Rapport
Projet Cryptographie
sous l'enseignement de Mohamed MAACHAOUI

Ing3 - Cybersécurité A
Groupe : Théo JULIEN | William KACZMAREK | Lucas TESTE

Cy Tech année 2022-2023

Table des matières

1. Introduction

Pour ce projet notre objectif est de créer un dispositif d'envoi par courrier électronique sécurisé d'attestation ou diplôme. Pour garantir l'authenticité des attestations que nous délivrons, l'image que reçoit le diplômé par mail comporte plusieurs points clés.

Une partie visible contenant Nom Prénom, la certification réussie et un QR code qui contient la signature de ces informations.
Mais aussi, une partie invisible dissimulée par stéganographie qui reprend les informations ci-dessus avec la signature certifiée par une autorité de timestamp.

Dans ce rapport vous trouverez tout d'abord une démonstration de comment utiliser notre programme, suivi de brèves explications sur son fonctionnement.

2. Démonstration

2.1 Générer un diplôme/une attestation

1ère étape : Remplir le fichier settings.py avec les informations de votre serveur SMTP.

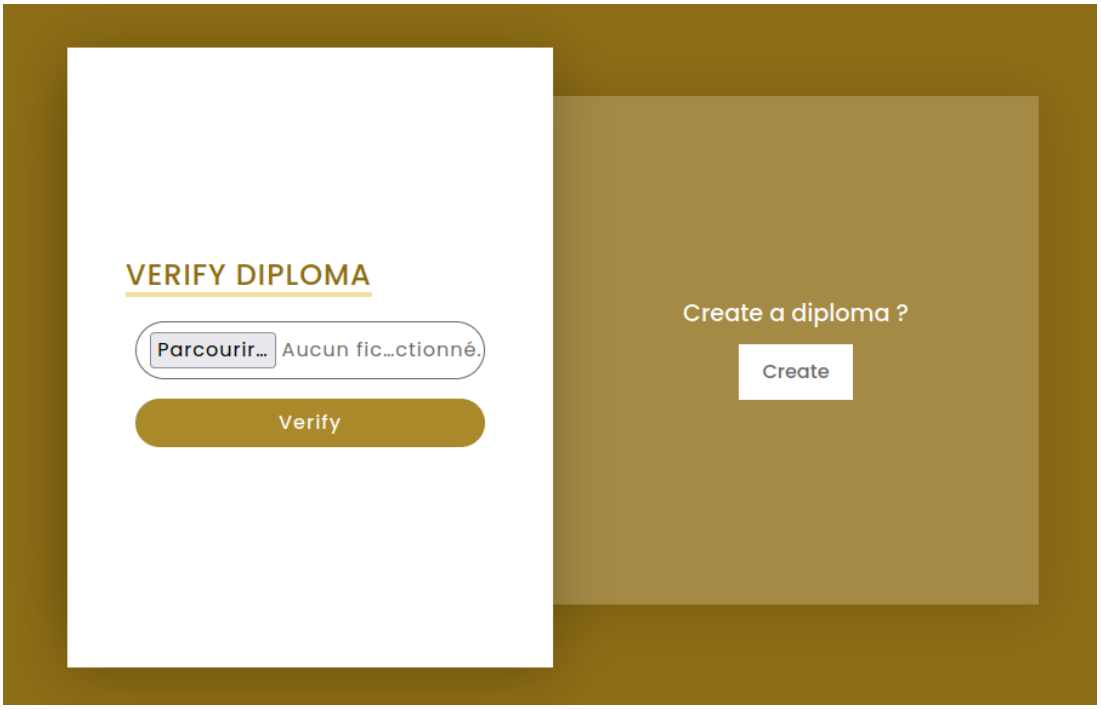
settings_example.py M

webapp > etc > settings_example.py > ...

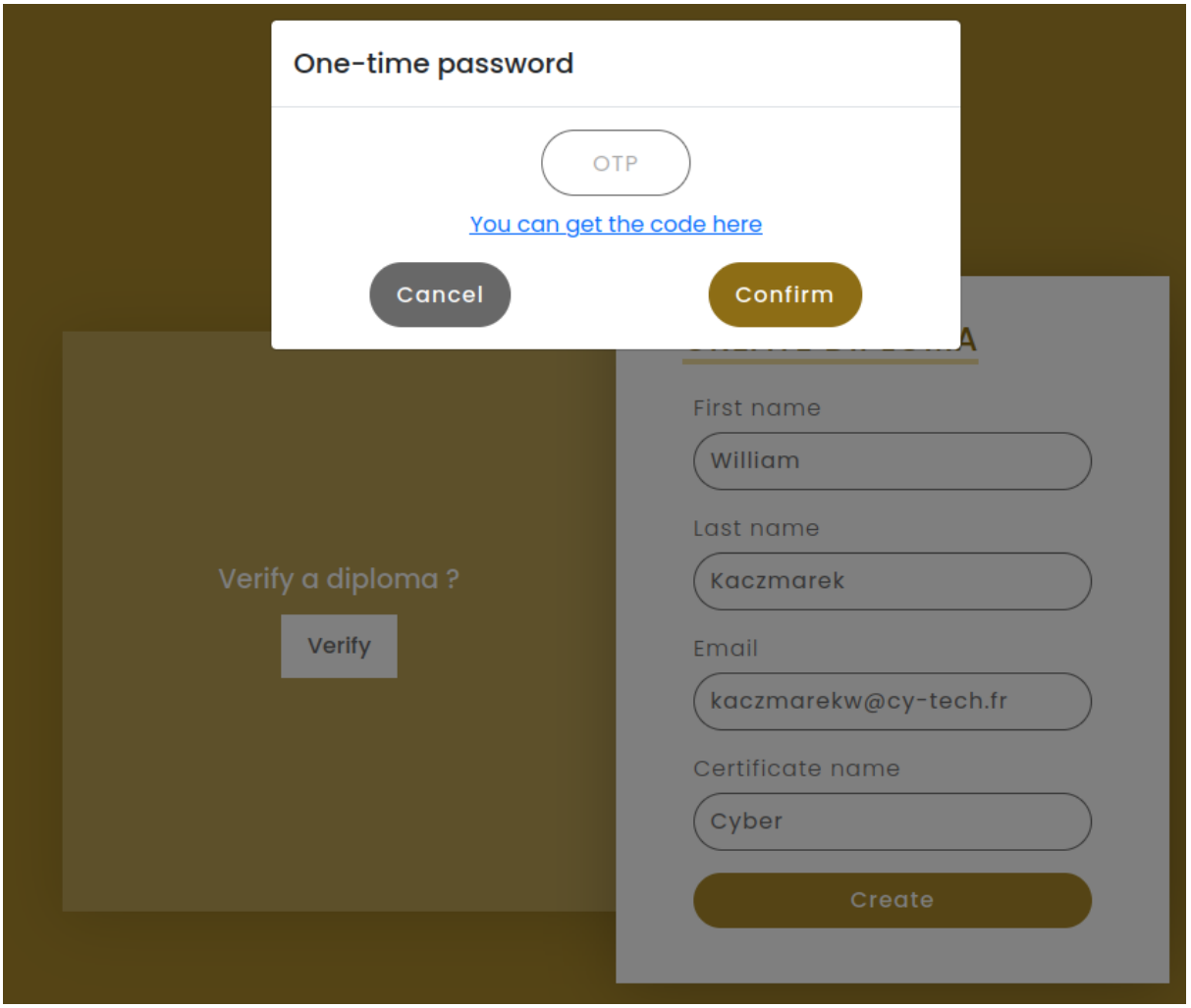
```
CONFIG = {
    'JWT_SECRET_KEY' : "zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz",
    'JWT_EXPIRES_HOURS' : 1,
    'OTP_KEY': "KRUGS4ZANFZSAYJAONSWG4TFOQQGWZLZ",

    'CA_PASSPHRASE' : {
        'EMAIL' : "passphrase",
        'SERVER' : "passphrase"
    },

    'SMTP' :  {
        'SERVER': 'my.host',
        'PORT': 587,
        'USERNAME': 'username.my.host',
        'PASSWORD': 'supersecret'
    }
}
```

2ème étape : lancer avec ***python3 webapp/setup.py*** puis se connecter à l'adresse.
(Penser à installer tous les modules situé dans ***requirements.txt*** si nécessaire et avoir)

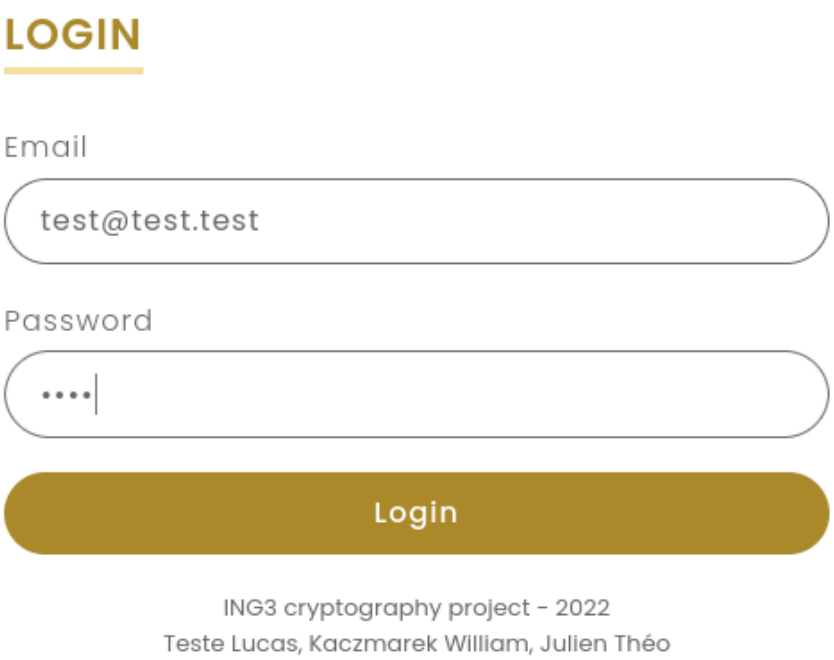
```
cytech@student-laptop:~/Desktop/ing3/diploma-generator$ python3 webapp/setup.py
 * Serving Flask app 'setup'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 130-989-302
```



<u>3ème étape :</u> Générons un diplôme, ici on rentre les informations de la personne diplômé et surtout son adresse mail à laquelle il recevra son diplôme, l'image que nous allons lui générer.

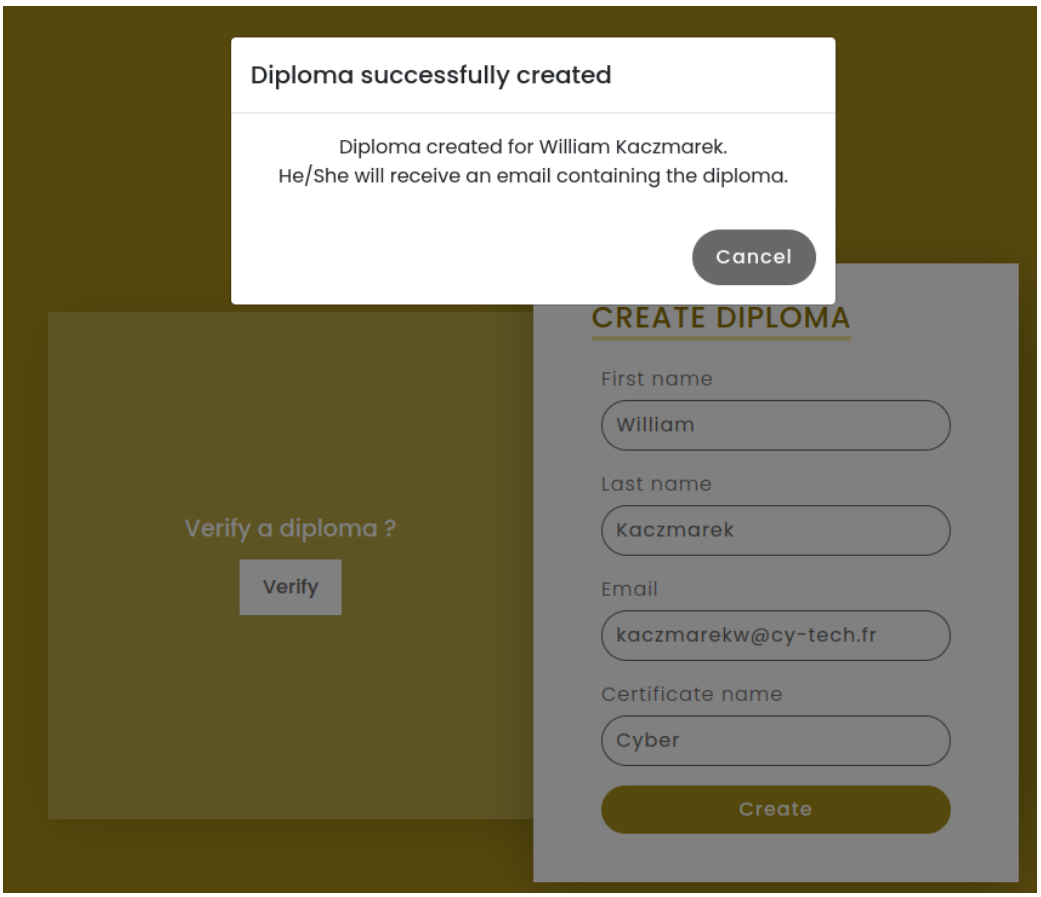


Un pop-up apparaît alors nous invitant à entrer un One-time password, que nous allons générer en cliquant sur le lien bleu.

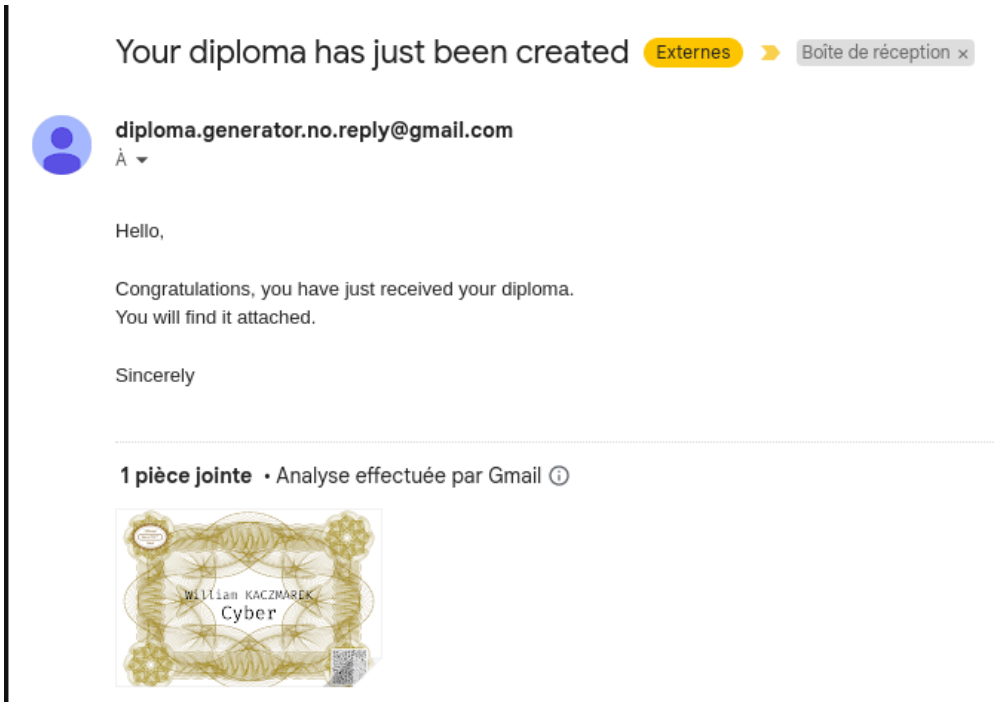


A l'aide des identifiants de connexion ***test@test.test*** et du mot de passe ***test.*** Nous pouvons avoir accès à un mot de passe temporaire qui change toutes les 30s.

En cliquant sur le numéro on le copie et nous pouvons le rentrer sur notre pop-up.

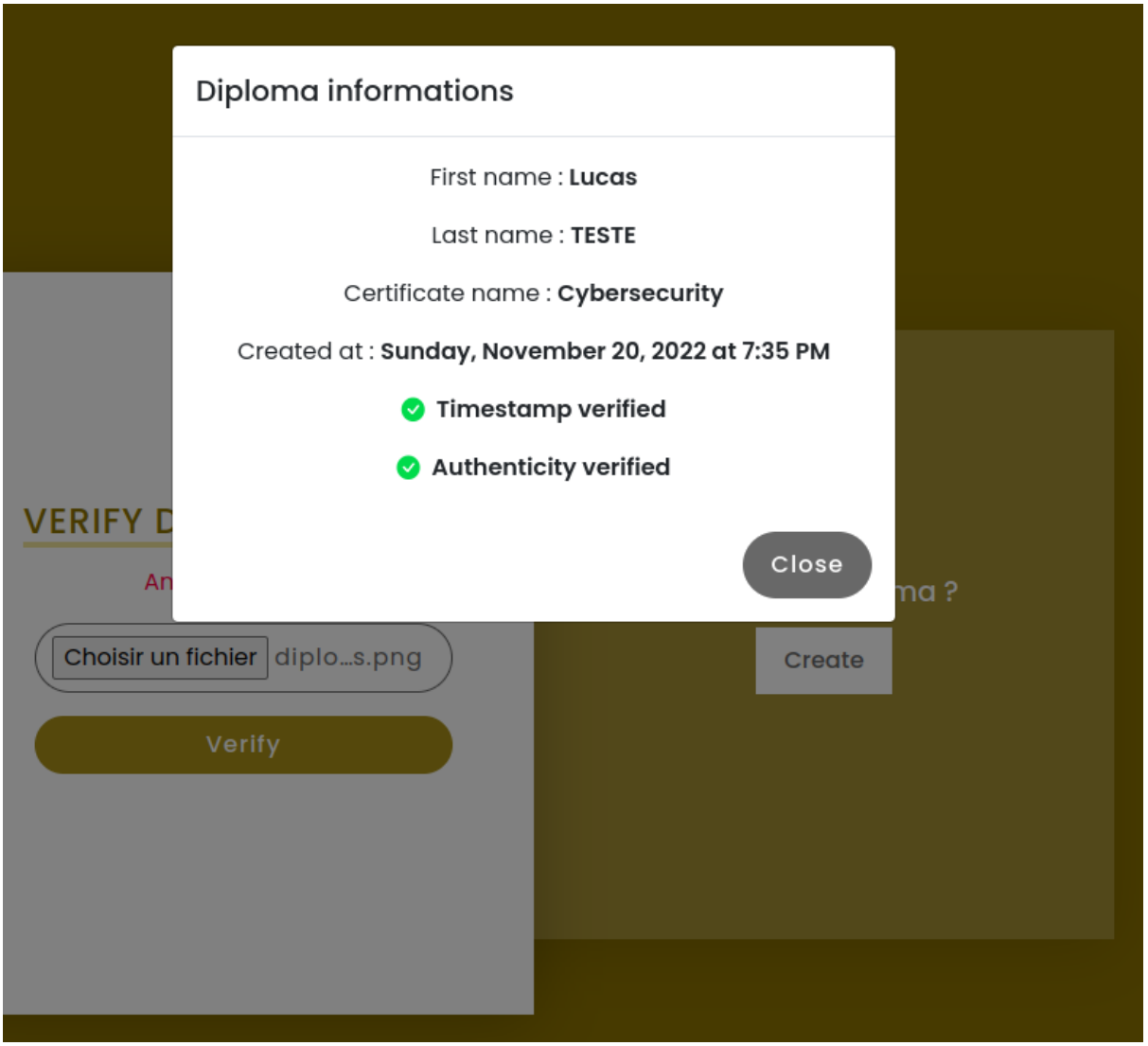


Le diplômé reçoit alors le mail avec en pièce jointe notre image générée.



2.2 Vérification d’un diplôme

Pour vérifier un diplôme/attestation il suffit de cliquer sur choisir un fichier et d’upload l’image que nous voulons vérifier.



3. Fonctionnement de notre programme

3.1 One Time Password

Pour générer un diplôme il faut entrer un mot de passe temporaire, qui change toutes les 30 secondes. Notre algorithme derrière est basé sur celui de Google Authenticator. A partir d'un mot de passe, un "secret" encodé en base 32, nous allons à chaque fois que l'heure de l'appareil est soit à 30s soit à pile générer un nouvel OTP.

Cette page OTP n'est accessible que par l'autorité de délivrance (CY TECH). Il faut donc se connecter pour y avoir accès.
Username: test@test.test
Password: test

3.2 Signature du diplôme et stéganographie

Dès que le formulaire est rempli, nous récupérons les données pour créer une chaîne de 64 bytes de la forme : "prenom;nom;Certif\x00\x00\x00".
En complétant de null byte (\x00) jusqu'à atteindre une taille de 64 bytes. Grâce à ce bloc de 64 bytes, on crée une signature de l'autorité de timestamp grâce a freetsa.org. Qu'on vient concaténer avec notre bloc de 64 bytes.

Ensuite nous générons notre image, avec les informations du diplômé que nous venons inscrire visuellement sur l'image (Nom, prénom, certification). Grâce à notre autorité de certification "serveur", nous venons signer le bloc de 64 bytes, et on rentre ses informations signées dans un QR code.

Une fois le QR code généré, nous l'ajoutons à notre image. Maintenant que l'image ne changera plus, nous pouvons faire l'étape de stéganographie, si nous le faisions avant nous risquions d'écraser par inadvertance nos informations cachés. Nous venons dissimuler le bloc de 64 bytes concaténé au timestamp dans la composante rouge de notre image (PNG).

3.3 Envoi du mail

Notre image maintenant créée et signée, il ne reste plus qu'à l'envoyer par mail à la personne concernée. Pour cela on utilise le format S/MIME, nous allons venir avec openssl et notre l'autorité de certification "Email" signer ce mail.

3.4 Vérification d'un diplôme

Contrairement à la génération précédente, la vérification d'un diplôme peut être faite par n'importe qui. Dans l'image qui est upload nous venons décoder la stéganographie pour en vérifier la signature avec l'autorité de certification Timestamp. Et vérifier la signature du QR code avec l'autorité de certification serveur.