Министерство науки и высшего образования Российской Федерации

ФГАОУ ВО «Уральский федеральный университет им. первого Президента России Б. Н. Ельцина»

Кафедра «школа бакалавриата (школа)»

ОТЧЕТ ПО ЗАДАНИЮ № 1.

Преподаватель: Зайцев Дмитрий

Студенты: Белоусов С.В.

Казаков И.П.

Попов П.С.

Прокопьев А.А.

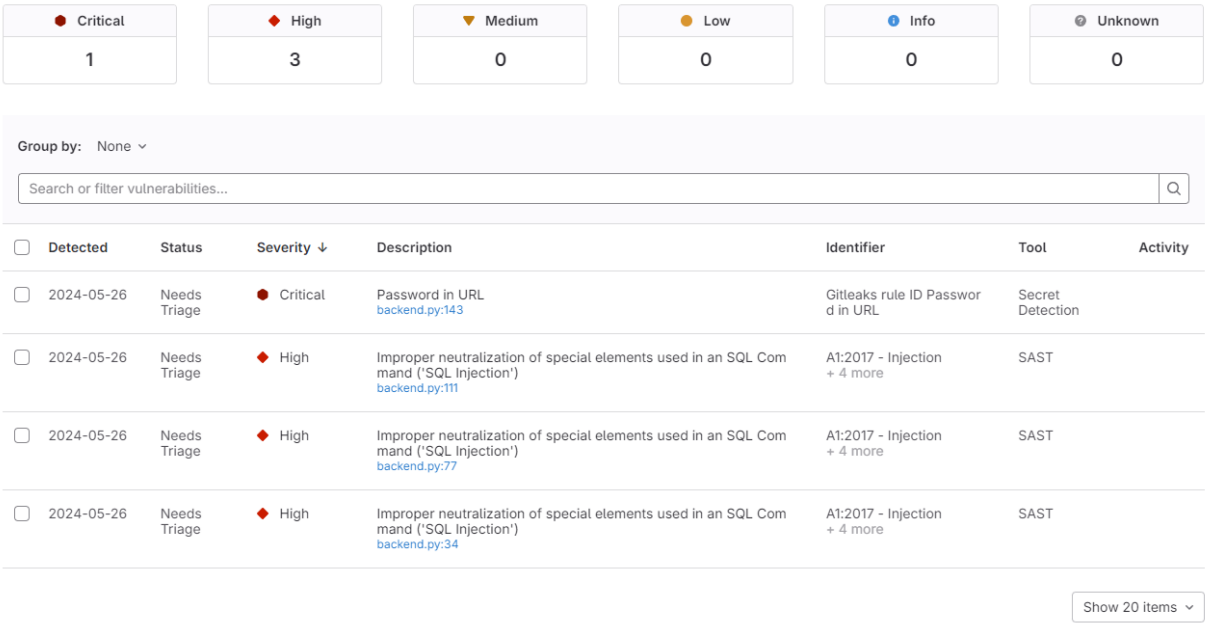
Семакин М.О.

Группа: РИ-221003

Екатеринбург
2024 г.

Объект сканирования: бэкенд, написанный на python + flask.

Исходя из отчета на GitLab, обнаружена SQL инъекция. Secret Detection дал ложное срабатывание.



Critical	High	Medium	Low	Info	Unknown
1	3	0	0	0	0

Group by: None

Search or filter vulnerabilities...

Detected	Status	Severity	Description	Identifier	Tool	Activity
2024-05-26	Needs Triage	Critical	Password in URL backend.py:143	Gitleaks rule ID Password in URL	Secret Detection	
2024-05-26	Needs Triage	High	Improper neutralization of special elements used in an SQL Command ('SQL Injection') backend.py:111	A1:2017 - Injection + 4 more	SAST	
2024-05-26	Needs Triage	High	Improper neutralization of special elements used in an SQL Command ('SQL Injection') backend.py:77	A1:2017 - Injection + 4 more	SAST	
2024-05-26	Needs Triage	High	Improper neutralization of special elements used in an SQL Command ('SQL Injection') backend.py:34	A1:2017 - Injection + 4 more	SAST	

Show 20 items

Password in URL:

Срабатывание ложное, в коде нет пароля для подключения к бд, он выведен в отдельный файл .env:

```
CONFIG = toml.load(".env")
DATABASE_USER = CONFIG["DATABASE_USER"]
DB_PASSWORD = CONFIG["DB_PASSWORD"]
DB_IP_PORT = CONFIG["DB_IP_PORT"]
DB_NAME = CONFIG["DB_NAME"]
conn =
psycopg2.connect(f'postgresql://{DATABASE_USER}:{DB_PASSWORD}@{DB_IP_PORT}/{DB_N
AME}')
```

SQL Injection

Я думал, что использую экранирование, но это не так и я не провел тестирование на инъекцию.

```
sql_query = "SELECT * FROM users WHERE username='%s'"
cursor.execute(sql_query % username)


sql_query = "SELECT rtoken FROM users WHERE rtoken='%s'"
cursor.execute(sql_query % RToken)
```