PHARMANET

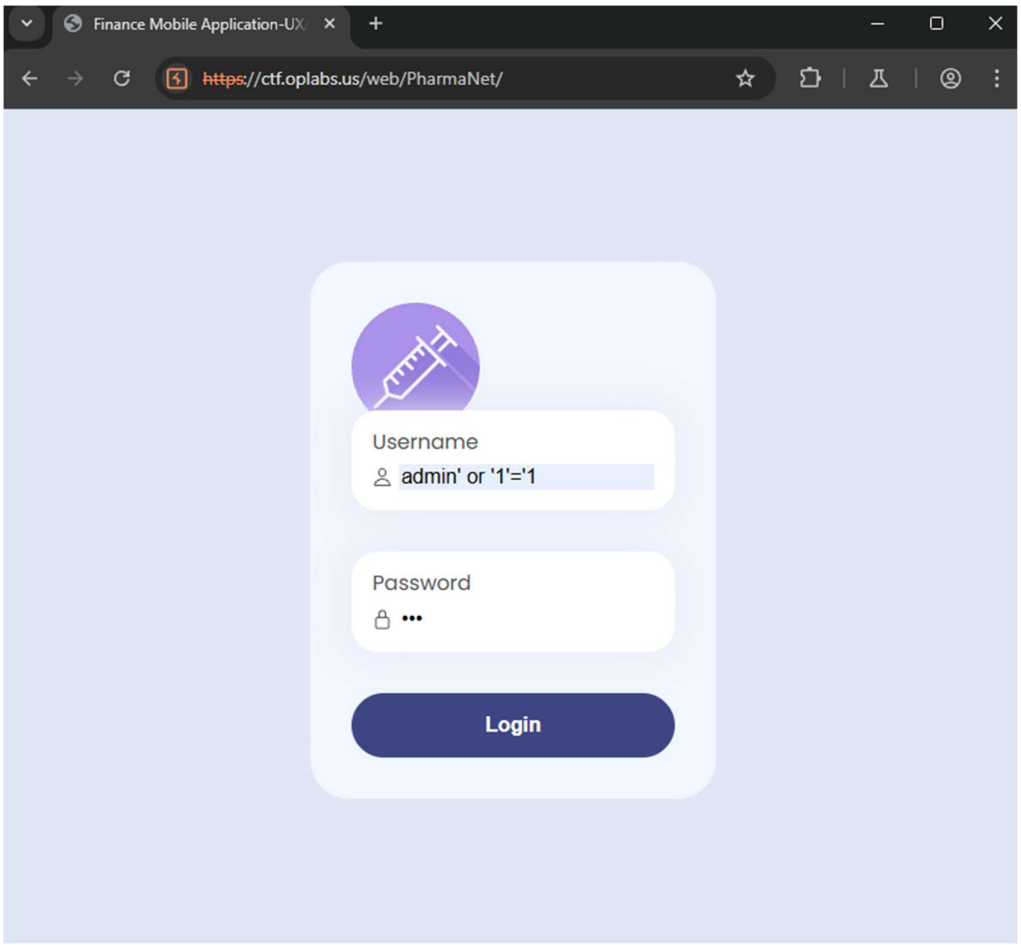
Description
Null

This time it’s a common SQL injection. Starting with a basic payload of sql injection. (Can refer my favorite cheat sheet: PayloadsAllTheThings/SQL Injection/README.md at master · swisskyrepo/PayloadsAllTheThings · GitHub)
SQL injection happens because of improper handling of user inputs within SQL queries. It occurs when user-supplied data is directly inserted into SQL statements without proper validation or sanitization, allowing attackers to manipulate the query structure.
Example Before:

```
SELECT * FROM users WHERE username = 'admin' AND password = 'password';
```

Example After:

```
SELECT * FROM users WHERE username = 'admin' or '1'='1' AND password = 'password';
```



Payload:

```
admin’ or ‘1’=’1
```

Flag	STOUTCTF{znjxwDeeXo1jNIz6JLyK77qOTyD2OVOh}