SYHUNT HYBRID: POC TEST PLAN

The information in this document applies to **version 6.9.15** of Syhunt Hybrid. This testing plan was designed for Syhunt Hybrid, the full-featured edition, and not Syhunt Community - because of restricted functionality and vulnerability checks in Community, some test cases are impossible to be performed and not all vulnerabilities will be detected.

INTRODUCTION

This software test plan is aimed at verifying the functionality, accuracy and correct working of all key aspects and parts of Syhunt Hybrid. The testing is to be conducted at customer's premises after Syhunt Hybrid has been deployed and activated and involves performing dynamic and static scans under various conditions to simulate actual usage of the tools. Upon completion, the user should be familiar with key product functionality and integration capabilities, and Syhunt be able to collect usability feedback from the user.

TEST CATEGORIES

Phase 1 - Dynamic Auditing
D1: Scan a live website for vulnerabilities
D2: Manually login via browser and scan a restricted website for vulnerabilities
D3: Automatically login and scan a restricted website for vulnerabilities
D4: Just map a website (crawling/spidering test with JavaScript execution)
D5: Perform an incremental dynamic scan
D6: Perform a concurrent dynamic scan
Phase 2 - Source Code Auditing
S1: Scan local source code files for vulnerabilities
S2: Scan remote GIT repositories for vulnerabilities

Phase 3 - Integration
N1: Launch a code scan via command-line interface
N2: Launch a dynamic scan via command-line interface
N3: Create a tracker issue based on a reported vulnerability
N4: Generate a F5 BigIP ASM compatible export
Phase 4 - Reporting
R1: Generate a standard HTML report for a scan session
R2: Generate a complete HTML report for a scan session
R3: Generate a XML results export for a scan session
R4: Edit the information about a reported vulnerability
R5: Generate a comparison report between scan sessions

ENVIRONMENTAL REQUIREMENTS

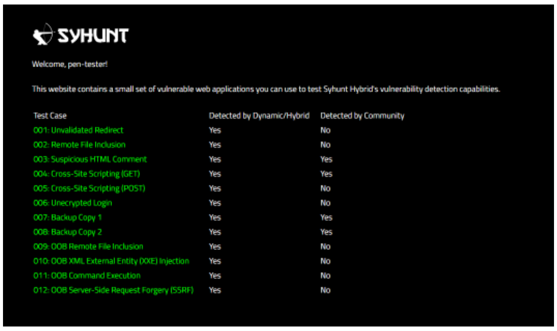
The results from this POC test plan were obtained on a Windows 10 x64 installation with an Intel Core i7, 16GB RAM, 500GB SSD and Internet access. Please make sure that you have a fast SSD, Internet access, and that at least the minimal system requirements are met (see the requirements). This testing plan assumes that Syhunt Hybrid is already installed on the Windows machine that will execute the tests. If not, please continue reading this section.

Click the executable setup download link provided by Syhunt. After downloading the exe file, double-click its icon to launch it. It's an easy next-next-finish installation process. When you click Finish, Syhunt Hybrid will be launched and you will be prompted to enter a Pen-Tester Key - enter the one provided in the email message containing the download link. After you click OK, a success message indicates that the Syhunt is ready for testing and you should immediately see the Launcher screen.

PREY SERVER

The Prey server is a portable Apache PHP web server containing a set of vulnerable web applications for demonstration purposes.

1. Download it from https://syhunt.fra1.cdn.digitaloceanspaces.com/tools/hybrid_xtras/syhunt-vulnphpserver.zip
2. Unzip it to a directory of your choice
3. Run PreyServer.exe to launch it
4. Finally, open http://127.0.0.1/syhunt/vulndemo in the browser and you will see the welcome page:



Welcome, pen-tester!

This website contains a small set of vulnerable web applications you can use to test Syhunt Hybrid's vulnerability detection capabilities.

Test Case	Detected by Dynamic/Hybrid	Detected by Community
001: Unvalidated Redirect	Yes	No
002: Remote File Inclusion	Yes	No
003: Suspicious HTML Comment	Yes	Yes
004: Cross-Site Scripting (GET)	Yes	Yes
005: Cross-Site Scripting (POST)	Yes	No
006: Unecrypted Login	Yes	No
007: Backup Copy 1	Yes	Yes
008: Backup Copy 2	Yes	Yes
009: OOB Remote File Inclusion	Yes	No
010: OOB XML External Entity (XXE) Injection	Yes	No
011: OOB Command Execution	Yes	No
012: OOB Server-Side Request Forgery (SSRF)	Yes	No

GIT FOR WINDOWS

If you execute any GIT related test case, you will need to install Git for Windows, which can be downloaded at https://gitforwindows.org/ After installing it with its default settings, make sure the git command is available through the Command Prompt - type `git` and hit enter.

ESTIMATED SCAN TIME

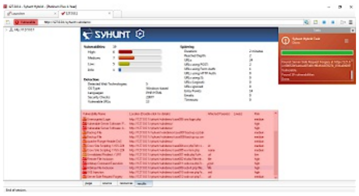
Dynamic scans from Phase 1 will take approximately **3 minutes** to complete each one when executed against the recommended targets. The incremental scan described in section D5 should take half this time.

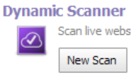
Source code scans from Phase 2 will take approximately **10 seconds** to complete when executed against the recommended targets. A code scan against a larger code base (not the ones listed in this document), like a Java+JavaScript project containing around 200K lines will take around 4 minutes to complete. An incremental scan of the same codebase can reduce the scan time by half. This means that Syhunt can analyze around 6 million lines of code per hour and around 12 million lines of code per hour in recurring scans against the same targets.

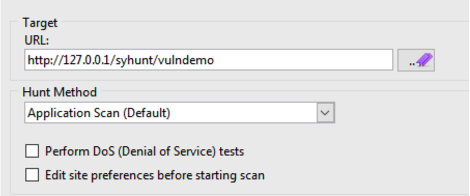
PHASE 1: DYNAMIC AUDITING

D1: SCAN A LIVE WEBSITE FOR VULNERABILITIES

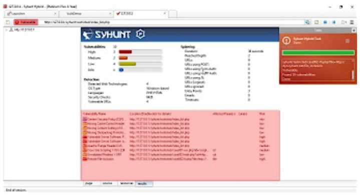
Action	Expected Results

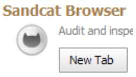
Scan http://127.0.0.1/syhunt/vulndemo for vulnerabilities FOLLOW THE STEPS BELOW	After the scan completes, the results tab must list all test cases  detected (from 001 to 011)

1. Make sure the Prey server is running (as explained in the Environment Requirements section at the beginning of this document)
2. Launch Syhunt Hybrid and click the Syhunt Dynamic icon or New Scan button in the welcome page.
   

3. Enter the http://127.0.0.1/syhunt/vulndemo as the target URL.
   
   Target
   URL: http://127.0.0.1/syhunt/vulndemo
   Hunt Method: Application Scan (Default)
   ☐ Perform DoS (Denial of Service) tests
   ☐ Edit site preferences before starting scan
4. Select the Application Scan (Default) hunt method, which scans for all vulnerabilities using the recommended settings.
5. Click the Start Scan button

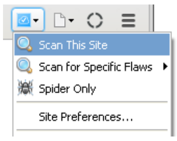
D2: MANUALLY LOGIN VIA BROWSER AND SCAN A RESTRICTED WEBSITE FOR VULNERABILITIES

Action	Expected Results
Scan http://127.0.0.1/syhunt/restricted, which uses web form authentication, for vulnerabilities FOLLOW THE STEPS BELOW	After the scan completes, the results tab must list all test cases (from 001 to 003) 

1. Make sure the Prey server is running (as explained in the Environment Requirements section at the beginning of this document)
2. Launch Syhunt Hybrid and double-click the Sandcat Browser icon or New Tab button in the welcome page.
   

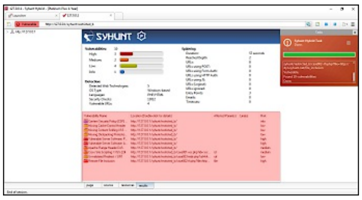
3. Navigate to http://127.0.0.1/syhunt/restricted - enter the URL using the address bar and press Enter.

4. Go to the Login area and login using the following credentials: username **test**, password **CUBPzjVy**
5. Click the Scan This Site menu option to start the scan.

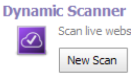


6. Select the Application Scan (Default) hunt method, which scans for all vulnerabilities using the recommended settings.
7. Click the Start Scan button to launch the scan

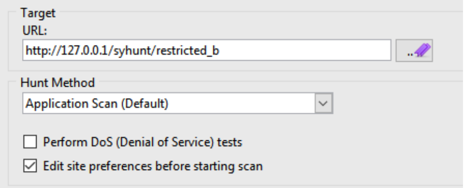
D3: AUTOMATICALLY LOGIN AND SCAN A RESTRICTED WEBSITE FOR VULNERABILITIES

Action	Expected Results
Scan http://127.0.0.1/syhunt/restricted_b, which uses basic authentication, for vulnerabilities FOLLOW THE STEPS BELOW	After the scan completes, the results tab must list all test cases detected (from 001 to 003) 

1. Make sure the Prey server is running (as explained in the Environment Requirements section at the beginning of this document)
2. Launch Syhunt Hybrid and click the Syhunt Dynamic icon or New Scan button in the welcome page.



3. Enter the http://127.0.0.1/syhunt/restricted_b as the target URL.



Target
URL: http://127.0.0.1/syhunt/restricted_b

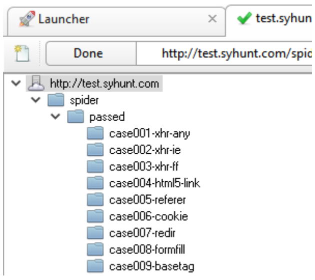
Hunt Method
Application Scan (Default)

☐ Perform DoS (Denial of Service) tests
☑ Edit site preferences before starting scan

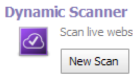
4. Select the Application Scan (Default) hunt method, which scans for all vulnerabilities using the recommended settings.
5. Check the option Edit site preferences before starting scan
6. Click the Start Scan button
7. In the next dialog, go to the Authentication tab. Switch Server Authentication from None to Basic
8. Enter username **test** and password **test**
9. Click the Ok button to launch the scan

D4: JUST MAP A WEBSITE (CRAWLING/SPIDERING TEST WITH JAVASCRIPT

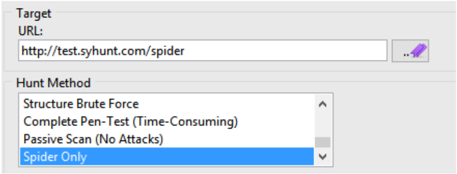
EXECUTION)

Action	Expected Results
Scan http://test.syhunt.com/spider FOLLOW THE STEPS BELOW	After the scan completes, the site tree (left sidebar) when expanded must list alongside the site structure, all test cases (from 001 to 009) under the /passed/ directory  Launcher test.syhun Done http://test.syhunt.com/spic http://test.syhunt.com spider passed case001-xhr-any case002-xhr-ie case003-xhr-ff case004-html5-link case005-referer case006-cookie case007-redir case008-formfill case009-basetag

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



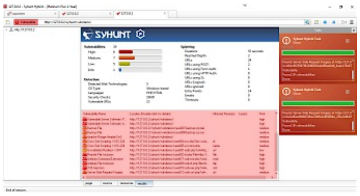
2. Enter the http://test.syhunt.com/spider as the target URL.


Target
URL: http://test.syhunt.com/spider

Hunt Method
Structure Brute Force
Complete Pen-Test (Time-Consuming)
Passive Scan (No Attacks)
Spider Only

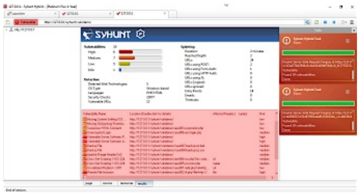
3. Select the Spider Only hunt method
4. Click the Start Scan button.

D5: PERFORM AN INCREMENTAL DYNAMIC SCAN

Action	Expected Results
Scan http://127.0.0.2/syhunt/vulndemo twice FOLLOW THE STEPS BELOW	The first scan should take around 4min to complete. The second one should take half this time (aprox. 2min) to complete. After each scan completes, the results tab must list all test cases detected (from 001 to 011) 

1. Follow the steps described in section D1, but use 127.0.0.2 instead of 127.0.0.1 as target because incremental scans are not enabled against 127.0.0.1.
2. Repeat the steps described in section D1 to perform a scan against 127.0.0.2.

D6: PERFORM A CONCURRENT DYNAMIC SCAN

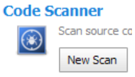
Action	Expected Results
Perform a concurrent scan against http://127.0.0.1/syhunt/vulndemo FOLLOW THE STEPS BELOW	After the scan completes, the results tab of each scan must list all test cases detected (from 001 to 011). The right sidebar will show the scan status of each scan marked in red. 

1. Follow the steps described in section D1.
2. Before the scan ends, go back to the Launcher tab and repeat the steps 2 to 5 described in section D1 to start a second scan against the same target.

PHASE 2: SOURCE CODE AUDITING

S1: SCAN LOCAL SOURCE CODE FILES FOR VULNERABILITIES

Action	Expected Results
Launch a code scan against a local directory via graphical user interface FOLLOW THE STEPS BELOW	After the scan completes, the results must list all test cases (from 001 to 009)

1. Download https://github.com/syhunt/vulnphp/archive/master.zip and unzip it to C:\Vulnerable\PHP\ or a directory of your preference
2. Launch Syhunt Hybrid and click the Syhunt Code icon or New Scan button in the welcome page.


3. Select the directory you unziped master.zip
4. Make sure the Code Scan (default) hunt method is selected
5. Press the **Start Scan** button to launch the scan.

You can try the above procedure with vulnerable samples in different languages:

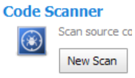
Java	https://github.com/syhunt/vulnjava-wavsep/archive/master.zip
Lua	https://github.com/syhunt/vulnlua/archive/master.zip
PHP	https://github.com/syhunt/vulnphp/archive/master.zip

Note: the number of test cases in each archive may vary.

S2: SCAN REMOTE GIT REPOSITORIES FOR VULNERABILITIES

Action	Expected Results
Launch a code scan against a remote GIT repository FOLLOW THE STEPS BELOW	After the scan completes, the results must list all test cases (from 001 to 009)

1. Launch Syhunt Hybrid and click the Syhunt Code icon or New Scan button in the welcome page.



2. Select type GIT URL and enter the URL: https://github.com/syhunt/vulnphp.git
3. Make sure the Code Scan (default) hunt method is selected
4. Press the **Start Scan** button to launch the scan.

You can try the above procedure with vulnerable samples in different languages:

Java	https://github.com/syhunt/vulnjava-wavsep.git
Lua	https://github.com/syhunt/vulnlua.git
PHP	https://github.com/syhunt/vulnphp.git

Note: the number of test cases in each archive may vary.

PHASE 3: INTEGRATION

N1: LAUNCH A CODE SCAN VIA COMMAND-LINE INTERFACE

Action	Expected Results
Launch a code scan against https://github.com/syhunt/vulnphp via command-line interface FOLLOW THE STEPS BELOW	After the scan completes, the results must list all test cases (from 001 to 009)

1. Go to the directory Syhunt Hybrid is installed using the command prompt.
2. Use the following command-line (with the -gr parameter, so that it can generate a report):

```
Scancode https://github.com/syhunt/vulnphp.git -gr
```

N2: LAUNCH A DYNAMIC SCAN VIA COMMAND-LINE INTERFACE

Action	Expected Results
Launch a dynamic scan against http://127.0.0.1/syhunt/vulndemo via command-line interface FOLLOW THE STEPS BELOW	After the scan completes, the results must list all test cases (from 001 to 011)

1. Make sure the Prey server is running (as explained in the Environment Requirements section at the beginning of this document)
2. Go to the directory Syhunt Hybrid is installed using the command prompt.
3. Use the following command-line (with the -gr parameter, so that it can generate a report):

```
Scanurl 127.0.0.1/syhunt/vulndemo -gr
```

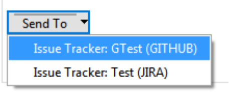
N3: CREATE A TRACKER ISSUE BASED ON A REPORTED VULNERABILITY

Action	Expected Results

Create a GitHub issue based on a reported vulnerability	After adding a GitHub tracker and submitting a vulnerability, your GitHub repository will list the vulnerability as an issue

FOLLOW THE STEPS BELOW

1. Create a GitHub.com account, if you don't have one, and create a test repository
2. Add a GitHub tracker in Syhunt as explained in Integrating Syhunt with JIRA and GitHub
3. Go to the menu ≡ -> Past Sessions option
4. Right click a session with status Vulnerable and click the View Vulnerabilities option
5. Check the vulnerability you want to send to GitHub
6. Click the button SendTo -> Your tracker name to submit the vulnerability



N4: GENERATE A F5 BIGIP ASM COMPATIBLE EXPORT

Action	Expected Results
Generate a ASM export file for a scan	After clicking the Save button, the browser will open the compatible XML file which you can then import in BigIP ASM

FOLLOW THE STEPS BELOW

1. Go to the menu ≡ -> Past Sessions option
2. Right click a session with status Vulnerable and click Generate Report option
3. Select Complete report template option
4. Click the Save Report button (at the bottom right corner of the tab)
5. Select Save as type XML ASM Generic Scanner Format and finally click the Save button

PHASE 4: REPORTING

R1: GENERATE A STANDARD HTML REPORT FOR A SCAN SESSION

Action	Expected Results

Generate a report for a scan using CVSS3 vulnerability sorting method FOLLOW THE STEPS BELOW	After clicking the Save button, the browser will open the HTML report file

1. Go to the menu ≡ -> Past Sessions option
2. Right click a session with status Vulnerable and click Generate Report option
3. Select Standard report template option (if not already selected)
4. Select CVSS vulnerability sorting method option (if not already selected)
5. Click the Save Report button (at the bottom right corner of the tab) and finally the Save button

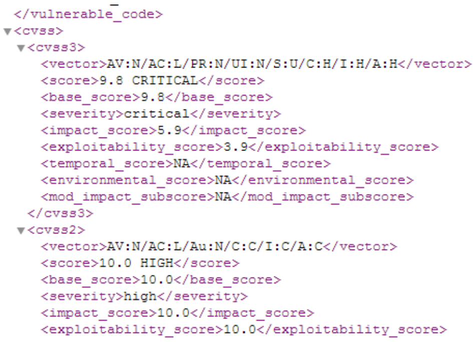
R2: GENERATE A COMPLETE HTML REPORT FOR A SCAN SESSION

Action	Expected Results
Generate a report for a scan using CVSS3 vulnerability sorting method FOLLOW THE STEPS BELOW	After clicking the Save button, the browser will open the HTML report file

1. Go to the menu ≡ -> Past Sessions option
2. Right click a session with status Vulnerable and click Generate Report option
3. Select Complete report template option
4. Select CVSS vulnerability sorting method option (if not already selected)
5. Click the Save Report button (at the bottom right corner of the tab) and finally the Save button

R3: GENERATE A XML RESULTS EXPORT FOR A SCAN SESSION

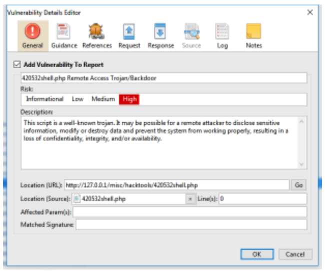
Action	Expected Results

Generate a XML results file for a scan FOLLOW THE STEPS BELOW	After clicking the Save button, the browser will open the XML results file 

```
 </vulnerable_code>
▼<cvss>
  ▼<cvss3>
     <vector>AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</vector>
     <score>9.8 CRITICAL</score>
     <base_score>9.8</base_score>
     <severity>critical</severity>
     <impact_score>5.9</impact_score>
     <exploitability_score>3.9</exploitability_score>
     <temporal_score>NA</temporal_score>
     <environmental_score>NA</environmental_score>
     <mod_impact_subscore>NA</mod_impact_subscore>
   </cvss3>
  ▼<cvss2>
     <vector>AV:N/AC:L/Au:N/C:C/I:C/A:C</vector>
     <score>10.0 HIGH</score>
     <base_score>10.0</base_score>
     <severity>high</severity>
     <impact_score>10.0</impact_score>
     <exploitability_score>10.0</exploitability_score>
```

1. Go to the menu ≡ -> Past Sessions option
2. Right click a session with status Vulnerable and click Generate Report option
3. Select Complete report template option
4. Click the Save Report button (at the bottom right corner of the tab)
5. Select Save as type XML File and finally click the Save button

R4: EDIT THE INFORMATION ABOUT A REPORTED VULNERABILITY

Action	Expected Results
Edit the information about a reported vulnerability FOLLOW THE STEPS BELOW	See the vulnerability edit screen. After editing and confirming the changes, if you generate a report, it will contain the edited information 

☑ Add Vulnerability To Report

420532shell.php Remote Access Trojan/Backdoor

Risk: Informational Low Medium [✓ High]

Description:
This script is a well-known trojan. It may be possible for a remote attacker to disclose sensitive information, modify or destroy data and prevent the system from working properly, resulting in a loss of confidentiality, integrity, and/or availability.

Location (URL): http://127.0.0.1/misc/hacktools/420532shell.php

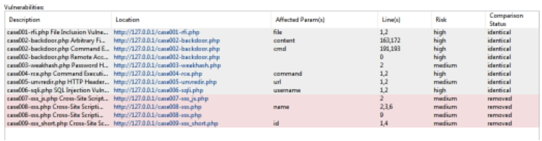
Location (Source): 420532shell.php Line(s): 0

Affected Param(s):

Matched Signature:

1. Go to the menu ≡ -> Past Sessions option
2. Right click a session with status Vulnerable and click the View Vulnerabilities option
3. Double-click a vulnerability item
4. Change the vulnerability description as you wish. Go to the Notes tab and also add some notes
5. Click the OK button to save changes

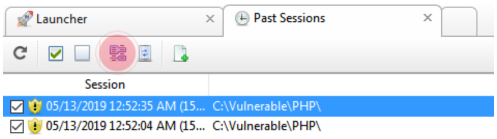
R5: GENERATE A COMPARISON REPORT BETWEEN SCAN SESSIONS

Action	Expected Results
Generate a comparison report between two scan sessions FOLLOW THE STEPS BELOW	A report must be generated with the same contents from the comparison screen, which should list test cases 007 to 009 as removed 

Vulnerabilities:

Description	Location	Affected Param(s)	Line(s)	Risk	Comparison Status
case001-rfi.php File Inclusion Vulne...	http://127.0.0.1/case001-rfi.php	file	1,2	high	identical
case002-backdoor.php Arbitrary Fi...	http://127.0.0.1/case002-backdoor.php	content	163,172	high	identical
case002-backdoor.php Command E...	http://127.0.0.1/case002-backdoor.php	cmd	191,193	high	identical
case002-backdoor.php Remote Acc...	http://127.0.0.1/case002-backdoor.php		0	high	identical
case003-weakhash.php Password H...	http://127.0.0.1/case003-weakhash.php		2	medium	identical
case004-rce.php Command Executi...	http://127.0.0.1/case004-rce.php	command	1,2	high	identical
case005-unvredir.php HTTP Header...	http://127.0.0.1/case005-unvredir.php	url	1,2	medium	identical
case006-sqli.php SQL Injection Vuln...	http://127.0.0.1/case006-sqli.php	username	1,2	high	identical
case007-xss_js.php Cross-Site Script...	http://127.0.0.1/case007-xss_js.php		2	medium	removed
case008-xss.php Cross-Site Scripti...	http://127.0.0.1/case008-xss.php	name	2,3,6	medium	removed
case008-xss.php Cross-Site Scripti...	http://127.0.0.1/case008-xss.php		9	medium	removed
case009-xss_short.php Cross-Site Sc...	http://127.0.0.1/case009-xss_short.php	id	1,4	medium	removed

1. Follow the steps described in section S1.
2. After completing the scan, go to the directory where you saved the vulnerable samples and delete test cases 007 to 009.
3. Scan the directory again as explained in section S1.
4. Go to the menu ≡ -> Past Sessions option
5. Check the two last scan sessions and click the Compare Sessions toolbar icon:



☑ 05/13/2019 12:52:35 AM (15... C:\Vulnerable\PHP\
☑ 05/13/2019 12:52:04 AM (15... C:\Vulnerable\PHP\

6. Click the Save Comparison As button (at the bottom right corner of the tab) and finally click the Save button

For additional product documentation, visit **syhunt.com/docs**