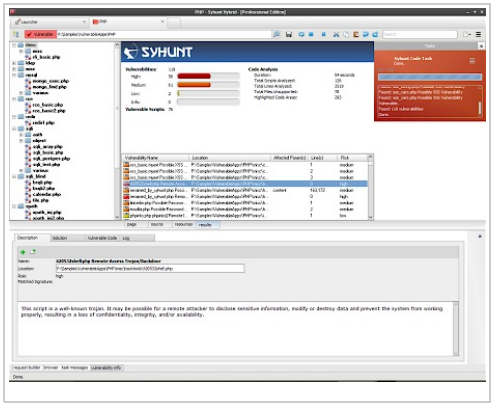
SYHUNT [CODE]

SOURCE CODE SECURITY ANALYZER

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

KEY FEATURES

Syhunt Code enables developers and QA testers to automatically scan any kind of web application source code for potential security vulnerabilities. Syhunt Code has been designed to scan web applications for various types of issues, such as Cross-Site Scripting (XSS), File Inclusion, SQL Injection, Command Execution and more. Additionally, by identifying key areas of the code, Syhunt Code helps auditors perform code reviews better, faster and more efficiently.



Syhunt Code is a perfect complement to the already extensive set of URL scanning capabilities available in the Syhunt Dynamic scanner, making the two products combined in the form of Syhunt Hybrid the most comprehensive solution for those concerned about web application security.

With Syhunt Code, 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, Lua, Perl, PHP, Python, Ruby (Rails / ERB) and TypeScript for vulnerabilities.
- 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 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	

MICROSOLVED, INC.

❝ We have identified significant vulnerabilities [using Syhunt Code]. Several products we reviewed were found to have various types of injection vulnerabilities, arbitrary file disclosure and access issues and tons of XSS problems.

Brent Huston, CEO,
MicroSolved, Inc.

STEALTH - ISS INC.

❝ We have used Syhunt for years because it`s been the best web app security assessment tool out there. Rapidly updated to cover new vulnerabilities as they arise and very easy to use

Robert Davies, CEO, Stealth-ISS

For more information about Syhunt, visit **www.syhunt.com**