

# Домашняя работа № 5

## Выполнила Вишняк Евгения

1. По приведенным на скриншоте результатам сканирования Metasploit составить отчет по шаблону, выбрав CVE-уязвимости. Подробности о CVE можно найти на <https://cve.mitre.org/>.

Описание методики можно оставить из шаблона.

Описания уязвимостей можно оставить на английском языке.

Формат сдачи: документ на google drive.

Документ в формате pdf прилагаю к отчету.

Ссылка на документ google drive:

<https://docs.google.com/document/d/1EZdthodobpJD3mCdSuir9tymr4ld-Fqx9HVF9gKy60g/edit?usp=sharing>

2. Распаковать архив DVWA-master в подкаталог bin папки сканера. Запустить сканирование, дождаться окончания. По полученным результатам сканирования Sonarqube составить отчет по шаблону, выбрав CWE-уязвимости. Подробности о CWE можно найти на <https://cwe.mitre.org/>.

Описание уязвимостей можно оставить на английском языке.

Если вероятность эксплойта не указана, поле оставить пустым.

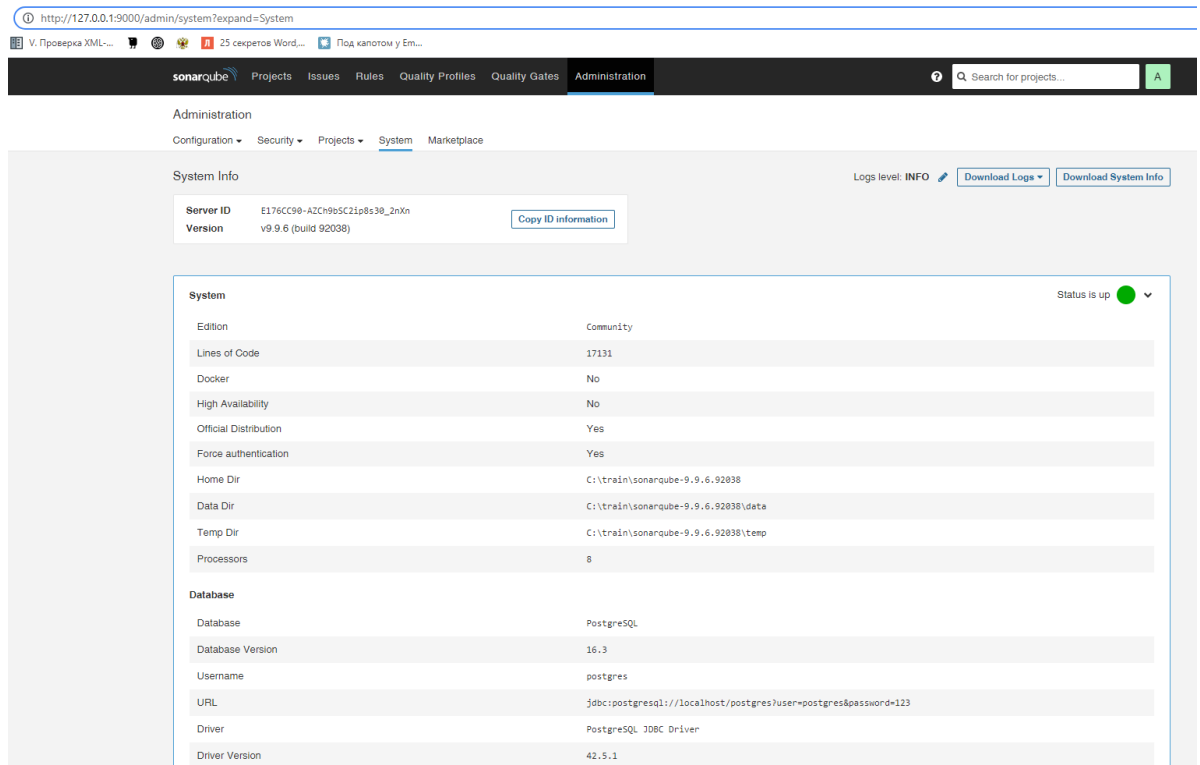
В качестве решения прикрепить документ с отчетом.

Перед выполнением задания убеждаюсь в том, что в системе установлена jdk 17, а также postgresql и pgadmin4. В pgadmin4 запущен сервер localhost. Скачиваю и распаковываю архив DVWA-master в подкаталог bin папки сканера. Запускаю SonarQube в командной строке Git:

```
Git CMD - StartSonar.bat
C:\Users\User>C:\train\sonarqube-9.9.6.92038\bin\windows-x86-64\StartSonar.bat
Синтаксическая ошибка в имени файла, имени папки или метке тома.

C:\Users\User>cd C:\train\sonarqube-9.9.6.92038\bin\windows-x86-64
C:\train\sonarqube-9.9.6.92038\bin\windows-x86-64>StartSonar.bat
Starting SonarQube...
2024.07.12 10:38:11 INFO app[o.s.a.AppFileSystem] Cleaning or creating temp directory C:\train\sonarqube-9.9.6.92038\temp
2024.07.12 10:38:11 INFO app[o.s.a.es.Elasticsearch] Elasticsearch listening on [HTTP: 127.0.0.1:9001, TCP: 127.0.0.1:51258]
2024.07.12 10:38:12 INFO app[o.s.a.ProcessLauncherImpl] Launch process[ELASTICSEARCH] from [C:\train\sonarqube-9.9.6.92038\bin\windows-x86-64\bin\java -XX:+UseG1GC -Djava.io.tmpdir=C:\train\sonarqube-9.9.6.92038\temp -XX:ErrorFile=C:\train\sonarqube-9.9.6.92038\logs\es_hs_err_pid%p.log -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:AlwaysPreTouch -Xss1m -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djna.nosys=true -Djna.tmpdir=C:\train\sonarqube-9.9.6.92038\temp -XX:-OmitStackTraceInFastThrow -Dio.netty.noUnsafe=true -Dio.netty.noKeySetOptimization=true -Dio.netty.recycler.maxCapacityPerThread=0 -Dio.netty.allocator.numDirectArenas=0 -Dlog4j.shutdownHookEnabled=false -Dlog4j2.disable.jmx=true -Dlog4j2.formatMsgNoLookups=true -Djava.locale.providers=COMPAT -Dcom.redhat.fips=false -Des.enforce.bootstrap.checks=true -Xmx512m -Xms512m -XX:MaxDirectMemorySize=256m -XX:HeapDumpOnOutOfMemoryError -Des.path.home=C:\train\sonarqube-9.9.6.92038\bin\windows-x86-64\bin -Des.path.conf=C:\train\sonarqube-9.9.6.92038\temp\conf\es -cp lib\ org.elasticsearch.bootstrap.Elasticsearch]
2024.07.12 10:38:12 INFO app[o.s.a.SchedulerImpl] Waiting for Elasticsearch to be up and running
2024.07.12 10:38:28 INFO app[o.s.a.SchedulerImpl] Process[es] is up
2024.07.12 10:38:28 INFO app[o.s.a.ProcessLauncherImpl] Launch process[WEB_SERVER] from [C:\train\sonarqube-9.9.6.92038\bin\windows-x86-64\bin\java -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djava.io.tmpdir=C:\train\sonarqube-9.9.6.92038\temp -XX:-OmitStackTraceInFastThrow --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED --add-exports=java.base/jdk.internal.ref=ALL-UNNAMED --add-opens=java.management/sun.management=ALL-UNNAMED --add-opens=jdk.management/com.sun.management=ALL-UNNAMED -Dcom.redhat.fips=false -Xmx512m -Xms128m -XX:HeapDumpOnOutOfMemoryError -Dhttp.nonProxyHosts=localhost*[:1] -cp ./lib/sonar-application-9.9.6.92038.jar;C:\train\sonarqube-9.9.6.92038\temp\sq-process10548373734361040598\properties -Dhttp.nonProxyHosts=localhost*[:1] -cp ./lib/sonar-application-9.9.6.92038.jar;C:\train\sonarqube-9.9.6.92038\temp\sq-process9338384454101502540\properties]
WARNING: A terminally deprecated method in java.lang.System has been called
WARNING: System::setSecurityManager has been called by org.sonar.process.PluginSecurityManager (file:C:\train\sonarqube-9.9.6.92038\lib\sonar-application-9.9.6.92038.jar)
WARNING: Please consider reporting this to the maintainers of org.sonar.process.PluginSecurityManager
WARNING: System::setSecurityManager will be removed in a future release
2024.07.12 10:38:59 INFO app[o.s.a.SchedulerImpl] Process[web] is up
2024.07.12 10:38:59 INFO app[o.s.a.ProcessLauncherImpl] Launch process[COMPUTE_ENGINE] from [C:\train\sonarqube-9.9.6.92038\bin\windows-x86-64\bin\java -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djava.io.tmpdir=C:\train\sonarqube-9.9.6.92038\temp -XX:-OmitStackTraceInFastThrow --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED --add-exports=java.base/jdk.internal.ref=ALL-UNNAMED --add-opens=java.management/sun.management=ALL-UNNAMED --add-opens=jdk.management/com.sun.management=ALL-UNNAMED -Dcom.redhat.fips=false -Xmx512m -Xms128m -XX:HeapDumpOnOutOfMemoryError -Dhttp.nonProxyHosts=localhost*[:1] -cp ./lib/sonar-application-9.9.6.92038.jar;C:\train\sonarqube-9.9.6.92038\temp\sq-process10548373734361040598\properties -Dhttp.nonProxyHosts=localhost*[:1] -cp ./lib/sonar-application-9.9.6.92038.jar;C:\train\sonarqube-9.9.6.92038\temp\sq-process9338384454101502540\properties]
WARNING: A terminally deprecated method in java.lang.System has been called
WARNING: System::setSecurityManager has been called by org.sonar.process.PluginSecurityManager (file:C:\train\sonarqube-9.9.6.92038\lib\sonar-application-9.9.6.92038.jar)
WARNING: Please consider reporting this to the maintainers of org.sonar.process.PluginSecurityManager
WARNING: System::setSecurityManager will be removed in a future release
2024.07.12 10:39:13 INFO app[o.s.a.SchedulerImpl] Process[ce] is up
2024.07.12 10:39:13 INFO app[o.s.a.SchedulerImpl] SonarQube is operational
```

В браузере по ссылке <http://127.0.0.1:9000/> открывается графический интерфейс SonarQube, база данных успешно подключилась:



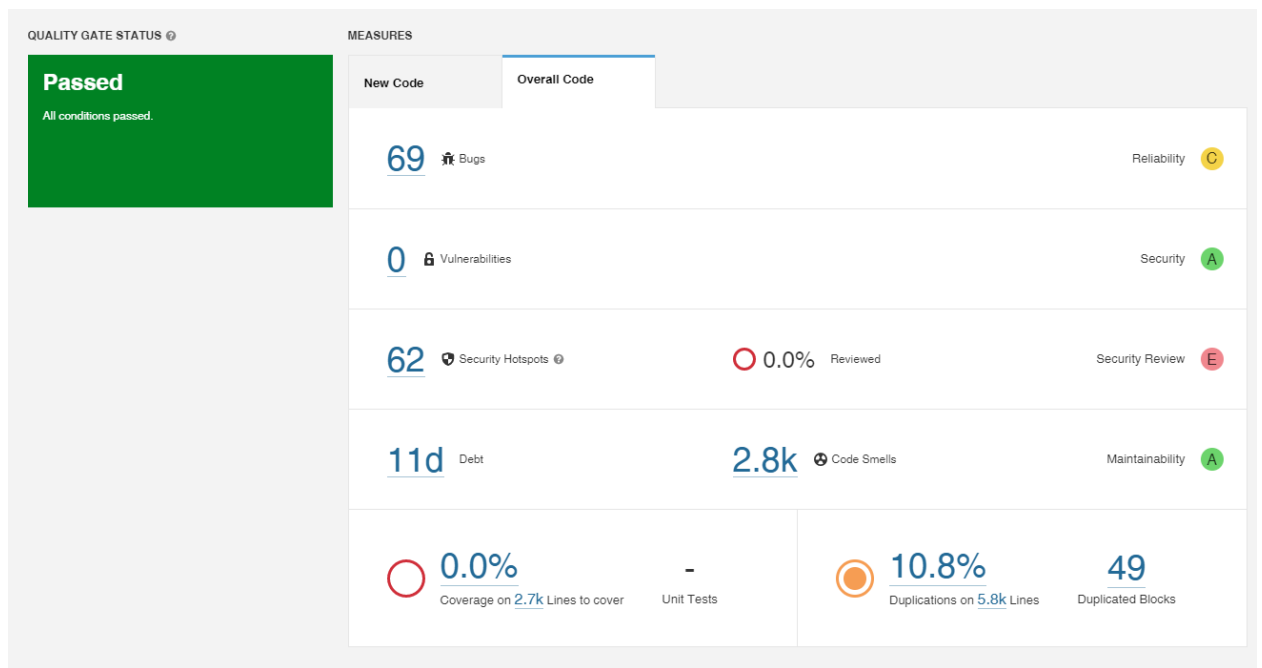
Создаю новый проект. Копирую команду и запускаю ее в командной строке внутри папки, где расположен сканер:

```
cmd Обработчик команд Windows
командой, исполняемой программой или пакетным файлом.

C:\Windows\System32>cd C:\train\sonar-scanner-6.1.0.4477-windows-x64\bin

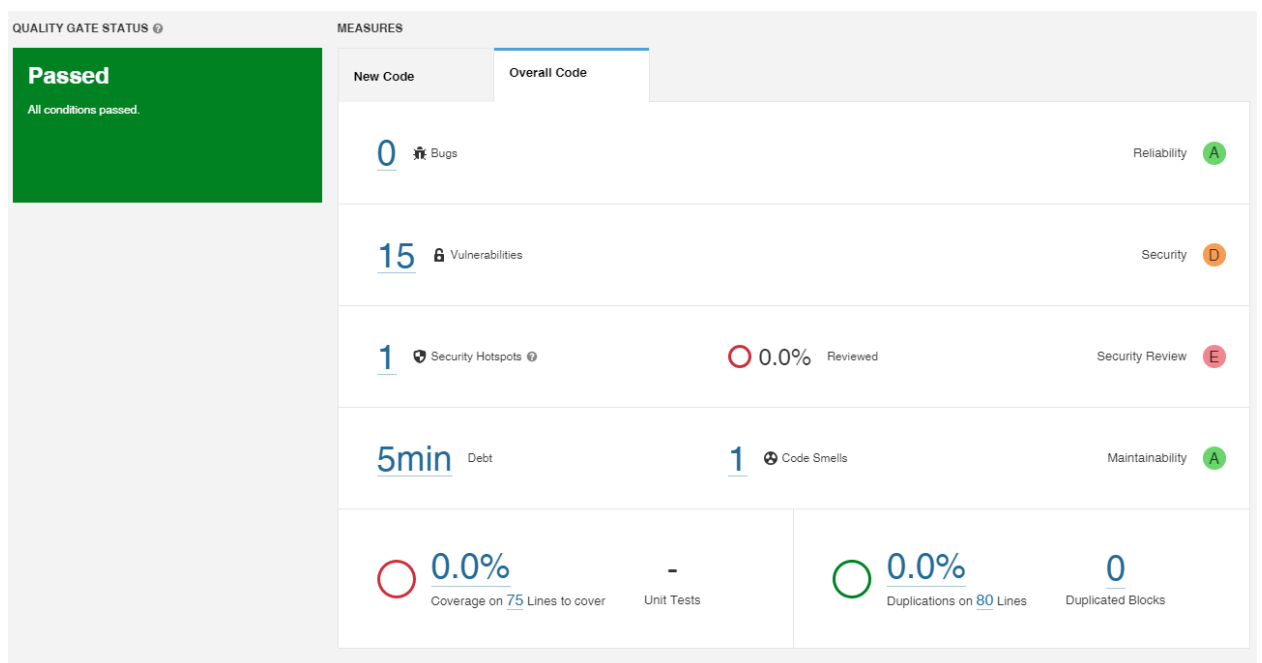
C:\train\sonar-scanner-6.1.0.4477-windows-x64\bin>sonar-scanner.bat -D"sonar.projectKey=new" -D"sonar.sources=." -D"sonar.host.url=http://127.0.0.1:9000" -D"sonar.login=sqp_c2d1d3d8cd650ea56cbf5e0319ae109dbefc8238"
10:48:42.877 INFO Scanner configuration file: C:\train\sonar-scanner-6.1.0.4477-windows-x64\bin\..conf\sonar-scanner.properties
10:48:42.884 INFO Project root configuration file: NONE
10:48:42.907 INFO SonarScanner CLI 6.1.0.4477
10:48:42.909 INFO Java 17.0.11 Eclipse Adoptium (64-bit)
10:48:42.910 INFO Windows 10 10.0 amd64
10:48:42.939 INFO User cache: C:\Users\User\.sonar\cache
10:48:56.244 INFO Communicating with SonarQube Server 9.9.6.92038
10:48:57.167 INFO Load global settings
10:48:57.309 INFO Load global settings (done) | time=144ms
10:48:57.313 INFO Server id: E176CC90-AZCh9bSC2ip8s30_2nXn
10:48:57.317 INFO User cache: C:\Users\User\.sonar\cache
10:48:57.321 INFO Load/download plugins
10:48:57.322 INFO Load plugins index
10:48:57.427 INFO Load plugins index (done) | time=105ms
10:48:57.615 INFO Load/download plugins (done) | time=293ms
10:48:58.342 INFO Process project properties
10:48:58.357 INFO Process project properties (done) | time=14ms
10:48:58.359 INFO Execute project builders
10:48:58.361 INFO Execute project builders (done) | time=2ms
10:48:58.370 INFO Project key: new
10:48:58.371 INFO Base dir: C:\train\sonar-scanner-6.1.0.4477-windows-x64\bin
10:48:58.371 INFO Working dir: C:\train\sonar-scanner-6.1.0.4477-windows-x64\bin\scannerwork
10:48:58.382 INFO Load project settings for component key: 'new'
```

Жду, пока завершится сканирование, и возвращаюсь в веб-интерфейс:



В результате сканирование прошло успешно, но уязвимостей не обнаружено. Сканирование данного архива было произведено на другой машине, с полной настройкой параметров и установкой необходимого программного обеспечения, но результат не изменился. Это подтверждает отсутствие в данном архиве уязвимостей.

Беру другой архив, `python_vuln`, и проделываю те же действия. Результат:



В разделе Issues можно найти подробную информацию о найденных CWE, а также их количестве:

vuln main

Last analysis of this Branch had 2 warnings July 12, 2024, 11:22 AM Version not provided

Overview Issues Security Hotspots Measures Code Activity

Project Settings Project Information

Resolution

Status

Security Category CWE-32... Clear

SonarSource

Weak Cryptography 9

OWASP Top 10 2021

OWASP Top 10 2017

SANS Top 25

CWE CWE-327 - USE OF... Clear

Search for CWES...

CWE-327 - Use of a Broken or Risky... 9

CWE-326 - Inadequate Encryption St... 8

CWE-297 - Improper Validation of C... 4

CWE-295 - Improper Certificate Valid... 2

CWE-780 - Use of RSA Algorithm wit... 1

5 shown

Press Ctrl to add to selection

Bulk Change

1 / 9 issues 2h 20min effort

python\_vuln/ciphers/pyca.py

Use a strong cipher algorithm. 2 hours ago L15

Vulnerability Critical Open Not assigned 15min effort Comment

python\_vuln/ciphers/pycryptodomex.py

Use a strong cipher algorithm. 2 hours ago L12

Vulnerability Critical Open Not assigned 15min effort Comment

Use a strong cipher algorithm. 2 hours ago L15

Vulnerability Critical Open Not assigned 15min effort Comment

Use a strong cipher algorithm. 2 hours ago L18

Vulnerability Critical Open Not assigned 15min effort Comment

Все найденные уязвимости описаны в отчете, документ в формате pdf прилагаю.

Ссылка на документ google drive:

[https://docs.google.com/document/d/1v9UerqhvFkH1WeNyW1oKBuqX\\_vY82cecDZjRTefgUSw/edit?usp=sharing](https://docs.google.com/document/d/1v9UerqhvFkH1WeNyW1oKBuqX_vY82cecDZjRTefgUSw/edit?usp=sharing)