SYHUNT HYBRID: CLI SCAN TOOLS

The information in this document applies to **version 6.9.1** of Syhunt Hybrid.

INTRODUCTION

Follow along with this guide to learn how to perform a dynamic or code scan and generate a vulnerability report via command-line.

Syhunt's CLI scan tools location depends on the Syhunt version and your OS:

OS	Default Location
Windows	C:\Program Files\Syhunt Hybrid\ C:\Program Files (x86)\Syhunt Hybrid\ C:\Program Files\Syhunt Community Core\
Linux	/home/[user]/syhunt-hybrid/carbon/ /home/[user]/syhunt-community/carbon/

HOW TO PERFORM A DYNAMIC SCAN VIA COMMAND-LINE

1. Go to the directory Syhunt Hybrid is installed using the command prompt.
2. Use the following command-line:

```
scanurl [starturl] -hm:[a huntmethod]] -gr
```

```
Example:
scanurl http://www.somehost.com -hm:appscan -gr
```

Syhunt scanurl tool reports are automatically generated and saved if the -gr parameter is provided. You can also open the session by launching Syhunt and using the ≡ Menu -> Past Sessions option.

The following parameters can be provided when calling the scanurl tool, all of which are **optional**:

Parameter	Description	Default Value
sn:[name]	A session name that must be unique. If omitted, an unique ID will be generated and assigned	auto generated ID
hm:[name]	the Hunt Method to be used during the scan. If omitted, the default method will be used	appscan
emu:[mode]	Browser Emulation Mode. Available modes include: chrome, edge, firefox, msie, safari	chrome
srcdir:[local dir]	Sets a Target Code Folder for a Hybrid Scan (eg. "C:\www\docs\" or "/home/user/www/")	
gr	Generates a report file after scanning	
gx	Generates an export file after scanning	
or	Opens report after generation	
er	Emails report after generation	
etrk: [trackername]	Email preferences to be used when emailing report	
esbj:[subject]	Email subject to be used when emailing report	Syhunt Hybrid Report
rout: [filename]	Sets the report output filename and report format	Report_[session name].html
rtpl:[name]	Sets the report template	Standard
xout: [filename]	Sets the export output filename and report format	Export_[session name].xml
xout2: [filename]	Sets a second export output filename and report format	Export_[session name].xml
pfcond: [condition]	Sets a pass/fail condition to be reported	
nv	Turn off verbose. Error and basic info still gets printed	

inc:[mode]	Sets the incremental scan mode	targetpref
inctag:[name]	Optionally stores the incremental scan data within a tag	
mnl:[n]	Sets the maximum number of links per server	10000
mnr:[n]	Sets the maximum number of retries	2
mcd:[n]	Sets the maximum crawling depth	0 (unlimited)
tmo:[ms]	Sets the timeout time	8000
ver:[v]	Sets the HTTP Version	1.1
nofris	Disables auto follow off-domain redirect in Start URL	
nodos	Disables Denial-of-Service tests	
nojs	Disables JavaScript emulation and execution	
atype:[type]	Sets the auth type; Basic, Form and Manual	
auser:[username]	Sets a username for authentication	
apass:[password]	Sets a password for authentication	
about	Displays information on the current version of Syhunt	
help (or /?)	Displays the list of available parameters	

SCANNING IPV6 ADDRESSES

Syhunt Dynamic fully supports the scanning of IPv6 addresses. To scan an IPv6 target, remember to enclose the address in square brackets, eg:

```
http://[2001:4860:0:2001::68]/index.php
```

HOW TO PERFORM A CODE SCAN VIA COMMAND-LINE

1. Go to the directory Syhunt is installed using the command prompt.
2. Use the following command-line:

```
scancode [target] -hm:[a huntmethod]] -gr
```

```
# Examples:
scancode git://sub.domain.com/repo.git -gr
scancode https://github.com/user/repo.git -rb:master -gr
scancode c:\source\www\ -gr
scancode c:\source\www\file.php -gr
scancode c:\mobile\myapp.apk -gr
scancode "c:\source code\www\" -gr
```

Syhunt scancode tool reports are automatically generated and saved if the -gr parameter is provided. You can also open the session by launching Syhunt and using the ≡ Menu -> Past Sessions option.

The following parameters can be provided when calling the scancode tool, all of which are **optional**:

Parameter	Description	Default Value
sn:[name]	A session name that must be unique. If omitted, an unique ID will be generated and assigned	auto generated ID
hm:[name]	the Hunt Method to be used during the scan. If omitted, the default method will be used	appscan
rb:[branch]	Sets a repository branch	master
gr	Generates a report file after scanning	
gx	Generates an export file after scanning	
or	Opens report after generation	
er	Emails report after generation	
etrk:[trackername]	Email preferences to be used when emailing report	
esbj:[subject]	Email subject to be used when emailing report	Syhunt Code Report

rout:[filename]	Sets the report output filename and report format	Report_[session name].html
rtpl:[name]	Sets the report template	Standard
xout:[filename]	Sets the export output filename and report format	Export_[session name].xml
xout2:[filename]	Sets a second export output filename and report format	Export_[session name].xml
pfcond:[condition]	Sets a pass/fail condition to be reported	
nv	Turn off verbose. Error and basic info still gets printed	
inc:[mode]	Sets the incremental scan mode	targetpref
inctag:[name]	Optionally stores the incremental scan data within a tag	
refurl:[url]	Sets an URL associated with the current source code for reference purposes only	
noifa	Disables input filtering analysis	
about	Displays information on the current version of Syhunt	
help (or /?)	Displays the list of available parameters	

PASS/FAIL CONDITIONS

A pass/fail testing condition can be passed to scancode or scanurl with the -pfcond parameter, The following are the pass/fail conditions currently supported by Syhunt:

- `fail-if:risk=high` - Fail if a High risk vulnerability is found
- `fail-if:risk=mediumup` - Fail if a Medium or High risk vulnerability is found
- `fail-if:risk=lowup` - Fail if a Low, Medium or High risk vulnerability is found

INCREMENTAL SCAN MODES

auto	Automatically manages the incremental scan cache (recommended option)
disabled	Disables the incremental scan cache. This will slow down scans, taking 3 to 4 more time to complete
forced	Forces the incremental scan to be always enabled. If you run scans with this mode, make sure you have a separate non-forced scan to be run every month or so
targetpref	Uses the incremental scan mode defined in target preferences

AVAILABLE REPORT FORMATS & TEMPLATES

.html	HTML report
.pdf	Adobe PDF report
.xml	XML export
.json	JSON vulnerabilities export
.csv	CSV (Comma-Separated Values)
.mse.csv	CSV (Comma-Separated Values) for MS Excel
.txt	Text report

The following templates are available:

Standard	This is the standard report with low to high-risk vulnerability information
Comparison	Includes the standard information plus evolution information about the vulnerabilities
Compliance	Includes OWASP Top 10, CWE/SANS Top 25 2019 and PCI DSS v3.2.1 compliance information
Mobile	Includes OWASP Mobile Top 10, CWE/SANS Top 25 2019 and PCI DSS v3.2.1 compliance information

Complete	Includes the standard information together with comparison, compliance, request response and coverage details

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
0. 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).

WORKING WITH THIRD-PARTY LAUNCHERS

See this document on how to generate a complete command-line that allows to start Syhunt from within batch files, third-party task schedulers, Jenkins and other launchers.