Pyces Automated Test Report

Test Run On : (23/10/2017 15:58:33 IST)

Contents:

Cloc Output:

```
http://cloc.sourceforge.net v 1.64  T=0.10 s (83.3 files/s, 57028.3 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
Python                           7            749            969           3358
YAML                             1             43              1            357
-------------------------------------------------------------------------------
SUM:                             8            792            970           3715
-------------------------------------------------------------------------------
```

Third Party Libraries detected in Code:

```
The following Third Party libraries were detected:
----------------------------------------------------

No Third Party Libraries are present in the folder.

-----------------
Reference Library
-----------------

No  Name of Component       Version number of component
1       boto - AWS for Python       2.26.0
2   Python httplib2                 0.9
3       Python sortedcontainer          0.9.5
4       Bootstrap               2.3.2
5       jqBootstrapValidation       1.3.7
6       select2                 3.5.2
7       RemotePDB                  1.2
8       jquery-cookie              1.4.1
9       pxGrid_Search.jar          NA
10  Bootstrap table                 1.9.1
11  BigSuds                     1.0.1
12  suds                        0.4
13  apache axis                 1.1
14  castor                      1.3
15  apache commons discovery   0.2
16  apache commons logging          1.1.1
17  gson                        2.2.4
18  hessian                     3.0.8
19  apache log4j                1.2
20  mx4j                        3
21  opencsv                     2.3
22  wsdl4j                      1.6
23  xerces                      2.x
24  simplejson                  3.6.2
25  javax.management.j2ee        6
26  jboss-cli-client        6.4
27  slf4j                   1.7.5
28  fastjson                1.2.5
29  apache commons configuration      1.1
30  apache commons collections  3.2.1
31  apache commons pool          2.3
32  apache commons io           2.4
33  guava                       18
34  Quartz.net                  2.1.1
35  Unity                       3.0.1304, 2.1.505.2
36  CommonServiceLocator        1
37  Common.Logging                  2.1.2
38  Common.Logging.NLog20           2.1.2
39  NLog                        2.0.1.2
40  SlowCheetah                 2.5.11
41  xUnit.net, xUnit.extensions     1.9.1
42  SpecFlow, SpecFlow.xUnit     1.9.0
43  defusedxml                  0.4.1
44  nfcapd & nfdump             1.6.8
45  Remote PDB                  1.1.3
46  futures                     3.0.3
```

Bandit Findings:

Metrics:

Total lines of code: 3474

Total lines skipped (#nosec): 0

Skipped files:

C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\pymcd.py **reason:** syntax error while parsing AST from file
C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\setup.py **reason:** syntax error while parsing AST from file

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.

Test ID: B101

Severity: LOW

Confidence: HIGH

CWE: CWE-703

File: C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\python-gdb.py

Line number: 451

More info: https://bandit.readthedocs.io/en/1.7.4/plugins/b101_assert_used.html

```
450                 dictoffset += size
451                 assert dictoffset > 0
452                 assert dictoffset % SIZEOF_VOID_P == 0
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.

Test ID: B101

Severity: LOW

Confidence: HIGH

CWE: CWE-703

File: C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\python-gdb.py

Line number: 452

More info: https://bandit.readthedocs.io/en/1.7.4/plugins/b101_assert_used.html

```
451                 assert dictoffset > 0
452                 assert dictoffset % SIZEOF_VOID_P == 0
453
```

blacklist: Consider possible security implications associated with the subprocess module.

Test ID: B404

Severity: LOW

Confidence: HIGH

CWE: CWE-78

File: C:\Users\bhanu\Documents\test\PyCes\Test_Project\pyces_runner.py

Line number: 1

More info: https://bandit.readthedocs.io/en/1.7.4/blacklists/blacklist_imports.html#b404-import-subprocess

```
1     import subprocess
2     import sys
3     import os
```

subprocess_popen_with_shell_equals_true: subprocess call with shell=True identified, security issue.

Test ID: B602

Severity: HIGH

Confidence: HIGH

CWE: CWE-78

File: C:\Users\bhanu\Documents\test\PyCes\Test_Project\pyces_runner.py

Line number: 15

More info: https://bandit.readthedocs.io/en/1.7.4/plugins/b602_subprocess_popen_with_shell_equals_true.html

```
14    def command_execution(args):
15     sub_ret = subprocess.Popen(args,stdout=subprocess.PIPE,shell=True)
16     return_code = sub_ret.stdout.read()
```

subprocess_popen_with_shell_equals_true: subprocess call with shell=True identified, security issue.

Test ID: B602

Severity: HIGH

Confidence: HIGH

CWE: CWE-78

File: C:\Users\bhanu\Documents\test\PyCes\Test_Project\pyces_runner.py

Line number: 20

More info: https://bandit.readthedocs.io/en/1.7.4/plugins/b602_subprocess_popen_with_shell_equals_true.html

```
19    def command_execution_2(args,working_directory):
20     sub_ret = subprocess.Popen(args,stdout=subprocess.PIPE,shell=True,cwd=working_directory)
21     return_code = sub_ret.stdout.read()
```

Dependency Check Output:

DEPENDENCY-CHECK

How to read the report |
Suppressing false positives |
Getting Help: github issues

Sponsor

Project: trial_project

Scan Information (show all):

- *dependency-check version*: 7.1.1
- *Report Generated On*: Tue, 28 Jun 2022 23:14:34 -0400
- *Dependencies Scanned*: 5 (5 unique)
- *Vulnerable Dependencies*: 1
- *Vulnerabilities Found*: 1
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
python27.dll	cpe:2.3:a:python:python:27:*:*:*:*:*:*:* cpe:2.3:a:python_software_foundation:python:27:*:*:*:*:*:*:*		MEDIUM	1	High	4

Dependencies

python27.dll

File Path: C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\python27.dll
MD5: 8a9982fb956104dfd6e0ecfb34f30ffe
SHA1: ffdd8e2583d2d26cffa6d72a37be35efdd8a236c
SHA256:da1669aaf15bc6d7f4783572dc635d38cff8137241864fd54b46a0d87abbdfc9

Evidence

Identifiers

- cpe:2.3:a:python:python:27:*:*:*:*:*:*:* (*Confidence*:High) suppress
- cpe:2.3:a:python_software_foundation:python:27:*:*:*:*:*:*:* (*Confidence*:High) suppress

Published Vulnerabilities

CVE-2007-4559 suppress

Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.
CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:

- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=263261
- MLIST - [python-dev] 20070824 tarfile and directory traversal vulnerability
- MLIST - [python-dev] 20070825 tarfile and directory traversal vulnerability
- SECUNIA - 26623
- VUPEN - ADV-2007-3022

Vulnerable Software & Versions:

- cpe:2.3:a:python_software_foundation:python:*:*:*:*:*:*:*:*

This report contains data retrieved from the National Vulnerability Database.
This report may contain data retrieved from the NPM Public Advisories.
This report may contain data retrieved from RetireJS.
This report may contain data retrieved from the Sonatype OSS Index.

CR Runner Output:

[Running the scanner at: Normal severity]

Finding Name	Finding Description	Finding Snippet	Srcfile:Lineno.
Reference to vulnerable algorithms	Reference to vulnerable algorithms	# The _md5 module implements the RSA Data Security, Inc. MD5	C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\setup.py:860
Pickle Library Used	Pickle library appears to be in use, possible security issue.	pickle.dump(MODULE_DB, handle)	C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\pymcd.py:347
Reference to vulnerable algorithms	Reference to vulnerable algorithms	# necessary files md5.c and md5.h are included here.	C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\setup.py:862
Reference to vulnerable algorithms	Reference to vulnerable algorithms	exts.append(Extension('_md5',	C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\setup.py:863
Reference to vulnerable algorithms	Reference to vulnerable algorithms	sources = ['md5module.c', 'md5.c'],	C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\setup.py:864
Reference to vulnerable algorithms	Reference to vulnerable algorithms	depends = ['md5.h']))	C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\setup.py:865
Pickle Library Used	Pickle library appears to be in use, possible security issue.	MODULE_DB = b = pickle.load(s)	C:\Users\bhanu\Documents\test\PyCes\Test_Project\Repository\Grep_Tool\python\pymcd.py:358