Faraday

Descripción

Faraday es una plataforma de gestión de vulnerabilidades que permite integrar resultados de herramientas de análisis de seguridad y centralizar reportes orientada a equipos de seguridad, pentesters y procesos de DevSecOps.

Permite:

- Consolidar hallazgos de múltiples herramientas de análisis.
- Gestionar y priorizar vulnerabilidades de forma centralizada.
- Colaborar en tiempo real en auditorías y pruebas de seguridad.

Funciona como un **servidor central** con una interfaz web y un cliente CLI (`faraday-cli`) que facilita la autenticación, gestión de workspaces y la carga automática de reportes a la plataforma, lo que permite integrarlo en pipelines de CI/CD. Soporta múltiples formatos de reportes y herramientas de seguridad, como Trivy, OpenVAS, Nessus, Burp Suite, etc.

Uso local

Faraday se puede ejecutar localmente mediante Docker o instalación directa en Linux.
Ejemplo con Docker:

```
docker run -it -p 5985:5985 -v faraday_data:/home/faraday/.faraday faradaysec/faraday
```

CLI básico

Iniciar sesión:

```
faraday-cli auth login --server https://<host>:5985 --username faraday --password <pass>
```

Subir un reporte:

```
faraday-cli tool report ./trivy-report.json --workspace <workspace>
```

Listar workspaces:

```
faraday-cli workspace list
```

Reportes

Faraday procesa los reportes de herramientas de seguridad y los almacena en un **workspace**.

- **Ubicación de datos**: Principalmente en la sección **Assets**, donde se relacionan vulnerabilidades con hosts, servicios o aplicaciones.
- **Dashboard**: No siempre muestra todo automáticamente, ya que prioriza métricas y gráficos generales.
- **Formatos soportados**: XML, JSON, CSV y formatos nativos de herramientas como Nessus, OpenVAS, Trivy, Burp, Nmap, etc.

Integración en CI/CD

Faraday puede integrarse en pipelines para subir reportes automáticamente después de un escaneo.

```
      - name: Generate Trivy Filesystem Report
        uses: aquasecurity/trivy-action@master
        with:
          scan-type: fs
          output: trivy-fs-report.json
          format: json
          scan-ref: .
          exit-code: 0

      - name: Upload Trivy reports
        run: |
          faraday-cli tool report -w "$WORKSPACE" trivy-fs-report.json
```

Integraciones

- **Herramientas compatibles**: Trivy, OpenVAS, Burp Suite, Nessus, Nikto, Nmap, OWASP ZAP, etc.
- **Colaboración**: Slack, Jira y otros mediante API.
- **Automatización**: API REST para crear workspaces, subir hallazgos y consultar datos.

UI

- Interfaz web accesible desde cualquier navegador.
- Funcionalidades:
  - Vista de **Assets** y vulnerabilidades asociadas.
  - **Dashboard** con métricas, severidad y gráficos.
  - Administración de **workspaces**, usuarios y roles.
  - Filtros avanzados para priorizar hallazgos.

Licencia

- Faraday **Community Edition**: Licencia GPLv3 (código abierto).
- Faraday **Professional & Corporate**: Licencia comercial con características avanzadas.

Facilidad de uso

- **Ventajas**:
  - Compatible con una gran variedad de herramientas.
  - CLI intuitiva y scripts de automatización.
  - Dashboard centralizado para equipos.
- **Desafíos**:
  - Requiere configuración inicial de SSL y credenciales.
  - Algunos formatos de reporte necesitan preprocesado, tienes que asegurarte de que esté en un formato estructurado y limpio que Faraday pueda leer.

Cumplimiento con estándares

Faraday no certifica por sí mismo estándares, pero **facilita el cumplimiento** al centralizar la gestión de vulnerabilidades y permitir auditorías trazables.

- **OWASP**: Compatible con flujos de seguridad recomendados, soporta OWASP ZAP y otras herramientas.
- **NIST 800-53 / 800-115**: Permite documentar, priorizar y remediar vulnerabilidades según guías NIST.
- **ISO 27001**: Ayuda a implementar controles de seguridad relacionados con la identificación y tratamiento de riesgos.

Revisión #3
Creado 2025-08-14 01:56:02 UTC
Actualizado 2025-08-14 02:25:29 UTC