Cyber Défense des infrastructures.

Date de début : 10/12/2022

Entreprise : POWERZIO

Nom de l’équipe : “C'est down ou quoi?”

INJECTIONS SQL

Fichier : server.py

```
84              req = "SELECT * FROM users WHERE email='"+login+"' AND password='"+md5(password)+"'"
85              out = sql_exec(req)
```

=> L'utilisation de la concaténation est un problème car l'attaquant peut manipuler les valeurs à remplir à sa guise, résultant ainsi à une manipulation de la database.

L'utilisateur peut se connecter sans avoir de compte en mettant uniquement des guillements "' '" à n'importe quel login et mot de passe qu'il saisira.

Sans oublier les "print" des données sensibles.

```
129 if request.form.get('pin'):
130     user = None
131     user = jwt.decode(request.cookies.get('mb_session_id'), JWT_SECRET, algorithms=['HS256'])
132     print(request.form.get('pin'))
```

```
137             req1 = f"UPDATE users SET account_sum = account_sum + {request.form.get('sum')} WHERE account_number='{request.form.get('recipient')
138             print(req1)
139             out1 = sql_exec(req1)
140             print(out1)
141             req2 = f"UPDATE users SET account_sum = account_sum - {request.form.get('sum')} WHERE account_number='{str(user['account_number'])}'
142             print(req2)
143             out2 = sql_exec(req2)
144             print(out2)
145             if out1 is None and out2 is None:
146                 req = "SELECT * FROM users WHERE email='"+user['email']+"'"
147                 out = sql_exec(req)
148                 print(out)
```

INJECTIONS HTML

```
1   <form action="/api/login" method="POST" class="login-form">
2       <h3>Connect to your account</h3>
```

Dans **login.html,** on a ici une injection “POST reflété”. Un attaquant peut vérifier le code source du formulaire de connexion et trouver la méthode utilisée.
On a également la même vulnérabilité dans **register.html** et **transfer.html**, démontrée ci-dessous.

```
1   <form action="/api/register" method="POST" class="login-form">
2       <h3>Open a bank account</h3>
3
```

```
1   <form action="/api/transfer" method="POST" class="login-form">
2       <h3>Logged in as {{user['first_name']}} {{user['last_name']}}</h3>
3       <h3>Transfer money to a bank account</h3>
```