INTEGRATING SYHUNT INTO JENKINS

The information in this document applies to **version 6.9** of Syhunt Hybrid.

Syhunt scans can be easily executed from within a Jenkins Pipeline script, allowing you to integrate the Syhunt Dynamic, Syhunt Code and Syhunt Mobile tools into your continuous delivery pipeline, schedule scans and more.

Important: Remember to install Syhunt after deploying and setting up Jenkins. This way the Syhunt setup will detect your Jenkins installation and automatically install the required extensions. If you use scanCode() to scan a GIT URL, you will need to install Git on Linux or Git for Windows, which can be downloaded at https://gitforwindows.org/

ADDING SYHUNT TO YOUR PIPELINE SCRIPT

1. From the Jenkins Dashboard, open the desired pipeline item.
2. Click Configure from the sidebar links
3. Go to the Pipeline tab and uncheck the "Use Groovy Sandbox" option if checked
4. Insert the below code at the appropriate position of your pipeline script:

```
def rootDir = pwd()
def syhunt = load "${rootDir}/../workspace@script/syhunt/syhunt.groovy"
syhunt.scanURL([target: 'http://somewebsite.com/', huntMethod: 'appscan', pfcond: 'fail-if-risk=mediumu
```

Example:

```
#!/usr/bin/env groovy

node {
    stage('Scan') {
        def rootDir = pwd()
        def syhunt = load "${rootDir}/../workspace@script/syhunt/syhunt.groovy"
        syhunt.scanURL([target: 'http://somewebsite.com/', huntMethod: 'appscan', pfcond: 'fail-if:risk
    }
}
```

Click the Save button to update the pipeline configuration.

RUNNING THE BUILD

After building and executing the above pipeline script, the Console Output for the project should contain something like:

```
Pipeline] echo
Preparing to scan URL: http://somewebsite.com/
[Pipeline] echo
VULNERABLE!
Found 2 vulnerabilities
SYHUNT URLSCAN 6.8.5.4 PLATINUM EDITION (c) 2020 Syhunt
...
[Pipeline] echo
Build problem: found Medium risk vulnerabilities.
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: FAILURE
```

SCANURL FUNCTION

Syhunt Dynamic can be launched through the scanURL() function. The following parameters must be provided when calling the scanURL() function:

- **target** - the target URL to be scanned (eg. http://www.somesite.com)
- **huntMethod** (optional) - the Hunt Method to be used during the scan, If omitted, the default method will be used.
- **pfcond** (optional) - allows the build to fail if a certain condition is met. See below a list of available pass/fail conditions.

After executing, the ScanURL() function returns a map containing the following keys:

- **outFilename** - The filename of the generated scan report

SCANCODE FUNCTION

Syhunt Code can be launched through the scanCode() function. The following parameters must be provided when calling the scanCode() function:

- **target** - the target URL of a GIT repository, local source code directory or file to be scanned
- **huntMethod** (optional) - the Hunt Method to be used during the scan. If omitted, the default method will be used.
- **pfcond** (optional) - allows the build to fail if a certain condition is met. See below a list of available pass/fail conditions.
- **branch** (optional) - the branch of the GIT repository to be scanned. If omitted, master will be used. This parameter is not necessary if the target is a local directory or file.

Examples:

```
syhunt.scanCode([target: 'https://github.com/someuser/somerepo.git', huntMethod: 'normal', pfcond: 'fai
syhunt.scanCode([target: 'C:\\www\\', huntMethod: 'normal', pfcond: 'fail-if:risk=mediumup'])
```

PASS/FAIL CONDITIONS

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

SCHEDULING SCANS

1. From the Jenkins Dashboard, open the desired pipeline item.
2. Click Configure from the sidebar links
3. Go to the Build Triggers tab, check the "Build periodically" option and enter the appropriate schedule
4. Click the Save button to update the pipeline configuration

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