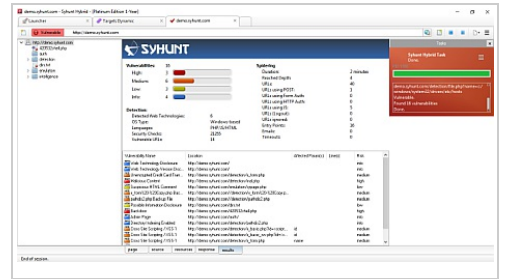


Syhunt Dynamic Augmented es un scanner de seguridad de aplicaciones web que automatiza completamente las pruebas de seguridad, protegiendo de forma proactiva la infraestructura **Web** de su organización contra todo tipo de amenazas de seguridad de aplicaciones, incluyendo ataques inferenciales, dentro y fuera de banda a través de su análisis dinámica aumentada



PRUEBAS DINÁMICAS DE SEGURIDAD

- **5700+** vulnerabilidades de seguridad en aplicaciones web en más de 70 categorías, incluyendo ataques **inferenciales, dentro y fuera de banda**.
- Prueba cualquier tipo de aplicación web en funcionamiento, incluídos **ASP.NET (C# y VB), Java (JEE / JSP), JavaScript, Node.js, Lua, Perl, PHP, Python y Ruby**
- Realiza una prueba de penetración web completa.
- **Mapeo profundo** (spidering) y automatizado de la estructura del sitio web, con localización de puntos de entrada (todos los enlaces, formularios y solicitudes XHR) con soporte **HTML5 y JS**.
- Optimizado para probar sitios web en una variedad de frameworks, servidores (**Apache, Tomcat, IIS, Nginx**, etc) y plataformas (Windows, Unix y otros sistemas).

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.

ANÁLISIS DINÁMICO AUMENTADO

- Detecta variantes invisibles (fuera de banda) de ejecución de comandos, inclusión de archivos, falsificación de petición en el lado del servidor, inyección de SQL y de XXE.
- Estas vulnerabilidades no se detectan por herramienta de DAST convencional.
- Observa requisiciones forzadas provenientes de un servidor web vulnerable a lo largo de un escaneo..
- Muestra la exfiltración de datos de un servidor web vulnerable objeto de análisis.
- Devuelve **cero falsos positivos**.

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