ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

*Московский институт электроники и математики им. А.Н.Тихонова*

**Домашнее задание по по теме 6. Разработка защищенных программных систем**

По направлению 10.04.01 – «Информационная безопасность»

Проверил:

преп.

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнил:

Новиков В. С. МКБ 241

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2025

# Задание

Научиться использовать средства анализа безопасности приложений — SAST и DAST

# Этап 1. Установка JDK и OWASP ZAP

ZAP требует установленный JDK версии ≥11. Использован **openjdk-17-jdk**.

sudo apt update

sudo apt install -y openjdk-17-jdk

cd ~/Downloads

chmod +x ZAP\_2\_15\_0\_unix.sh

sudo ./ZAP\_2\_15\_0\_unix.sh

# Этап 2. Установка и настройка Bandit (SAST)

sudo apt install -y python3-pip python3-venv

python3 -m venv ~/bandit\_env

source ~/bandit\_env/bin/activate

pip install bandit

bandit –version

Запуск анализа PyGoat:

cd ~/devsecops/hw02/PyGoat-master

bandit -r . -ll -f txt -o bandit\_report.txt

deactivate

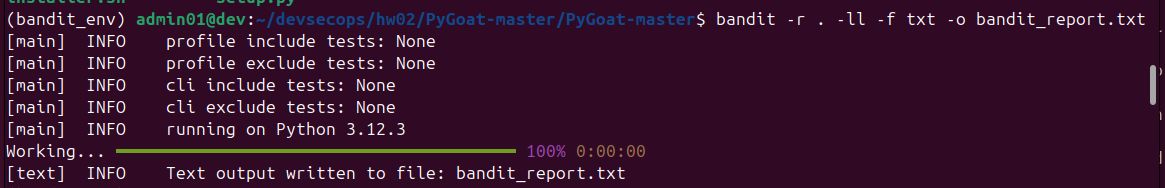


Рисунок 1. Отчет bandit

# Этап 3. Запуск приложения PyGoat

cd ~/devsecops/hw02/PyGoat-master

sudo docker build -t pygoat:latest .

sudo docker run -d --name pygoat -p 8000:8000 pygoat:latest

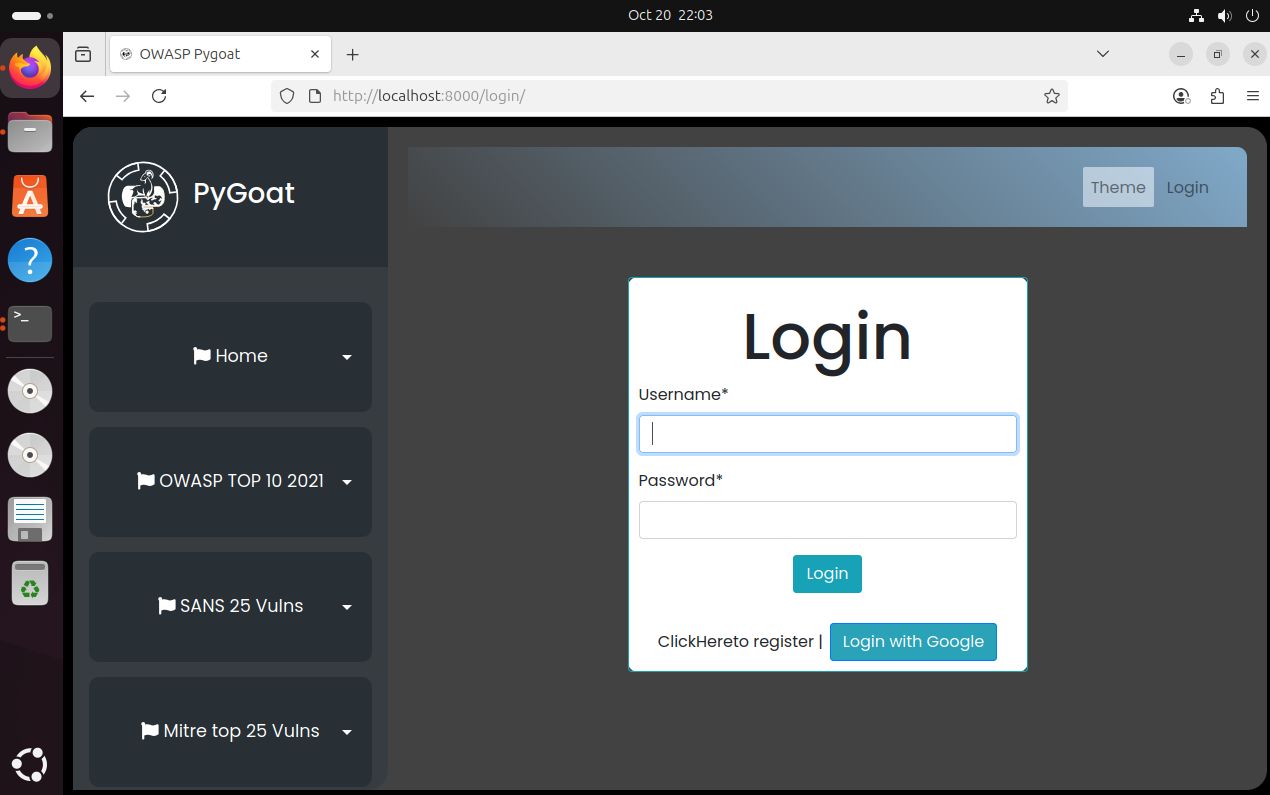


Рисунок 2. Запуск pygoat

# Этап 4. Проведение DAST-теста OWASP ZAP (GUI)

Запустить ZAP

В **Automated Scan** указать:

<http://localhost:8000>

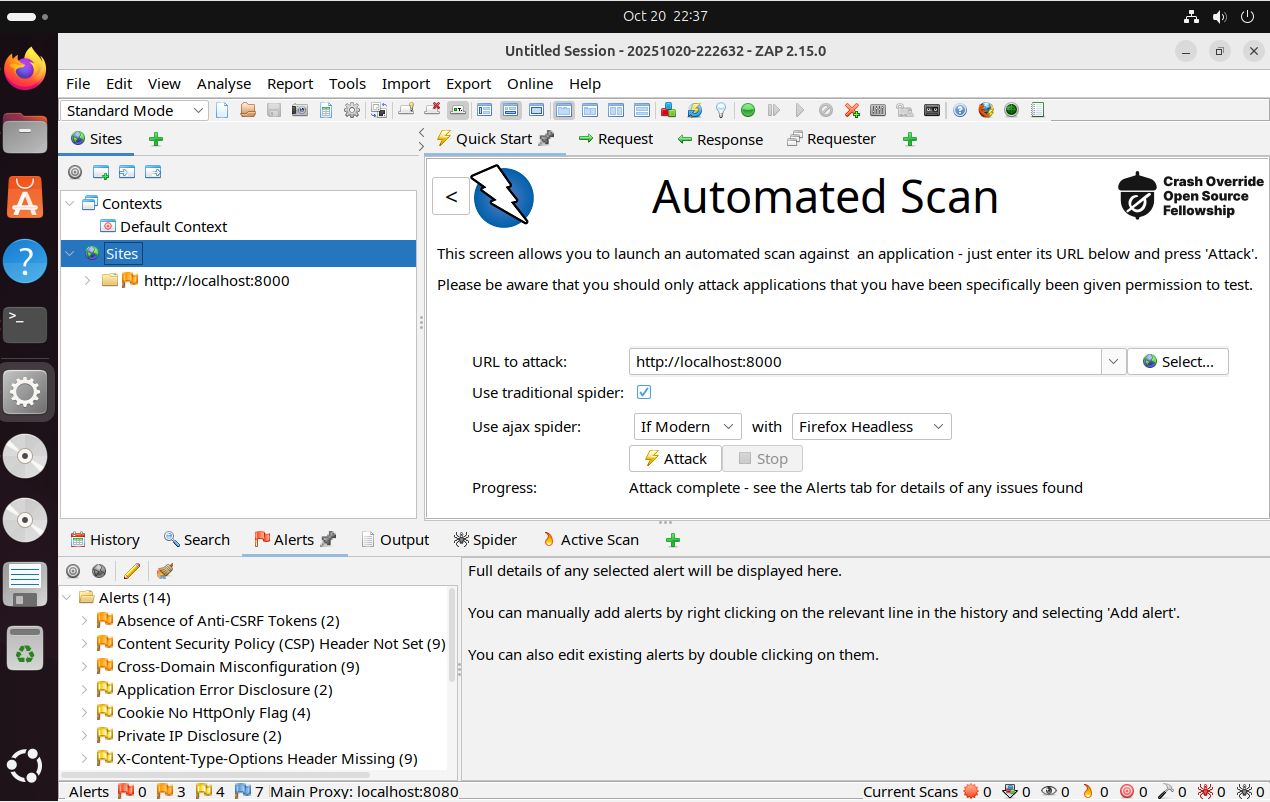


Рисунок 3. Запуск ZAP

# Этап 5. Результаты анализа

## Bandit (SAST)

| **Категория** | **Проблема** | **Рекомендация** |
| --- | --- | --- |
| **B301** | Использование pickle | Заменить на безопасный формат (JSON) |
| **B303** | MD5 используется для хешей | Использовать bcrypt или argon2 |
| **B602** | subprocess с shell=True | Использовать безопасный вызов без оболочки |
| **B506** | yaml.load() без safe\_loader | Использовать yaml.safe\_load() |

## OWASP ZAP (DAST)

| **Уровень** | **Уязвимость** | **Рекомендация** |
| --- | --- | --- |
| High | Отсутствует Content-Security-Policy | Добавить CSP в заголовки HTTP |
| Medium | Cookie без HttpOnly / Secure | Добавить флаги безопасности |
| Medium | Отсутствует X-Content-Type-Options | Добавить nosniff |
| Info | Server Disclosure | Удалить заголовки Server, X-Powered-By |

# Выводы и предложения по улучшению

1. Усилить HTTP-защиту: добавить CSP, HSTS, X-Frame-Options.
2. Секреты хранить в .env и Kubernetes Secrets.
3. Использовать безопасные хеши (bcrypt, argon2).
4. Переписать YAML-загрузку с safe\_load и валидацией.
5. Добавить SAST/DAST в CI/CD (GitHub Actions).
6. Ограничить права контейнера PyGoat: USER nonroot, read-only filesystem.
7. Интегрировать результаты ZAP в SIEM