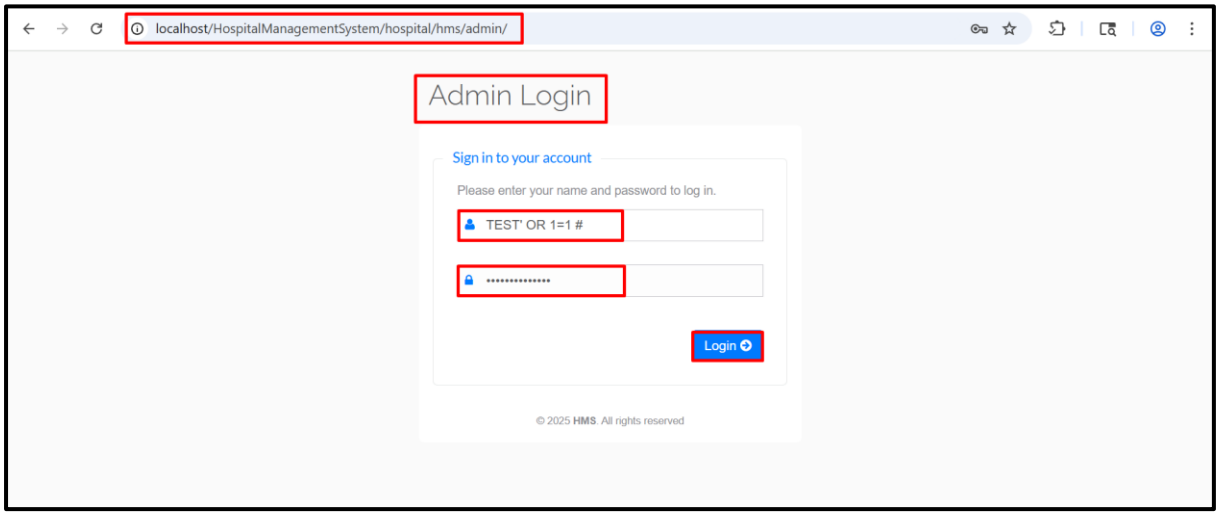
1. Authentication Bypass

Software Name: Hospital Management System
Download Link: *https://www.campcodes.com/downloads/complete-online-hospital-management-system-using-php-and-mysql-source-code/*

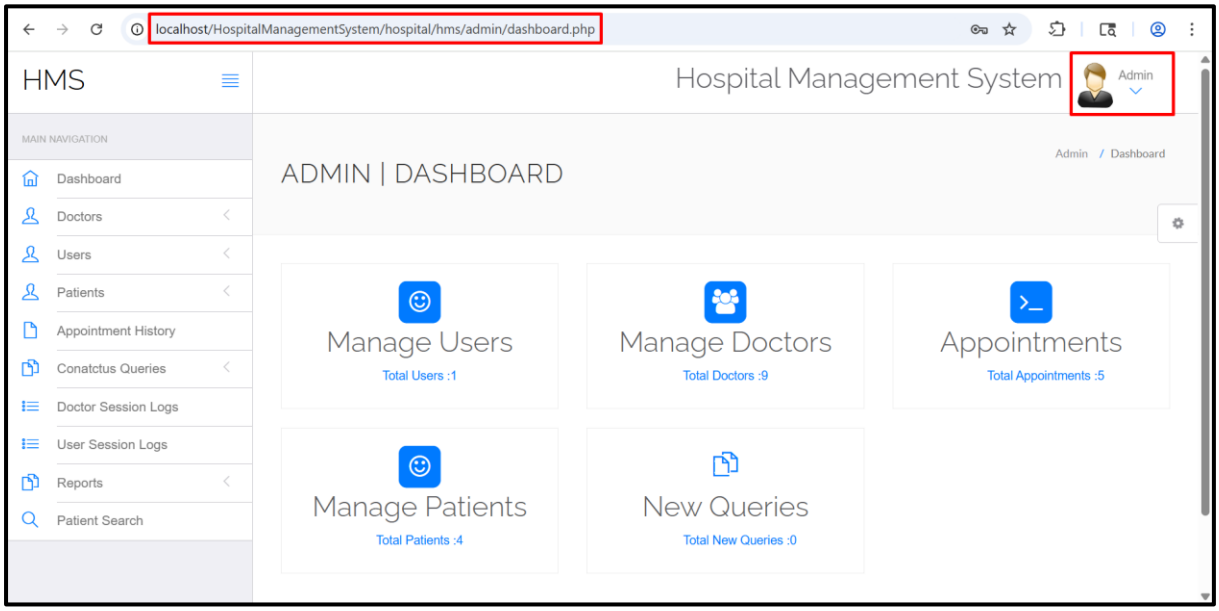
Observation:
The login module of the application is vulnerable to SQL Injection. By using the payload Test' OR 1=1 # in both the username and password fields, we were able to bypass the authentication mechanism successfully. This indicates that user input is directly concatenated into SQL queries without proper sanitization, allowing unauthorized access to the application without valid credentials.

POC(s):
Step 1: Access the URL and click on the "Click Here" button under Admin login, as shown in the screenshot.

Step 2: Enter the following payload into "username" and "password" parameters and click on the login button, as shown in the screenshot below.
Payload: *TEST' OR 1=1 #*



Step 3: It can be observed that the application does not properly validate user input in the authentication process. Using the payload Test' OR 1=1 # in the username and password fields, I was able to bypass authentication and gain unauthorized access, as shown in the screenshot below.



Remediation:

- Use parameterized queries / prepared statements
- Validate and sanitize all user inputs
- Avoid dynamic SQL in authentication
- Implement MFA for stronger auth
- Apply least-privilege to DB accounts