Zadanie 7

I-UPB

29. novembra 2021

Obsah

Tvorba WSGI servera

Server je vytvorený pomocou nástroja gunicorn.

Webová aplikácia

Použil som formulár na registráciu z predošlého zadania, takto si môžem odchytiť aj nejaký zaujímavejší traffic. Aplikácia je jednoduchá, používateľ sa zaregistruje, aplikácia skontroluje záznam v databáze pri prihlásení.

Konfigurácia

Pred inštaláciou dotiahnuť pip packages:

```
pip install -r requierements.txt
```

Keďže som sa rozhodol pre self-signed certifikáty, pred spustením ich treba vytvoriť. Urobím tak jednoducho cez openssl.

```
openssl req -x509 -newkey rsa:4096 -nodes -out
    cert.pem -keyout key.pem -days 365
```

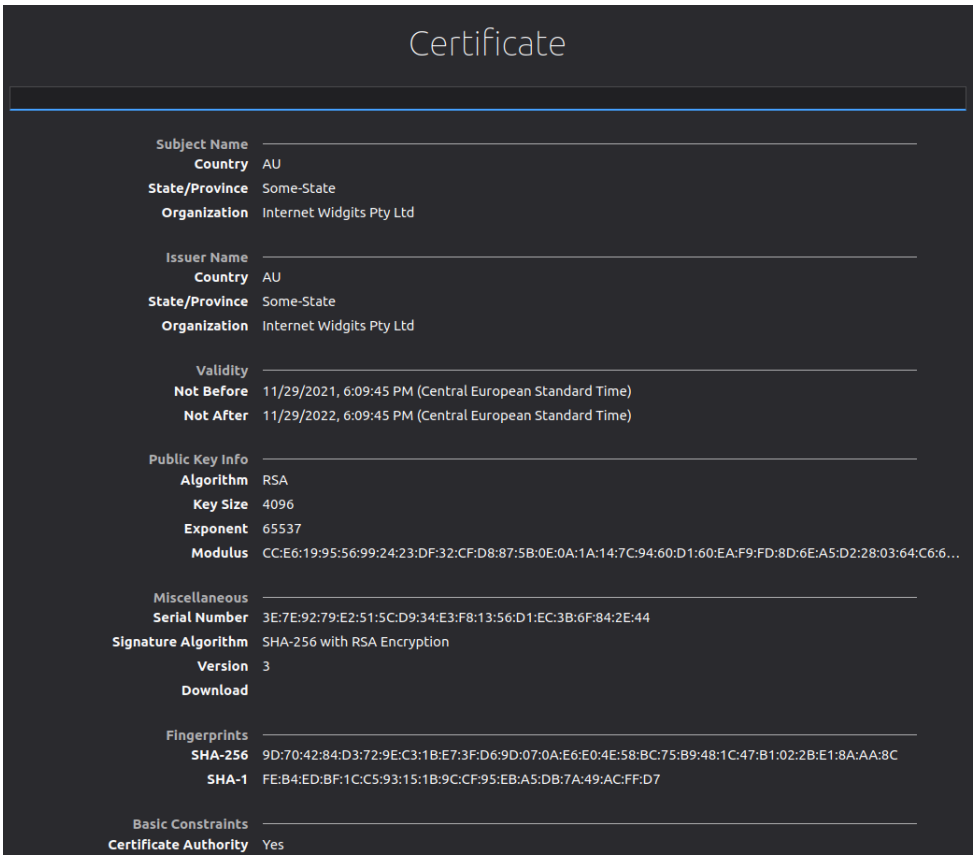
Vysvetlenie príkazu:

- req - spracovanie requestu pre certifikát, tvorba self-signed certifikátu
- newkey - generuj nový kľúč
- nodes - možnosť pri vytvorení cert.pem aj key.pem v jednom riadku
- out - výstupný súbor
- days - dĺžka validácie klúča

Spustenie

```
flask run --cert=cert.pem --key=key.pem
```

Skontrolujeme platnosť certifikátu na adrese https://127.0.0.1:5000/ nasledovné:



Obr. 1: Príklad vygenerovaného certifikátu

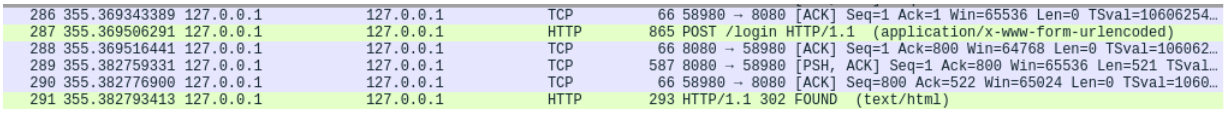
Spustenie servera

```
gunicorn --certfile cert.pem --keyfile key.pem -w 4 -b 0.0.0.0:8080 app:app
```

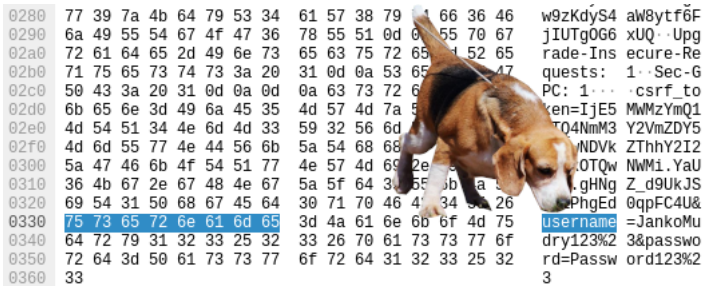
Server je nakonfigurovaný na porte **8080** a posledným arguntom je modul app, teda prepojenie s Flaskom. Certifikát ako aj key sú definované aj pri spustení app.py.

Sledovanie komunikácie

Prihlásim sa ako **JankoMudry123!** a moje heslo bude **Password123!** (nechodil do školy na UPB, tak nevie že to nieje dobré heslo). Skúsime túto správu odchytiť cez wireshark. Záznam už existuje v *database.db*.



Obr. 2: Zachytenie loginu pomocou wireshark



Obr. 3: Odhalený HTTP login packet

Vidím v plain texte prihlasovacie meno ako aj heslo.

Poznámky

Celý projekt je dostupný aj na https://github.com/behindbone/upb-08.

Zdroje

- https://www.educba.com/flask-https/
- https://stackoverflow.com/questions/62649807/serve-flask-application-with-
- https://www.digicert.com/kb/ssl-support/openssl-quick-reference-guide.htm
- https://blog.didierstevens.com/2020/12/14/decrypting-tls-streams-with-wire
- https://www.datasciencelearner.com/how-to-deploy-flask-app-using-nginx-and