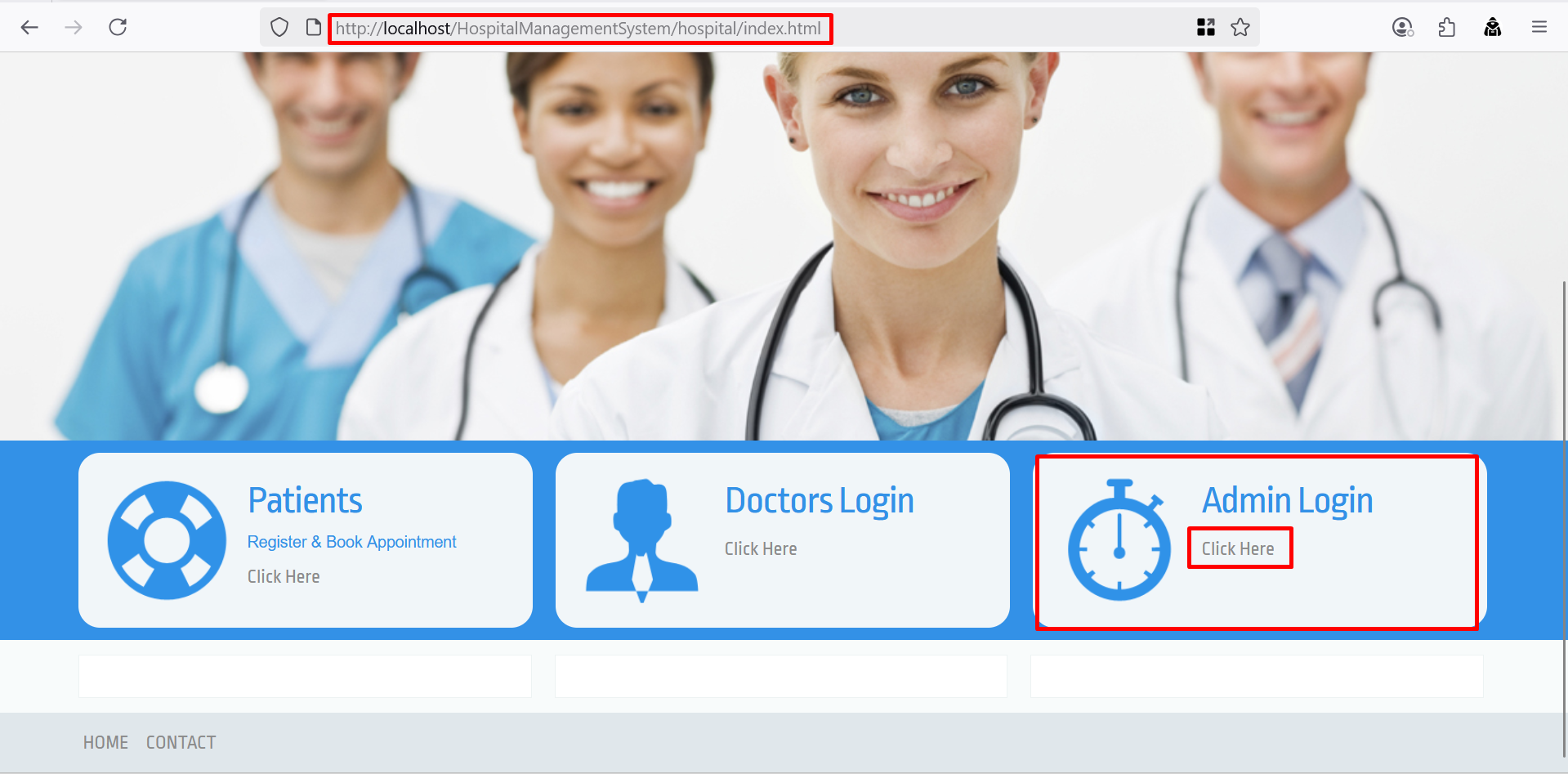
## Stored Cross-Site Scripting

**Software Name:** Hospital Management System

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

**POC(s):**

**Step 1:** Access the URL and log in as an admin, as shown in the screenshot.



**A screenshot of a login page

AI-generated content may be incorrect.**

**Step 2:** After successfully logging in, click on “Doctors” and then select “Doctor Specialization,” as shown in the screenshot below.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3:** Click the edit icon under the “Action” column, as shown in the screenshot below.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 4:** Enter the following payload into the “Edit Doctor Specialization” field and click the “Update” button, as shown in the screenshot below.

**Payload:** “*<img src=x onerror=confirm(document.cookie)>*”

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 5:** After successfully updating the doctor specialization, click on “Doctors” and then select “Doctor Specialization.” It can be observed that the payload executes successfully, indicating that the application does not properly sanitize user input, resulting in Stored Cross-Site Scripting (XSS).

*A screenshot of a computer

AI-generated content may be incorrect.*

*A screenshot of a computer

AI-generated content may be incorrect.*