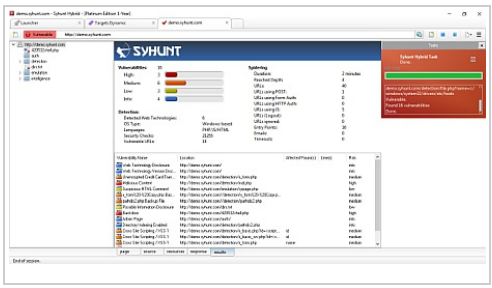
SYHUNT

HYBRID PLA/STD



Syhunt Hybrid is a hybrid web application security scanner designed for testing **Web** applications written in a variety of languages. Syhunt combines dynamic and static testing approaches, performing over 1500 checks, proactively defending websites against security threats and quickly finding existing vulnerabilities before the hackers.

DYNAMIC APPLICATION SECURITY TESTING

- **5700+** dynamic web application security vulnerabilities in over 70 categories of web attacks, including **inferential**, **in-band** and **out-of-band** attacks.
- Scans any kind of live web application, especially web applications written in **ASP.NET (C# & VB.Net), Java (JEE / JSP), JavaScript, Node.js, Lua, Perl, PHP, Python & Ruby**
- Able to perform a complete penetration test of the web application layer.
- **Deep crawling** (spidering), complete and automated website structure mapping, locating entry points (all links, forms and XHR requests) with **HTML5** and **JS** support.
- Optimized for testing websites using a variety of frameworks running under a variety of servers (**Apache, Tomcat, IIS, Nginx**, and so on) and platforms (Windows, Unix, and other systems).

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 vulnerabilities involving over 17 database types.
- Integrates with **GitLab** and **Jenkins** for Continuous Integration (CI), **JIRA**, **GitHub** and **GitLab** for issue tracking, **Imperva** and **F5 BIG-IP ASM** for virtual vulnerability patching.

STATIC APPLICATION SECURITY TESTING

- **1300+** vulnerabilities detected, covering over 40 types of security attacks.
- Performs deep analysis of the source code of **Web applications** in **ASP.Net (C# & VB.Net), Java (JEE / JSP), JavaScript, Lua, 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**.

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