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.

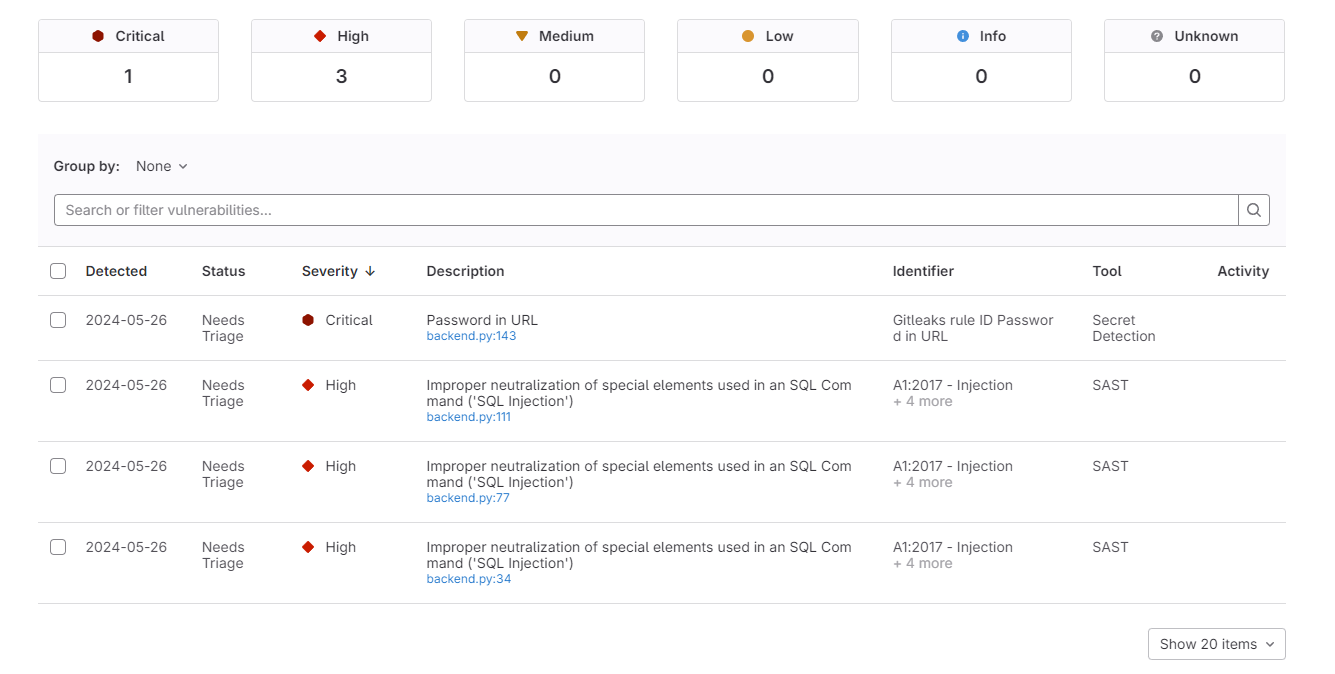
Семакин М.О.

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.



**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\_NAME}'**)**

**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**)**