GMV Penbot

INNOVATING SOLUTIONS

INTELIGENCIA ARTIFICIAL Y BIG DATA

Aplicación de pentesting automático impulsada por IA para la detección automatizada de vulnerabilidades web

Las vulnerabilidades de la web son una amenaza importante para las organizaciones que puede hacer que los atacantes accedan a datos confidenciales, comprometan los sistemas y causen daños económicos. Estas vulnerabilidades se destacan en los 10 principales riesgos de seguridad de las aplicaciones web del OWASP, una lista anual en la que se identifican las diez vulnerabilidades de seguridad de las aplicaciones web más críticas, publicada por el Open Web Application Security Project (OWASP).

GMV Penbot es una herramienta de pentesting automático basada en Inteligencia Artificial mediante Aprendizaje por Refuerzo, cuyo objetivo es la detección de vulnerabilidades de ciberseguridad descritas en el TOP 10 de OWASP.

marketing.TIC@gmv.com

gmv.com

IA PARA PROTEGERTE DE LAS VULNERABILIDADES EN LA WEB

Recopilación de información → Evaluación de vulnerabilidades/ Scanning → Explotación → Informe de vulnerabilidades

¿Para qué sirve?

- **Detección de vulnerabilidades**
  Tanto de ataques de inyección ® SQL, roban información de bases de datos, como de ataques ® XSS, se utilizan para redirigir a los usuarios a sitios web donde los atacantes pueden robarles datos.

- **Elaboración de informes**
  Informes de pentesting sobre las vulnerabilidades encontradas.

¿Qué ventajas ofrece?

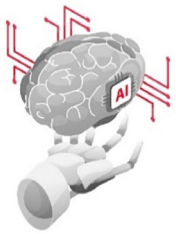
- **Técnicas de Aprendizaje por Refuerzo**
  Aprende y optimiza sus acciones mediante retroalimentación continua y se entrena en entornos de laboratorio que simulan escenarios de vulnerabilidad del mundo real.

- **Automatización Inteligente**
  Herramienta automática, programable y parametrizable a través de una interfaz gráfica intuitiva y funcional.

- **Cobertura total**
  Detecta vulnerabilidades según OWASP Top Ten WEB.

- **Integración de herramientas profesionales de pentesters**
  Integra y automatiza herramientas probadas y utilizadas por pentester expertos que el agente parametriza de forma inteligente y sin intervención humana, maximizando la efectividad en forma de reducción de tiempos de ataque y extracción de vulnerabilidades con diferentes niveles de criticidad.

Beneficios para tu empresa



- **Ahorro de tiempo y costes**
  Reduce los costes asociados a las brechas de la seguridad, como la pérdida de datos y los daños a la reputación. Al reducir la necesidad de intervención humana constante, la empresa puede optimizar el uso de sus recursos.

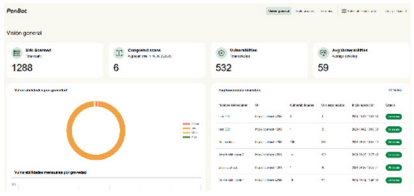
- **Supervisión continua**
  Las exploraciones periódicas garantizan que las nuevas vulnerabilidades introducidas con las actualizaciones de software se detecten y mitiguen rápidamente.

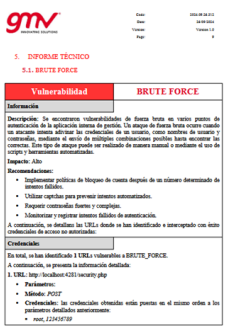
- **Cumplimiento de la normativa**
  Cumplimiento de las normas de seguridad mediante demostraciones de pruebas de seguridad continuas y eficaces.

- **Eficiencia operativa**
  Automatiza las tareas repetitivas. Las pruebas automatizadas garantizan que todos los componentes se prueben de forma exhaustiva, coherente y uniforme.

- **Sencillez y facilidad de uso**
  La interfaz intuitiva facilita el uso de la aplicación por personal no técnico, democratizando el acceso a las herramientas de seguridad dentro de la organización.

- **Escalabilidad**
  La automatización permite que las pruebas de seguridad escalen con el crecimiento de la empresa.





gmv.com