SeeCode Scanner

Release 1.0.0

Sep 30, 2019

Table of Contents

CHAPTER 1

What Is This?

`seecode-scanner` SAST SeeCode Audit GitLabGitHub

`seecode-scanner` `seecode-scanner` SonarScannerRuleScannerPluginScanner

- PMD TscanCode
-
- **//Docker**

  Celery

  Docker Dockfile

  FTPAWS(TODO)
- clocwalk Java MavenNodeJspipRuby
- RSA
-
  - 70%
  - Sonar tests

Note: seecode-scanner python3 Linux CentOS 7

CHAPTER 2

1

2.1 1.1

```
$ pip install seecode-scanner
```

cli.py

```
$ cd seecode_scanner
$ python3 cli.py
```

2.2 1.2

seecode_scanner.yml seecode-scanner /etc/seecode_scanner.yml SeeCode Audit

```
$ vim /etc/seecode_scanner.yml
```

```
server:
  domain: "http://seecode.com"
  api_uri: "/api/v2/"
  token: "dca58d563917b9325252f8a4b6c57e7331349052"
  public_key_path:
  private_key_path:

celery:
  broker_url: ""
  timezone: "Asia/Shanghai"
  c_force_root: False
  task_timeout: 7200
```

(continues on next page)

(continued from previous page)

```yaml
http:
  timeout: 10
  timeout_try: 3
  failed_try: 3
  try_status_code: 500, 502, 503
  proxies:
    http:
    https:
    socks5:
  headers:
    accept-encoding: "gzip, deflate"

distributed:
  ftp:
    host: "192.168.1.1"
    port: 21
    username: "seecode"
    password: "test1234"
    path: "/home/seecode/"
```

2.3 1.3

1). :

```
$ seecode-scanner --scan-path /tmp/java_demo --name java_demo -o java_demo.
↪json
```

2). :

```
$ seecode-scanner -c java_demo.yml
```

3). Celery :

```
$ seecode-scanner --celery
```

CHAPTER 3

2

```
$ python cli.py

--------------------------------------------------------------------------------
↪-----
      _____      U _____ u U _____ u     _____      U  ___ u    _____     U _____ u
     / __"| u  \| ___"|/ \| ___"|/ U /"___|     \/"_ \/   |  _"\    \| ___"|/
    <\___ \/     |  _|"     |  _|"    \| | u        | | | | /| | | |    |  _|"
     u___) |     | |___     | |___     | |/__  .-,_| |_| | U| |_| |\   | |___
     |____/>>    |_____|    |_____|     \____|  \_)-\___/   |____/ u   |_____|
      )(  (__)   <<   >>    <<   >>    _// \\         \\       |||_      <<   >>
     (__)       (__) (__)  (__) (__)  (__)(__)       (__)     (__)_)    (__) (__)
                 _____       _____       _          _   _        _   _      U _____ u     _____
                / __"| u   U /"___| U   /"\  u     | \ |"|      | \ |"|     \| ___"|/ U |  _"\␣
↪u
               <\___ \/    \| | u     \/ _ \/    <|  \| |>    <|  \| |>     |  _|"     \| |_)␣
↪|/
                u___) |     | |/__    / ___ \    U| |\  |u    U| |\  |u     | |___      |  _ <
                |____/>>     \_____| /_/   \_\    |_| \_|      |_| \_|      |_____|     |_| \_\
                 )(  (__)   _// \\    \\     >>    ||   \\,-.   ||   \\,-.   <<   >>     //  ␣
↪\\_
                (__)       (__)(__)  (__)   (__)   (_")  (_/    (_")  (_/   (__) (__)   (__)   (_
↪_)

                SeeCode Audit  seecode-scanner/1.0.0-20190903 xsseroot#gmail.com

--------------------------------------------------------------------------------
↪-----

usage: seecode-scanner [-h] [-v {warn,debug,info,error}] [--test]
                       [--no-banner] [--version] [--upgrade] [--monitor]
                       [-c CONFIG] [--scan-template TEMPLATE]
                       [--scan-threads THREADS] [--scan-path PROJECT_PATH]
                       [--name PROJECT_NAME] [--result-file RESULT_FILE]
                       [--celery] [--celery-concurrency CELERY_CONCURRENCY]
```

(continues on next page)

(continued from previous page)

```
                      [--celery-name CELERY_NAME]

optional arguments:
  -h, --help            show this help message and exit
  -v {warn,debug,info,error}
                        Verbosity level, default: info.
  --test, -t            Test the status of all system services, default:
                        False.
  --no-banner           Do not display banner information, default: False.
  --version             Show current software version.
  --upgrade             Connect to the server for scanning configuration
                        upgrade, default: False.
  --monitor             SeeCode Scanner client heartbeat monitoring service,
                        default: False.

scan arguments:
  -c CONFIG             Project scan configuration file based on yaml format.
  --scan-template TEMPLATE
                        Scan the name of the template, default: normal
  --scan-threads THREADS
                        The number of threads when the engine scans, default:
                        20.
  --scan-path PROJECT_PATH, -p PROJECT_PATH
                        The absolute path of the item to be scanned.
  --name PROJECT_NAME, -n PROJECT_NAME
                        The name of the project to scan.
  --result-file RESULT_FILE, -o RESULT_FILE
                        Scan the path saved by the report.

task arguments:
  --celery              Start celery's work tasks.
  --celery-concurrency CELERY_CONCURRENCY
                        Number of child processes processing the queue,
                        default: 4
  --celery-name CELERY_NAME
                        Set custom hostname, default: sca-1
```

3.1 2.1

3.1.1 -v

warndebuginfoerror

3.1.2 --test

False

3.1.3 --no-banner

banner False

3.1.4 --upgrade

SeeCode Audit seecode_scanner.yml False

3.1.5 --monitor

IP SeeCode Audit False

3.2 2.2

3.2.1 -c

3.2.2 --scan-template

profiles xml defaultnormalcomponent_scan

3.2.3 --scan-threads

() 20

3.2.4 --scan-path

–name

3.2.5 --name

–scan-path

3.2.6 --result-file

json

3.3 2.3 Celery

3.3.1 --celery

celery False

3.3.2 --celery-concurrency

celery -c 4

3.3.3 --celery-name

celery -n sca1

CHAPTER 4

TODO

- https://github.com/OWASP/wpBullet
- https://github.com/pmd/pmd
- https://github.com/Tencent/TscanCode

CHAPTER 5

- BTC 18F4VFDX2MCEXod7zjUF8NepUdAspEcJR8
- ETH 0xB3Bc55F4AAa8E87D3675B547e31d3eEbb585175c
- HT 0x952b4cd9f18126987fdbfab55e1ea72c5ae72e16

5.1 1

5.1.1 1.1 Server

SeeCode Audit Token

```
server:
  domain: "http://seecode.com"
  api_uri: "/api/v2/"
  token: "dca58d563917b9325252f8a*********"
  public_key_path:
  private_key_path:
```

1.1.1 domain

SeeCode Audit http://seecode.example.com

1.1.2 api_uri

SeeCode Audit API URI /api/v2/

1.1.3 token

SeeCode Audit Token

1.1.4 public_key_path

SeeCode Audit RSA /home/seecode/public.pem

1.1.5 private_key_path

SeeCode Audit RSA /home/seecode/private.pem

5.1.2 1.2 Celery

Celery border_url, timezonec_force_roottask_timeout

```
celery:
  broker_url: ""
  timezone: "Asia/Shanghai"
  c_force_root: False
  task_timeout: 7200
```

1.2.1 broker_url

Celery Broker URL RedisRabbitMQR

1.2.2 timezone

Celery ”Asia/Shanghai”

1.2.3 c_force_root

Celery Root False

1.2.4 task_timeout

Celery 7200

5.1.3 1.3 HTTP

HTTP

```
http:
  timeout: 10
  timeout_try: 3
  failed_try: 3
  try_status_code: 500, 502, 503
  proxies:
    http:
```

(continues on next page)

(continued from previous page)

```
    https:
    socks5:
  headers:
    accept-encoding: "gzip, deflate"
```

1.3.1 timeout

SeeCode Audit requests.exceptions.Timeout 10

1.3.2 timeout_try

SeeCode Audit 3

1.3.3 failed_try

SeeCode Audit 3

1.3.4 try_status_code

200500502503

1.3.5 proxies

SeeCode Audit

http

http http://192.168.1.1:8080

https

https https://192.168.1.1:8080

socks5

socks5 socks5://192.168.1.1:8080

1.3.6 headers

HTTP accept-encodinguser-agent

5.1.4 1.4 Distributed

FTPAWS

```
distributed:
  ftp:
    host: "192.168.1.1"
    port: 21
    username: "seecode"
    password: "test1234"
    path: "/home/seecode/"
```

1.4.1 FTP

host

FTP IP 192.168.1.10

port

FTP 21

username

FTP seecode

password

FTP

path

FTP /home/seecode/

1.4.2 AWS (TODO)

5.2 2

SeeCode Audit `seecode-scanner --upgrade`

SonarScannerRuleScannerPluginScanner

seecode-scanner xml config engines

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<template version="1.0.0">
    <config>
        <name>normal</name>
```

(continues on next page)

(continued from previous page)

```
        <version>6.0</version>
        <exclude_dir>.git/,bin/,node_modules/,assets/,static/,.svn/</exclude_dir>
        <exclude_ext>.jpg,.jpeg,.png,.bmp,.gif,.ico,.cur,</exclude_ext>
        <exclude_file></exclude_file>
    </config>
    <engines>
        <engine></engine>
    </engines>
</template>
```

5.2.1 2.1 template

version

5.2.2 2.2 config

name

defaultnormalcomponent_scan

version

2.1

exclude_dir

.git/,.svn/(,)

exclude_ext

readme.md(,)

exclude_file

.log,.txt(,)

5.2.3 2.3 engine

engine engines engines engine

name

SonarScannerRuleScannerPluginScanner

parameters

, SonarScanner

```
<parameters>
      <!-- SonarQube  Token -->
      <item name="API_TOKEN">80828d9343317970f*********</item>

      <!-- SonarQube  API  -->
      <item name="API_DOMAIN">http://sonar7.example.com</item>

      <!-- sonar-scanner  -->
      <item name="SONAR_SCANNER_PATH">/usr/bin/sonar-scanner</item>

      <!-- SonarScanner  -->
      <item name="ENGINE_TIMEOUT">1200</item>

      <!-- SonarScanner  SonarQube  -->
      <item name="HTTP_TIMEOUT">10</item>

      <!-- SonarScanner  SonarQube  -->
      <item name="HTTP_TIMEOUT_RETRY">3</item>

      <!-- SonarScanner  SonarQube  -->
      <item name="HTTP_FAILED_RETRY">3</item>

      <!-- sonar ,
      {{project_key}} key
      {{project_name}}
      {{sonar_host}}sonarqube  API_DOMAIN
      {{sonar_login}}sonarqube token API_TOKEN
      -->
      <item name="SONAR_PROJECT_PROPERTIES">sonar.projectKey={{project_key}}&#13;
                sonar.projectName={{project_name}}&#13;
                sonar.projectVersion=1.0&#13;
                sonar.sources=.&#13;
                sonar.sourceEncoding=UTF-8&#13;
                sonar.exclusions=**/node_modules/**/*.*,&#13;
                sonar.host.url={{sonar_host}}&#13;
                sonar.login={{sonar_login}}&#13;
                sonar.java.binaries=.
      </item>
</parameters>
```

item

- name
  - []
- item
  -

component

RuleScanner SonarScannerPuginScanner

RuleScanner

```
<component>
    <item id="7582">
        <name>Apache Solr (CVE-2019-0192)</name>
        <key>java:apache-solr-cve-2019-0192</key>
        <revision>0.43</revision>
        <risk id="3"></risk>
        <category>Vulnerability</category>
        <match_type>name</match_type>
        <match_content><![CDATA[solr-solrj]]></match_content>
        <match_regex flag="I"><![CDATA[(5\.[0-5]{1}) ### 5.0-5.5
            (5\.2\.1) ### 5.0-5.5
            (5\.3\.[1-2]{1}) ### 5.3.1 - 5.3.2
            (5\.4\.1) ### 5.4.1
            (5\.5\.[1-5]{1}) ### 5.5.1 - 5.5.5
            (6\.[0-6]{1})
            (6\.0\.1)
            (6\.1\.1)
            (6\.2\.1)
            (6\.4\.[1-2]{1})
            (6\.5\.1)
            (6\.6\.[1-5]{1})]]>
        </match_regex>
    </item>
</component>
```

item

- id
  - [] SeeCode Audit ID
- name
  - *Apache Solr (CVE-2019-0192)*
- key
  - Key (:)
- revision
  -
- risk
  - id SeeCode Audit risk
  -
- category
  - Code SmellBugVulnerability sonarqube
- match_type

  - namegroupId
- match_content
  -
- match_regex
  -
  - flag I()M()I|M()

---

blacklist

SonarScanner () SONAR_PROJECT_PROPERTIES

(1) RuleScanner

```
<blacklist>
    <item id="7583">
        <name></name>
        <key>common:password-hard</key>
        <revision>0.27</revision>
        <risk id="3"></risk>
        <category>Vulnerability</category>
        <match_type>content</match_type>
        <file_ext>.java</file_ext>
        <match_regex flag="I"><![CDATA[PARAM_NAME_password\s+=\s+['"].+['"]]]></match_
↪regex>
    </item>
</blacklist>
```

item

- id *componentid*
- name *componentname*
- key *componentkey*
- revision *componentrevision*
- risk *componentrisk*
- category *componentcategory*
- match_type
  - dirfilecontent
- file_ext ※
  - match_type content , (,), .java,.jsp
- match_regex
  - ↑ *componentmatch_regex*

(2) PluginScanner

```
<blacklist>
    <item id="7583">
        <name>XSS</name>
        <key>java:reflective-xss</key>
        <revision>0.03</revision>
        <risk id="4"></risk>
        <category id="3">Vulnerability</category>
        <module>seecode_scanner.plugins.blacklist.reflective_xss_java</module>
        <script>plugins/whitelist/reflective_xss_java.py</script>
    </item>
</blacklist>
```

item

- id
- name
- key
- revision
- risk
- category
- module
  - seecode_scanner
- script
  - py

---

whitelist

(1) RuleScanner

```
<whitelist>
    <item id="7580">
        <name></name>
        <key>common:password-exclude</key>
        <revision>0.27</revision>
        <risk id="4"></risk>
        <category>BUG</category>
        <match_type>content</match_type>
        <match_regex flag=""><![CDATA[PARAM_NAME_PASSWORD\s+=\s+['"].+['"]]]></match_
↪regex>
    </item>
</whitelist>
```

item

- id *componentid*
- name *componentname*
- key *componentkey*
- revision *componentrevision*

- risk *componentrisk*
- category *componentcategory*
- match_type
  - dirfilecontent
- file_ext ※
  - match_type content , (,), .java,.jsp
- match_regex
  - ↑ *componentmatch_regex*

(2)PluginScanner

```
<whitelist>
    <item id="7583">
        <name></name>
        <key>java:pass-test-file-dir</key>
        <revision>0.03</revision>
        <risk id="5"></risk>
        <category id="3">Vulnerability</category>
        <module>seecode_scanner.plugins.whitelist.pass_file_dir</module>
        <script>plugins/whitelist/pass_file_dir.py</script>
    </item>
</whitelist>
```

item

- id
- name
- key
- revision
- risk
- category
- module
  - seecode_scanner
- script
  - py

5.3 3

yaml seecode-scanner -c Celery

5.3.1 3.1

(online)

```
scan:
  # ID
  task_id: 9527
  #
  template: "normal"
  #
  threads: 20
  #
  log_level: "debug"
  #
  work_dir: "/data/seecode/"
  #  git
  project_ssh: "git@github.com:seecode-audit/vuln_java.git"
  # web
  project_web: "https://github.com/seecode-audit/vuln_java"
  #
  project_name: "vuln_java"
  #
  project_branch: "master"
  #  online offline
  project_type: "online"
  # : local, ftp, aws
  project_storage_type: "local"
  #
  project_file_origin_name: ""
  # MD5
  project_file_hash: ""
  #
  group_name: "seecode-audit"
  # key
  group_key: "seecode-audit"
  #
  evidence_start_line_offset: -1
  #
  evidence_count: 5
  #
  force_sync_code: True
  #  server  task_id
  sync_vuln_to_server: True
  #
  result_format: "json"
  #
  result_file: "9527.json"
```

(offline)

```
scan:
  task_id: 184
  template: "normal"
  log_level: "debug"
  work_dir: "/data/seecode/"
  project_name: "xxxxx"
  project_branch: "master"
  project_ssh: "ftp://192.168.1.100:21/home/seecode/projects/XIANXIAXIANGMUZU/
↪1566816638.zip"
  project_web: ""
  project_file_origin_name: "xxxxx.zip"
```

(continues on next page)

(continued from previous page)

```
  project_file_hash: "1b6d61ee077eb0b9c12465e24b388033"
  group_name: ""
  group_key: "xianxiaxiangmuzu"
  project_type: "offline"
  project_storage_type: "ftp"
  evidence_start_line_offset: -1
  evidence_count: 5
  result_file: "184.json"
  sync_vuln_to_server: True
  force_sync_code: False
```

5.3.2 3.2

scan yaml

task_id

id id SeeCode Audit id

template

: defaultnormalcomponent_scan

- default RuleScannerPluginScanner
- normal RuleScannerPluginScannerSonarScanner
- component_scan RuleScanner

threads

20

log_level

infodebugerror

work_dir

: "/data/seecode/"

project_ssh

git : "git@github.com/seecode-audit/vuln_java.git" "https://github.com/seecode-audit/vuln_java.git"

project_web

http : "https://github.com/seecode-audit/vuln_java"

project_name

: “vuln_java”

project_branch

: “master”

project_type

onlineoffline

- online project_ssh git
- offline project_ssh zip

project_storage_type

: local, ftp, aws

- local
- ftp ftp
- aws aws

project_file_origin_name

, project_type offline

project_file_hash

MD5, project_type offline

group_name

: “”

group_key

key: “xianxiaxiangmuzu”

evidence_start_line_offset

-1

evidence_count

5

force_sync_code

True

sync_vuln_to_server

server task_id True

result_format

“json” (json)

result_file

task_id : “453.json”

5.4 4

json

```
{
    "749c86838b5d24a64ed2b40fb18f5af4": {
        "rule_key": "java:apache-solr-cve-2019-0192",
        "risk_id": 3,
        "category": "vulnerability",
        "title": "Apache Solr \u8fdc\u7a0b\u4ee3\u7801\u6267\u884c(CVE-2019-0192)",
        "file": "pom.xml",
        "author": "MyKings",
        "author_email": "xsseroot@gmail.com",
        "hash": "d3f491ad09eaa9f7923edd2e041099e81171eb38",
        "start_line": 37,
        "end_line": 38,
        "report": "https://github.com/seecode-audit/vuln_java/blob/master/pom.xml#L37
↪",
        "code_example": "            <artifactId>solr-solrj</artifactId>\n
↪<version>5.5.3</version>\n        </dependency>\n        <dependency>\n
↪<groupId>org.apache.shiro</groupId>\n",
        "is_false_positive": false,
        "whitelist_rule_id": "",
        "evidence_content": "5.5.3",
        "engine": 2
}
```

5.4.1 4.1

rule_key

key

risk_id

ID

category

Code SmellBugVulnerability

title

file

author

author_email

hash

commit id

start_line

end_line

report

URL

- SonarScanner SonarQube
- gitlab github

code_example

6

evidence_content

is_false_positive

whitelist_rule_id

ID

engine

- 1 SonarScanner
- 2 RuleScanner
- 3 PluginScanner

5.5 1

5.5.1 1.1

```
$ sudo yum install -y perl perl-Digest-MD5 unzip git
```

python 3.6

```
$ sudo yum install -y centos-release-scl rh-python36 && scl enable rh-python36 bash
$ curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py && python get-pip.py
$ echo "export PYTHONIOENCODING=utf-8" >> ~/.bashrc && source ~/.bashrc
```

sonarscanner

sonarscanner https://docs.sonarqube.org/latest/analysis/scan/sonarscanner/ sonarscanner /usr/local/ sonarscanner /usr/bin/sonar-scanner

```
$ wget https://binaries.sonarsource.com/Distribution/sonar-scanner-cli/sonar-scanner-
↪cli-4.0.0.1744-linux.zip
$ sudo unzip sonar-scanner-cli-4.0.0.1744-linux.zip -d /usr/local/ && \
  ln -s /usr/local/sonar-scanner-4.0.0.1744-linux/bin/sonar-scanner /usr/bin/sonar-
↪scanner
```

cloc

yum yum

```
$ sudo yum install -y cloc
```

cloc-1.82

```
$ sudo wget https://github.com/AlDanial/cloc/releases/download/1.82/cloc-1.82.pl && \
  cp cloc-1.82.pl /usr/bin/cloc
```

seecode ,

```
$ sudo useradd -m -s /bin/bash seecode && passwd seecode
```

seecode SSH /home/seecode/.ssh/id_rsa /home/seecode/.ssh/id_rsa.pub

```
$ su - seecode
$ mkdir ~/.ssh && ssh-keygen
```

gitlab “” -> “SSH ” id_rsa.pub

```
$ cat /home/seecode/.ssh/id_rsa.pub
```

5.5.2 1.2

```
$  seecode-scanner --upgrade
------------------------------------------------------------------------------------------
↪-------------
        _____      U _____ u U _____ u     _____      U  ___ u    _____     U _____ u
       / __"| u   \| ___"|/ \| ___"|/ U /"___|      \/"_ \/   |  _"\    \| ___"|/
      <\___ \/     |  _|"     |  _|"    \| | u        | | | | /| | | |    |  _|"
       u___) |     | |___     | |___     | |/__  .-,_| |_| | U| |_| |\   | |___
       |____/>>    |_____|    |_____|     \____|  \_)-\___/   |____/ u   |_____|
        )(  (__)   <<   >>    <<   >>    _// \\          \\       |||_      <<   >>
       (__)        (__) (__)  (__) (__)  (__)(__)        (__)     (__)_)    (__) (__)
                  _____       _____       _          _    _        _    _      U _____ u     _____
                 / __"| u   U /"___| U   /"\  u     | \ |"|      | \ |"|     \| ___"|/ U |  _
↪"\ u
                <\___ \/    \| | u     \/ _ \/    <|  \| |>    <|  \| |>     |  _|"     \| |_
↪) |/
                 u___) |     | |/__    / ___ \    U| |\  |u    U| |\  |u     | |___      |  _
↪<
                 |____/>>     \____| /_/   \_\    |_| \_|      |_| \_|      |_____|     |_|␣
↪\_\
                  )(  (__)   _// \\    \\     >>    ||    \\,-.   ||    \\,-.   <<   >>     //  ␣
↪\\_
                 (__)        (__)(__)  (__)   (__)   (_")   (_/    (_")   (_/   (__) (__)   (__) ␣
↪(__)

                 SeeCode Audit  seecode-scanner/1.0.0-20190903 xsseroot#gmail.com

------------------------------------------------------------------------------------------
↪-------------

[15:18:36] [INFO] Check the latest version...
[15:18:36] [INFO] [+] The server has opened the encrypted communication.
[15:18:36] [INFO] The latest version of: [v1.85.14]
[15:18:36] [INFO] Initialize the upgrade environment and create an upgrade directory..
↪.
[15:18:36] [INFO] Start upgrading, check if the local version is consistent with the␣
↪server version...
[15:18:36] [INFO] current version: [v1.1.1], new version: [v1.85.14].
[15:18:36] [INFO] Start downloading the upgrade package...
[15:18:36] [INFO] Start decompressing the encryption upgrade package...
[15:18:37] [INFO] Unzip the encryption upgrade package to complete.
[15:18:37] [INFO] Start decompressing the decryption upgrade package...
[15:18:37] [INFO] Decompression and decryption upgrade package completed
[15:18:37] [INFO] Start syncing scan templates...
[15:18:37] [INFO] Synchronous scan template completion.
[15:18:37] [INFO] Start syncing whitelist plugin...
[15:18:37] [INFO] Synchronous whitelist plugin completed.
[15:18:37] [INFO] Start updating the current version to v1.85.14.
[15:18:37] [INFO] Upgrade completed, current version: v1.85.14
```

5.5.3 1.3

5.5.4 1.4

```
$  seecode-scanner -t
  ------------------------------------------------------------------------------------
↪---------------
        _____      U _____ u U _____ u     _____      U  ___ u    _____     U _____ u
       / __"| u  \| ___"|/ \| ___"|/ U /"___|     \/"_ \/  |  _"\    \| ___"|/
      <\___ \/     |  _|"     |  _|"    \| | u       | | | | /| | | |    |  _|"
       u___) |    | |___     | |___     | |/__  .-,_| |_| | U| |_| |\   | |___
       |____/>>   |_____|    |_____|     \____|  \_)-\___/   |____/ u   |_____|
        )(  (__)  <<   >>    <<   >>    _// \\         \\       |||_     <<   >>
       (__)      (__) (__)  (__) (__)  (__)(__)       (__)     (__)_)   (__) (__)
                  _____          _          _    _          _    _       U _____ u     _____
                 / __"| u  U /"___| U  /"\  u   | \ |"|      | \ |"|      \| ___"|/ U |  _
↪"\ u
                <\___ \/   \| | u    \/ _ \/   <|  \| |>    <|  \| |>     |  _|"     \| |_
↪) |/
                 u___) |    | |/__   / ___ \   U| |\  |u    U| |\  |u     | |___       |  _
↪<
                 |____/>>    \____| /_/   \_\   |_| \_|      |_| \_|      |_____|     |_|␣
↪\_\
                  )(  (__)  _// \\   \\    >>   ||   \\,-.  ||   \\,-.  <<   >>     //  ␣
↪\\_
                 (__)      (__)(__) (__)  (__)  (_")  (_/   (_")  (_/   (__) (__)   (__) ␣
↪(__)

                 SeeCode Audit  seecode-scanner/1.0.0-20190911 xsseroot#gmail.com

  ------------------------------------------------------------------------------------
↪---------------

  [07:24:03] [INFO] [CORE] Start testing whether the core file of seecode-scanner␣
↪exists...
  [07:24:03] [ERROR] [-] "/etc/seecode_scanner.yml" file not found.
  [07:24:03] [INFO] [+] Discover "/data/seecode/" directory.
  [07:24:03] [INFO] [SERVER] Start detecting service list files...
  [07:24:03] [ERROR] [-] "/usr/local/etc/seecode/conf/services.json" file not found.
  [07:24:03] [INFO] [SERVER] Start detecting core files...
  [07:24:03] [ERROR] [-] "monitor_url" is not set, the current content is: None.
  [07:24:03] [ERROR] [-] "upgrade_url" is not set, the current content is: None.
  [07:24:03] [ERROR] [-] "task_url" is not set, the current content is: None.
  [07:24:03] [INFO] [SCAN] Start testing whether the scan template of seecode-scanner␣
↪exists...
  [07:24:03] [INFO] [+] Found "/seecode_scanner/profiles/normal.xml" file.
  [07:24:03] [INFO] [+] Found "/seecode_scanner/profiles/component_scan.xml" file.
  [07:24:03] [INFO] [+] Found "/seecode_scanner/profiles/default.xml" file.
  [07:24:03] [INFO] [ENGINE] Start detecting the scan engine...
  [07:24:03] [INFO] [+] Found the "sonar-scanner" tool with the path "/usr/bin/sonar-
↪scanner"
␣
↪=============================================================================================
    NAME          ||    STATUS    ||    VERSION    ||          DESCRIPTION
␣
↪=============================================================================================
    Core          |    MISSING   |       -       |    -
```

(continues on next page)

(continued from previous page)

```
  ------------------------------------------------------------------------------------
↪-----------------------------------
     Server         |     MISSING    |        -        |     -
  ------------------------------------------------------------------------------------
↪-----------------------------------
     Scan Template |     FOUND      |        -        | /seecode_scanner/profiles/normal.
↪xml
     Scan Template |     FOUND      |        -        | /seecode_scanner/profiles/
↪component_scan.xml
     Scan Template |     FOUND      |        -        | /seecode_scanner/profiles/default.
↪xml
  ------------------------------------------------------------------------------------
↪-----------------------------------
     Engine         |     FOUND      |        -        | seecode_scanner.lib.engines.
↪sonarscanner (/usr/bin/sonar-scanner)
     Engine         |     FOUND      |        -        | seecode_scanner.lib.engines.
↪rulescanner
     Engine         |     FOUND      |        -        | seecode_scanner.lib.engines.
↪pluginscanner
  ------------------------------------------------------------------------------------
↪-----------------------------------
```

5.6 2 Docker

Docker seecode_scanner.yml

5.6.1 2.1

seecode-scanner docker images

```
$ docker build -t seecode-scanner .
```

5.6.2 2.2

seecode_scanner.yml

sca1 shell bash

```
$ docker run -it --name sca1 seecode-scanner /bin/bash
```

sca1 supervisord

```
$ docker run -d --name sca1 seecode-scanner
```

sca1

```
$ docker exec -it sca1 sh
```

5.7 1

json

vuln_java (default.xml)

```
$ python cli.py --scan-path ./tmp/vuln_java --name vuln_java -o 1.json
-------------------------------------------------------------------------------
↪--------------
          _____      U _____ u U _____ u     _____      U  ___ u    _____     U _____ u
         / __"| u  \| ___"|/ \| ___"|/ U /"___|      \/"_ \/   |  _"\    \| ___"|/
        <\___ \/     |  _|"     |  _|"    \| | u        | | | | /| | | |    |  _|"
         u___) |    | |___     | |___     | |/__  .-,_| |_| | U| |_| |\   | |___
         |____/>>   |_____|    |_____|     \____|  \_)-\___/   |____/ u   |_____|
          )(  (__)  <<   >>    <<   >>    _// \\          \\       |||_     <<   >>
         (__)       (__) (__)  (__) (__)(__)       (__)     (__)_)    (__) (__)
                   _____         _____       _          _    _        _    _      U _____ u     __
↪__
                  / __"| u  U /"___| U  /"\  u    | \ |"|      | \ |"|     \| ___"|/ U | ␣
↪_"\ u
                 <\___ \/   \| | u    \/ _ \/    <|  \| |>    <|  \| |>     |  _|"     \|␣
↪|_) |/
                  u___) |    | |/__   / ___ \    U| |\  |u    U| |\  |u     | |___      | ␣
↪_ <
                  |____/>>    \_____| /_/   \_\    |_| \_|      |_| \_|      |_____|     |_
↪| \_\
                   )(  (__)  _// \\   \\     >>    ||   \\,-.   ||   \\,-.   <<   >>     //␣
↪  \\_
                  (__)       (__)(__) (__)   (__)   (_")  (_/    (_")  (_/   (__) (__)   (__
↪)  (__)

                  SeeCode Audit  seecode-scanner/1.0.0-20190911 xsseroot#gmail.com

-------------------------------------------------------------------------------
↪--------------

[02:36:13] [INFO] [ScanProject] Start syncing project code into the scan directory...
[02:36:13] [INFO] [ScanProject] Synchronization project code completion.
[02:36:13] [INFO] [ScanProject] Start executing exclusion rules...
[02:36:13] [INFO] [ScanProject] Exclusion rule execution completed.
[02:36:13] [INFO] [ScanProject] Start analyzing components...
[02:36:13] [/opt/rh/rh-python36/root/usr/lib/python3.6/site-packages/clocwalk/cli.
↪py(70)start()] [INFO] analysis statistics code ...
[02:36:14] [INFO] [ScanProject] Project code line: [419], language: [Python], size:␣
↪[116] KB
[02:36:14] [INFO] [ScanProject] Start executing exclusion rules...
[02:36:14] [INFO] [ScanProject] Exclusion rule execution completed.
[02:36:14] [INFO] [RuleScanner] Begin to perform rule-based component vulnerability␣
↪analysis...
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'Apache Solr (CVE-2019-0192)'␣
↪vulnerability.
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'Apache Shiro  (RCE)'␣
↪vulnerability.
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'Spring Framework (CVE-2018-
↪1270)' vulnerability.
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'fastjson ' vulnerability.
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind  (CVE-2019-
↪12384)' vulnerability.
```

(continues on next page)

(continued from previous page)

```
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind CVE-2017-17485
↪' vulnerability.
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind CVE-2017-7525
↪' vulnerability.
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind polymorphic␣
↪(CVE-2018-12022)' vulnerability.
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind polymorphic␣
↪(CVE-2018-14719)' vulnerability.
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind polymorphic␣
↪(CVE-2018-19362)' vulnerability.
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind␣
↪SubTypeValidator.java  (CVE-2019-14379)' vulnerability.
[02:36:14] [INFO] [RuleScanner] [Component] [+] Found 'Fastjson' vulnerability.
[02:36:14] [INFO] [RuleScanner] Rule component scan completed.
[02:36:14] [INFO] [RuleScanner] ...
[02:36:14] [INFO] [RuleScanner] Begin to perform rule-based blacklist vulnerability␣
↪analysis...
[02:36:14] [INFO] [RuleScanner] Rule blacklist scan completed.
[02:36:14] [INFO] [PluginScanner] ...
[02:36:14] [INFO] [RuleScanner] ...
[02:36:14] [INFO] [RuleScanner] False positive rule processing...
[02:36:14] [INFO] [RuleScanner] Rule whitelist scan completed.
[02:36:14] [INFO] [PluginScanner] ...
[02:36:14] [INFO] [PluginScanner] False positive plugin processing...
[02:36:14] [INFO] [PluginScanner] Plugin whitelist scan completed.
[02:36:14] [INFO] [ScanProject] [+] Save the scan results to '/data/seecode/logs/vuln_
↪java/1.json', total: 12.
[02:36:14] [INFO] Analysis completed, time consuming: 1.57s
```

5.8 2

gitlab/github -c

```
$ python cli.py -c vuln_java.yaml
------------------------------------------------------------------------------------
↪-------------
          _____      U _____ u U _____ u     _____      U  ___ u   _____     U _____ u
         / __"| u  \| ___"|/ \| ___"|/ U /"___|     \/"_ \/  |  _"\    \| ___"|/
        <\___ \/    |  _|"     |  _|"    \| | u       | | | | /| | | |    |  _|"
         u___) |    | |___     | |___     | |/__  .-,_| |_| | U| |_| |\   | |___
         |____/>>   |_____|    |_____|    \____|  \_)-\___/   |____/ u   |_____|
          )(  (__)  <<   >>    <<   >>   _// \\        \\       |||_      <<   >>
         (__)      (__) (__)  (__) (__) (__)(__)      (__)     (__)_)    (__) (__)
                  ____         ____       _         _   _       _   _      U _____ u     __
↪__
                 / __"| u  U /"___| U  /"\  u    | \ |"|      | \ |"|     \| ___"|/ U | ␣
↪_"\ u
                <\___ \/   \| | u     \/ _ \/    <|  \| |>    <|  \| |>     |  _|"     \|␣
↪|_) |/
                 u___) |     | |/__    / ___ \    U| |\  |u    U| |\  |u     | |___      | ␣
↪_ <
                 |____/>>     \____| /_/   \_\    |_| \_|      |_| \_|      |_____|     |_
↪| \_\
                  )(  (__)   _// \\    \\     >>    ||    \\,-.  ||    \\,-.  <<    >>     //␣
↪  \\_
```

(continues on next page)

(continued from previous page)

```
                  (__)       (__)(__)  (__)   (__)   (_")  (_/    (_")  (_/   (__)  (__)   (__
↪)   (__)

                  SeeCode Audit  seecode-scanner/1.0.0-20190911 xsseroot#gmail.com

------------------------------------------------------------------------------
↪-------------

[02:52:18] [WARNING] [TaskStatus] Query scan task information failed, returned '404 -␣
↪Not Found' when accessing [http://seecode.com/api/v2/task/9527/] API interface.
[02:52:18] [INFO] [ScanProject] Start syncing project code into the scan directory...
[02:52:18] [INFO] [GitOperator] Force update of local code...
[02:52:22] [INFO] [GitOperator] Code synchronization completed.
[02:52:22] [INFO] [ScanProject] current branch␣
↪commit:d3f491ad09eaa9f7923edd2e041099e81171eb38, branch name:master
[02:52:22] [INFO] [ScanProject] Synchronization project code completion.
[02:52:22] [INFO] [ScanProject] Start executing exclusion rules...
[02:52:22] [INFO] [ScanProject] Exclusion rule execution completed.
[02:52:22] [INFO] [ScanProject] Start analyzing components...
[02:52:22] [/opt/rh/rh-python36/root/usr/lib/python3.6/site-packages/clocwalk/cli.
↪py(70)start()] [INFO] analysis statistics code ...
[02:52:22] [INFO] [ScanProject] Project code line: [419], language: [Python], size:␣
↪[124] KB
[02:52:22] [INFO] [ScanProject] Start executing exclusion rules...
[02:52:23] [INFO] [ScanProject] Exclusion rule execution completed.
[02:52:23] [INFO] [RuleScanner] Begin to perform rule-based component vulnerability␣
↪analysis...
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'Apache Solr (CVE-2019-0192)'␣
↪vulnerability.
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'Apache Shiro  (RCE)'␣
↪vulnerability.
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'Spring Framework (CVE-2018-
↪1270)' vulnerability.
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'fastjson ' vulnerability.
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind  (CVE-2019-
↪12384)' vulnerability.
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind CVE-2017-17485
↪' vulnerability.
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind CVE-2017-7525
↪' vulnerability.
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind polymorphic␣
↪(CVE-2018-12022)' vulnerability.
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind polymorphic␣
↪(CVE-2018-14719)' vulnerability.
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind polymorphic␣
↪(CVE-2018-19362)' vulnerability.
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'Jackson-databind␣
↪SubTypeValidator.java  (CVE-2019-14379)' vulnerability.
[02:52:23] [INFO] [RuleScanner] [Component] [+] Found 'Fastjson' vulnerability.
[02:52:23] [INFO] [RuleScanner] Rule component scan completed.
[02:52:23] [INFO] [RuleScanner] ...
[02:52:23] [INFO] [RuleScanner] Begin to perform rule-based blacklist vulnerability␣
↪analysis...
[02:52:23] [INFO] [RuleScanner] Rule blacklist scan completed.
[02:52:23] [INFO] [RuleScanner] ...
[02:52:23] [INFO] [RuleScanner] False positive rule processing...
[02:52:23] [INFO] [RuleScanner] Rule whitelist scan completed.
```

(continues on next page)

(continued from previous page)

```
[02:52:23] [INFO] [ScanProject] [+] Save the scan results to '/data/seecode/logs/9527/
↪9527.json', total: 12.
[02:52:23] [INFO] Analysis completed, time consuming: 5.59s
```

vuln_java.yaml

```
scan:
  task_id: 9527
  template: "component_scan"
  threads: 20
  log_level: "info"
  work_dir: "/data/seecode/"
  project_ssh: "https://github.com/seecode-audit/vuln_java.git"
  project_web: "https://github.com/seecode-audit/vuln_java"
  project_name: "vuln_java"
  project_branch: "master"
  project_type: "online"
  project_storage_type: "local"
  project_file_origin_name: ""
  project_file_hash: ""
  group_name: "seecode-audit"
  group_key: "seecode-audit"
  evidence_start_line_offset: -1
  evidence_count: 5
  force_sync_code: True
  sync_vuln_to_server: False
  result_format: "json"
  result_file: "9527.json"
```

5.9 Changelog

- #1: test
- #2: test