OWASP ZAP

Descripción

OWASP ZAP es una herramienta de escaneo de seguridad para aplicaciones web, mantenida por OWASP. Detecta vulnerabilidades como XSS, SQLi, etc.

Uso local

```
# Interfaz gráfica
zap.sh

# Escaneo desde CLI
zap-baseline.py -t http://localhost:8080 -r reporte.html
```

Reportes

- HTML, XML, Markdown.
- Exportables a JIRA, DefectDojo, etc.

Integración en CI/CD

- Una acción de GitHub para ejecutar el ZAP Baseline scan para encontrar vulnerabilidades en su aplicación web.

```
  - name: ZAP Scan
    uses: zaproxy/action-baseline@v0.14.0
    with:
      token: ${{ secrets.GITHUB_TOKEN }}
      docker_name: 'ghcr.io/zaproxy/zaproxy:stable'
      target: 'https://www.zaproxy.org'
      rules_file_name: '.zap/rules.tsv'
      cmd_options: '-a'
```

Integraciones

- GitHub, Jira (plugin).
- Slack, Teams: notificaciones mediante scripting.

- VSCode: sin integración directa, pero puede abrirse con CLI.

UI

- GUI muy completa (modo GUI, CLI y daemon).

Licencia

- **Open source (Apache 2.0)**.
- Disponible para máquinas virtuales, también en Docker.

Facilidad de uso

- Moderado. Ideal para usuarios con conocimiento en pruebas de seguridad web.

Cumplimiento con estándares:

- **OWASP:** Está alineado directamente con el OWASP Top 10, siendo una herramienta oficial de la fundación.
- **NIST:** Se alinea con NIST 800-53 (RA-5: escaneo de vulnerabilidades, CA-7: monitoreo continuo).
- **ISO/IEC 27001:** Permite cumplir con controles como A.12.6.1 (gestión de vulnerabilidades) y A.14.2.8 (pruebas técnicas).
- **PCI DSS:** Soporta los requerimientos de pruebas de seguridad continuas (requisito 11.2).

Revisión #12
Creado 16 julio 2025 17:40:51
Actualizado 16 julio 2025 22:37:39