Testing de Seguridad con Owasp Zap (10%)

Autor: Jimmis J. Simanca

Tecnología en Desarrollo de Software, Corporación Universitaria Uniremington

Asignatura: Lenguaje de Programación 3

Director: Milton Javier Mateus Hernández

28 de noviembre de 2024

Tabla de contenido

Diligenciar la tabla característica de técnicas y herramientas para realizar pruebas de seguridad al software

Tabla1

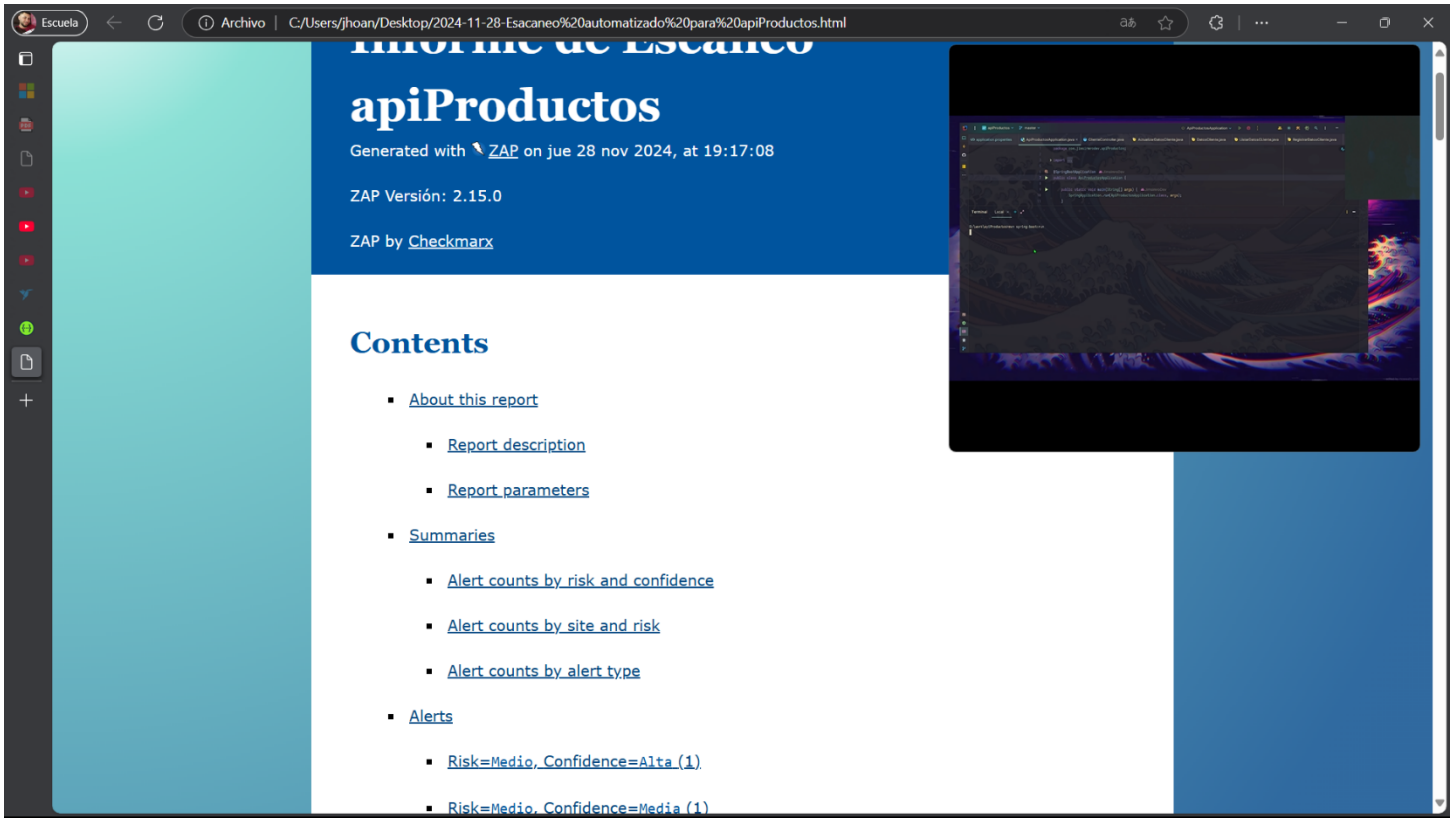
Técnica	Descripción	Herramientas	Ventajas	Desventajas
Análisis estático (SAST)	De acuerdo con (CHECK POINT, s.f. párr 1) es una prueba de seguridad que se le realiza al software con el fin de identificar vulnerabilidades, realizando un escaneo en el código fuente de la aplicación, los archivos binarios y el código en bytes.	• **SonarQube** • **Checkmarx** • **Fortify** • **Veracode** • **Synopsys** • **Coverity**	Segun (CHECK POINT, s.f. párr 6) una de sus ventajas son Aparición temprana en SDLC y Detección de vulnerabilidad común	Segun (CHECK POINT, s.f. párr 8)sus desventajas son: Ser específico del idioma, La incapacidad de detectar todas las vulnerabilidades, Tasas altas de falsos positivos y Pruebas frecuentes y que requieren mucho tiempo
Análisis dinámico (DAST)	Es una prueba de seguridad que se realiza a el software en tiempo de ejecución para detectar vulnerabilidades mediante pruebas de instrucción en aplicaciones móviles o web atreves del frontend (Morales, 2023)	Burp Suite: Ofrece una amplia gama de herramientas para pruebas de seguridad de aplicaciones web. Acunetix: Detecta vulnerabilidades como inyecciones SQL y cross-site scripting (XSS). Netsparker: Realiza pruebas automatizadas de seguridad para aplicaciones web. AppScan: Proporciona análisis de seguridad y gestión de vulnerabilidades. OpenVAS:	Es independiente de la aplicación, detecta inmediatamente vulnerabilidades que podrían ser explotadas y no requieren acceso al código fuente	No encuentra la ubicación exacta de una vulnerabilidad en el código, se necesitan conocimientos de seguridad para interpretar los informes, las pruebas pueden llevar mucho tiempo,
Pruebas de penetración	Es un ciberataque simulado “hacking etico” con el fin de encontrar	Metasploit: Es una plataforma muy conocida que ofrece una	Según ((easydmarc, 2022)) algunas de sus ventajas son encontrar vulnerabilidades, detecta	Puede causar daño si hace de forma incorrecta, los

	vulnerabilidades en el sistema informático (IBM, s.f. pàrr 1)	amplia colección de exploits listos para usar. Nmap: Herramienta gratuita y de código abierto diseñada para el escaneo rápido y el mapeo de redes. Burp Suite: Utilizada principalmente para pruebas de seguridad de aplicaciones web. Nessus: Detecta vulnerabilidades en sistemas operativos, aplicaciones y dispositivos de red. SQLMap: Especializada en la detección y explotación de vulnerabilidades de inyección SQL. Wireshark: Utilizada para el análisis de redes y captura de paquetes. BeEF (Browser Exploitation Framework): Se enfoca en pruebas de seguridad de navegadores web. John the Ripper: Herramienta para pruebas de fuerza bruta en contraseñas. (Microsoft Copilot, 2024).	debilidades grandes que resultan de vulnerabilidades pequeñás	resultados pueden ser engañosos
Pruebas de caja negra	Las pruebas de caja negra evalúan la funcionalidad del software sin conocer su código fuente	Selenium: Utilizada principalmente para pruebas de automatización de navegadores web. JUnit: Un marco de pruebas unitarias para Java. QTP (Quick Test Professional): Herramienta de pruebas funcionales y de regresión.	No ayuda a medir la capacidad que tiene de respuesta el software ante un posible riesgo, evalúan al software de manera imparcial y objetiva y detecta de manera ágil los errores que afectan la	Tiene limitaciones ya que necesitan permisos específicos para evaluar todo el sistema, no detectar todos los atauques cibernéticos, no identifica la causa de algún fallo o erro al no tener acceso al código fuente. (Chavez, 2024)

		LoadRunner: Utilizada para pruebas de carga y rendimiento. JMeter: Herramienta de pruebas de rendimiento y carga para aplicaciones web.	experiencia de usabilidad	
Pruebas de caja blanca	Las pruebas de caja blanca evalúan el software con conocimiento del código fuente y su estructura interna	JUnit: Utilizada para pruebas unitarias en aplicaciones Java. NUnit: Similar a JUnit, pero para aplicaciones .NET. TestNG: Una herramienta poderosa para pruebas en Java que supera algunas limitaciones de JUnit. Emma/JaCoCo: Utilizadas para análisis de cobertura de código en proyectos Java. Clover Groovy CppUnit PyTest	Las ventajas que tiene es que necesitan menos tiempo ya que el evaluador conoce el sistema, es fácil visualizar los problemas y las vulnerabilidades.	Las desventajas es que requiere tener amplio conocimiento de programación, tiene altas limitaciones para realizar simulaciones y puede dejar pasar vulnerabilidades que son notables para los atacantes externos.

Realizar un testing de seguridad a su API con la herramienta OwaspZAP, para eso siga los siguientes pasos:

Imagen autoría propia



Enlace del video: https://youtu.be/7OOH2w0qzrg

Referencias

Chavez, J. J. (30 de 06 de 2024). *deltaprotect*. Obtenido de deltaprotect: https://www.deltaprotect.com/blog/pruebas-de-caja-negra

checkpoint. (s.f.). *checkpoint*. Obtenido de checkpoint: https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-dynamic-application-security-testing-dast/