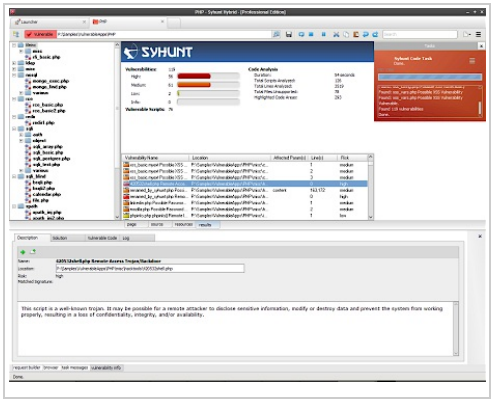
SYHUNT®

SYHUNT CODE PLUS

SOURCE CODE SECURITY ANALYZER

Syhunt® Code Plus is the first friendly, easy to use and capable commercial tool for doing deep analysis of the source code of web and mobile applications. Syhunt Code makes developers and QA testers life easier by automatically uncovering multiple classes of application vulnerabilities.

KEY FEATURES



Syhunt Code Plus is a leading-edge static application security testing tool, expertly crafted to assess and fortify the security of mobile and web applications. It is distinguished by its support for a diverse array of programming languages and technologies, including ASP.Net, Java, and Python, among others. This robust tool excels in detecting a wide range of vulnerabilities, over 1300 in total, making it an indispensable asset for identifying critical security issues promptly and accurately.

At the core of its functionality, Syhunt Code Plus offers deep source code analysis, ensuring thorough examination and security assessment of various code types. Its compatibility with numerous web and mobile application frameworks further enhances its versatility. The tool's seamless integration with a variety of Continuous Integration/Continuous Deployment (CI/CD) and issue tracking tools streamlines the development process, embedding security into the software development lifecycle.

Furthermore, Syhunt Code Plus is renowned for its detailed reporting capabilities. It generates comprehensive reports, complete with vulnerability severity scores and compliance information, which are invaluable in prioritizing and addressing security concerns in an efficient and effective manner. These reports serve as a critical resource for developers and security professionals alike, providing actionable insights to fortify application security.

With Syhunt Code Plus, you can:

- Detect over **1300** vulnerabilities, covering over **40** types of web security attacks.
- Scan the source code of web applications written in ASP.Net (C# & VB.Net), Java (JEE / JSP), JavaScript, Kotlin, Lua, Object Pascal / Delphi, Perl, PHP, Python, Ruby (Rails / ERB) and TypeScript for vulnerabilities.
- Perform deep analysis of the source code of Mobile applications (Android & iOS) written in Java, Kotlin, Object Pascal (Delphi XE), Objective-C, C, C++ and Swift, and find OWASP Mobile Top 10 vulnerabilities, such as Insecure Data Storage, Insecure Communication, Insecure Authentication, Insufficient Cryptography, Insecure Authorization and more.
- Analyze the source code of web applications and detect cross-site scripting, file inclusion, SQL injection,

command execution, validation problems and more.

- Identify key areas of the code, such as key HTML tags, JavaScript, XHR requests, entry points and interesting keywords.
- Generate reports in HTML and multiple other formats - reported vulnerabilities are sorted by default based on their CVSS3 score.

Some of the key technologies supported by the Syhunt Code Plus scanner:

CHECK FOR ALL KINDS OF VULNERABILITIES

Check	CWE
>_ **Command Execution**	CWE-78
SQL Injection	CWE-89
SQL Injection (Functional)	
SQL Injection (Object-Oriented)	
SQL Injection (Hibernate/HQL)	

File Inclusion	CWE-98
Local File Inclusion	
Remote File Inclusion	
Cross-Site Scripting (XSS)	CWE-79
Weak XSS Validation	CWE-79
Hidden Entry Points	
Web-Backdoors	
Debug Parameters	
NoSQL Injection	
Unvalidated Redirects	CWE-601
Arbitrary File Manipulation	CWE-73
HTTP Response Splitting	CWE-113
LDAP Injection	CWE-90
XML External Entity (XXE) Injection	CWE-827
XPath Injection	CWE-643
Server-Side Request Forgery	CWE-918
Log Forging	CWE-117
Information Disclosure	CWE-497
Common Form Weaknesses	
Weak Password Hashing	