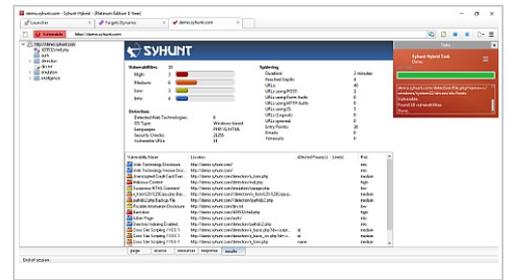


Syhunt Code Plus es un scanner estático de seguridad diseñado para probar aplicaciones **móviles** y **web** escritas en una variedad de lenguajes.

Encuentre las partes vulnerables del código en minutos y aplique parches antes de poner las actualizaciones de la aplicación móvil a disposición o antes de poner una aplicación web en producción.



ANÁLISIS DE SEGURIDAD DE CÓDIGO WEB

- **1300+** vulnerabilidades detectadas, que cubren más de 40 tipos de ataques de seguridad.
- Realiza un análisis profundo del código fuente de **aplicaciones web** en **ASP.Net (C# & VB.Net), Java (JEE / JSP), JavaScript, Lua, Perl, PHP, Python, Ruby (Rails / ERB) y TypeScript**, por vulnerabilidades e destacando áreas clave del código para revisión inmediata.
- Compatible con aplicaciones web que utilizan **MongoDB, Express.js, Angular, AngularJS, Node.js y Koa**.
- Compatible con aplicaciones web creadas con **Django, mod_python, Python CGI y WSGI**.

COBERTURA E INTEGRACIONES

- Analiza las Diez Principales Vulnerabilidades de Seguridad de Aplicaciones Web Más críticas y otras listas OWASP, XSS, inyección SQL, inclusión de archivos, ejecución de comandos y más, vía análisis estático o dinámico (**Ver todos las verificaciones**).
- Detecta vulnerabilidades de inyección SQL que afectan a más de 17 tipos de bases de datos.
- Es compatible con **GitLab** y **Jenkins** para la Integración Continua (CI), **JIRA, GitHub** y **GitLab** para el seguimiento de problemas, **Imperva** y **F5 BIG-IP ASM** para remediación virtual de vulnerabilidades.

SEGURIDAD DE APLICACIONES MÓVILES

- Realiza un análisis profundo del código fuente de **aplicaciones móviles** (Android y iOS) escritas en **Java, Objective-C, C, C++ y Swift**
- Encuentra las 10 principales vulnerabilidades de OWASP Mobile, como almacenamiento inseguro de datos, comunicación insegura, autenticación insegura, criptografía insuficiente, autorización insegura y más.
- Realiza análisis de **APK de Android**.
- Compatible con aplicaciones que utilizan **MongoDB, Express.js, Angular, AngularJS, Node.js y Koa**.

ELABORACIÓN DE INFORMES

- Crea informes completos que contienen todos los detalles sobre las vulnerabilidades identificadas, gráficos, estadísticas, referencias como **CVE, CWE** y también:
- Vectores **CVSS3**, que transmiten la gravedad de la vulnerabilidad y ayudan a determinar la urgencia y la prioridad de respuesta.
- Informe de conformidad relacionado con OWASP Top 10, OWASP PHP Top 5, CWE / SANS Top 25, Clasificación de amenazas WASC, el estándar PCI DSS, etc.
- La evolución de las vulnerabilidades a lo largo del tiempo.
- Disponible en **HTML, PDF, JSON, XML, texto y CSV**.

Para obtener más información sobre Syhunt, visite:

www.syhunt.com/es