ACTIVITAT AVALUABLE AC4

Mòdul: MP02- Bases de dades

UF: UF3: llenguatges SQL: DCL i extensió procedimental

Professor: Albert Guardiola

Data límit d'entrega: 12/03/2023

Mètode d'entrega: Per mitjà del Clickedu de l'assignatura. Les activitats entregades més enllà de la data límit només podran obtenir una nota de 5.

Instruccions:

Les tasques s'han d'entregar totes en un únic document PDF.

Resultats de l'aprenentatge:

RA1. Implanta mètodes de control d'accés utilitzant assistents, eines gràfiques i comandes del llenguatge del sistema gestor de bases de dades corporatiu.

RA2. Desenvolupa procediments emmagatzemats avaluant i utilitzant les sentències del llenguatge incorporat en el sistema gestor de bases de dades corporatiu.

És indispesable documentar correctament totes les passes de l'exercici, amb captures de pantalla, segons convingui.

Tasca 1 (4 punts) Anàlisis d'una situació d'injecció de codi:

a)Fes un fork del següent repositori al teu compte de GitHub. A continuació, clona'l a la teva màquina local.

https://github.com/albertetpx/m02-uf3-ac4.git

b)Fes les següents operacions per poder desplegar l'aplicació web que s'adjunta (*formulario.rar*).

> **-A L'APLICACIÓ FLASK: canvia els paràmetres de connexió a la base de dades (en concret, l'usuari i la contrassenya) perquè pugui connectar al teu servidor MySQL.**
>
> **-AL SERVIDOR MYSQL: crea la base de dades *users*. No cal que creis cap taula; serà creada per la pròpia aplicació web (observa la funció**

c)Executa l'aplicació (*app.py*) i comprova que arrenca sense errors. Obre el navegador a http://localhost:5000, i comprova que:

> **-L'usuari *user01* amb contrassenya *admin* pot fer login correcte i consultar les seves dades.**

Aplicació web amb base de dades (M02-UF3-AC4)

LOGIN CORRECTO

User	Name	Surname 1	Surname 2	Age	Genre
user01	Ramón	Sigüenza	López	35	H

ETPX 2022-2023

-L'usuari *user01* amb contrassenya *1234* fa un login incorrecte.

Aplicació web amb base de dades (M02-UF3-AC4)

LOGIN INCORRECTO

ETPX 2022-2023

d)Prova a autenticar l'usuari *user01* i la contrassenya *' OR 1=1;* (valor exacte).

Aplicació web amb base de dades (M02-UF3-AC4)

LOGIN CORRECTO

User	Name	Surname 1	Surname 2	Age	Genre
user01	Ramón	Sigüenza	López	35	H

ETPX 2022-2023

e)Explica què ocorre, i per què estem davant d'una <u>situació d'injecció de codi.</u>

Usa un código SQL malicioso para manipular la base de datos de backend y acceder a información privada

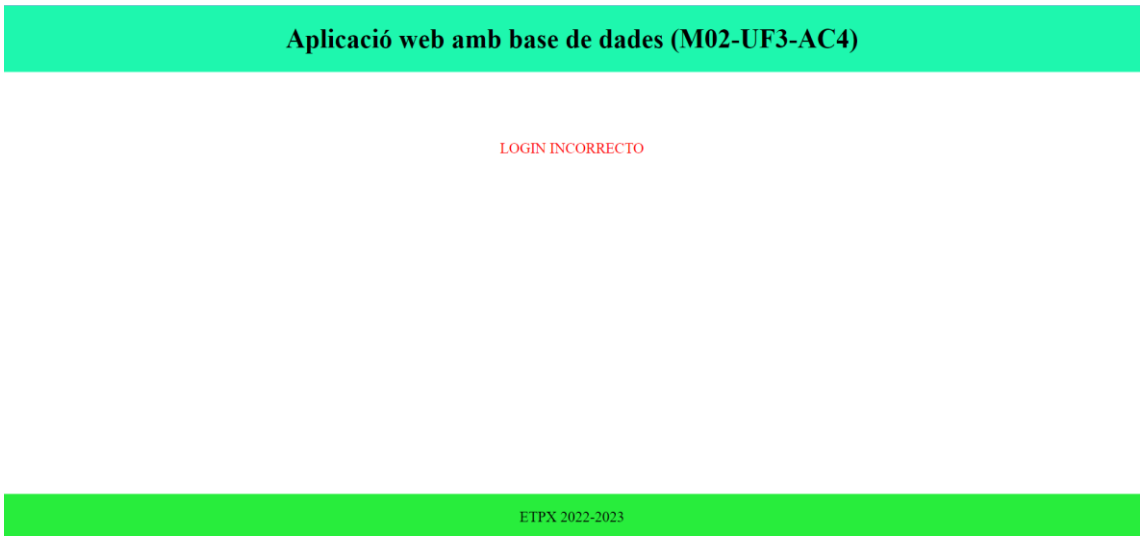
f)Reimplementa la funció *checkUser* perquè faci servir una <u>sentència parametritzada</u> que eviti la situació d'injecció de codi:

Per exemple:

query = """Update employee set Salary = %s where id = %s"""
values = (8000, 5)
cursor.execute(query, values)

```
def checkUser(user, password):
    bd = connectBD()
    cursor = bd.cursor()
    query = f"""SELECT user,name,surname1,surname2,age,genre FROM users WHERE user=%s\
            AND password=%s"""
    params = (user, password)
    cursor.execute(query, params)
    userData = cursor.fetchall()
    bd.close()
    if userData == []:
        return False
    else:
        return userData[0]
```

g)Comprova que, ara, el formulari de login ja no és vulnerable a la injecció de codi.



h)Explica per què la instrucció parametritzada resol la vulnerabilitat.

Se que con %s se cancela ese error pero no se donde ejecutralo.

Tasca 2 (6 punts). Completa l'aplicació web amb la funcionalitat de poder crear nous usuaris:

a)Crea una altra plantilla (*signin.html*), seguint l'estructura de *login.html*. Aquesta pàgina haurà de contenir un formulari de registre d'usuari, en que es pugui donar d'alta un usuari amb: nom d'usuari, contrassenya, nom, cognom1, cognom2, edat i salari.

Aqui el codigo añadido:

```
<main>
    <form action="{{url_for('results')}}" method="POST" class="formulario">
        <h2>Log in to application</h2>
        <input type="text" name="usuario" placeholder="login" />
        <input type="text" name="contrasena" placeholder="contraseña" />
        <input type="text" name="nombre" id="nombre">
        <input type="text" name="cognom1" placeholder="cognom1">
        <input type="text" name="cognom2" placeholder="cognom2">
        <input type="number" name="edad" placeholder="edad">
        <input type="submit" value="Enviar">
    </form>
```

b)Modifica la ruta *"/signin"* a l'aplicació flask per a que mostri la plantilla *signin.html* que acabes de crear.

```
@app.route("/signin")
def signin():
    return render_template("signin.html")
```

c)Crea una nova ruta ("/newUser") a l'aplicació flask per a rebre i processar les dades del formulari de registre. T'hauràs d'inspirar en la ruta *"/results"* ja existent. Des d'aquesta ruta, crida la funció *createUser*.7epi

```
@app.route("/newUser",methods=('GET', 'POST'))
def newUser():
    if request.method == ('POST'):
        formData = request.form
        user=formData['usuario']
        password=formData['contrasena']
        name=formData['nombre']
        surname1=formData['apellido1']
        surname2=formData['apellido2']
        age=formData['edad']
        genre=formData['salario']

        userData = createUser(user,password,name,surname1,surname2,age,

        if userData == False:
            return render_template("home.html")
        else:
            return render_template("results.html")
```

d)Associa l'acció del formulari de registre (atribut *action*) a la nova ruta que acabes de crear. Observa com es fa en el formulari de login.

d)Implementa la funció *createUser* perquè s'escriguin les dades del nou usuari en la base de dades. Utilitza sentencies parametritzades.

```
def createUser(user,password,name,surname1,surname2,age,genre):
    bd = connectBD()
    cursor = bd.cursor()
    query_1 = "insert into users (user,password,name,surname1,surname2,
    val_1 = user, password, name, surname1, surname2, age, genre
    cursor.execute(query_1, val_1)
    nuevoUsuario = cursor.rowcount
    bd.commit()
    bd.close()
    return nuevoUsuario
```

e)Comprova el correcte funcionament de l'aplicació.

f)Puja el codi complet de l'aplicació a un repositori del teu compte de GitHub i inclou l'enllaç en el PDF que entreguis.