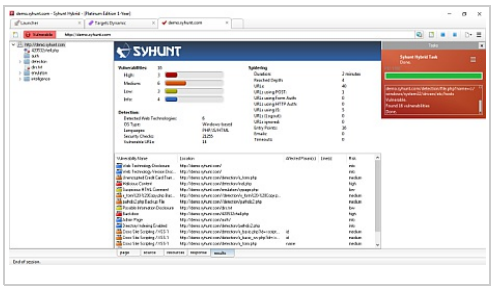
../SYHUNT/DYNAMIC

WEB APPLICATION SECURITY SCANNER

Syhunt Dynamic® (formerly known as Sandcat scanner) is a web application security scanner that fully automates security testing, proactively guarding your organization's Web infrastructure against all kinds of application security threats.

KEY FEATURES



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

- Perform over **800** dynamic web application security checks 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 and directory and authentication brute force checks
- Scan any type of web application

DEEP CRAWLER

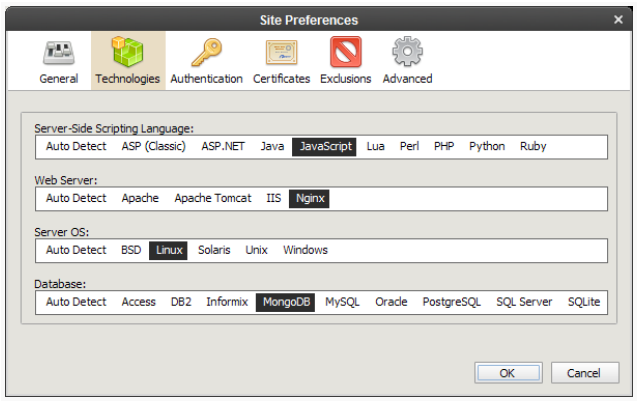
Syhunt Dynamic maps the entire web site structure (all links, forms, XHR requests and other entry points) and locates custom, unique vulnerabilities by simulating a wide range of attacks/sending thousands of requests. The scanner behaves as Chrome, Firefox and IE, and even simulates user interaction (key press, mouse click, etc).

ADVANCED INJECTOR

Tests for SQL Injection, XSS, File Inclusion and many other web application vulnerability classes. While performing a scan, Syhunt injects data in the web apps and subsequently analyzes the application response in order to determine if the application code is vulnerable.

SCAN ANY KIND OF WEB ENVIRONMENT

Syhunt Dynamic offers the degree of flexibility and versatility required to support any web environment, anywhere. It has been designed to intelligently handle complex, large web sites and automatically adapt to different web environments and technologies. While spidering a web site and hunting vulnerabilities, Syhunt Dynamic emulates a modern, HTML 5-aware web browser, making sure every web application gets fully tested. Syhunt's browser emulation feature set includes:



- Intelligent HTML parsing (handles malformed HTML like a web browser)
- JavaScript emulation (ability to behave as Chrome, Firefox and IE) with XHR request support
- User interaction simulation (key press, mouse click, etc)
- HTML 5-aware and CSS 3-aware
- Auto form filling & form login
- Process isolation/Multi-process scanning (each website scan you start is a different process on your operating system)
- Cookies support
- HTTPS support (SSL 2/SSL 3/TLS 1)
- Certificates support
- Basic & NTLM authentication support
- HTTP 1.0 and 1.1 support
- Keep-Alive support
- HTTP redirection support

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

GENERATE DETAILED REPORTS

Syhunt Dynamic 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 Dynamic'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 session data.
- Compliance Information - Such as OWASP Top 10, PHP Top 5, CWE/SANS Top 25, Payment Card Industry (PCI), etc.

Currently, Syhunt Dynamic 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

CHECK FOR THE TOP VULNERABILITIES

Syhunt Dynamic 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 Dynamic 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 Dynamic 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.

> It has discovered a number of SQL injections and XSS vulnerabilities we would have missed if tested by hand. One of the best ways of using Syhunt is by combining the source code analysis with the dynamic scanner to quickly zoom in on the real issues.

Arthur Donkers, Security Officer

> Tools like Syhunt make an application's vulnerability much simpler to detect, no longer requiring a "hacker" level skill set.

SC Magazine

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