

Zad 1

[debian]

Apt update

Apt install sudo

Apt install curl

curl -fsSL https://get.casaos.io | sudo bash

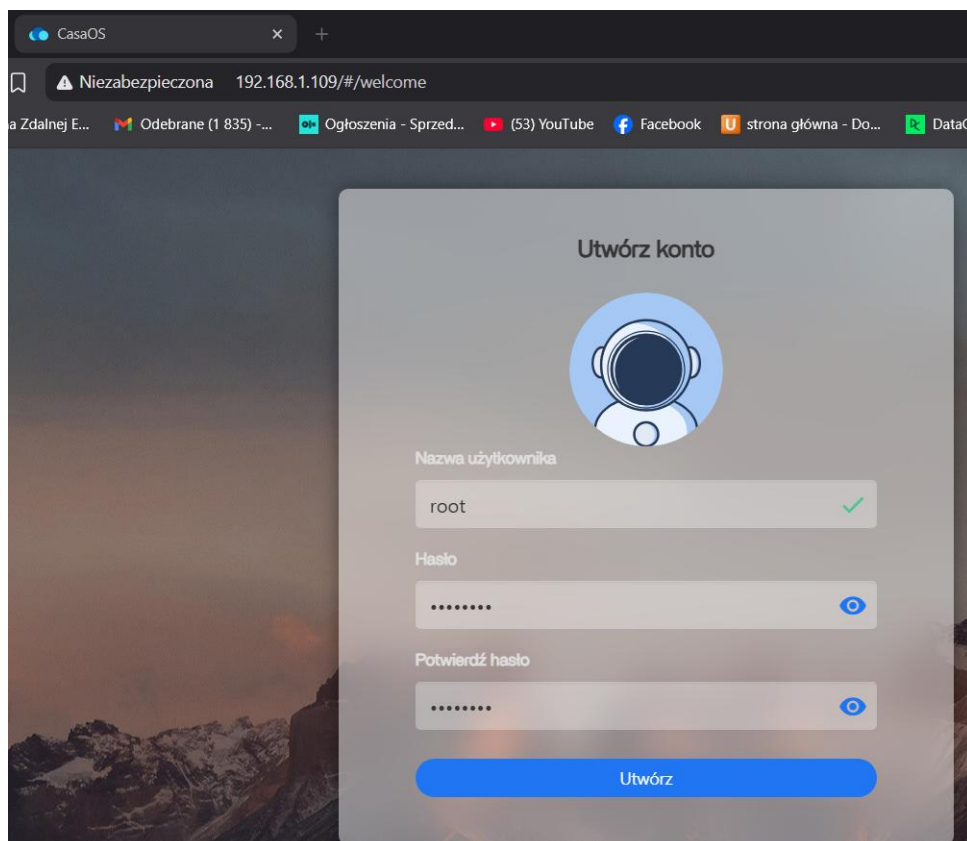
```
CasaOS v0.4.15 is running at:
- http://192.168.1.109 (enp0s3)
Open your browser and visit the above address.

CasaOS Project : https://github.com/IceWhaleTech/CasaOS
CasaOS Team    : https://github.com/IceWhaleTech/CasaOS#maintainers
CasaOS Discord  : https://discord.gg/knqAbbBbeX
Website        : https://www.casaos.io
Online Demo    : http://demo.casaos.io

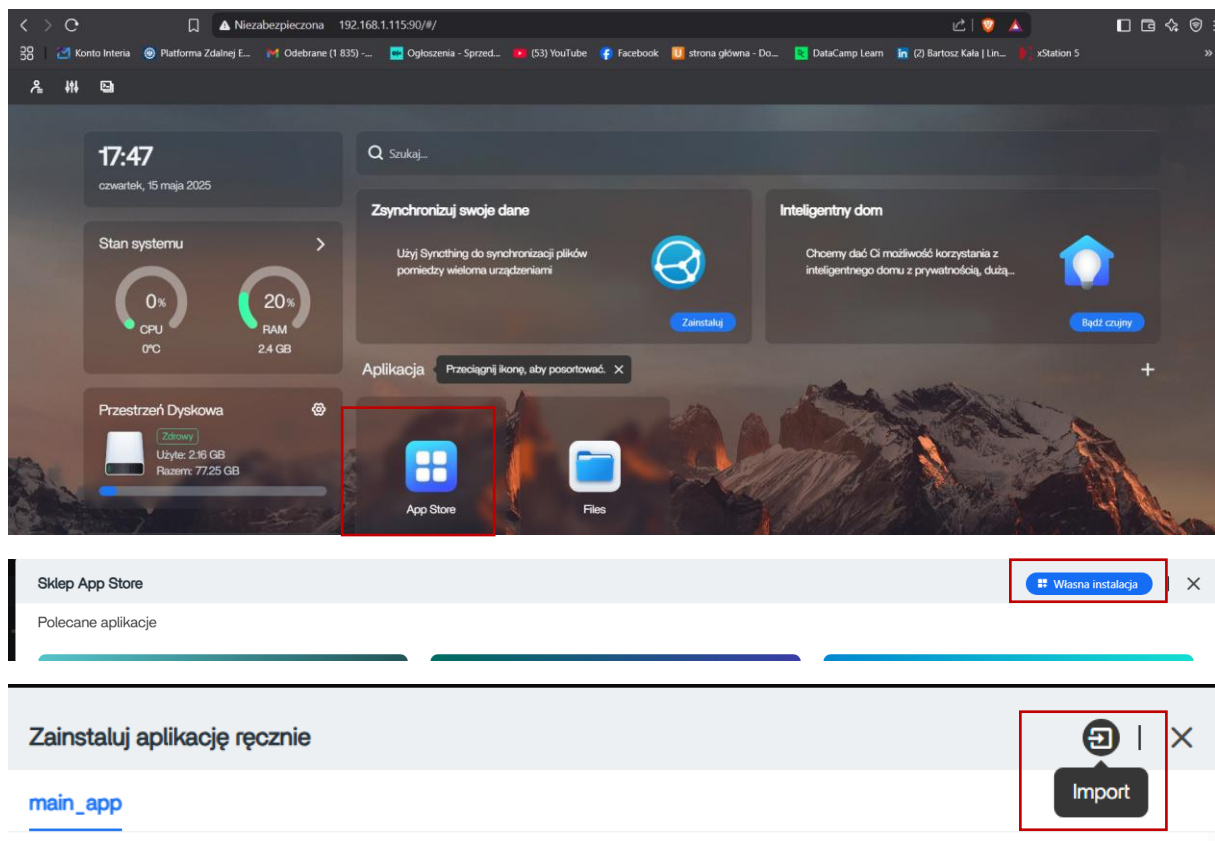
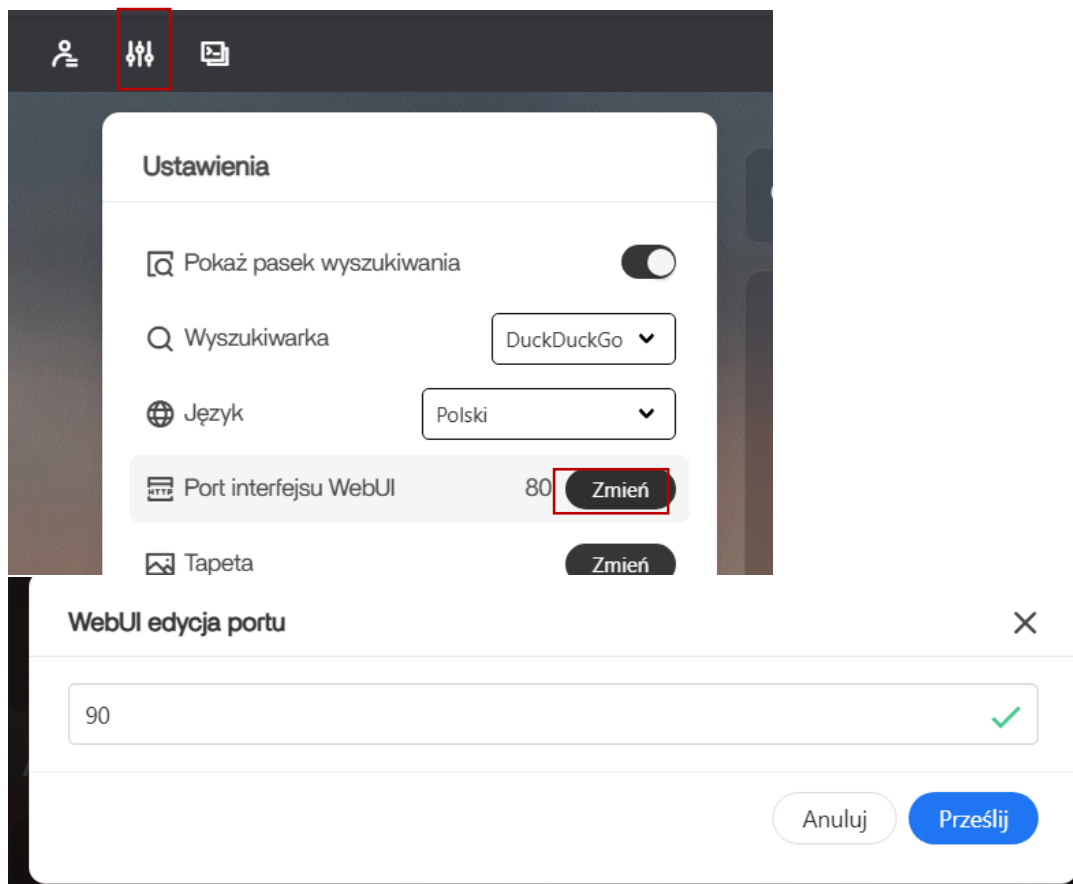
Uninstall      : casaos-uninstall

root@debian11:~# |
```

Wklejamy powyższy link w przeglądarkę i tworzymy konto:



Zmieniamy port na którym działa aplikacja:



```
root@debian11:~# mkdir /docker && mkdir /docker/npm && mkdir /docker/npm/data
root@debian11:~# mkdir /docker/npm/letsencrypt
root@debian11:~#
```

Import

[Docker Compose](#) [Docker CLI](#)

```
version: '3'
services:
  app:
    image: 'jc21/nginx-proxy-manager:latest'
    container_name: nginx-proxy-manager
    restart: always
    ports:
      - '80:80' #HTTP Traffic
      - '443:443' #HTTPS Traffic
      - '81:81' #Dashboard Port
    volumes:
      - '/docker/npm/data:/data'
      - '/docker/npm/letsencrypt:/etc/letsencrypt'
```

Upuść plik aplikacji (Docker Compose) tutaj lub kliknij, aby przesać

Anuluj **Prześlij**

Zainstaluj aplikację ręcznie

[app](#)


Obraz Dockera * Tag

jc21/nginx-proxy-manager latest

Tytuł *

app

URL ikony

 https://icon.casaos.io/main/all/app.png

Web UI

http:// 192.168.1.115 :81 /index.html Opcjonalne

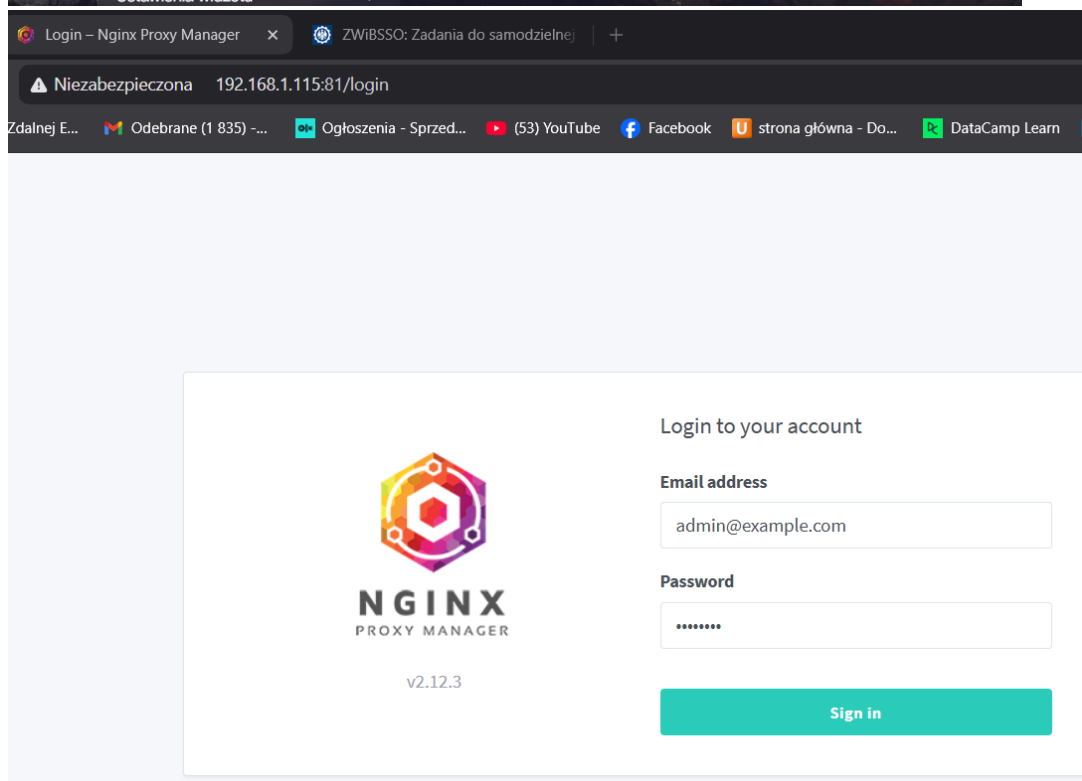
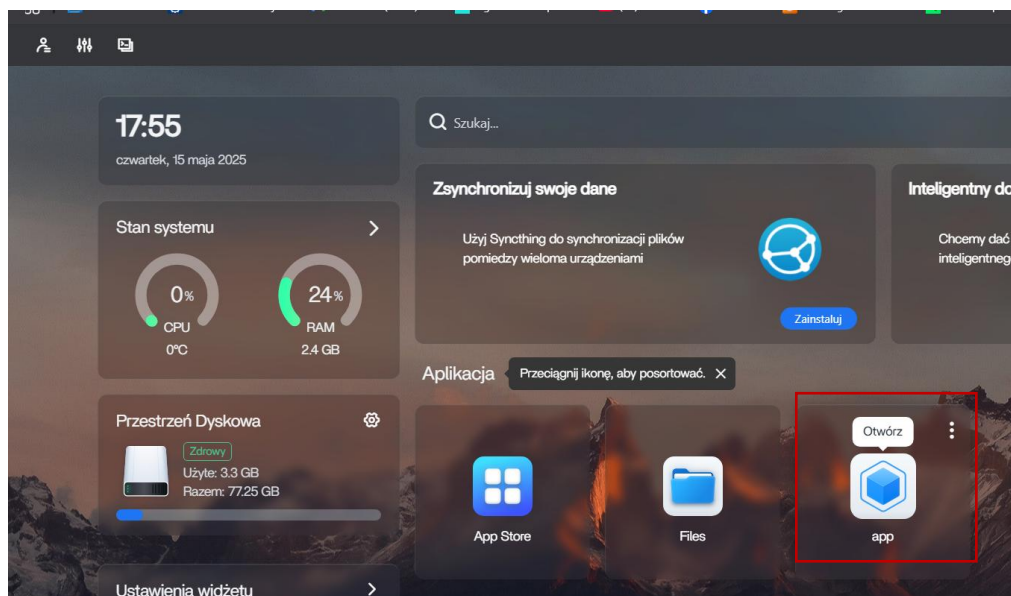
Sieć

bridge

Port

Zainstaluj

Czekamy na koniec instalacji

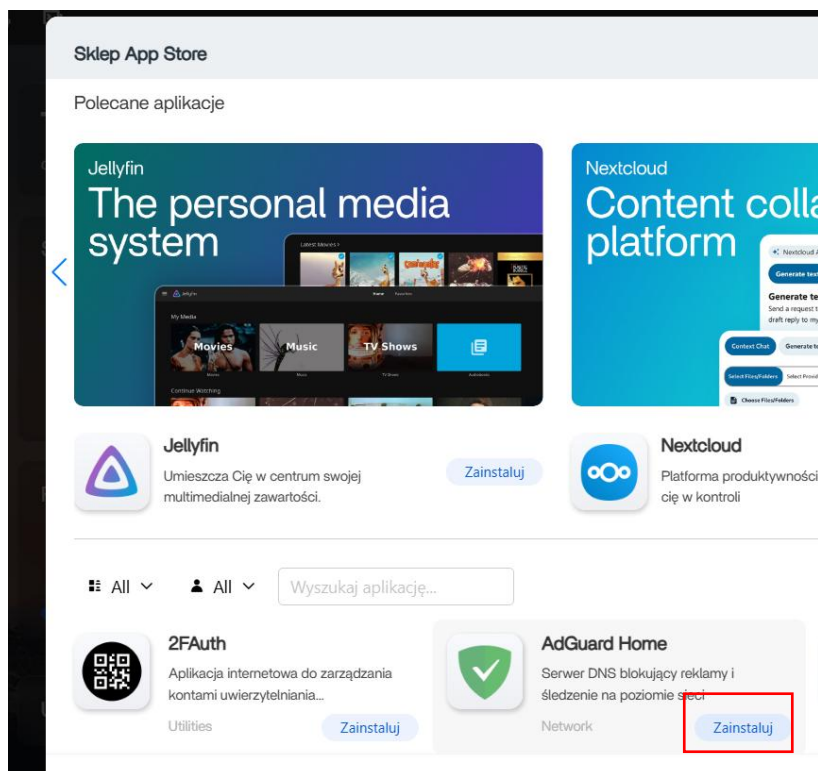
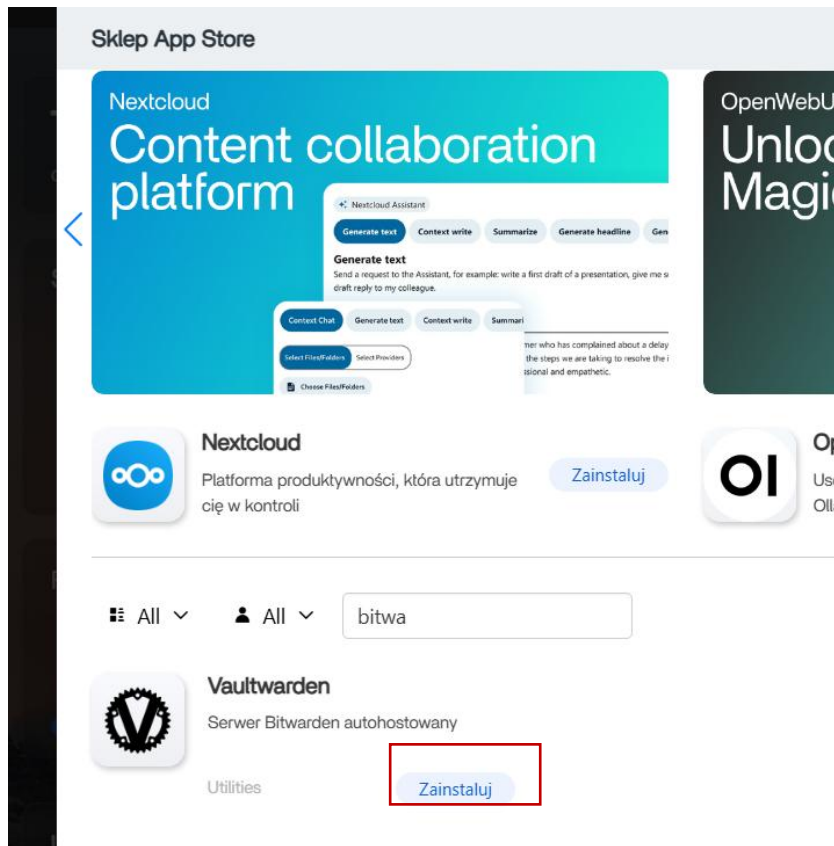


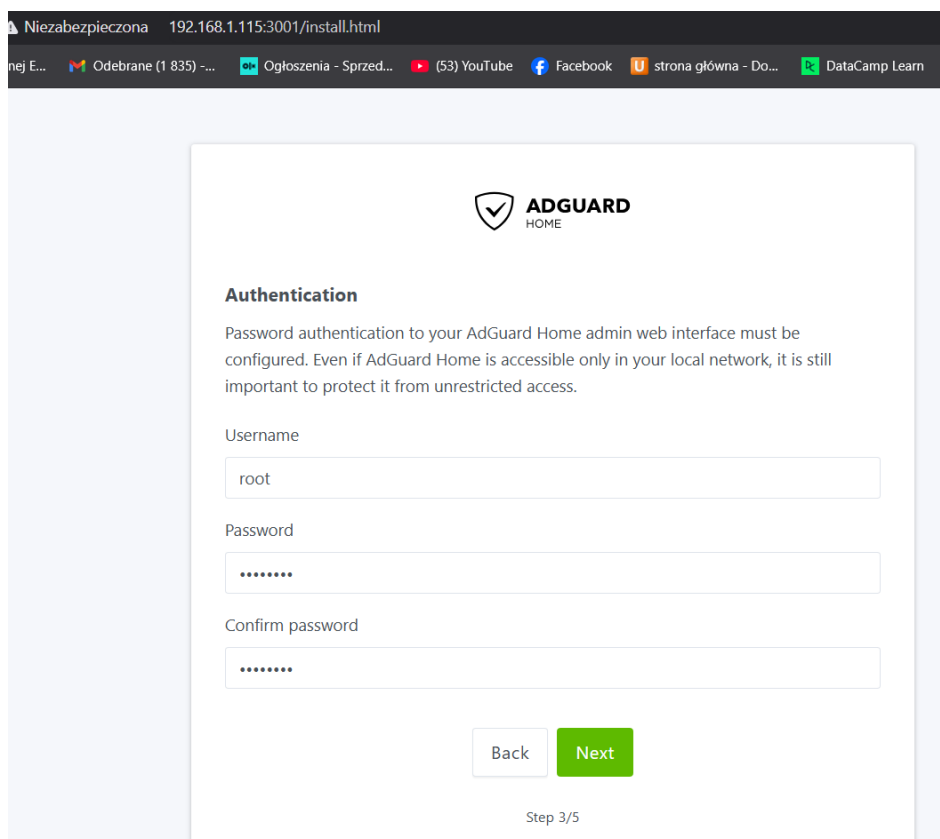
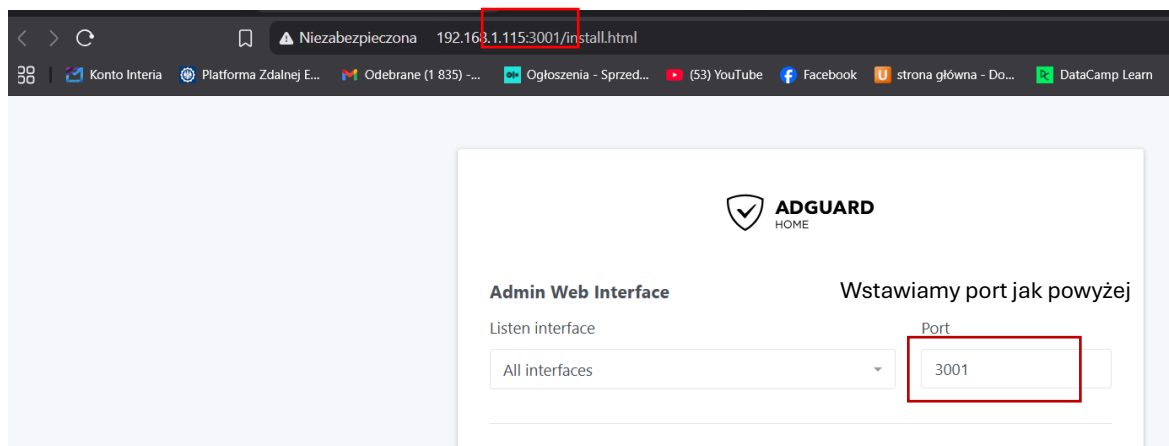
L: admin@example.com


H: changeme

Zad 2

W AppStore:





 **ADGUARD**
HOME

[Dashboard](#) [Settings](#) [Filters](#) [Queries](#)

DNS settings

General settings

DNS settings

Encryption settings

Client settings

DHCP settings

Upstream DNS servers

Enter one server address per line. [Learn more](#) about configuring upstream DNS servers. [Here is a list of public DNS servers.](#)

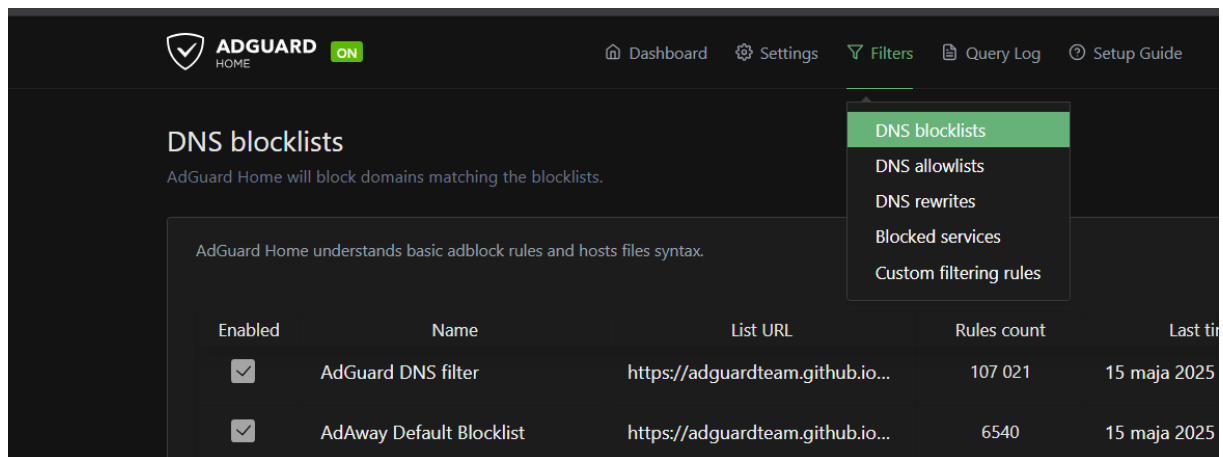
```
https://dns10.quad9.net/dns-query
https://security.cloudflare-dns.com/dns-query
```

☒ **Use private reverse DNS resolvers**
Resolve PTR, SOA, and NS requests for ARPA domains containing private IP addresses. If enabled, AdGuard will respond to all such requests with NXDOMAIN.

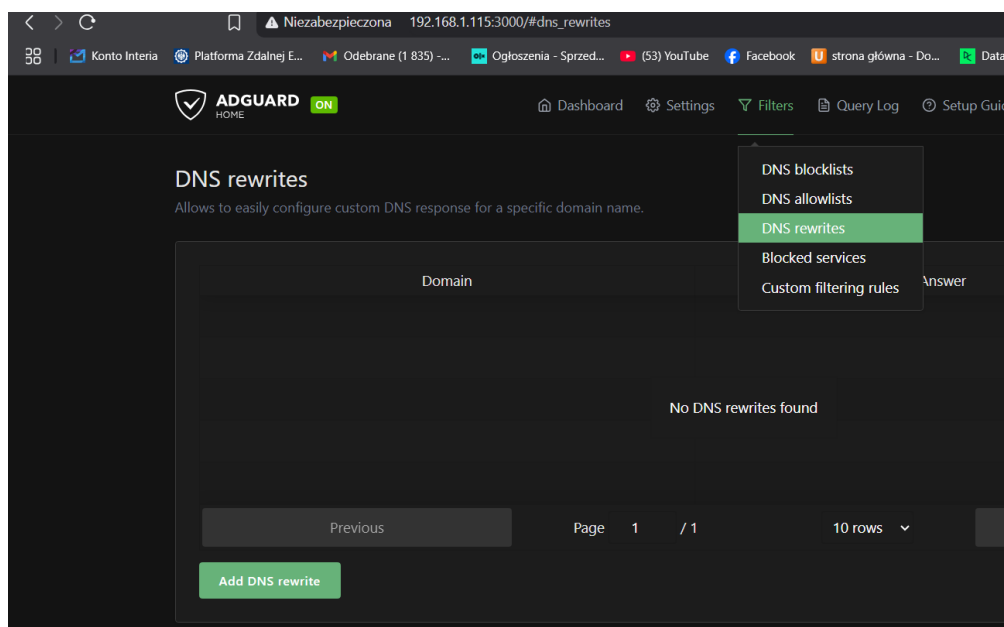
☒ **Enable reverse resolving of clients' IP addresses**
Reversely resolve clients' IP addresses into their hostnames by sending queries to upstream DNS servers (works only with public IP addresses).

[Test upstreams](#) [Apply](#)

DNS server configuration



Dodajemy nazwę:



Add DNS rewrite

Enter the domain name or wildcard you want to be rewritten.

Examples:

- example.org – rewrite responses for this domain name only.
- *.example.org – rewrite responses for all example.org subdomains.

- IP address: use this IP in an A or AAAA response
- Domain name: add a CNAME record
- A : special value, keep A records from the upstream
- AAAA : special value, keep AAAA records from the upstream

CancelSave

Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel

```
C:\Users\mkowalski>ping bitwarden.kala.pl

Pinging bitwarden.kala.pl [192.168.1.115] with 32 bytes of data:
Reply from 192.168.1.115: bytes=32 time<1ms TTL=64
Reply from 192.168.1.115: bytes=32 time<1ms TTL=64
Reply from 192.168.1.115: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.115:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\mkowalski>
```

Vaultwarden Web

Not secure bitwarden.kala.pl/#/login

Microsoft Edge
Would you like to set Microsoft Edge as your default browser?

Vaultwarden

Log in or create a new account to access your secure vault.

Email address (required)

⊗ Input is required.

☐ Remember email

Continue

New around here? [Create account](#)



Nginx Proxy Manager

Dashboard

Hosts

Access Lists

SSL

Hi Admin



0 Proxy Hosts



New Proxy Host



Details

Custom locations

SSL

Advanced

Domain Names *

bitwarden.kala.pl

Scheme *

http

Forward Hostname / IP *

192.168.1.115

Forward Port *

10380

☐ Cache Assets

☐ Block Common Exploits

☐ Websockets Support

Access List

Publicly Accessible

Cancel

Save

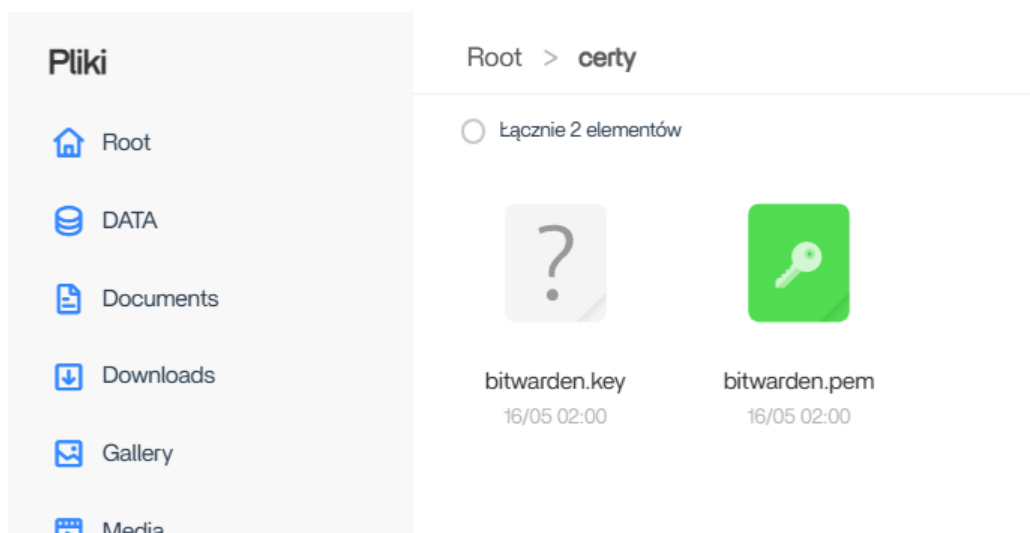
Zad 3

W terminalu CasaOS wydajemy polecenia:

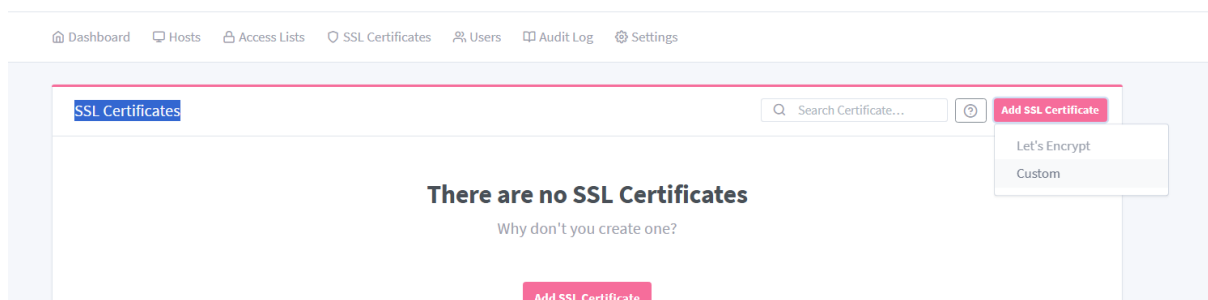
[Terminal](#) [Logi](#)

```
root@debian11:~# mkdir /certy
root@debian11:~# cd /certy
root@debian11:/certy# openssl req -new -days 365 -nodes -x509 -newkey ec -pkeyopt ec_paramgen_curve:prime256v1 -subj "/C=PL/ST=SLASK/L=Gliwice/O=Contoso/OU=IT/CN=bitwarden.kala.pl/emailAddress=admin@admin.net" -keyout bitwarden.key -out bitwarden.pem -addext "subjectAltName=DNS:bitwarden.kala.pl,DNS:*.bitwarden.kala.pl"
Generating an EC private key
writing new private key to 'bitwarden.key'
-----
root@debian11:/certy# ls
bitwarden.key  bitwarden.pem
root@debian11:/certy# _
```

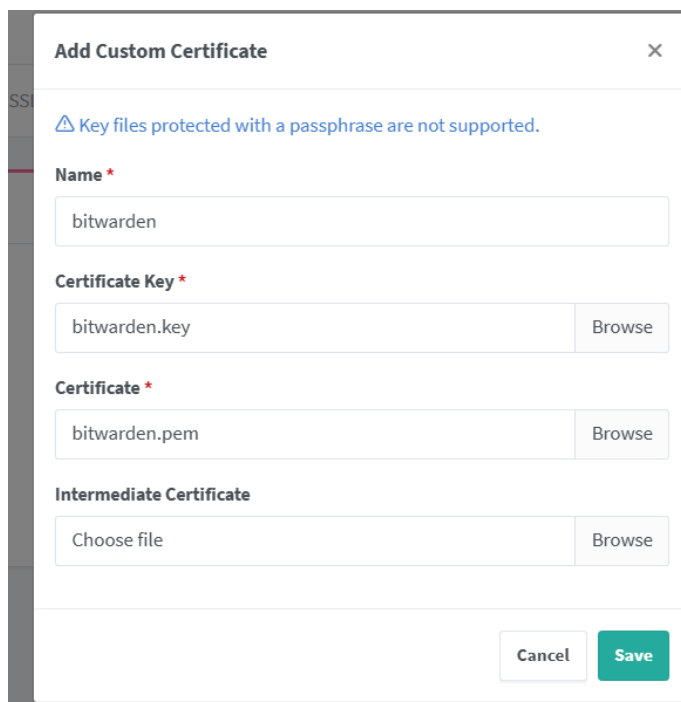
Przechodzimy do katalogu z utworzonymi plikami i pobieramy je:



Na NGINX, wchodzimy do zakładki SSLSSL Certificates:

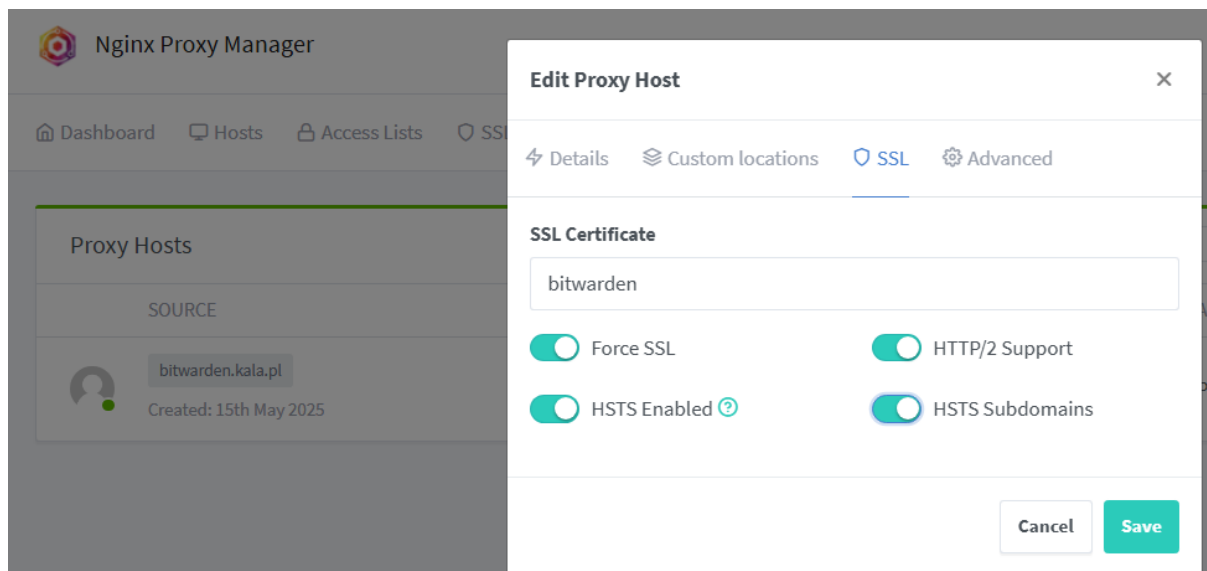


Wybieramy odpowiednie pliki:



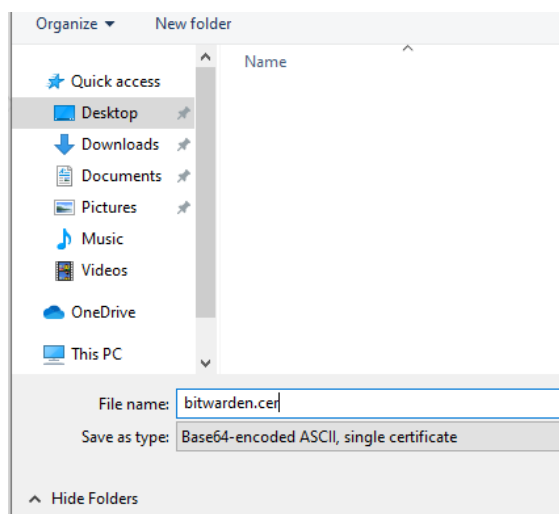
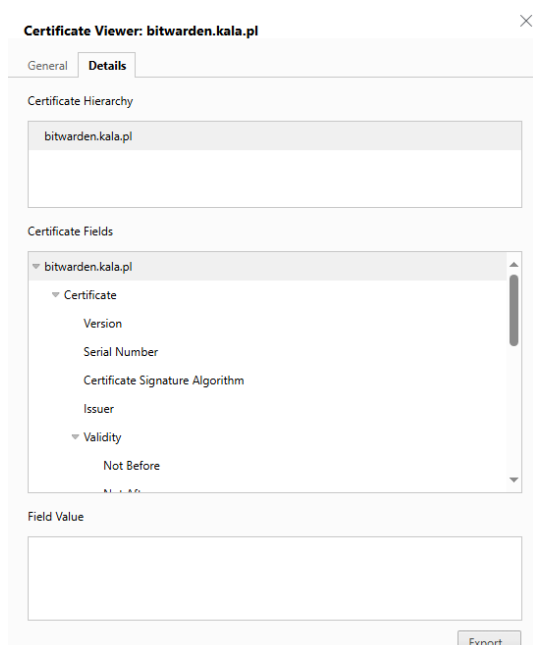
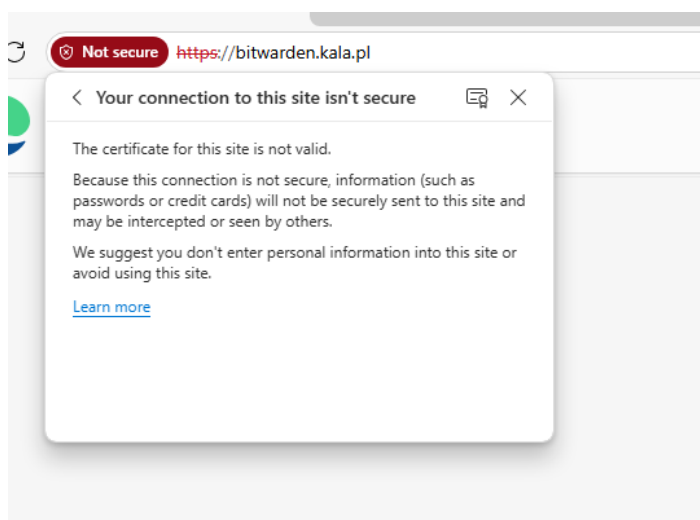
The dialog box titled "Add Custom Certificate" contains a warning message: "Key files protected with a passphrase are not supported." Below this, there are four fields with "Browse" buttons: "Name" (containing "bitwarden"), "Certificate Key" (containing "bitwarden.key"), "Certificate" (containing "bitwarden.pem"), and "Intermediate Certificate" (containing "Choose file"). At the bottom are "Cancel" and "Save" buttons.

Dashboard → Proxy hosts, edytujemy istniejący poprzez wybranie w zakładce SSL odpowiedniego pola:

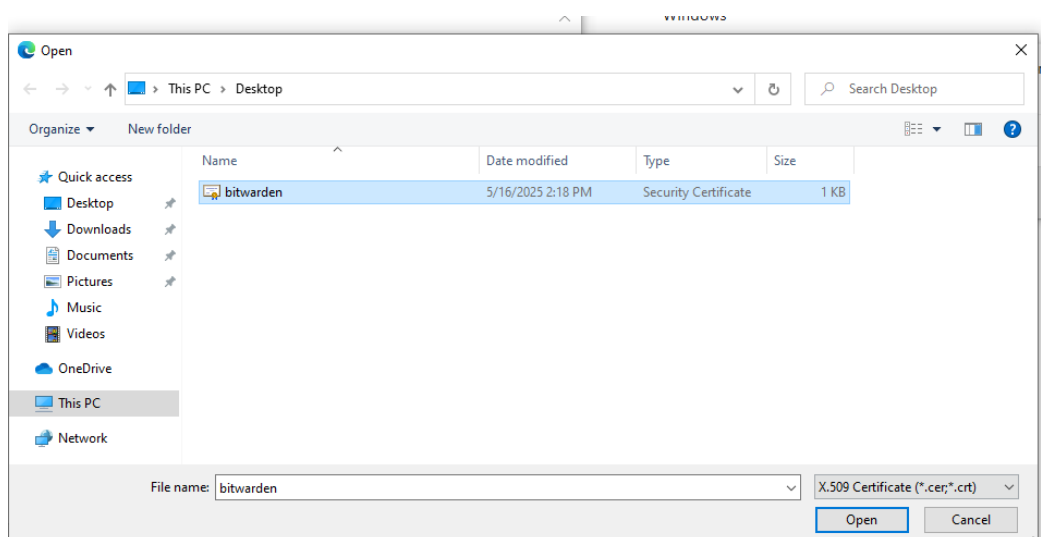
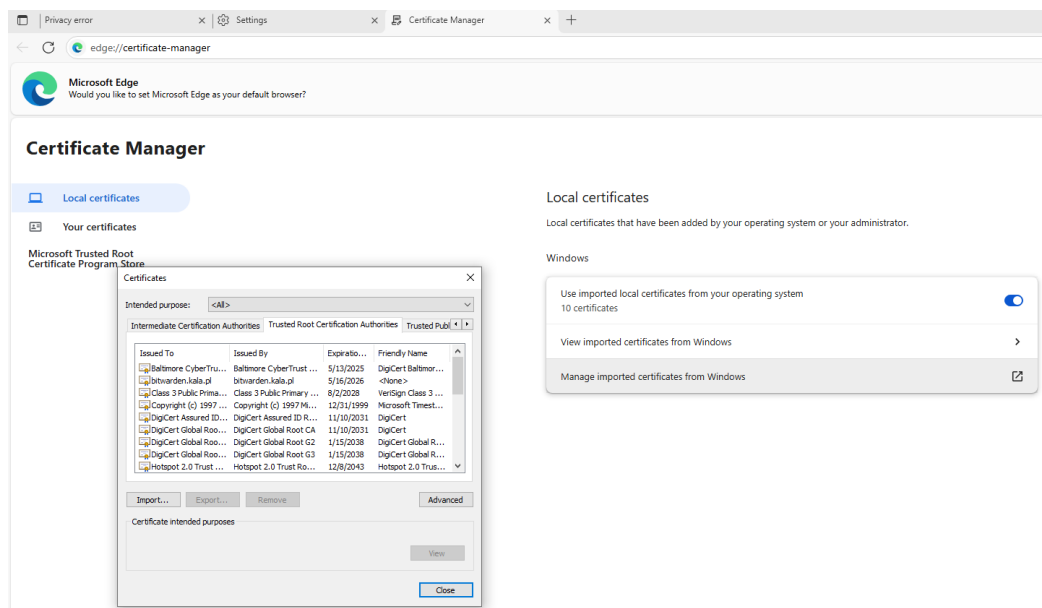


The Nginx Proxy Manager interface shows the "Proxy Hosts" section with a table containing one entry: "bitwarden.kala.pl" created on "15th May 2025". An "Edit Proxy Host" dialog is open, showing the "SSL" tab. The "SSL Certificate" field contains "bitwarden". Four toggle switches are visible: "Force SSL", "HTTP/2 Support", "HSTS Enabled", and "HSTS Subdomains", all of which are turned on. "Cancel" and "Save" buttons are at the bottom right.

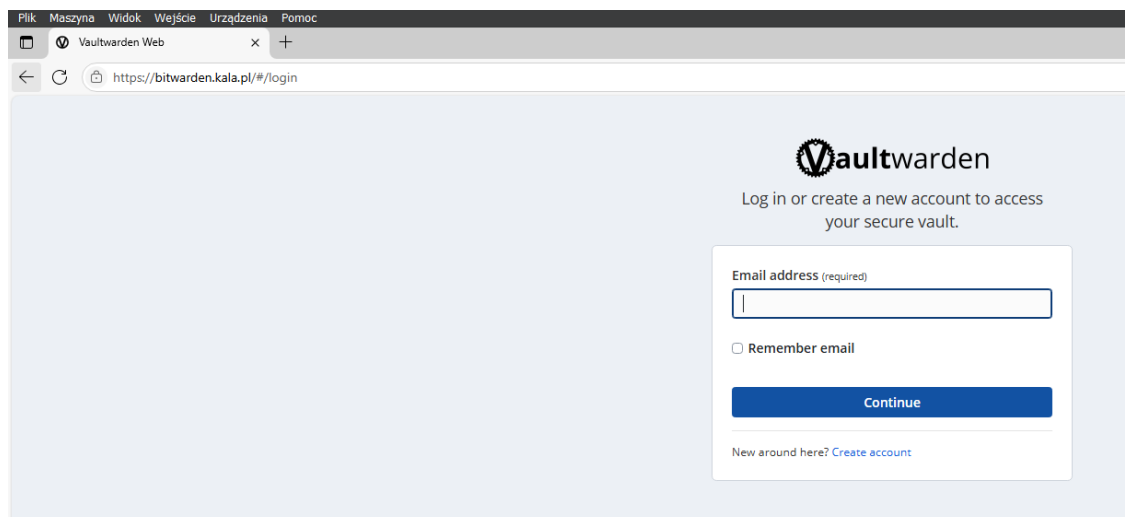
Na przeglądarce przechodzimy do szczegółów certyfikatów i eksportujemy :



Wyszukujemy zażądanie certyfikatami w przeglądarce i przechodzimy do odpowiedniej zakładki i importujemy wcześniej wyeksportowany plik:



Zamykamy i otwieramy przeglądarkę ponownie:



Możemy utworzyć konto i odpalić aplikację:

