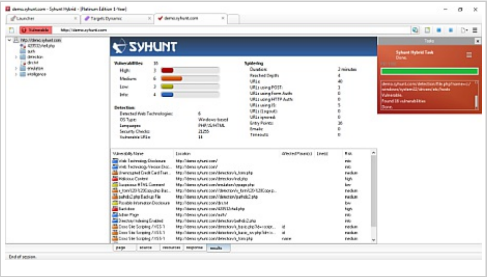
SYHUNT® CODE PLUS



Syhunt Code Plus is a static application security scanner designed for testing **Mobile** and **Web** applications written in a variety of languages. Find the vulnerable portions of the code in minutes and patch them before making mobile application updates available to users or before putting a web application in production.

STATIC APPLICATION SECURITY TESTING

- **1300+** vulnerabilities detected in over 40 types of flaws.
- Performs deep analysis of the source code of **Web applications** in **ASP.Net (C# & VB.Net), Java (JEE / JSP), JavaScript, Kotlin, Lua, Object Pascal / Delphi, Perl, PHP, Python, Ruby (Rails / ERB) & TypeScript**, finding vulnerabilities, and identifying and highlighting key areas of the code for prompt review.
- Supports web applications that use **MongoDB, Express.js, Angular, AngularJS, Node.js & Koa**.
- Supports web applications built using **Django, mod_python, Python CGI & WSGI**.

COVERAGE & INTEGRATIONS

- Scans for the Top Ten Most Critical Web Application Security Vulnerabilities, PHP Top 5 Vulnerabilities and other OWASP lists, XSS (Cross-Site Scripting), SQL Injection, File Inclusion, Command Execution, and more, both via static and dynamic analysis (View All Checks).
- Detects SQL Injection involving over 17 database types.
- Integrates with **DefectDojo**, **Faraday**, **GitHub**, **GitLab**, **Jenkins** and **JIRA** for Continuous Integration (CI) and issue tracking, **Imperva**, **F5 BIG-IP ASM** and **ModSecurity** for virtual bug patching.

MOBILE APPLICATION SECURITY TESTING

- Performs deep analysis of the source code of **Mobile applications** (Android & iOS) written in **Java, Kotlin, Object Pascal (Delphi XE), Objective-C, C, C++ & Swift**
- Finds OWASP Mobile Top 10 vulnerabilities, such as Insecure Data Storage, Insecure Communication, Insecure Authentication, Insufficient Cryptography, Insecure Authorization and more.
- Performs **Android APK** analysis.
- Supports applications that use **MongoDB, Express.js, Angular, AngularJS, Node.js & Koa**.

REPORT GENERATION

- Generates comprehensive reports containing all the details about the identified vulnerabilities, charts, statistics, references such as **CVE** and **CWE** and also:
- **CVSS3** Vectors, which convey vulnerability severity and help determine urgency and priority of response, with sorting of the identified flaws based on their CVSS score.
- Compliance information related to the OWASP Top 10, OWASP PHP Top 5, CWE/SANS Top 25, WASC Threat Classification, the PCI DSS standard, and so on.
- Displays the evolution of vulnerabilities over time.
- Available in several file formats, including **HTML, PDF, JSON, XML, text** and **CSV**.

For more information about Syhunt, visit:

www.syhunt.com