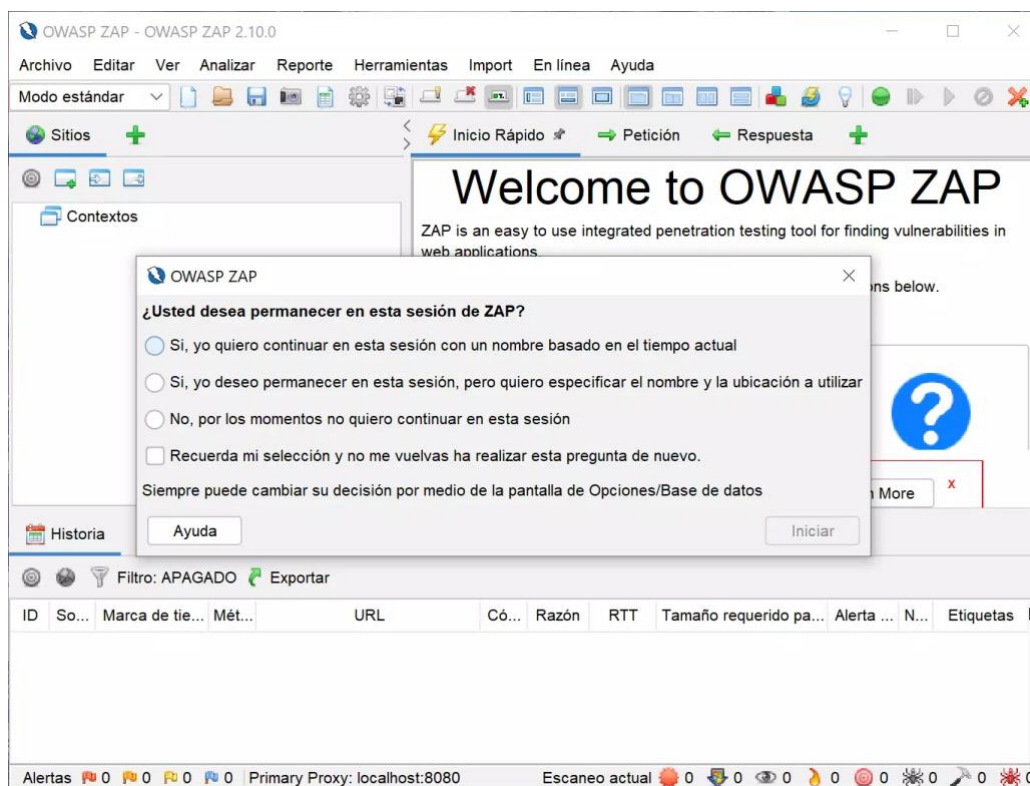
- f. Verifique que el botón de selección se encuentre en Instalación estándar, sino selecciónela y dé clic en el botón Siguiente dos veces.



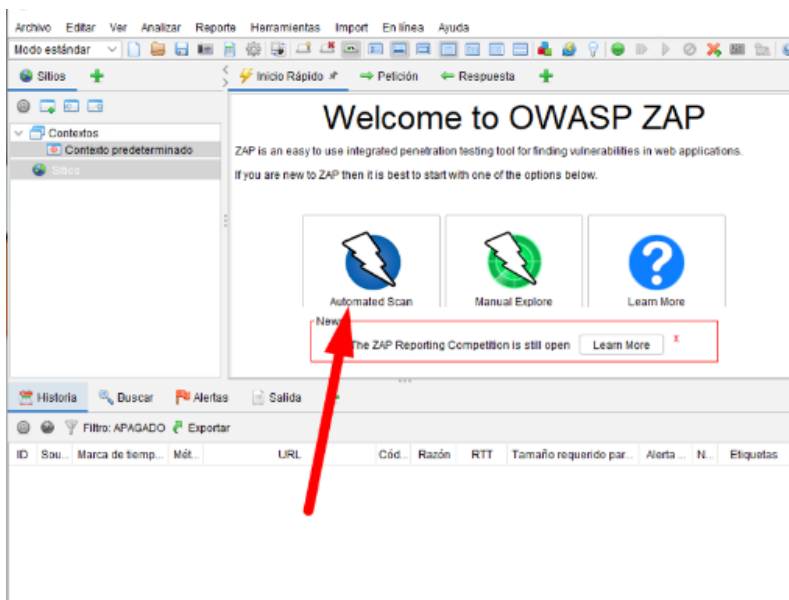
- g. Después de instalar la aplicación hay que ejecutarla, para ello, busque en aplicaciones recientes o en el menú de inicio y dé clic en ella.



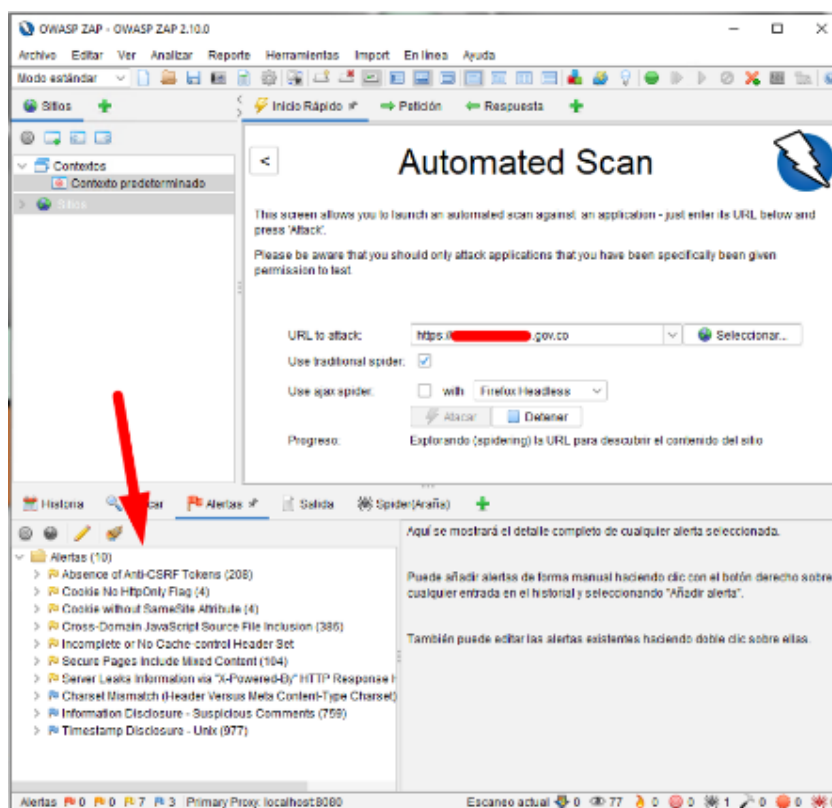
- h. El programa le pregunta si quiere continuar con esta sesión de la aplicación, se contesta “Sí, yo quiero continuar...”



- i. Ahora se verá cómo hacer el escaneo más básico, es el de “test” sin credenciales de acceso. Porque se puede configurar un “proxy” que capture y genere un “script” de inicio de sesión, para pruebas más completas, pero es un tema más avanzado que no está al alcance en este momento por ahora. Haga clic en “Automated Scan” (escaneo automático).



- j. Por temas de tiempo no solo se toma un pantallazo los 6 minutos, seguramente si la prueba dura unos 20 minutos encontraría más vulnerabilidades.




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

- **“Absence of Anti-CSRF Tokens”**. Según el reporte en la imagen, la página web tiene 208 formularios vulnerables a ataques de SCRF.
- **“Cookie No HttpOnly Flag”**. Esta vulnerabilidad trata que otras webs pueden acceder a los datos de usuario o datos de sesión basados en “cookies”. Se resuelve de varias maneras, tal vez la más sencilla es agregando una configuración en el servidor.

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

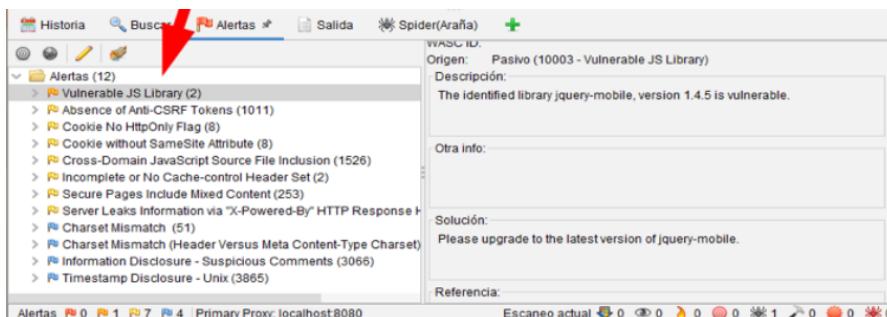
El siguiente es otro ejemplo de un caso también crítico y fácilmente explotable.



```
HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
cache-control: max-age=31536000, public
expires: Fri, 02 Jul 2021 04:09:38 GMT
content-type: application/javascript
last-modified: Tue, 18 May 2021 14:22:56 GMT
etag: "060a3cdc0-0;;"
accept-ranges: bytes
content-length: 25173

/*! jQuery Mobile v1.4.5 | Copyright 2010, 2014 jQuery Foundation, Inc. | jquery.org/
license */

!function(e,t,n){"function"==typeof define&&define(["jquery"],function(i){
return n(i,e,t),i.mobile});n(e.jQuery,e,t)}(this,document,function(e,t,n,i){!function
(e,t,i){function o(e){return "#"+(e=e||location.href).replace(/^[^#]*#?(.*)$/, "$1")}
var a,r="hashchange",s=n,l=e.event.special,c=s.documentMode,u="on"+r in t&&(void 0===
c||c>7);e.fn[r]=function(e){return e?this.bind(r,e):this.trigger(r)},e.fn[r].delay=50
,l[r]=e.extend(l[r],{setup:function(){if(u)return!1;e(a.start)},teardown:function(){
if(u)return!1;e(a.stop)}},a=function(){function n(){var a=o(),s=h(1);a!==1?(d(1=a,s)
,e(t).trigger(r)):s!==1&&(location.href=location.href.replace(/#\/"/,"")+s),i=
setTimeout(n,e.fn[r].delay)}var i,a={},l=o(),c=function(e){return e},d=c,h=c;return a
```



Alertas (12)	WASC ID:
Vulnerable JS Library (2)	Origen: Pasivo (10003 - Vulnerable JS Library)
Absence of Anti-CSRF Tokens (1011)	Descripción: The identified library jquery-mobile, version 1.4.5 is vulnerable.
Cookie No HttpOnly Flag (8)	Otra info:
Cookie without SameSite Attribute (8)	Solución: Please upgrade to the latest version of jquery-mobile.
Cross-Domain JavaScript Source File Inclusion (1526)	Referencia:
Incomplete or No Cache-control Header Set (2)	
Secure Pages Include Mixed Content (253)	
Server Leaks Information via "X-Powered-By" HTTP Response	
Charset Mismatch (51)	
Charset Mismatch (Header Versus Meta Content-Type Charset)	
Information Disclosure - Suspicious Comments (3066)	
Timestamp Disclosure - Unix (3865)	

Alertas 0 0 1 7 4 Primary Proxy: localhost:8080 Escaneo actual 0 0 0 0 1 0 0 0

Este sitio web utiliza la librería jQuery Mobile en su versión 1.4.5. Sin embargo, esta versión tiene vulnerabilidades detectadas por la comunidad jQuery, las cuales podrían ser aprovechadas por atacantes. En la imagen se propone una solución: actualizar la librería a la versión más reciente.

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.

4. 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.). Esta documentación 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.

Video 4. Instructivo Descarga Reporte Vulnerabilidades



[Enlace de reproducción del video](#)

Síntesis del video: Instructivo Descarga Reporte Vulnerabilidades

Después de haber ejecutado la prueba con la herramienta OWASP ZAP y de que se hayan realizado los ataques, se empiezan a presentar las vulnerabilidades ya mencionadas, ahora se mostrará cómo se descarga el reporte en PDF.

Hay que dirigirse al menú principal y dar clic en la opción **reporte**. Después, se desplegará un submenú y se debe hacer clic en la opción **Generar reporte**.

Luego, se despliega una ventana donde se puede configurar el reporte según las necesidades, inicialmente se le da un título al reporte, cambiar el nombre del reporte, cambiar la ruta donde va a quedar guardado el reporte, agregar una descripción y, por último, seleccionar el dominio al cual se le realizaron las pruebas.

En la opción de “**template**”, se puede cambiar el estilo como se quiere que se genere el reporte, escoger la plantilla en la que se va a presentar el reporte, seleccionar el tema y configurar qué información se mostrará.

Finalmente, se hace clic en el botón **Aceptar** y muestra el reporte según las configuraciones establecidas.

La documentación y la presentación de los resultados de las pruebas a clientes u organizaciones es muy importante. Además, el aprendizaje de su interpretación ayudará a darle una visión al trabajo posterior de las pruebas, ofreciendo recomendaciones para corregir las vulnerabilidades encontradas.

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.

Video 5. Reporte OWASP



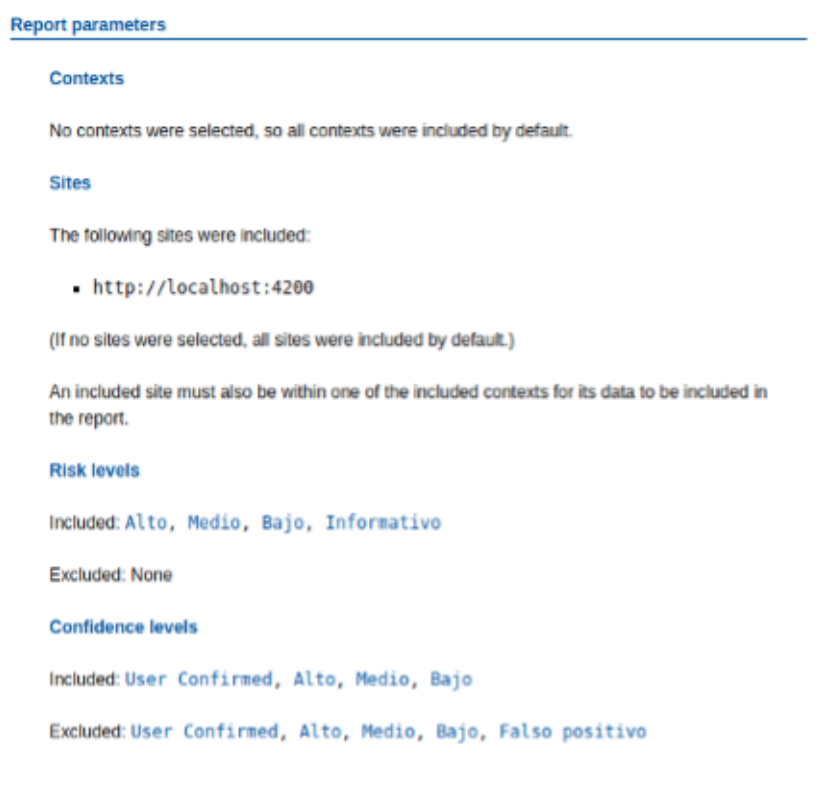
[Enlace de reproducción del video](#)

Síntesis del video: Reporte OWASP

Videotutorial en el que se explica cómo obtener reportes de OWASP ZAP para dimensionar la magnitud de las fallas. Este inicia realizando un escaneo con la herramienta para visualizar las diferentes alertas en el momento que se realizó el ataque al sitio. Luego, se dirige a la opción **Reporte** para generarlo y configurarlo como se desee, tanto en su contenido como en su presentación final. Finalmente, se expone un ejemplo del resultado del reporte en HTML y a qué hace referencia cada resumen, alerta y apéndice que este arroja. De tal forma, que se comprenda cómo dar una evaluación a las personas interesadas.

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.

- a. **Tomar la información general del reporte.** En esta primera sección se muestran algunos datos generales del reporte, como el dominio donde está la aplicación a la que se le realizaron las pruebas, la descripción del nivel de los riesgos y los niveles de confianza.



- b. **Revisar los resúmenes.** En esta segunda sección se muestra el conteo de las alertas en una matriz de riesgos (filas) contra confianzas (columnas), con su debido porcentaje de una contra la otra.

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	Alto	Medio	Bajo	Total
Risk	Alto	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Medio	0 (0,0 %)	1 (14,3 %)	2 (28,6 %)	0 (0,0 %)	3 (42,9 %)
	Bajo	0 (0,0 %)	0 (0,0 %)	2 (28,6 %)	1 (14,3 %)	3 (42,9 %)
	Informativo	0 (0,0 %)	0 (0,0 %)	1 (14,3 %)	0 (0,0 %)	1 (14,3 %)
	Total	0 (0,0 %)	1 (14,3 %)	5 (71,4 %)	1 (14,3 %)	7 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

- c. **Revisar la matriz.** Luego, haciendo parte de la segunda sección, se revisa la matriz en la que se cruzan los riesgos contra el dominio de prueba.

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
Site		Alto	Medio	Bajo	Informativo
		(= Alto)	(>= Medio)	(>= Bajo)	(>= Informativo)
	http://localhost:4200	0 (0)	3 (3)	3 (6)	1 (7)

- d. **Observar los tipos de riesgos arrojados.** Y por último, en esta segunda sección, se muestran los tipos de riesgos que se detectaron en las pruebas al sitio.

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medio	1 (14,3 %)
Desconfiguración de Dominio cruzado	Medio	10 (142,9 %)
Missing Anti-clickjacking Header	Medio	1 (14,3 %)
Divulgación de la marca de hora - Unix	Bajo	6 (85,7 %)
El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ""X-Powered-By""	Bajo	9 (128,6 %)
X-Content-Type-Options Header Missing	Bajo	10 (142,9 %)
Divulgación de información - Comentarios sospechosos	Informativo	26 (371,4 %)
Total		7

- e. **Identificar las alertas.** En esta tercera sección se muestran todas las alertas detectadas en la prueba por el nivel de riesgo.

Alerts

Risk=Medio, Confidence=Alto (1)

<http://localhost:4200/> (1)

[Content Security Policy \(CSP\) Header Not Set](#) (1)

► GET <http://localhost:4200/>

Risk=Medio, Confidence=Medio (2)

<http://localhost:4200/> (2)

[Desconfiguración de Dominio cruzado](#) (1)

► GET <http://localhost:4200/>

[Missing Anti-clickjacking Header](#) (1)

► GET <http://localhost:4200/>

Risk=Bajo, Confidence=Medio (2)

<http://localhost:4200/> (2)

[El servidor divulga información mediante un campo\(s\) de encabezado de respuesta HTTP ""X-Powered-By""](#) (1)

► GET <http://localhost:4200/>

- f. **Reconocer el apéndice.** En esta tercera sección, el apéndice muestra cada una de las alertas, así como algunas referencias para más información de cada una.

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

Content Security Policy (CSP) Header Not Set

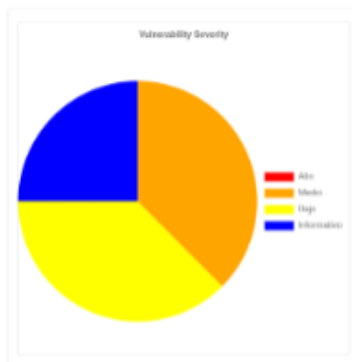
Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none"> https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification-dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/

- k. **Diferenciar los tipos de apéndice y elegir el de tipo gerencial.** También vale resaltar que existen muchos más reportes, los cuales puedes configurar, como el siguiente que es más gerencial.

ZAP Scanning Report

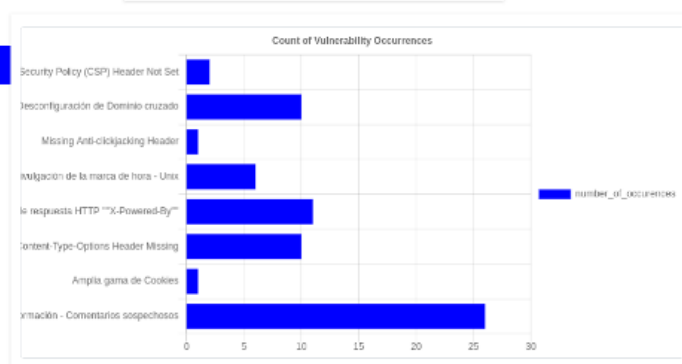
Generated on via, 17 Jun. 2022 00:53:07

Most Severe Alert
Medium



Most Common Bug

Divulgación de información -
Comentarios sospechosos (26)



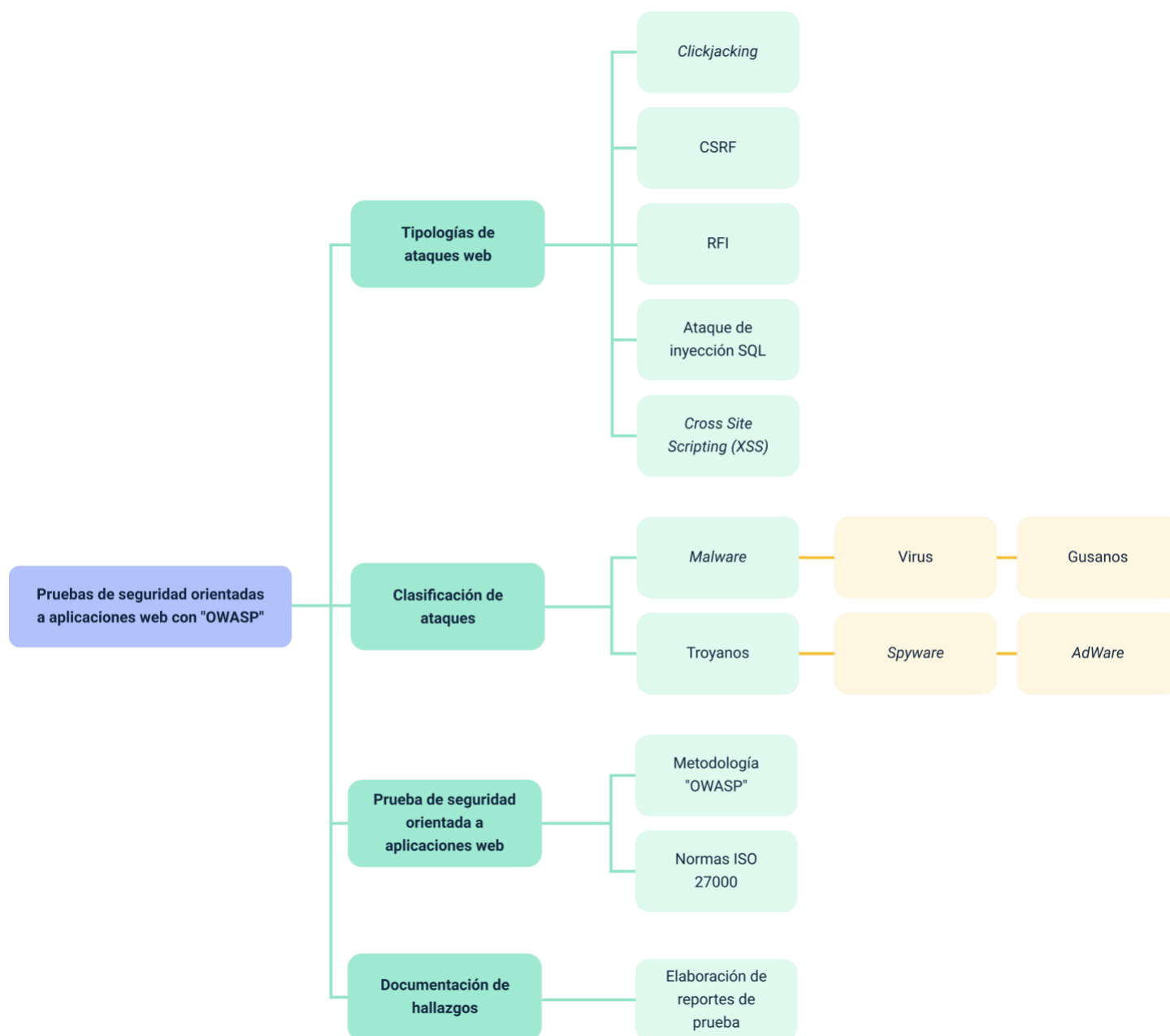
Vulnerability Impact

#	Name	Impact
Content Security Policy (CSP)	Content Security Policy (CSP) is an added layer of	

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.

Síntesis

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



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1. Tipología de ataques web.	Belcic, I. (2020). ¿Qué es la inyección de SQL y cómo funciona? Avast.	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.	Video	https://www.youtube.com/embed/kNo9fZC1lsw
1. Tipología de ataques web.	Roelcode. (2021). Cómo Descargar e Instalar Java JDK 16 en Windows 10 - 2021. [Video]. YouTube.	Video	https://www.youtube.com/watch?v=hCBEavs08as&feature=youtu.be
1. Tipología de ataques web.	Kumar, C. (2015). Cookie segura con HttpOnly y bandera segura en Apache. Geekflare.	Página web	https://geekflare.com/es/http-only-secure-cookie-apache/
2. Clasificación de ataques.	GioCode [giova50000]. (2020). Los tipos de malware GioCode [Video]. YouTube.	Video	https://www.youtube.com/embed/A6FAqk2QDjM
3. Prueba de seguridad orientada a aplicaciones web.	De Genez, G. (2021). Owasp ZAP, audita la seguridad de webs y evita vulnerabilidades. SeguridadPy	Página web	https://seguridadpy.info/2021/05/owasp-zap-audita-la-seguridad-de-webs-y-evita-vulnerabilidades/

Glosario

Amenaza: cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas.

Aplicación: es un 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: es una 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: es la 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: es un conjunto de computadoras capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

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%BAAn-el-isoiec-gianncarlo-g%C3%B3mez-morales>

ISO/IEC. (2020). Tecnologías de la información. Técnicas de seguridad. Directrices para ciberseguridad.

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>

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.

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Responsable del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Regional Santander - Centro Industrial del Diseño y la Manufactura
David Eduardo Lozada Cerón	Experto Temático	Regional Cauca - Centro de Teleinformática y Producción Industrial
Paula Andrea Taborda Ortiz	Diseñadora Instruccional	Regional Norte de Santander - Centro de la Industria, la Empresa y Los Servicios CIES
Andrés Felipe Velandia Espitia	Asesor Metodológico	Regional Distrito Capital – Centro de Diseño y Metrología
José Gabriel Ortiz Abella	Corrector de Estilo	Regional Distrito Capital – Centro de Diseño y Metrología.
Fabian Andres Zarate	Diseñador de Contenidos Digitales	Regional Santander - Centro Industrial del Diseño y la Manufactura
Camilo Andres Bolaño Rey	Desarrollador Full-Stack	Regional Santander - Centro Industrial del Diseño y la Manufactura
Carlos Eduardo Garavito Parada	Animador y Productor Multimedia	Regional Santander - Centro Industrial del Diseño y la Manufactura
Camilo Andres Bolaño Rey	Actividad Didáctica	Regional Santander - Centro Industrial del Diseño y la Manufactura
Zuleidy María Ruiz Torres	Validador de Recursos Educativos Digitales	Regional Santander - Centro Industrial del Diseño y la Manufactura
Luis Gabriel Urueta Alvarez	Validador de Recursos Educativos Digitales	Regional Santander - Centro Industrial del Diseño y la Manufactura

Nombre	Cargo	Regional y Centro de Formación
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Regional Santander - Centro Industrial del Diseño y la Manufactura