



SYHUNT (HYBRID)

WEB APPLICATION SECURITY SCANNER

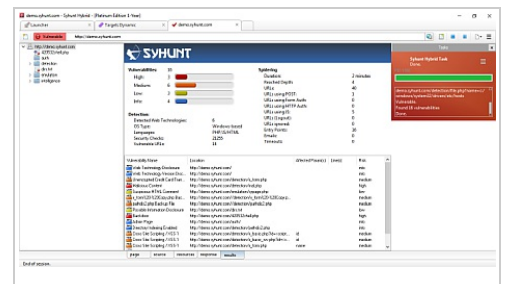


Syhunt Hybrid® (formerly known as Sandcat scanner) is a hybrid multilanguage web application security assessment suite - a software suite that simulates web-based attacks by combining different approaches. Through this combination, Syhunt effectively and proactively guards an organization's Web infrastructure against web application security threats, quickly finding existing vulnerabilities before the hackers.

HALF DYNAMIC, HALF CODE SCANNER

With Syhunt Hybrid, you can:

- Pen-test websites, scanning live web applications for multiple classes of vulnerabilities - an approach known as blackbox which equals to the hacker's perspective.
- Scan the source of web applications for the same classes of vulnerabilities - an internal code review (also known as whitebox).
- Combine both approaches, performing what is known as hybrid analysis (or greybox)
- Perform over **1500** application checks, covering over **100** types of web security attacks.
- Run checks specially tailored for Access, DB2, dbx, Firebird/InterBase, FrontBase, Informix, Ingres, MaxDB, mSQL, MySQL, Oracle, Ovrimos, PostgreSQL, SQL Server, SQLite, Swish, Sybase and other DBs.



DYNAMIC SCANNER

Syhunt dynamically injects data in web applications and analyzes the application response in order to determine if the application code is vulnerable, automating the web application security testing and proactively guarding your organization's Web infrastructure against several kinds of web application security threats. Includes a HTML5-aware spider and JavaScript emulation capabilities.

CODE SCANNER

Designed to scan web applications for various types of issues, such as Cross-Site Scripting (XSS), File Inclusion, SQL Injection, Command Execution and weak validation, the Code scanner is a perfect complement to the already extensive set of remote scanning capabilities available in the Dynamic scanner.

GET EVERY SECURITY ASPECT COVERED

With Syhunt Hybrid and a simple input of a URL, you can:



- Detect over **5700** vulnerabilities in over 70 categories of web attacks - including:
- XSS (Cross-Site Scripting), SQL Injection, File Inclusion, Command Execution, etc.
- OWASP's Top Ten Most Critical Web Application Security Vulnerabilities & PHP Top 5 Vulnerabilities
- Perform thousands of additional dynamic checks for known vulnerabilities affecting specific web application and servers.
- Perform deep web crawling (spidering), automatically mapping an entire web site structure and running injection, directory and authentication brute force checks
- Scan any type of web application

With a simple input of a source code directory, you can:



- Detect over **1300** source code vulnerabilities, covering 21 types of web security attacks.
- Scan the source code of web applications written in ASP.NET (C# & VB.Net), Java (JEE / JSP), JavaScript, Node.js, Lua, Perl, PHP, Python and Ruby for vulnerabilities
- Identify key areas of the code, such as key HTML tags, JavaScript, XHR requests, entry points and interesting keywords

Some of the key technologies supported by the Syhunt Hybrid scanner:



GENERATE DETAILED REPORTS

Syhunt Hybrid comes with the ability to generate a comprehensive report containing details about the vulnerabilities. After examining the application's response to the attacks, if the target URL is found vulnerable, it gets added to the report. Syhunt Hybrid's reports also contain charts, statistics and compliance information - a set of report templates tailored for different audiences is available. A complete Syhunt report usually includes:

- Full vulnerability information and references - CVE, NVD, CWE, Bugtraq & OSVDB.
- CVSS3/CVSS2 score and vector information.
- Comparison Information - Evolution of vulnerabilities over time by comparing previous scan results.
- Compliance Information - Such as OWASP Top 10, PHP Top 5, CWE/SANS Top 25, Payment Card Industry (PCI), etc.

Currently, Syhunt Hybrid is able to generate reports and export data in several formats - including HTML, PDF, XML, Text, CSV, RTF, XLS, DOC & NBE. Results can be converted at any time to HTML or any of multiple available formats, and compared to determine new, unchanged or removed vulnerabilities.



CVSS SUPPORT

Syhunt Hybrid comes with full support for the Common Vulnerability Scoring System, an industry standard designed to convey vulnerability severity and help determine urgency and priority of response. When a report is generated, vulnerabilities are sorted by default based on their CVSS3 score.

CHECK FOR THE TOP VULNERABILITIES

Syhunt Hybrid allows you to scan for the top vulnerabilities attackers use against web applications.

OWASP TOP 10

The OWASP Top Ten is a list of vulnerabilities that require immediate remediation. Existing code should be checked for these vulnerabilities immediately, as these flaws are being actively targeted by attackers. The OWASP Foundation encourage companies to adopt the OWASP Top Ten as a minimum standard for securing web applications.

SANS TOP 20

The SANS Top 20 includes step-by-step instructions and pointers to additional information useful for correcting the security flaws. The SANS Institute updates the list and the instructions as more critical threats and more current or convenient methods of protection are identified. It is a community consensus document.

COMPLIANCE AUDITING

Syhunt Hybrid can help your organization address the most pressing compliance issues such as:

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley (GLBA)
- Payment Card Industry (PCI) Data Security Standard
- CA-SB1
- Sarbanes-Oxley

CVE & CWE

Syhunt Hybrid fully supports CVE (Common Vulnerabilities and Exposures) & CWE (Common Weakness Enumeration), being able to scan for the top CWE entries related to web applications. Syhunt is also on the Mitre Corporation's CVE-compatible list of products and services. The Mitre Corporation is the author of the standard itself.

“...the best web app security assessment tool out there. Rapidly updated to cover new vulnerabilities as they arise and very easy to use.



“...one of the most effective and valuable tools on the market today.

Matt McDermott, Security Engineer II, Solutionary, USA

**Robert Davies, CEO, Stealth-
ISS, USA**

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

