Федеральное государственное автономное
образовательное учреждение высшего образования «Национальный
исследовательский университет ИТМО»

Дисциплина «Информационная безопасность»

Работа №1: Разработка защищенного REST API с интеграцией в CI/CD

Выполнил:
Султанов Артур Радикович
Студент группы P3413

2025г.

Ссылка на публичный git-репозиторий (GitLab) с кодом проекта

https://gitlab.com/sultanowskii/infosec-lab1

Описание

Описание проекта и API

Сервис, позволяет создавать/входить в аккаунт и создавать/просматривать комментарии.

Установка и запуск:

```
python -m venv .venv
source .venv/bin/activate
python -m pip install .
make run
```

Эндпоинты

Регистрация пользователя

Эндпоинт: /auth/signup

Метод: POST

Описание: Регистрирует нового пользователя

Тело запроса:

```
{
    "username": "user",
    "password": "pass"
}
```

curl:

```
curl -X POST http://localhost:5000/auth/signup \
    -H "Content-Type: application/json" \
    -d '{"username": "user", "password": "pass"}'
```

Аутентификация пользователя

Эндпоинт: /auth/login

Метод: POST

Описание: Аутентифицирует пользователя и возвращает JWT-токен

Тело запроса:

```
{
    "username": "user",
    "password": "pass"
}
```

curl:

```
curl -X POST http://localhost:5000/auth/login \
    -H "Content-Type: application/json" \
    -d '{"username": "user", "password": "pass"}'
```

Получение всех комментариев

Эндпоинт: /api/data

Метод: GET

Описание: Возвращает список всех комментариев. Доступ только для аутентифицированных пользователей.

Заголовки:

```
Authorization: Bearer ${YOUR_JWT_TOKEN}
```

curl:

```
curl -X GET http://localhost:5000/api/data \
    -H "Content-Type: application/json" \
    -H "Authorization: Bearer ${YOUR_JWT_TOKEN}"
```

Создание комментария

Эндпоинт: /api/comments

Метод: POST

Описание: Создает новый комментарий. Доступ только для аутентифицированных пользователей.

Заголовки:

```
Authorization: Bearer ${YOUR_JWT_TOKEN}
```

Тело запроса:

```
{
    "content": "hello!"
}
```

curl:

```
curl -X POST http://localhost:5000/api/comments \
    -H "Content-Type: application/json" \
    -H "Authorization: Bearer ${YOUR_JWT_TOKEN}" \
    -d '{"content": "hello!"}'
```

Просмотр комментариев в виде HTML

Эндпоинт: /comments

Метод: GET

Описание: Возвращает список всех комментариев в виде HTML-страницы. Доступ только для аутентифицированных пользователей.

Заголовки:

```
Authorization: Bearer ${YOUR_JWT_TOKEN}
```

curl:

```
curl -v -X GET http://localhost:5000/comments \
    -H "Authorization: Bearer ${YOUR_JWT_TOKEN}"
```

Описание мер защиты

Защита от SQL-инъекции

Для этого используется ORM - SQLAlchemy.

Вообще, SQL-инъекции возможны, если часть query строится посредством конкатенации с пользовательским вводом - тогда он может "сбежать" из запроса, например:

- обойти какую-нибудь проверку (' OR 1=1)
- изменить структуру запроса, получив лишние данные (' UNION ...)

Предотвращается с помощью параметризованных запросов или ORM (которые сами под капотом строят параметризованные запросы). Собственно, SQLAlchemy является одним из наиболее популярных ORM для python.

Защита от XSS

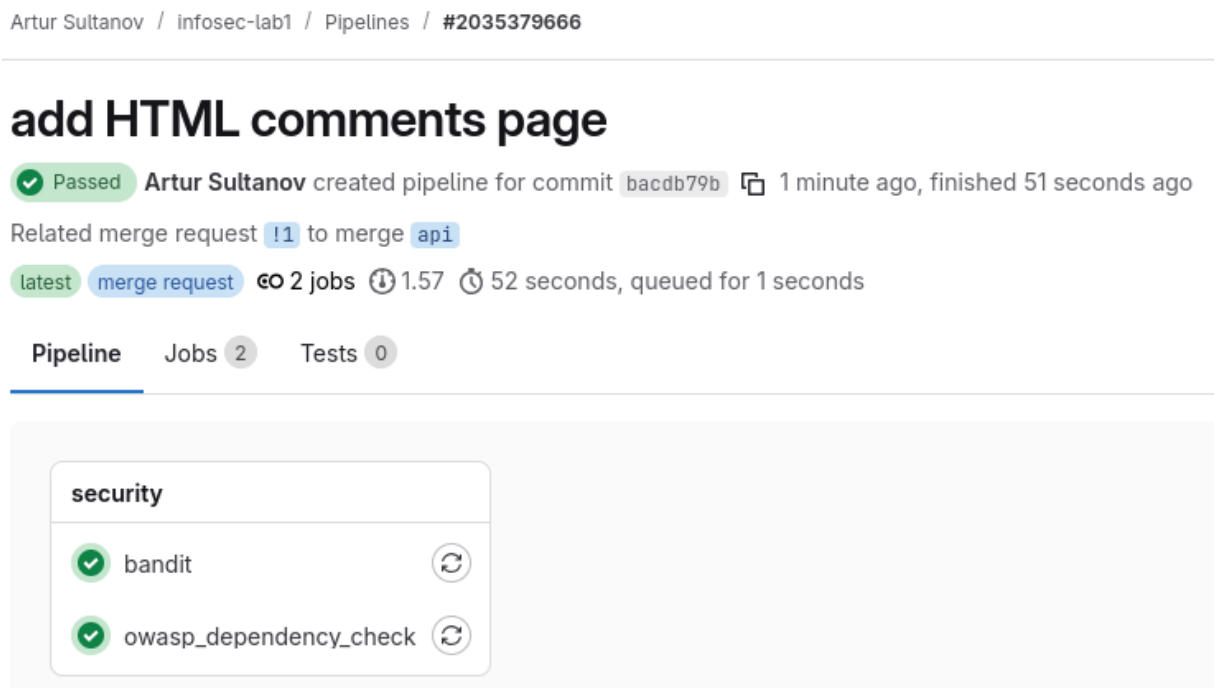
Здесь основной вектор защиты - при рендере HTML-ки просанитайзить пользовательский ввод. Для этого во всех популярных ЯПах есть специальные функции, которые эскейпят <, > и прочее для предотвращения возможности XSS. Здесь я использовал markupsafe.escape

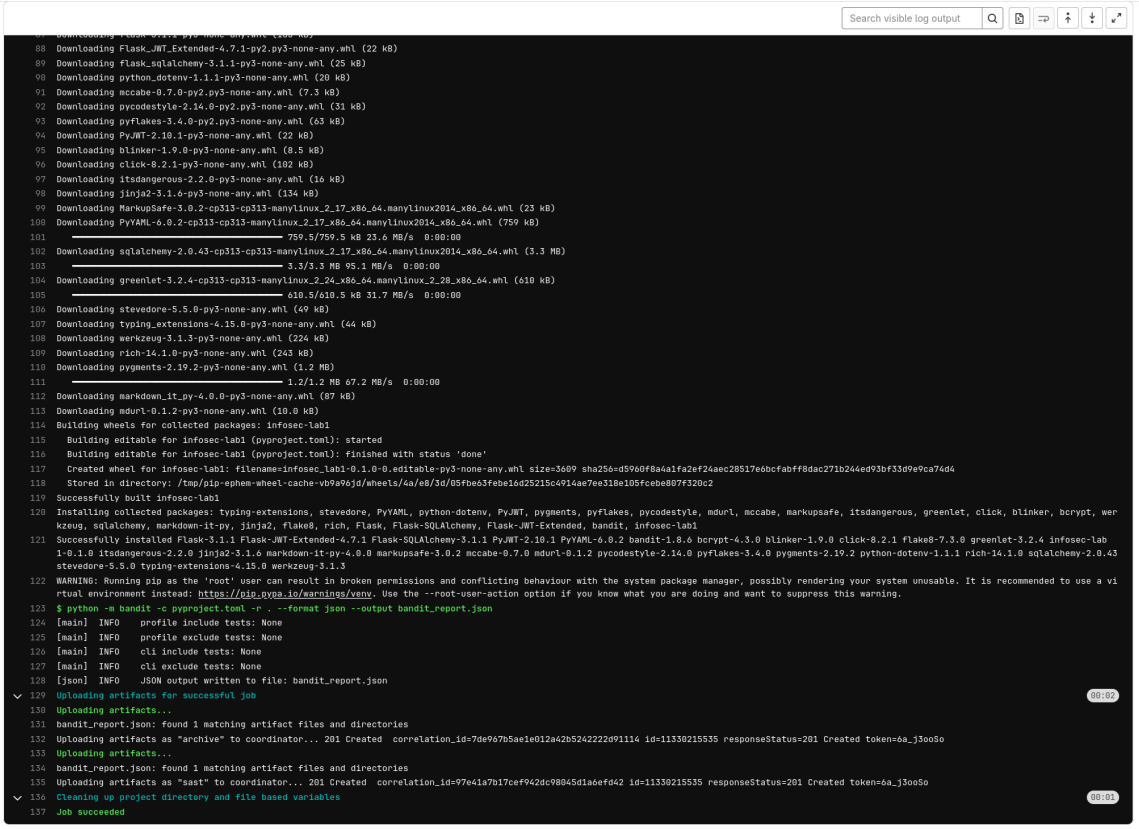
Аутентификация

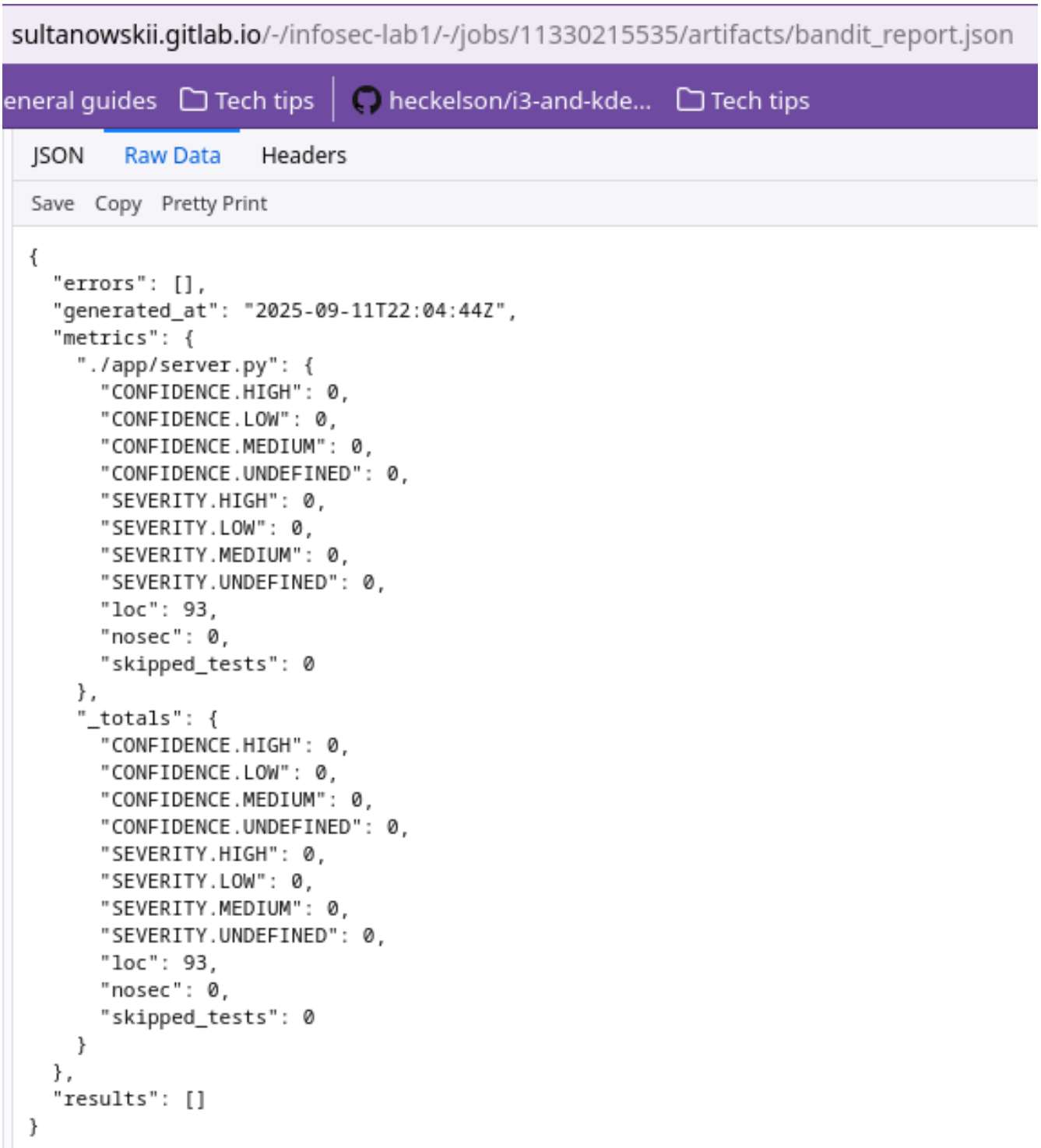
Реализована с помощью JWT-токенов. Токен выпускается и отдается пользователю при логине. Токен состоит из трех base64-encoded частей: заголовок (задает алгоритм шифрования и прочие данные), payload (смысловое наполнение, нередко там указывается юзернейм) и подпись. Основная идея в том, что подпись формируется на основе данных и секретного ключа на стороне сервера - без него невозможно сформировать валидную подпись, а значит и подделать JWT-токен.

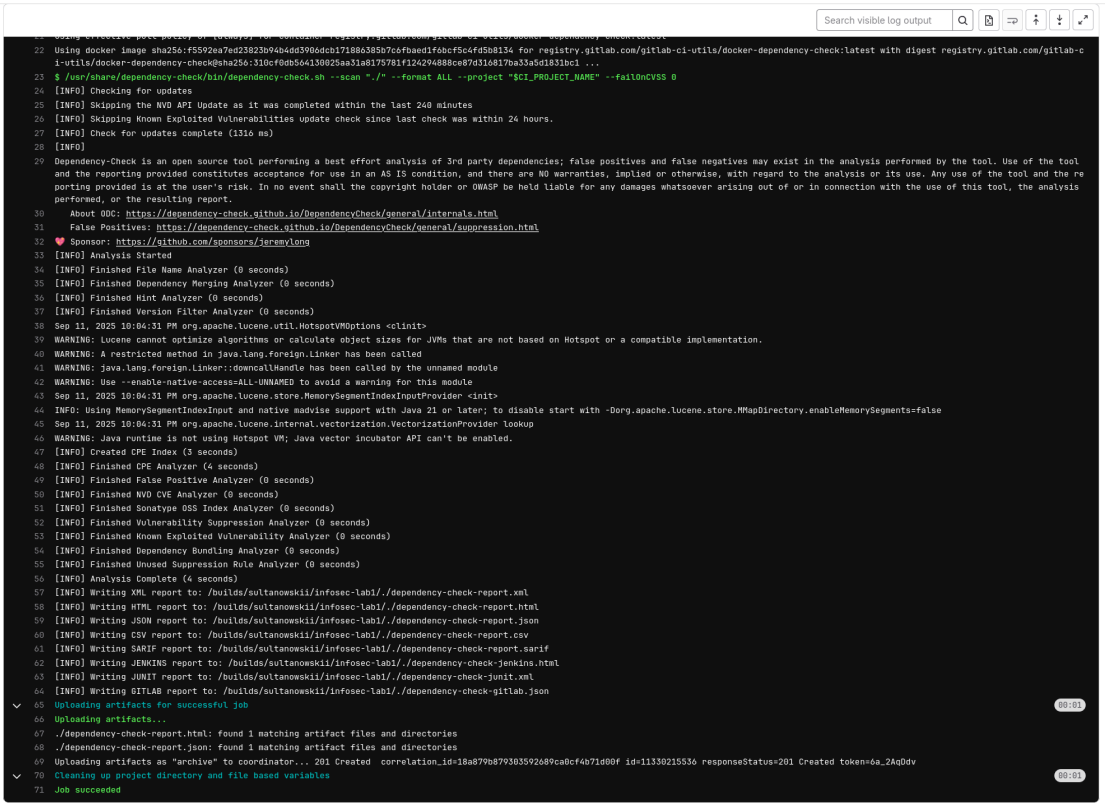
Для удобства использовал библиотеку FLask-JWT-Extended: функцию для выпуска токена create_access_token, а также декоратор @jwt_required() для оборачивания эндпоинтов, которые нужно защитить от доступа без токена.

Скриншоты отчетов




Search visible log output
Downloading Flask_JWT_Extended-4.7.1-py2.py3-none-any.whl (22 kB)
Downloading flask_sqlalchemy-3.1.1-py3-none-any.whl (25 kB)
Downloading python_dotenv-1.1.1-py3-none-any.whl (20 kB)
Downloading mccabe-0.7.0-py2.py3-none-any.whl (7.3 kB)
Downloading pycodestyle-2.14.0-py2.py3-none-any.whl (31 kB)
Downloading pyflakes-3.4.0-py2.py3-none-any.whl (63 kB)
Downloading PyJWT-2.10.1-py3-none-any.whl (22 kB)
Downloading blinker-1.9.0-py3-none-any.whl (8.5 kB)
Downloading click-8.2.1-py3-none-any.whl (102 kB)
Downloading itsdangerous-2.2.0-py3-none-any.whl (16 kB)
Downloading jinja2-3.1.6-py3-none-any.whl (134 kB)
Downloading MarkupSafe-3.0.2-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (23 kB)
Downloading PyYAML-6.0.2-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (759 kB)
759.5/759.5 kB 23.6 MB/s 0:00:00
Downloading sqlalchemy-2.0.43-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (3.3 MB)
3.3/3.3 MB 95.1 MB/s 0:00:00
Downloading greenlet-3.2.4-cp313-cp313-manylinux_2_24_x86_64.manylinux_2_28_x86_64.whl (610 kB)
610.5/610.5 kB 31.7 MB/s 0:00:00
Downloading stevedore-5.5.0-py3-none-any.whl (49 kB)
Downloading typing_extensions-4.15.0-py3-none-any.whl (44 kB)
Downloading werkzeug-3.1.3-py3-none-any.whl (224 kB)
Downloading rich-14.1.0-py3-none-any.whl (243 kB)
Downloading pygments-2.19.2-py3-none-any.whl (1.2 MB)
1.2/1.2 MB 67.2 MB/s 0:00:00
Downloading markdown_it_py-4.0.0-py3-none-any.whl (87 kB)
Downloading mdurl-0.1.2-py3-none-any.whl (10.0 kB)
Building wheels for collected packages: infosec-lab1
Building editable for infosec-lab1 (pyproject.toml): started
Building editable for infosec-lab1 (pyproject.toml): finished with status 'done'
Created wheel for infosec-lab1: filename=infosec_lab1-0.1.0-0.editable-py3-none-any.whl size=3609 sha256=d5960f8a4a1fa2ef24aec28517e6bcfabff8dac271b244ed93bf33d9e9ca74d4
Stored in directory: /tmp/pip-ephem-wheel-cache-vb9a96jd/wheels/4a/e8/3d/05fbe63febe16d25215c4914ae7ee318e105fcebe807f320c2
Successfully built infosec-lab1
Installing collected packages: typing-extensions, stevedore, PyYAML, python-dotenv, PyJWT, pygments, pyflakes, pycodestyle, mdurl, mccabe, markupsafe, itsdangerous, greenlet, click, blinker, bcrypt, werkzeug, sqlalchemy, markdown-it-py, jinja2, flake8, rich, Flask, Flask-SQLAlchemy, Flask-JWT-Extended, bandit, infosec-lab1
Successfully installed Flask-3.1.1 Flask-JWT-Extended-4.7.1 Flask-SQLAlchemy-3.1.1 PyJWT-2.10.1 PyYAML-6.0.2 bandit-1.8.6 bcrypt-4.3.0 blinker-1.9.0 click-8.2.1 flake8-7.3.0 greenlet-3.2.4 infosec-lab1-0.1.0 itsdangerous-2.2.0 jinja2-3.1.6 markdown-it-py-4.0.0 markupsafe-3.0.2 mccabe-0.7.0 mdurl-0.1.2 pycodestyle-2.14.0 pyflakes-3.4.0 pygments-2.19.2 python-dotenv-1.1.1 rich-14.1.0 sqlalchemy-2.0.43 stevedore-5.5.0 typing-extensions-4.15.0 werkzeug-3.1.3
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager, possibly rendering your system unusable. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv. Use the --root-user-action option if you know what you are doing and want to suppress this warning.
$ python -m bandit -c pyproject.toml -r . --format json --output bandit_report.json
[main] INFO profile include tests: None
[main] INFO profile exclude tests: None
[main] INFO cli include tests: None
[main] INFO cli exclude tests: None
[json] INFO JSON output written to file: bandit_report.json
Uploading artifacts for successful job
00:02
Uploading artifacts...
bandit_report.json: found 1 matching artifact files and directories
Uploading artifacts as "archive" to coordinator... 201 Created correlation_id=7de967b5ae1e012a42b5242222d91114 id=11330215535 responseStatus=201 Created token=6a_j3ooSo
Uploading artifacts...
bandit_report.json: found 1 matching artifact files and directories
Uploading artifacts as "sast" to coordinator... 201 Created correlation_id=97e41a7b17cef942dc98045d1a6efd42 id=11330215535 responseStatus=201 Created token=6a_j3ooSo
Cleaning up project directory and file based variables
00:01
Job succeeded
Duration: 52 seconds
Finished: 1 minute ago
Queued: 0 seconds
Timeout: 1h (from project)
Runner: #12270859 (xS6Vzpvo) 5-green.saas-linux-small-amd64.runners-manager.gitlab.com/default
Source: Merge Request
Job artifacts
sast
These artifacts are the latest. They will not be deleted (even if expired) until newer artifacts are available.
Keep
Download
Browse
Download SAST report
Commit bacdb79b in !1
add HTML comments page
Pipeline #2035379666 Passed for !1 with api
security
Related jobs
bandit
owasp_dependency_check


sultanowskii.gitlab.io/-/infosec-lab1/-/jobs/11330215535/artifacts/bandit_report.json
eneral guides
Tech tips
heckelson/i3-and-kde...
Tech tips
JSON
Raw Data
Headers
Save
Copy
Pretty Print
{
"errors": [],
"generated_at": "2025-09-11T22:04:44Z",
"metrics": {
"./app/server.py": {
"CONFIDENCE.HIGH": 0,
"CONFIDENCE.LOW": 0,
"CONFIDENCE.MEDIUM": 0,
"CONFIDENCE.UNDEFINED": 0,
"SEVERITY.HIGH": 0,
"SEVERITY.LOW": 0,
"SEVERITY.MEDIUM": 0,
"SEVERITY.UNDEFINED": 0,
"loc": 93,
"nosec": 0,
"skipped_tests": 0
},
"_totals": {
"CONFIDENCE.HIGH": 0,
"CONFIDENCE.LOW": 0,
"CONFIDENCE.MEDIUM": 0,
"CONFIDENCE.UNDEFINED": 0,
"SEVERITY.HIGH": 0,
"SEVERITY.LOW": 0,
"SEVERITY.MEDIUM": 0,
"SEVERITY.UNDEFINED": 0,
"loc": 93,
"nosec": 0,
"skipped_tests": 0
}
},
"results": []
}


Search visible log output
Using docker image sha256:f5592ea7ed23823b94b4dd3906dcb17188635b5b7c6fbaed1f6bcf5c4fd5b8134 for registry.gitlab.com/gitlab-ci-utils/docker-dependency-check:latest with digest registry.gitlab.com/gitlab-ci-utils/docker-dependency-check@sha256:310cf0db564130025aa31a8175781f124294888ce87d316817ba33a5d1831bc1 ...
$ /usr/share/dependency-check/bin/dependency-check.sh --scan "./" --format ALL --project "$CI_PROJECT_NAME" --failOnCVSS 0
[INFO] Checking for updates
[INFO] Skipping the NVD API Update as it was completed within the last 240 minutes
[INFO] Skipping Known Exploited Vulnerabilities update check since last check was within 24 hours.
[INFO] Check for updates complete (1316 ms)
[INFO]
Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.
About ODC: https://dependency-check.github.io/DependencyCheck/general/internals.html
False Positives: https://dependency-check.github.io/DependencyCheck/general/suppression.html
Sponsor: https://github.com/sponsors/jeremylong
[INFO] Analysis Started
[INFO] Finished File Name Analyzer (0 seconds)
[INFO] Finished Dependency Merging Analyzer (0 seconds)
[INFO] Finished Hint Analyzer (0 seconds)
[INFO] Finished Version Filter Analyzer (0 seconds)
Sep 11, 2025 10:04:31 PM org.apache.lucene.util.HotspotVMOptions <clinit>
WARNING: Lucene cannot optimize algorithms or calculate object sizes for JVMs that are not based on Hotspot or a compatible implementation.
WARNING: A restricted method in java.lang.foreign.Linker has been called
WARNING: java.lang.foreign.Linker::downcallHandle has been called by the unnamed module
WARNING: Use --enable-native-access=ALL-UNNAMED to avoid a warning for this module
Sep 11, 2025 10:04:31 PM org.apache.lucene.store.MemorySegmentIndexInputProvider <init>
INFO: Using MemorySegmentIndexInput and native madvise support with Java 21 or later; to disable start with -Dorg.apache.lucene.store.MMapDirectory.enableMemorySegments=false
Sep 11, 2025 10:04:31 PM org.apache.lucene.internal.vectorization.VectorizationProvider lookup
WARNING: Java runtime is not using Hotspot VM; Java vector incubator API can't be enabled.
[INFO] Created CPE Index (3 seconds)
[INFO] Finished CPE Analyzer (4 seconds)
[INFO] Finished False Positive Analyzer (0 seconds)
[INFO] Finished NVD CVE Analyzer (0 seconds)
[INFO] Finished Sonatype OSS Index Analyzer (0 seconds)
[INFO] Finished Vulnerability Suppression Analyzer (0 seconds)
[INFO] Finished Known Exploited Vulnerability Analyzer (0 seconds)
[INFO] Finished Dependency Bundling Analyzer (0 seconds)
[INFO] Finished Unused Suppression Rule Analyzer (0 seconds)
[INFO] Analysis Complete (4 seconds)
[INFO] Writing XML report to: /builds/sultanowskii/infosec-lab1/./dependency-check-report.xml
[INFO] Writing HTML report to: /builds/sultanowskii/infosec-lab1/./dependency-check-report.html
[INFO] Writing JSON report to: /builds/sultanowskii/infosec-lab1/./dependency-check-report.json
[INFO] Writing CSV report to: /builds/sultanowskii/infosec-lab1/./dependency-check-report.csv
[INFO] Writing SARIF report to: /builds/sultanowskii/infosec-lab1/./dependency-check-report.sarif
[INFO] Writing JENKINS report to: /builds/sultanowskii/infosec-lab1/./dependency-check-jenkins.html
[INFO] Writing JUNIT report to: /builds/sultanowskii/infosec-lab1/./dependency-check-junit.xml
[INFO] Writing GITLAB report to: /builds/sultanowskii/infosec-lab1/./dependency-check-gitlab.json
Uploading artifacts for successful job
00:01
Uploading artifacts...
./dependency-check-report.html: found 1 matching artifact files and directories
./dependency-check-report.json: found 1 matching artifact files and directories
Uploading artifacts as "archive" to coordinator... 201 Created correlation_id=18a879b879303592689ca0cf4b71d00f id=11330215536 responseStatus=201 Created token=6a_2AqOdv
Cleaning up project directory and file based variables
00:01
Job succeeded
Duration: 42 seconds
Finished: 3 minutes ago
Queued: 0 seconds
Timeout: 1h (from project)
Runner: #12270848 (ns46NMmJ) 2-green.saas-linux-small-amd64.runners-manager.gitlab.com/default
Source: Merge Request
Job artifacts
These artifacts are the latest. They will not be deleted (even if expired) until newer artifacts are available.
Keep
Download
Browse
Commit bacdb79b in !1
add HTML comments page
Pipeline #2035379666 Passed for !1 with api
security
Related jobs
bandit
owasp_dependency_check

sultanowskii.gitlab.io/-/infosec-lab1/-/jobs/11330215536/artifacts/dependency-check-report.html

eneral guides | Tech tips | heckelson/i3-and-kde... | Tech tips

DEPENDENCY-CHECK

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the connection with the use of this tool, the analysis performed, or the resulting report.

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

Sponsor

Project: infosec-lab1

Scan Information (show less):

- *dependency-check version*: 12.1.3
- *Report Generated On*: Thu, 11 Sep 2025 22:04:34 GMT
- *Dependencies Scanned*: 0 (0 unique)
- *Vulnerable Dependencies*: 0
- *Vulnerabilities Found*: 0
- *Vulnerabilities Suppressed*: 0
- *NVD API Last Checked*: 2025-09-11T20:01:54Z
- *NVD API Last Modified*: 2025-09-11T19:55:59Z

Summary

Summary of Vulnerable Dependencies(click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count

Dependencies (vulnerable)

This report contains data retrieved from the National Vulnerability Database.
This report may contain data retrieved from the CISA Known Exploited Vulnerability Catalog.
This report may contain data retrieved from the Github Advisory Database (via NPM Audit API).
This report may contain data retrieved from RetireJS.
This report may contain data retrieved from the Sonatype OSS Index.

Ссылка на последний успешный запуск pipeline в вашем репозитории

https://gitlab.com/sultanowskii/infosec-lab1/-/pipelines/2035426685