



ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

Кафедра

«Криптология и кибербезопасность»

ОТЧЕТ о лабораторной работе №2

Проведения ручного поиска уязвимостей пакетов приложения
«Remediation-Demo»

Исполнитель: студент гр. Б21-515

Тимин А. С.

подпись, дата

Преподаватель:

Карапетьянц М.

подпись, дата

Москва — 2025

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ.....	2
1 ПАКЕТЫ ПРИЛОЖЕНИЯ	3
1.1 BLINKER 1.9.0.....	4
1.2 CLICK 8.1.8.....	5
1.3 FLASK 3.1.0.....	5
1.4 FLASK-CORS 5.0.1.....	6
1.4.1 Improper Access Control	7
1.5 ITSDANGEROUS 2.2.0	9
1.6 JINJA2 3.1.6.....	10
1.6.1 Template Injection	11
1.7 MARKUPSAFE 3.0.2.....	12
1.8 WERKZEUG 3.1.3.....	13
1.9 WHEEL 0.45.1	14
1.10 ИТОГИ.....	15

1 Пакеты приложения

Для точного определения пакетов приложения и их версий приложение было запущено с помощью docker compose, после чего было осуществлено подключение к контейнеру и вывод всех пакетов, установленных с помощью пакетного менеджера pip (рисунок 1.1).

```
vagrant@ubuntu:~/shared$ sudo docker compose up -d
WARN[0000] /home/vagrant/shared/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid po
[+] Running 2/2
 ✓ Network shared_default Created
 ✓ Container shared-api-1 Started
vagrant@ubuntu:~/shared$ sudo docker ps
CONTAINER ID   IMAGE      COMMAND                  CREATED        STATUS        PORTS                               NAMES
33eebea2ae00   shared-api "python app.py"         7 seconds ago Up 6 seconds  0.0.0.0:5000->5000/tcp, [::]:5000->5000/tcp  shared-api-1
vagrant@ubuntu:~/shared$ sudo docker exec -it 33 sh
/app # pip list
Package        Version
-----
blinker        1.9.0
click          8.1.8
Flask          3.1.0
flask-cors     5.0.1
itsdangerous   2.2.0
Jinja2         3.1.6
MarkupSafe     3.0.2
pip            24.0
Werkzeug       3.1.3
wheel          0.45.1

[notice] A new release of pip is available: 24.0 -> 25.0.1
[notice] To update, run: pip install --upgrade pip
```

Рисунок 1 – пакеты приложения

Как видно из скриншота, в контейнере установлены следующие пакеты, представленные в таблице 1.1.

Таблица 1 – установленные пакеты

Пакет	Версия
blinker	1.9.0
click	8.1.8
Flask	3.1.0
flask-cors	5.0.1
Itsdangerous	2.2.0
Jinja2	3.1.6
MarkupSafe	3.0.2
pip	24.0
Werkzeug	3.1.3
wheel	0.45.1

Проанализируем каждый из пакетов на наличие уязвимостей с помощью сервисов: [nvd](#) и [cnyk](#). Данные актуальны 11 марта 2025 года.

1.1 blinker 1.9.0

Поиск по базе данных [NVD](#) не выявил актуальных для данной версии пакета уязвимостей (рисунок 2).

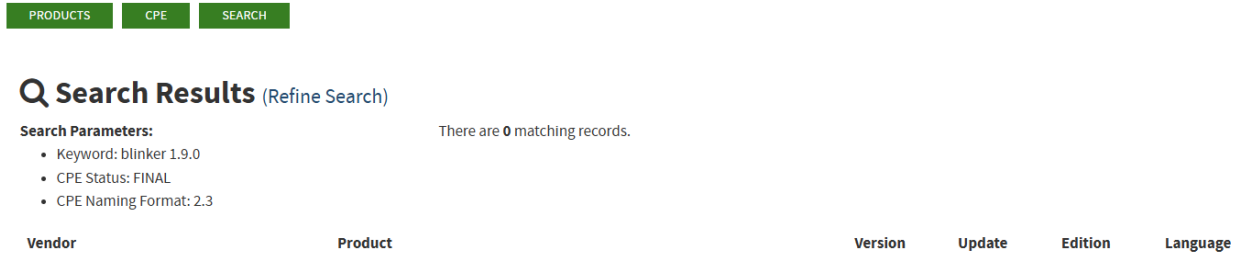


Рисунок 2 – актуальные уязвимости blinker 1.9.0 в NVD

Аналогичная ситуация и с поиском через сервис [SNYK](#) (рисунок 3).

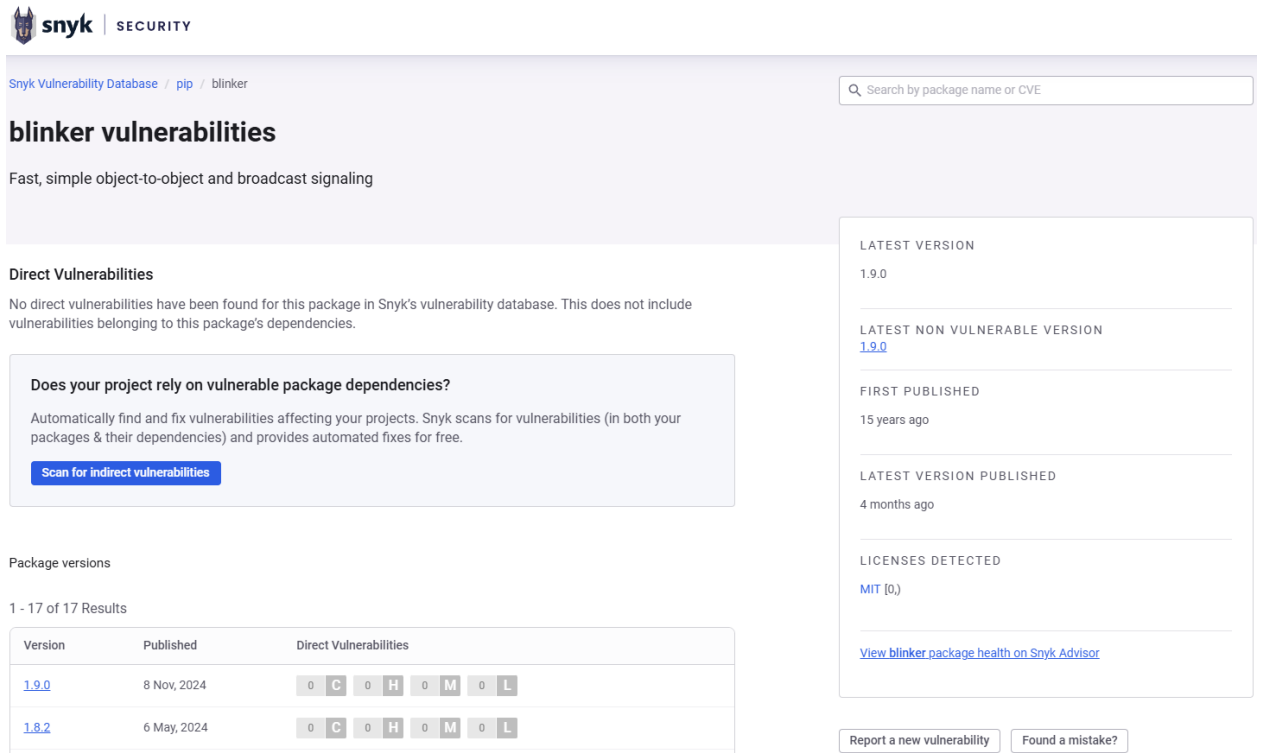


Рисунок 3 – актуальные уязвимости blinker 1.9.0 в SNYK

Выходит, что пакет blinker 1.9.0 не содержит актуальных выявленных уязвимостей.

1.2 click 8.1.8

С пакетом click 8.1.8 – аналогичный результат поиска по базам данных [NVD](#) и [SNYK](#) (рисунки 4 и 5).

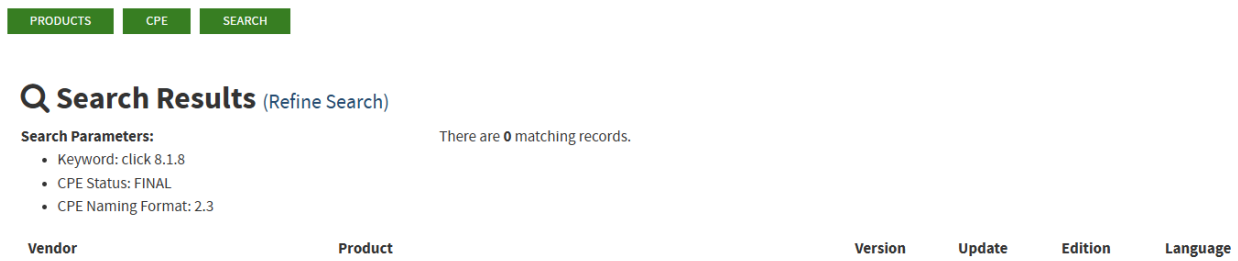


Рисунок 4 – актуальные уязвимости click 8.1.8 в NVD

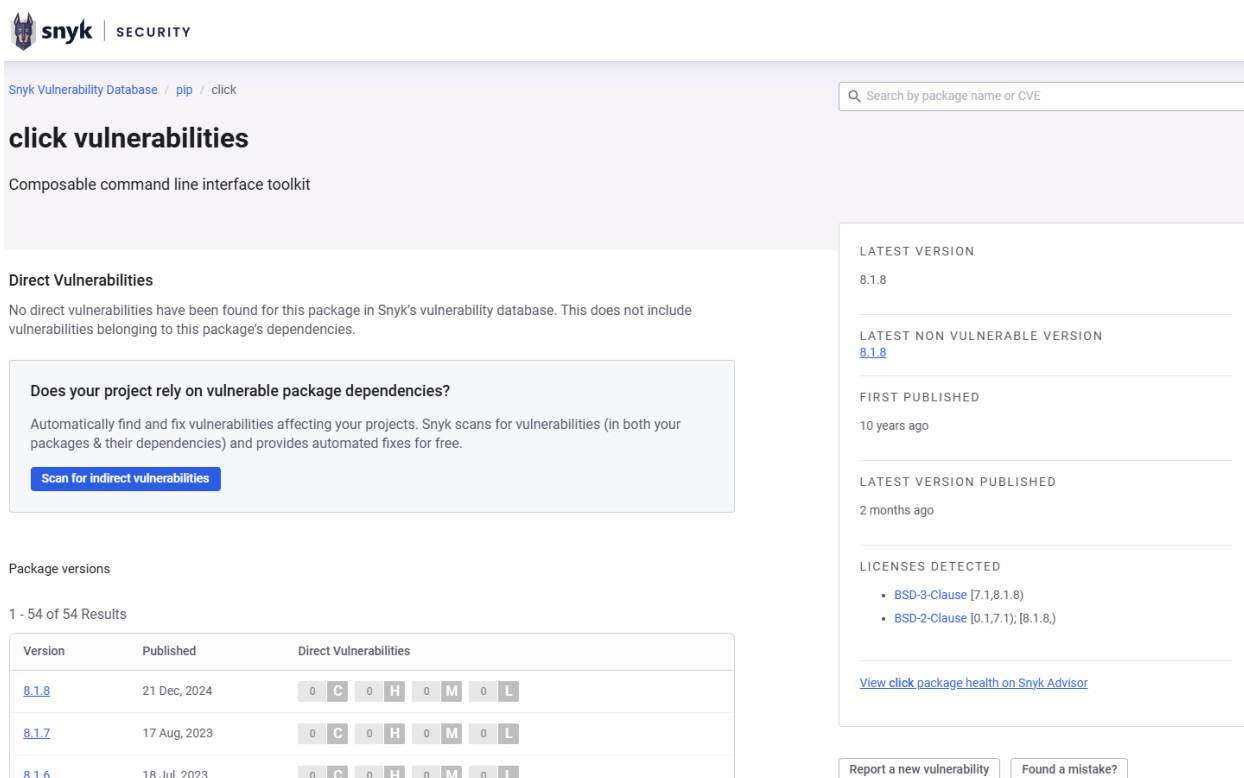


Рисунок 5 – актуальные уязвимости click 8.1.8 в SNYK

1.3 Flask 3.1.0

Касается пакета Flask 3.1.0, в базе данных [NVD](#) нет сведений об уязвимостях самого пакета, хотя имеются уязвимости в проектах, использующих данный пакет (рисунок 6).

Search Results (Refine Search)

Search Parameters:


- Keyword: flask 3.1.0
- CPE Status: FINAL
- CPE Naming Format: 2.3

There are 3 matching records.

Vendor	Product	Version	Update	Edition	Language
cpe:2.3:a:dpgaspar:flask-appbuilder:3.1.0:*:*:*:*:*	flask-appbuilder	3.1.0			
cpe:2.3:a:flask-security_project:flask-security:3.1.0:rc1:*:*:*:*	flask-security	3.1.0	rc1		
cpe:2.3:a:flask-security-too_project:flask-security-too:3.1.0:rc1:*:*:*:*	flask-security-too	3.1.0	rc1		

Рисунок 6 – актуальные уязвимости Flask 3.1.0 в NVD

Поиск по базе данных сервиса [CNYK](#) также не выявил актуальных уязвимостей, однако некоторые старые версии пакета были не так безопасны (рисунок 7).



Snyk Vulnerability Database / pip / flask

flask vulnerabilities

A simple framework for building complex web applications.



Direct Vulnerabilities

Known vulnerabilities in the flask package. This does not include vulnerabilities belonging to this package's dependencies.

How to fix?

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.

[Fix for free](#)

Vulnerability	Vulnerable Version
 Information Exposure	[2.2.5] [2.3.0,2.3.2]
 Denial of Service (DoS)	[0.12.3]

Search by package name or CVE

LATEST VERSION

3.1.0

LATEST NON VULNERABLE VERSION

[3.1.0](#)

FIRST PUBLISHED

14 years ago

LATEST VERSION PUBLISHED

3 months ago

LICENSES DETECTED

[BSD-3-Clause \[0,\]](#)

[View flask package health on Snyk Advisor](#)

Рисунок 7 – актуальные уязвимости Flask 3.1.0 в SNYK

1.4 flask-cors 5.0.1

База данных сервиса [NVD](#) не содержит информации об актуальных уязвимостях пакета flask-cors 5.0.1 (рисунок 8).

Q Search Results (Refine Search)

Search Parameters:

- Keyword: flask-cors 5.0.1
- CPE Status: FINAL
- CPE Naming Format: 2.3

There are 0 matching records.

Vendor	Product	Version	Update	Edition	Language
--------	---------	---------	--------	---------	----------

Рисунок 8 – актуальные уязвимости flask-cors 5.0.1 в NVD

Аналогичная ситуация и с результатом поиска на сервисе [SNYK](#) (рисунок 9).

flask-cors vulnerabilities

A Flask extension simplifying CORS support

Direct Vulnerabilities

Known vulnerabilities in the flask-cors package. This does not include vulnerabilities belonging to this package's dependencies.

How to fix?

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.

[Fix for free](#)

Vulnerability	Vulnerable Version
Improper Access Control	[4.0.0, 5.0.0]
Log Injection	[4.0.1]
Directory Traversal	[3.0.9]

LATEST VERSION
5.0.1

LATEST NON VULNERABLE VERSION
[5.0.1](#)

FIRST PUBLISHED
11 years ago

LATEST VERSION PUBLISHED
15 days ago

LICENSES DETECTED

- [Unknown](#) [5.0.1,)
- [MIT](#) [0.0.0.dev3, 5.0.1)

[View flask-cors package health on Snyk Advisor](#)

[Report a new vulnerability](#) [Found a mistake?](#)

Рисунок 9 – актуальные уязвимости flask-cors 5.0.1 в SNYK

Из скриншота видно, что до версии 5.0.0 пакет flask-cors имел уязвимость [Improper Access Control](#). Проанализируем ее подробнее.

1.4.1 Improper Access Control

Кратко об уязвимости Improper Access Control:

- уязвимость: неправильный контроль доступа;

- затронутые версии: 4.0.0–5.0.0;
- исправлено в версии: 5.0.0 и выше;
- критичность: CVSS 4.0 – 7.1 (High).

Данная уязвимость связана с неправильной настройкой CORS в расширении Flask-Cors. По умолчанию в уязвимых версиях включена поддержка заголовка Access-Control-Allow-Private-Network, что может привести к разглашению ресурсов внутренней сети (Intranet) через браузерные запросы. Это позволяет злоумышленнику взаимодействовать с внутренними сервисами, если пользователь случайно переходит по вредоносной ссылке.

Если приложение с Flask-Cors обрабатывает запросы от неизвестных источников, злоумышленник может отправить запросы к локальным ресурсам (например, 192.168.x.x, 10.x.x.x, localhost) через браузер жертвы.

Эксплуатация уязвимости позволяет:

- собирать информацию о внутренних сервисах;
- получать доступ к защищенным API;
- обходить меры защиты, такие как Same-Origin Policy.

Если жертва откроет вредоносный сайт, он сможет выполнить запрос, обращающийся к внутренним ресурсам:

```
fetch("http://192.168.1.1/admin", { credentials: "include" })  
  .then(response => response.text())  
  .then(data => console.log(data));
```

Если сервер с Flask-Cors на уязвимой версии разрешает такие запросы, злоумышленник получит доступ к ресурсам внутренней сети.

Существует несколько способов устранить уязвимость:

- обновить Flask-Cors до версии 5.0.0 или выше. В этой версии изменена обработка Access-Control-Allow-Private-Network, что исключает автоматический доступ к внутренним ресурсам;
- настроить CORS вручную, если обновление невозможно. Если обновить библиотеку нельзя, в коде нужно жестко ограничить источники запросов;
- запретить заголовок Access-Control-Allow-Private-Network в middleware перед отправкой ответа.

1.5 itsdangerous 2.2.0

В базах данных [NVD](#) и [SNYK](#) не выявлено актуальных уязвимостей пакета itsdangerous версии 2.2.0 (рисунки 10 и 11).

PRODUCTS	CPE	SEARCH
----------	-----	--------

Q Search Results (Refine Search)					
Search Parameters: <ul style="list-style-type: none"> Keyword: itsdangerous 2.2.0 CPE Status: FINAL CPE Naming Format: 2.3 		There are 0 matching records.			
Vendor	Product	Version	Update	Edition	Language

Рисунок 10 – актуальные уязвимости itsdangerous 2.2.0 в NVD

Snyk Vulnerability Database / pip / itsdangerous

itsdangerous vulnerabilities

Safely pass data to untrusted environments and back.

Direct Vulnerabilities

No direct vulnerabilities have been found for this package in Snyk's vulnerability database. This does not include vulnerabilities belonging to this package's dependencies.

Does your project rely on vulnerable package dependencies?

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities (in both your packages & their dependencies) and provides automated fixes for free.

Scan for indirect vulnerabilities

Package versions

1 - 27 of 27 Results

Version	Published	Direct Vulnerabilities
2.2.0	16 Apr, 2024	0 C 0 H 0 M 0 L
2.1.2	24 Mar, 2022	0 C 0 H 0 M 0 L
2.1.1	9 Mar, 2022	0 C 0 H 0 M 0 L

LATEST VERSION
2.2.0

LATEST NON VULNERABLE VERSION
2.2.0

FIRST PUBLISHED
13 years ago

LATEST VERSION PUBLISHED
10 months ago

LICENSES DETECTED

- BSD-2-Clause [0.9,2.0.0a1]; [2.2.0]
- BSD-3-Clause [2.0.0a1,2.2.0]

[View itsdangerous package health on Snyk Advisor](#)

Report a new vulnerability Found a mistake?

Рисунок 11 – актуальные уязвимости itsdangerous 2.2.0 в SNYK

1.6 Jinja2 3.1.6

Аналогичный результат поиска уязвимостей пакета Jinja2 3.1.6 в базах данных [NVD](#) и [SNYK](#) (рисунки 12 и 13).

PRODUCTS

CPE

SEARCH

Q Search Results (Refine Search)

Search Parameters:

- Keyword: Jinja2 3.1.6
- CPE Status: FINAL
- CPE Naming Format: 2.3

There are 0 matching records.

Vendor	Product	Version	Update	Edition	Language
--------	---------	---------	--------	---------	----------

Рисунок 12 – актуальные уязвимости Jinja2 3.1.6 в NVD

Однако лишь в текущей версии пакета была исправлена уязвимость [Template Injection](#), рассмотрим ее подробнее.

Jinja2 vulnerabilities

A very fast and expressive template engine.



Direct Vulnerabilities

Known vulnerabilities in the Jinja2 package. This does not include vulnerabilities belonging to this package's dependencies.

How to fix?

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.

[Fix for free](#)

Vulnerability	Vulnerable Version
 Template Injection	[3.1.6)
 Improper Neutralization	[3.1.5)

LATEST VERSION

3.1.6

LATEST NON VULNERABLE VERSION

[3.1.6](#)

FIRST PUBLISHED

16 years ago

LATEST VERSION PUBLISHED

5 days ago

LICENSES DETECTED

- [BSD-3-Clause](#) [2.10.2,3.1.4)
- [BSD-2-Clause](#) [2.0rc1,2.10.2); [3.1.4)

[View Jinja2 package health on Snyk Advisor](#)

Рисунок 13 – актуальные уязвимости Jinja2 3.1.6 в SNYK

1.6.1 Template Injection

Обнаруженная уязвимость в пакете Jinja2 связана с инъекцией шаблонов (Template Injection). Уязвимые версии (до 3.1.6) допускают выполнение произвольного кода через фильтр |attr, который позволяет злоумышленнику обойти защитные механизмы среды и получить доступ к критическим функциям Python. Критичность: CVSS 4.0: 5.4 (Medium).

Уязвимость может привести к выполнению произвольного кода на сервере, если злоумышленник имеет возможность передавать пользовательские шаблоны в движок Jinja2. Это делает атаку особенно опасной в веб-приложениях, которые рендерят шаблоны с динамическим вводом.

Условия эксплуатации:

- приложение использует Jinja2 и позволяет пользователям загружать или изменять шаблоны;

- приложение не ограничивает список доступных фильтров в Jinja2;
- отсутствуют дополнительные меры защиты, такие как строгая валидация вводимых данных.

Следующий код приводит к выполнению команды `id` на сервере:

```
{{ "".format.__globals__['os'].system('id') }}
```

С учетом использования фильтра `|attr`, злоумышленник может вызвать уязвимые методы следующим образом:

```
{{ ''|attr('__class__')|attr('__mro__')[-1]|attr('__subclasses__')() }}
```

Этот вызов позволяет получить список всех классов в системе, после чего можно найти и использовать `subprocess.Popen` для выполнения команд.

Существует ряд способов исправления уязвимости:

- обновить Jinja2 до версии 3.1.6 или выше;
- ограничить использование пользовательских шаблонов: запрещать передачу динамически изменяемых шаблонов от пользователей или использовать predetermined шаблоны, хранящиеся в безопасных местах;
- отключить фильтр `attr` через Environment.

1.7 MarkupSafe 3.0.2

В базах данных [NVD](#) и [SNYK](#) не обнаружено сведений об актуальных уязвимостях пакета MarkupSafe 3.0.2 (рисунки 14 и 15).

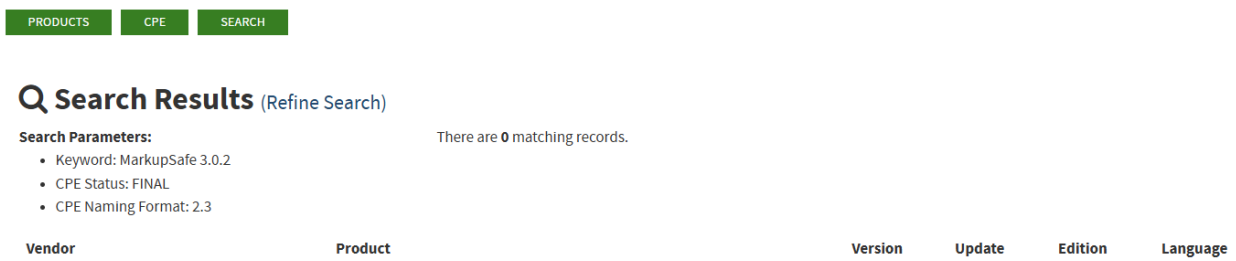


Рисунок 14 – актуальные уязвимости MarkupSafe 3.0.2 в NVD

markupsafe vulnerabilities

Safely add untrusted strings to HTML/XML markup.

Direct Vulnerabilities

No direct vulnerabilities have been found for this package in Snyk's vulnerability database. This does not include vulnerabilities belonging to this package's dependencies.

Does your project rely on vulnerable package dependencies?

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities (in both your packages & their dependencies) and provides automated fixes for free.

Scan for indirect vulnerabilities

Package versions

1 - 34 of 34 Results

Version	Published	Direct Vulnerabilities
3.0.2	18 Oct, 2024	0 C 0 H 0 M 0 L
3.0.1	8 Oct, 2024	0 C 0 H 0 M 0 L
3.0.0	7 Oct, 2024	0 C 0 H 0 M 0 L

LATEST VERSION

3.0.2

LATEST NON VULNERABLE VERSION

3.0.2

FIRST PUBLISHED

14 years ago

LATEST VERSION PUBLISHED

4 months ago

LICENSES DETECTED

- BSD-3-Clause [1.1.1,3.0.0]
- BSD-2-Clause [0.9,1.1.1]; [3.0.0]

View markupsafe package health on Snyk Advisor

Report a new vulnerability

Found a mistake?

Рисунок 15 – актуальные уязвимости MarkupSafe 3.1.2 в SNYK

1.8 Werkzeug 3.1.3

Аналогичный результат по поиску уязвимостей пакета Werkzeug 3.1.3 по базам данных [NVD](#) и [SNYK](#) (рисунки 16 и 17).

PRODUCTS CPE SEARCH

Q Search Results (Refine Search)

Search Parameters:

- Keyword: Werkzeug 3.1.3
- CPE Status: FINAL
- CPE Naming Format: 2.3

There are 0 matching records.

Vendor	Product	Version	Update	Edition	Language
--------	---------	---------	--------	---------	----------

Рисунок 16 – актуальные уязвимости Werkzeug 3.1.3 в NVD

werkzeug vulnerabilities

The comprehensive WSGI web application library.

Direct Vulnerabilities

Known vulnerabilities in the werkzeug package. This does not include vulnerabilities belonging to this package's dependencies.

How to fix?

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.

[Fix for free](#)

LATEST VERSION

3.1.3

LATEST NON VULNERABLE VERSION

[3.1.3](#)

FIRST PUBLISHED

17 years ago

LATEST VERSION PUBLISHED

4 months ago

Рисунок 17 – актуальные уязвимости Werkzeug 3.1.3 в SNYK

1.9 wheel 0.45.1

Такая же ситуация и с пакетом wheel 0.45.1 – поиск по базам данных [NVD](#) и [SNYK](#) не выявил актуальных уязвимостей (рисунки 18 и 19).

PRODUCTS CPE SEARCH

Q Search Results (Refine Search)

Search Parameters:

- Keyword: wheel 0.45.1
- CPE Status: FINAL
- CPE Naming Format: 2.3

There are 0 matching records.

Vendor	Product	Version	Update	Edition	Language
--------	---------	---------	--------	---------	----------

Рисунок 18 – актуальные уязвимости wheel 0.45.1 в NVD

wheel vulnerabilities

A built-package format for Python

Direct Vulnerabilities

Known vulnerabilities in the wheel package. This does not include vulnerabilities belonging to this package's dependencies.

How to fix?

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.

[Fix for free](#)

LATEST VERSION

0.45.1

LATEST NON VULNERABLE VERSION

[0.45.1](#)

FIRST PUBLISHED

12 years ago

LATEST VERSION PUBLISHED

3 months ago

LICENSES DETECTED

MIT [0]

Vulnerability

Vulnerable Version



Regular Expression Denial of Service (ReDoS)

[0.38.0]

Рисунок 19 – актуальные уязвимости wheel 0.45.1 в SNYK

1.10 Итоги

Проанализировав по открытым источникам пакеты, используемые в приложении Remediation-Demo, можно сделать вывод, что оно безопасно, так как в своей работе использует новейшие версии зависимостей. При этом назвать его абсолютно безопасным никак нельзя, потому что существует вероятность, что ряд уязвимостей просто еще не выявлен, а также имеются серьезные ошибки в исходном коде, позволяющие эксплуатировать уязвимости: SQL-инъекции и утечку конфиденциальных данных (однако эти уязвимости выходят за рамки темы настоящей лабораторной работы).