The information in this document applies to **version 6.8.3** of Syhunt Hybrid.

DIFFERENCES BETWEEN HUNT METHODS

Hunt Method	CLI name	Type	Brute F.	Injection	DoS	Time-Con.
Application Scan (Default)	appscan	▨	Y	Y	Y	N
Structure Brute Force	structbf	■	Y (Deep)	N	N	Y (Very)
Old & Backup Files	fileold	■	Y	N	N	Y
Fault Injection	faultinj	▨	N	Y	Y	N
Top 10 (OWASP)	top10	▨	N	P (TOP10)	Y	N
Top 25 (CWE)	top25cwe	▨	N	P (TOP25)	Y	N
Top 5 (OWASP PHP)	top5php	▨	N	P (TOP5)	N	N
Cross-Site Scripting	xss	▨	N	P (XSS)	N	N
SQL Injection	sqlinj	▨	N	P (SQL)	N	N
File Inclusion	fileinc	▨	N	P (FI)	N	N
Unvalidated Redirects	unvredir	▨	N	P (UR)	N	N
Malware Content	malscan	▨	P (Malware)	P (Malware)	N	N
Passive	passive	▨	N	N	N	N
Spider Only	spider	■	N	N	N	N
Complete Scan	complete	▨	Y	Y	Y	Y (Very)
Complete Scan, No DoS	compnodos	▨	Y	Y	N	Y (Very)
Complete Scan, Paranoid	comppnoid	▨	Y (Deep)	Y	Y	Y (Very)

Letters: Yes/No/Partial (**Y/N/P**)

TYPE OF TESTING

- ▨ - Hybrid (Gray Box), Dynamic & Code
- ■ - Dynamic Only (Black Box)
- □ - Code Only (White Box)

TIME-CONSUMING

A Yes means that extra checks and attack mutations will be performed and the number of checks will be influenced by the number of directories found during the spidering stage.

DESCRIPTION

The Application Scan method is the default scan method in Syhunt. If you want to use a different scan method, you will be able to select one of the following options:

APPLICATION SCAN

Identifies flaws in custom web applications, web server software and third-party components. This scan method crawls the web site and performs attacks against the web site structure and the web applications. This includes looking for fault injection vulnerabilities such as XSS, SQL Injection, File Inclusion, and more.

STRUCTURE BRUTE FORCE

A structure brute force will check for:

- Common Vulnerable Scripts
- Common File Checks
- Custom File Checks (User File Checks)
- Database Disclosure
- Web-Based Backdoors

The number of checks is influenced by the number of directories found during the spidering stage.

OLD & BACKUP FILES

Executes extension checking around the mapped web site structure.

OWASP TOP 10

Scans specifically for the OWASP Top 10 2017 vulnerabilities:

1. A1 2017: Injection
2. A2 2017: Broken Authentication
3. A3 2017: Sensitive Data Exposure
4. A4 2017: XML External Entities (XXE)
5. A5 2017: Broken Access Control
6. A6 2017: Security Misconfiguration
7. A7 2017: Cross-Site Scripting (XSS)
8. A8 2017: Insecure Deserialization
9. A9 2017: Using Components with Known Vulnerabilities
10. A10 2017: Insufficient Logging & Monitoring

CWE TOP 25

Scans specifically for the 2019 CWE Top 25 Most Dangerous Software Errors.

See the full list at: https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html

OWASP PHP TOP 5

Scans specifically for the OWASP Top Five List of PHP Vulnerabilities:

1. Remote Command Execution
2. Cross-Site Scripting (XSS), including DOM XSS
3. SQL Injection
4. PHP Misconfiguration
5. File System Attacks, including File Inclusion

FAULT INJECTION

Scans specifically for fault injection vulnerabilities. If this scan method is selected, all other checks that does not require injection are disabled and Syhunt will then specifically check for SQL injection, XSS, file inclusion, and similar flaws.

CROSS-SITE SCRIPTING (XSS)

Scans specifically for XSS vulnerabilities, including DOM XSS.

SQL INJECTION

Scans specifically for SQL & NoSQL Injection vulnerabilities.

FILE INCLUSION

Scans specifically for File Inclusion and Directory Traversal vulnerabilities.

UNVALIDATED REDIRECTS

Scans specifically for Unvalidated Redirect vulnerabilities.

MALWARE SCAN

Scans specifically for malware content, such as:

- Web Backdoors
- Malicious Content
- Hidden Debug Parameters

PASSIVE SCAN

Maps the web site structure and reports vulnerabilities discovered without launching any kind of attacks, such as:

1. Vulnerabilities in Client-Side JavaScript
2. Various Form Weaknesses
3. Web Technology Disclosure
4. Insecure HTTP Headers
5. Outdated, Vulnerable Server Software
6. Outdated, Vulnerable Referenced Scripts
7. Suspicious HTML Comments
8. Source Code Disclosure
9. Malicious Content being served

SPIDER ONLY

Maps the web site structure without testing or reporting any kind of vulnerability or weakness.

COMPLETE SCAN

Scans for all kinds of web application vulnerabilities using all kinds of mutantions and pen-tester methods, including Header Manipulation attacks. A Complete Scan can sometimes be very time-consuming when performed against a web server that has a large quantity of web folders and entry points.

COMPLETE SCAN (NO DOS)

Same as before, but with denial-of-service tests disabled.

COMPLETE SCAN (PARANOID)

Scans for all kinds of web application vulnerabilities using deep structure brute force, all kinds of mutantions and pen-tester methods, including Header Manipulation attacks. This scan method can be very time-consuming, specially when executed against large web sites. This method also executes triple checking structure brute force, which applies to case-sensitive servers - Syhunt will try all file name possibilities (all uppercase, all lowercase, all leading capitals, etc).