Author Name : Mayur Salve

9823323362

Bug Report 1

Title: **SQL Injection Vulnerability in Login Interface**
Description:
The login interface is vulnerable to SQL injection attacks, allowing unauthorized access to the system.

Steps to Reproduce:

1. Navigate to the login page.
2. In the **Username** field, enter: ' OR 1=1 --
3. Enter any text in the **Password** field.
4.

Click **Login**.

Expected Result:

- Error message: "Invalid username or password."

Actual Result:

- User is logged in without valid credentials.

Severity: Critical
Priority: High
Environment:

- Browser: Chrome v115
- OS: Windows 11

Attachments:

- Screenshot of SQL payload input.
- Log snippet showing unauthorized access.

Bug Report 2

Title: **Duplicate MRN Allowed in Add Patient Form**
Description:
The system accepts duplicate Medical Record Numbers (MRN), leading to data integrity issues.

Steps to Reproduce:

1. Log in to the system.

2. Navigate to **Add Patient**.

3. Enter an existing MRN (e.g., 1001).

4. Fill in other mandatory fields.

5. Click **Submit**.

Expected Result:

- Error message: "MRN must be unique."

Actual Result:

- Patient is added with a duplicate MRN.

Severity: High
Priority: High
Environment:

- Browser: Firefox v120
- OS: macOS Sonoma

Attachments:

- Screenshot of duplicate MRN submission.
- Database query result showing duplicate entries.

Bug Report 3

Title: **Password Field Not Masked in Login Interface**
Description:
The password field displays plain text instead of masking characters (e.g., •••••), exposing sensitive information.

Steps to Reproduce:

1. Navigate to the login page.
2. Click on the **Password** field.
3. Type any text (e.g., Password123).

Expected Result:

- Password characters are masked (e.g., •••••••••).

Actual Result:

- Password is visible in plain text.

Severity: High
Priority: High
Environment:

- Browser: Safari v16
- OS: iOS 17

Attachments:

- Screenshot of unmasked password field.
- Video recording of the issue.