<https://subgraph.com/vega/>

Vega es una plataforma de pruebas de seguridad de aplicaciones web de código abierto desarrollada para identificar vulnerabilidades en aplicaciones web. Es especialmente útil para profesionales de la seguridad, desarrolladores y auditores de seguridad que desean realizar análisis de seguridad en sus aplicaciones web.

**Características Principales de Vega**

1. **Escaneo Automático de Vulnerabilidades**: Detecta vulnerabilidades comunes como inyecciones SQL, inyecciones de comando, inyecciones de código, y vulnerabilidades de Cross-Site Scripting (XSS).
2. **Interfaz Gráfica de Usuario (GUI)**: Ofrece una interfaz gráfica intuitiva que facilita la configuración y ejecución de escaneos.
3. **Intercepción de Proxy**: Funciona como un proxy interceptador que permite a los usuarios inspeccionar y modificar el tráfico HTTP/HTTPS.
4. **Scripts Personalizados**: Permite a los usuarios escribir scripts personalizados en JavaScript para extender la funcionalidad de escaneo.
5. **Actualizaciones de Vulnerabilidades**: Se actualiza regularmente para incluir nuevas reglas de detección de vulnerabilidades.

**Instalación y Configuración**

**Requisitos del Sistema**

* Java Runtime Environment (JRE) 1.7 o superior.
* Sistema operativo compatible (Windows, macOS, Linux).

**Paso 1: Descargar Vega**

1. Visita la página oficial de Vega.
2. Descarga la versión adecuada para tu sistema operativo.

**Paso 2: Instalar Vega**

1. Extrae el archivo descargado.
2. En Windows, ejecuta Vega.exe. En macOS, arrastra la aplicación a la carpeta de aplicaciones. En Linux, navega al directorio de Vega y ejecuta ./vega.

**Uso de Vega**

**Paso 1: Configurar un Nuevo Escaneo**

1. Abre Vega.
2. Ve a Scan > Start New Scan (Escaneo > Iniciar Nuevo Escaneo).
3. Introduce la URL del objetivo que deseas escanear.
4. Configura las opciones de escaneo según tus necesidades, como la profundidad del escaneo y los módulos de análisis a utilizar.

**Paso 2: Ejecutar el Escaneo**

1. Haz clic en Next (Siguiente) después de configurar las opciones del escaneo.
2. Revisa la configuración y haz clic en Finish (Finalizar) para iniciar el escaneo.
3. Vega comenzará a escanear la aplicación web objetivo y mostrará el progreso en tiempo real.

**Paso 3: Revisar los Resultados**

1. Una vez completado el escaneo, revisa los resultados en la interfaz de Vega.
2. Los resultados estarán clasificados por tipo de vulnerabilidad y severidad.
3. Haz clic en cada vulnerabilidad para obtener más detalles y recomendaciones sobre cómo remediarla.

**Funcionalidades Adicionales**

* **Proxy Interceptador**:
  + Ve a Proxy > Start Proxy (Proxy > Iniciar Proxy).
  + Configura tu navegador para usar Vega como proxy (puedes encontrar las instrucciones detalladas en la documentación de Vega).
  + Inspecciona y modifica las solicitudes y respuestas HTTP/HTTPS en tiempo real.
* **Scripts Personalizados**:
  + Ve a Scripts > Script Manager (Scripts > Gestor de Scripts).
  + Crea y administra scripts personalizados en JavaScript para automatizar tareas específicas de escaneo.

**Mejoras Continuas**

* **Actualizaciones**: Asegúrate de mantener Vega actualizado para beneficiarte de las últimas mejoras y detecciones de vulnerabilidades.
* **Contribuciones**: Al ser de código abierto, puedes contribuir al desarrollo de Vega a través de su repositorio en GitHub.

Vega es una herramienta poderosa y flexible para la seguridad de aplicaciones web, ideal tanto para usuarios principiantes como para profesionales avanzados que buscan identificar y remediar vulnerabilidades en sus aplicaciones.