SYHUNT DYNAMIC: GETTING STARTED

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

HOW TO PERFORM A DYNAMIC SCAN

While performing a standard, dynamic scan (also known as black box) the Syhunt scanner injects data in the web applications and subsequently analyzes the application response in order to determine if the application code is vulnerable to specific web application security attacks.

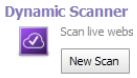
MAIN SUPPORTED LANGUAGES

</> ASP (Classic)
</> ASP.Net
</> Java / JSP
</> JavaScript
</> Lua
</> Perl
</> PHP
</> Python
</> Ruby

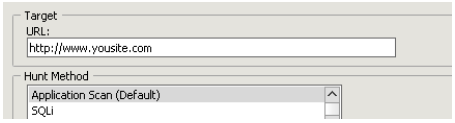
Follow along with this guide to learn how to perform a dynamic scan and generate a vulnerability report.

1. ⚠ Make sure you meet the pre-scan requirements and are properly authorized to perform the scan against the target.

2. Launch Syhunt Hybrid and click the Syhunt Dynamic icon or New Scan button in the welcome page.



3. Enter the URL of the website you want to scan.



4. Select a scan method. We recommend the Application Scan (Default) method, which scans for all vulnerabilities using the recommended settings - the different methods are explained in the Hunt Methods document.
5. Check edit site preferences.
6. Click the Start Scan button. On the next screen, go to the Technologies tab and select the technologies used by the target website. You can also use this screen to change additional preferences associated with the website. Review the settings and then click OK to start the scan.

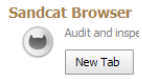
In the end of the scan, you can click Generate a Report to save the results as a HTML report or any other prefered format.

The next time you perform a scan (unless you want to change site preferences again) you can jump from the step 3 to 5.

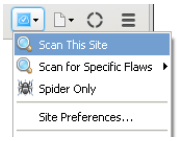
HOW TO PERFORM MANUAL LOGIN VIA BROWSER

If you need to manually login first before you can scan a website, you may prefer to start the scan from within the Sandcat Browser.

1. Launch Syhunt Hybrid and double-click the Sandcat Browser icon or New Tab button in the welcome page.

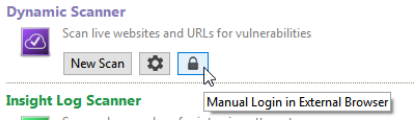


2. Navigate to the website you want to scan - enter the target URL using the address bar and press Enter.
3. Go to the Login area and login using your credentials.
4. Click the Scan This Site menu option to start the scan.



Alternatively, you can manually login using an external browser like Google Chrome or Mozilla Firefox:

1. Launch Syhunt Hybrid and click the lock button in the welcome page.



2. Follow the instructions that will appear at the bottom of the Syhunt screen.

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
```

USING CLIENT CERTIFICATES

SSL support in Syhunt Dynamic relies on two Dynamic Link Library (DLL) files (SSLeay32.dll''' and libeay32.dll) developed by the OpenSSL Project. When these two DLL files are present then SSL support is available, which means that you can scan secure sites with https addresses.

The Site Preferences screen allows you to configure the client certificates. To view this screen, navigate to the website you want to scan, click the scan button -> Site Preferences and go to Certificates tab.

ADVANCED FEATURES

PREVENTING A VULNERABILITY FROM BEING REPORTED

You can create rules that prevent specific vulnerabilities to be reported:

1. Click the purple bookmark icon in the Launcher toolbar and add a Target URL to the list of Dynamic targets.
2. Right-click the URL you just added and click the Edit Site Preferences menu option.
3. Go to the Exclusions tab and click the **Vulnerabilities...** button
4. Click the plus button and add using the input dialog a new rule. Examples:

- `path=*,name=XSS` would prevent any vulnerability with XSS in the title from being reported
- `path=/demo/*,name=XSS` would prevent any vulnerability with a path starting with /demo/ and XSS in the title from being reported
- `path=*,"name=Web Technology Disclosure"` would prevent any vulnerability with Web Technology Disclosure in the title from being reported

The following parameters can be used as part of a rule:

- **path** (required) - a wildcard text (which can contain the special characters ? and *) that will be matched against the affected path
- **name** - a text that will be matched against the vulnerability title
- **params** - a param name that will be matched against the affected param(s). If multiple params are provided, they must be separated by comma.
- **risk** - a risk that will be matched against the vulnerability risk (can be low, medium, high or info)
- **module** - a module name that will be matched against the module that detected the vulnerability (can be dyn or code). If omitted, the rule will work for both Dynamic and Code vulnerabilities
- **lines** - a number or numbers that will be matched against the affected source code line(s). If multiple lines are provided, they must be separated by comma.
- **cve** - a CVE ID that will be matched against the vulnerability's CVE references
- **cwe** - a CWE number that will be matched against the vulnerability's CWE references

AUTOMATED FORM LOGIN TRAINING

If your web site requires authentication prior to allowing access to all or most of the website contents, Syhunt Dynamic can auto-detect most form logins and login using the credentials you entered in the Site Preferences screen, but if you have a form login with non-standard fields you have two options:

1. Manually login as explained above in the manual login section (easier and recommended), or
2. Teach Syhunt Dynamic to auto log into the application through a simple procedure (explained below)

Let's suppose you are having an issue with Syhunt Dynamic with the following web form login:

```
<input name="ClientUTBox" id="ClientUTBox" type="hidden" value="1234">
<input name="ClientUNBox" id="ClientUNBox" type="text" class="InputBox"/>User Name
<input name="ClientPWBox" id="ClientPWBox" type="password" class="InputBox" >Password
```

The following procedure will reprogram Syhunt to recognize the form login:

1. Click the purple bookmark icon in the Launcher toolbar and add a Target URL to the list of Dynamic

targets.
2. Right-click the URL you just added and click the Edit Site Preferences menu option.
3. Enter the username and password in the Form Authentication area of the Authentication tab.
4. Click OK to save the preferences. The Site Preferences window will close.
5. Switch back to the Launcher tab, and go to the Dynamic Preferences screen (≡ -> Preferences -> Dynamic Preferences).
6. Go to the Emulation tab, click the Custom Values button and add the following values:

```
ClientUTBox=1234
ClientUNBox=@syhunt_web_form_username
ClientPWBox=@syhunt_web_form_password
```

Values above after the equal sign starting with an @ are internal variables, they ensure that the web form login information you entered in the Site Preferences screen is used in the two form inputs you provided.

Syhunt Dynamic is now ready to detect this form login during a scan.

PREVENTING ACCIDENTAL LOGOUT

Syhunt Dynamic can auto-detect most logout pages, but if the logout page does not match standard names and common patterns, you will need to add the logout page URL to your Site Preferences. This will prevent Syhunt Dynamic from accidentally logging out during a scan:

1. Click the purple bookmark icon in the Launcher toolbar and right click to Edit Site Preferences of the target.
2. Go to the Exclusions tab
3. Click the Logout URLs button and add the custom logout URL, example:

```
/getmeout.php
```

1. Click OK to confirm the preferences. The input dialog will close.
2. Hit OK to save the preferences.

BASIC FAQS

How many time Syhunt Dynamic will take to run all the tests?
Duration depends on the number of pages and applications your website contains and the scan method you selected. The web application checks (after the crawling stage) is usually the part of the scan that can take more time and depends on the size of the target site.

Can I load a previous scan session and re-run reports again?
Yes, select the Past Sessions option from the Menu. The Session Manager screen will open. Click Generate Report for the session you want and you will see the session results and the options to export data and generate reports.

Is there a list of tests that are conducted using the updated version of Syhunt?
You can get an idea of the tests by clicking the Menu -> Help, and then select Vulnerability List.

Do any of the tests crash the tested host?
As far as crashing the host - there are denial of service checks which may crash the tested host - you can turn those off when scanning though.

Does Syhunt Dynamic have any problems with personal firewalls?
Yes, you'll just have to let the firewall know that Syhunt is authorized to make connections to the Internet. However, some software firewalls do not handle high loads very well. It is not recommended to run both a personal firewall and Syhunt on the same machine.

If you're running a PC firewall on the scanning system that does outbound filtering, try disabling it - we've occassionally seen firewalls automatically block a program's socket calls without first prompting the user as to whether or not it should be allowed to make connections.

Is there any way to scan ports 23 (telnet) and 21 (ftp)?
No, Syhunt Dynamic is not a general purpose security scanner, it is specialized for evaluating web applications.

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.

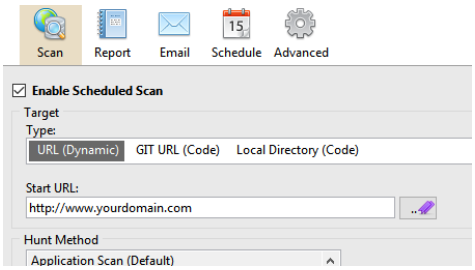
COMPLETE SCAN (PARANOID)

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).

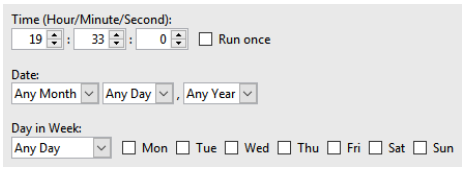
HOW TO SCHEDULE A SCAN

Adding and configuring a scheduled scan is an easy task:

1. Click the Scheduled Scans icon in the launcher toolbar. The Scheduled Scans screen will open.
2. Click the Add Scheduled Scan icon in the Scheduled Scans screen toolbar.
3. Enter a reference name for the new scheduled scan (like MyScan) and hit **OK**. A preferences dialog window will open.
4. In the Scan tab, enter the scan target details and select the desired scan method and options.



5. In the Report tab, enter the desired report generation options.
6. In the Schedule tab, enter the desired event plan.

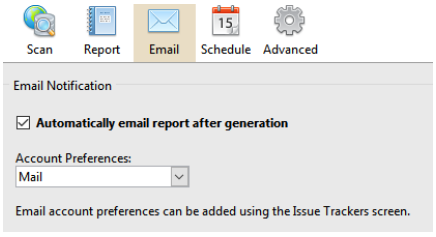


7. Click the **OK** button when you're done.

SENDING REPORTS VIA EMAIL

Firstly, you have to add an Email tracker:

1. Click the Issue Trackers icon in the launcher toolbar. The Issue Trackers screen will open.
2. Click the Add Tracker icon in the Issue Trackers screen toolbar and choose the Add tracker: Email menu option.
3. Enter a reference name for the new tracker (like Mail) and hit **OK**. A preferences dialog window will open.
4. Enter Sender/Recipient email addresses.
5. Enter the SMTP Authentication host and credentials and click the **OK** button.
6. Click the Scheduled Scans icon in the launcher toolbar. The Scheduled Scans screen will open.
7. Right-click the scheduled scan and click the Edit Schedule Preferences option. A preferences dialog window will open.
8. Go to the Email tab and check the **Automatically email report after generation** option.



9. Select the account preferences.
10. Click the **OK** button when you're done.

REVIEWING RESULTS FROM SCHEDULED SCANS

At any time you can see the results of past and current scans and generate a report. Just launch the Syhunt Hybrid application and click the Past Sessions icon in the launcher toolbar.

WORKING WITH THIRD-PARTY LAUNCHERS AND SCHEDULERS

See this document on how to start Syhunt from within third-party task schedulers, Jenkins and other launchers

PRE-DYNAMIC SCAN REQUIREMENTS

1. ⚠ **This software should be used only by system administrators (or other people in charge). It should not be used to scan websites outside of your direct control.**
    1. If you need to scan a website outside of your direct control, it is recommended that you obtain a written permission from the website's owner or administrator.
    2. It is recommended and a good practice that a backup of the website's source code and database is carried out before launching any scans against it. This helps in very rare cases on which injection testing against an insecure and not resilient website cause database pollution or unintended file manipulation that interfers with proper website functioning.

2. Make sure you meet the Internet connection requirements.
3. You must read and agree with the Syhunt EULA before launching any scans.

SYSTEM REQUIREMENTS

Syhunt Hybrid (including its Community Edition) can be installed on 64-bit Windows or 64-bit Linux, but it is able to analyze applications designed for any target platform, including Android, Apple iOS and MacOS, BSD, Linux, Windows, Solaris and Unix, independently of the platform it is executed from.

1. 4GB of available RAM (8GB recommended)
2. 1GB of free disk space*
3. Internet Connection (recommended for code scans and dynamic scans and some features)
4. One of the following compatible 64-bit operating systems:
    1. Windows 7, 8 or 10, or Windows Server 2008 to 2019
    2. Ubuntu Server or Desktop 18 or higher
    3. CentOS 7 or 8 (Minimal or Everything)
    4. Any unofficially supported Linux distribution such as the ones listed below.

5. (Optional) GIT on Linux or GIT for Windows (optional for GIT repository scans)
6. Java or Java Headless installed on Linux OS
7. If native binary is not available for your specific Linux distribution yet, Wine64 Stable (3, 4 or 5) is required to be installed.
8. (Optional) Java 8 or higher (optional for Android APK file scan)

* This does not include the space required to save scan session data, which varies depending on the website or source code being analyzed and the scan frequency.

COMPATIBLE LINUX DISTRIBUTIONS

Officially Supported:

✔ Ubuntu Server/Desktop 18.10 and later

✔ CentOS 7.7 and later (Minimal or Everything)

Unofficially (Successfully Tested):

✔ Kali Linux 2019 and later

✔ Parrot OS 4.1, 4.7 and later

✔ Debian 9.11 and later

✔ Linux Mint 19.2 and later

✔ OpenSUSE Leap 15.1 and later

✔ Fedora 32

✔ MX Linux 19.1 and later

✔ KDE Neon 2020.03 and later

✔ Deepin 15.9

✔ Manjaro 19

✔ Arch Linux 2019 and later

Unsupported:

⊘ Elementary OS 5.1 (Successfully Tested), 5.0 (Unsupported)

⊘ CentOS 6.1 (Successfully Tested)

⊘ Solus 4.1 (Unstable)