JULIO ANTHONY ENGELS RUIZ COTO - 1284719

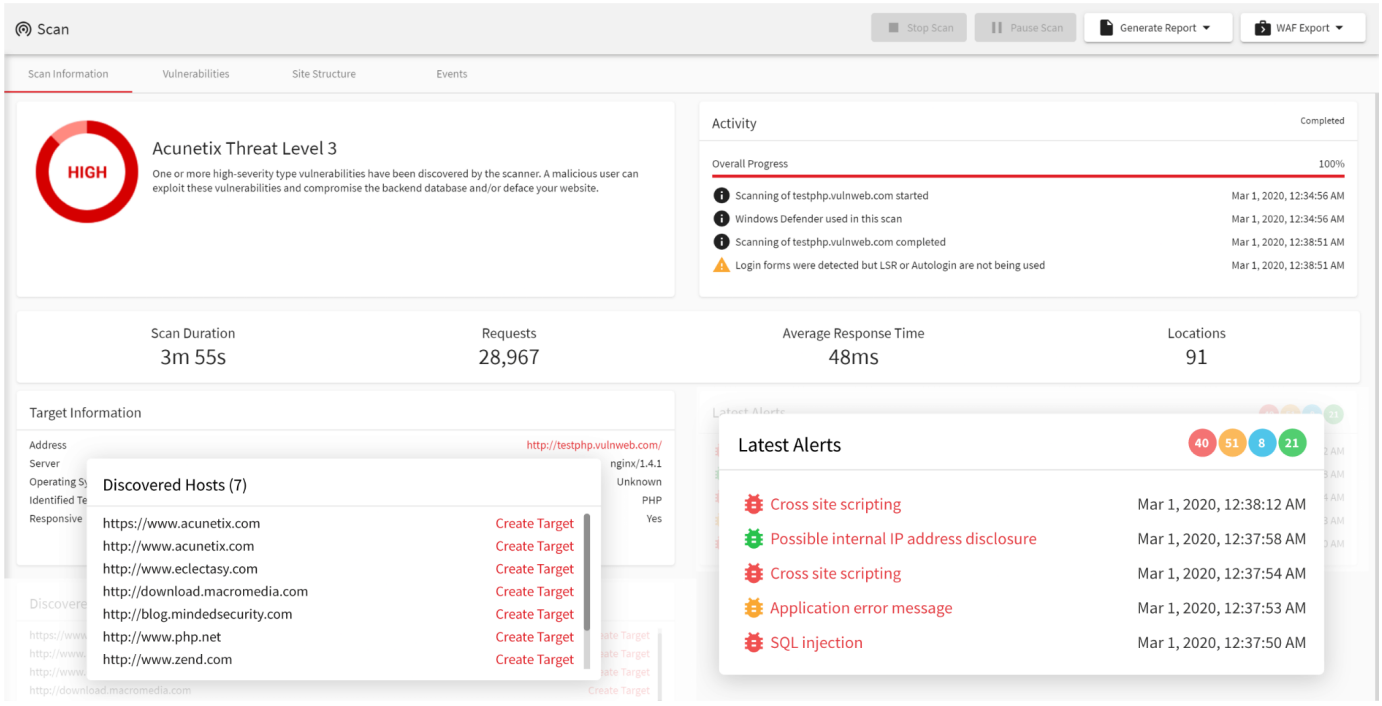
EDDIE ALEJANDRO GIRÓN CARRANZA - 1307419

1. Deberán investigar 2 diferentes escáneres de seguridad caja negra para aplicaciones web. Indicar sus: Ventajas

- Limitaciones
- Un pantallazo de sus posibles resultados

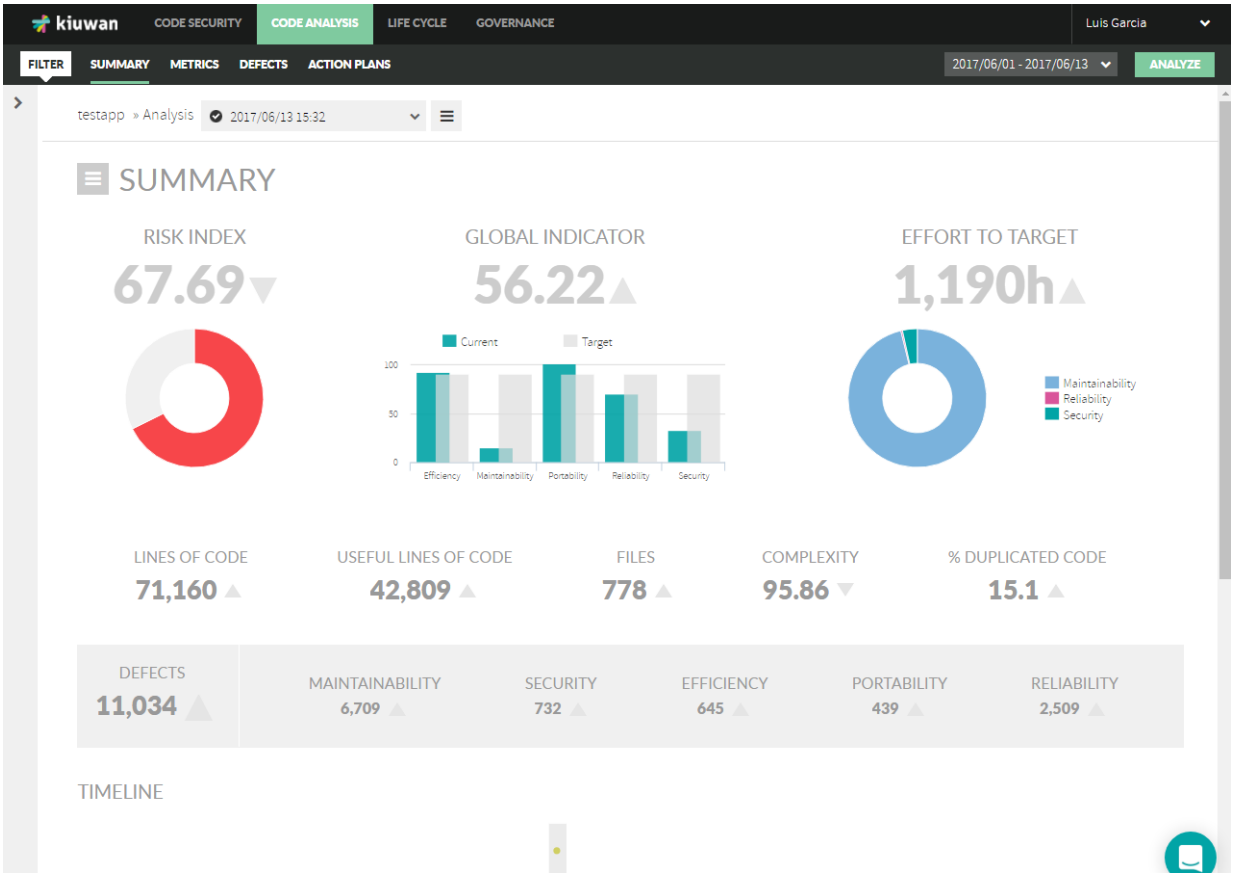
Acunetix

- **Ventajas**:
  - Proporciona informes detallados y soluciones a problemas.
  - Escáner web automatizado que detecta vulnerabilidades como SQL Injection, XSS, entre otros.
  - Interfaz amigable y fácil de usar.
- **Limitaciones**:
  - La versión completa es de pago.
  - Puede tener problemas al escanear aplicaciones web muy grandes o complejas.



Kiuwan Code Security Insights

- **Ventajas**:
  - **Integración con el ciclo de vida del desarrollo**: Se integra fácilmente con herramientas de CI/CD, lo que permite a los equipos detectar y solucionar problemas de seguridad en las primeras etapas del desarrollo.
  - **Análisis estático (SAST)**: Proporciona análisis estático de código fuente para identificar vulnerabilidades sin necesidad de ejecutar el código.
  - **Cumplimiento de estándares**: Ayuda a los equipos a cumplir con estándares de seguridad y regulaciones específicas, como OWASP Top 10, PCI DSS, entre otros.
- **Limitaciones**:
  - **Curva de aprendizaje**: Aunque ofrece una interfaz intuitiva, los usuarios pueden necesitar tiempo para familiarizarse completamente con todas sus características y capacidades.
  - **Dependencia de la nube**: Algunas empresas pueden tener restricciones en cuanto a enviar código a soluciones basadas en la nube debido a políticas de seguridad.



2. Investigar sobre al menos 3 de las herramientas disponibles en Kali linux e indicar:

- Cómo éstas pueden aplicarse a mejorar la seguridad de un equipo de TI

Metasploit

- **Aplicación para mejorar la seguridad**: Metasploit es un marco de pruebas de penetración que permite a los profesionales de TI simular ataques en sus sistemas en un entorno controlado. Al identificar vulnerabilidades utilizando Metasploit, el equipo de TI puede corregirlas antes de que sean explotadas por actores maliciosos.

Hydra

- **Aplicación para mejorar la seguridad**: Hydra es una herramienta de ataque de fuerza bruta rápida y flexible que permite a los administradores de sistemas comprobar la robustez de las contraseñas en sus sistemas. Puede ser utilizado para asegurarse de que los usuarios y administradores estén utilizando contraseñas fuertes y no fácilmente adivinables o crackeables.

Nmap

- **Aplicación para mejorar la seguridad**: Nmap es una herramienta de escaneo de puertos que puede ser utilizada para descubrir dispositivos que se ejecutan en una red y encontrar puertos abiertos junto con diversos atributos del mismo. El equipo de TI puede usar Nmap para identificar puertos abiertos y servicios innecesarios que se ejecutan, y cerrarlos o bloquearlos para mejorar la seguridad.