A2
SEGURETAT A LES APLICACIONS

Aitor Sánchez Salgado

DAM2 2024/25

Contingut:

Xifrat d'usuaris

- Implementa la funció encrypt_data per xifrar la informació dels usuaris.(2p)

```
gpg = gnupg.GPG()
def encrypt_data(data, output_file):
    ret = gpg.encrypt(data,recipients="aitorsansal@gmail.com",passphrase="safePassPhrase")
    if(os.path.exists("users.txt")):
        with open(output_file,'a') as file:
            file.write(str(ret)+"////")
    else:
        with open(output_file,'w') as file:
            file.write(str(ret)+"////")
```

- Implementa la funció decrypt_data per desencriptar la informació.(2p)

```
def decrypt_data(input_file):
    lst = []
    if(os.path.exists("users.txt")):
        with open(input_file,'r') as file:
            splited = file.read().split("////")
            for s in splited:
                lst.append(str(gpg.decrypt(s)).strip())
    else:
        print("l'arxiu no existeix")

    return lst
```

- Podràs fer servir qualsevol algorisme de xifrat (simètric o asimètric) amb gnupg, però hauràs de justificar per què has escollit aquest algorisme i per què és adequat per a l'escenari de la pràctica. (1p)

Una manera per a tenir guardada la passPhrase i que no sigui visible, seria tenir-la com a variable d'entorn i que python la demanés a través de la base de dades al servidor on es guarden totes les dades.

Gestió d'usuaris

- Implementa la funció save_user per guardar les credencials dels usuaris en un arxiu, utilitzant xifrat.

```
def save_user(username, password):
    encrypt_data(f"{username};{password}","users.txt")
```

- Implementa la funció verify_user per verificar l'usuari i contrasenya proporcionats durant el procés de login.

```
def verify_user(username, password):
    list = []
    list = decrypt_data("users.txt")
    if list.__contains__(f"{username};{password}"):
        return True
    return False
```

Arxiu d'usuaris

- Implementa un mecanisme per generar un arxiu que emmagatzemi els usuaris registrats de forma segura (xifrat).

L'arxiu generat és un arxiu on es guarden la clau i l'usuari junts estant encriptades. Després, es separen entre elles amb "////" per a poder-les separar i tractar a l'hora de desencriptar-ho després.