

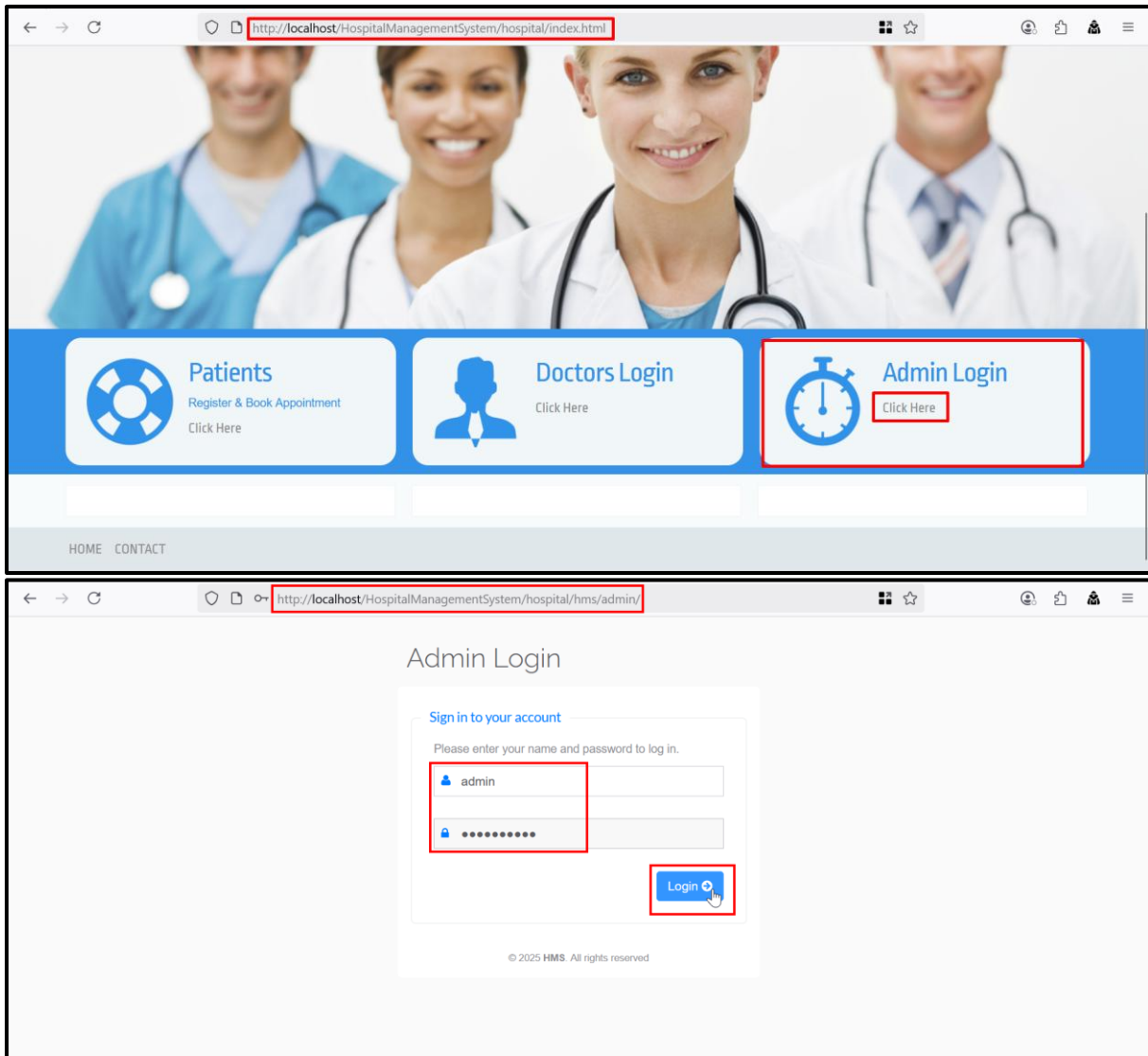
## 1. Stored Cross-Site Scripting

**Software Name:** Hospital Management System

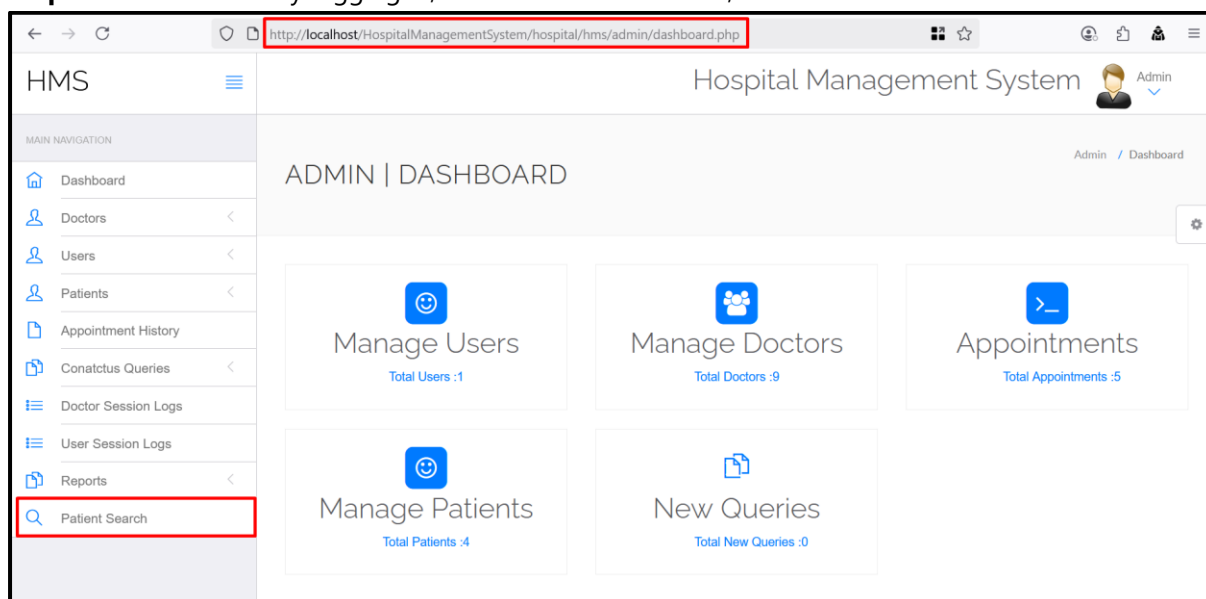
**Download Link:** <https://www.campcodes.com/downloads/complete-online-hospital-management-system-using-php-and-mysql-source-code/>

**POC(s):**

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

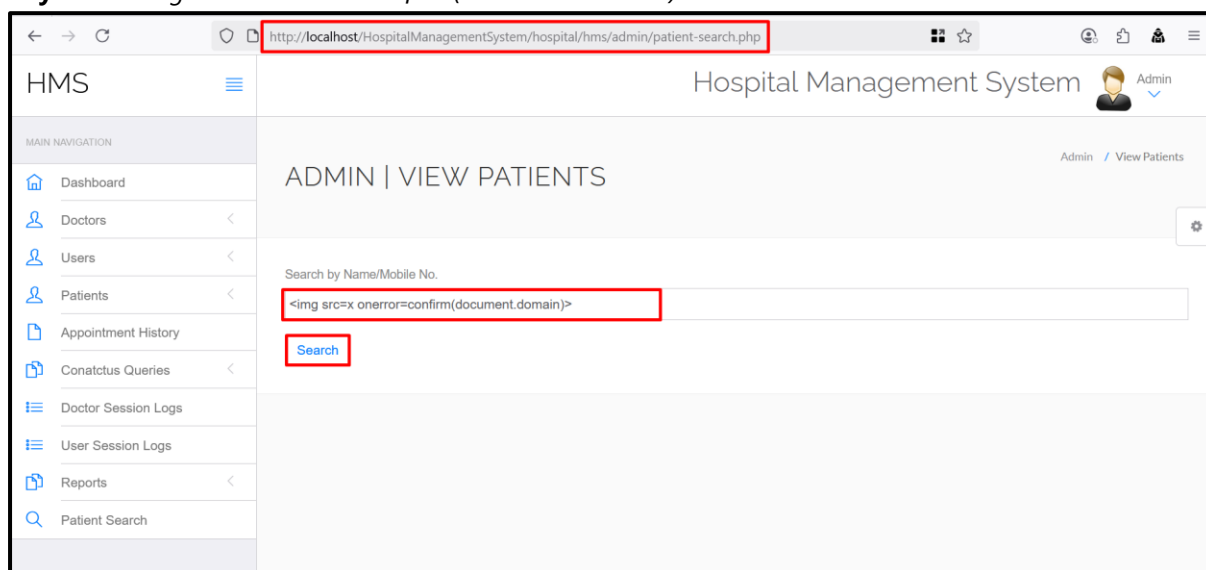


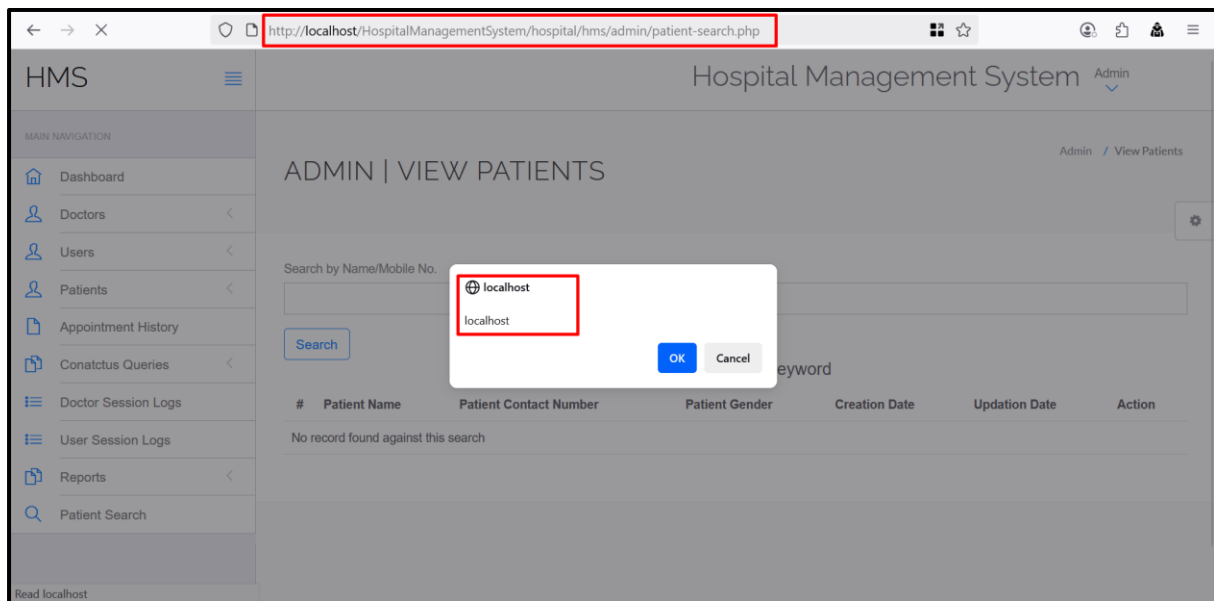
**Step 2:** After successfully logging in, click on “Patient Search”, as shown in the screenshot below.



**Step 3:** Enter the following payload into the “Search by Name/Mobile No” field and hit search button, as shown in the screenshot below. It can be observed that the payload executes successfully, indicating that the application does not properly sanitize user input.

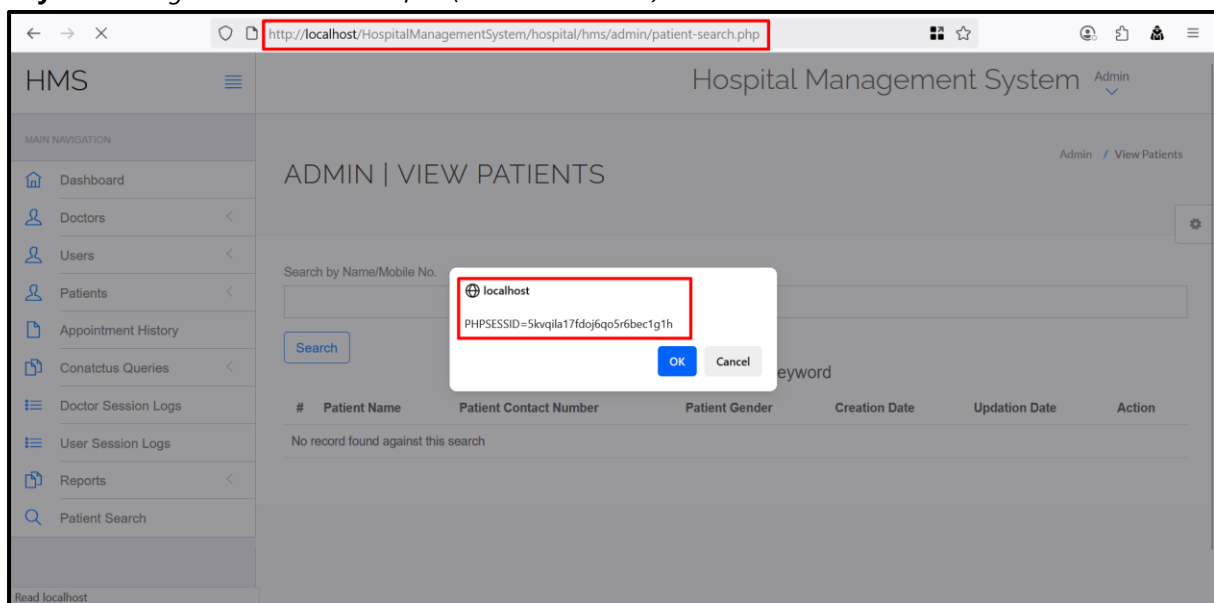
**Payload:** `<img src=x onerror=confirm(document.domain)>`





For the screenshot below, we have used the following payload:

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



### Remediation:

Implement proper input validation and output encoding for user-supplied data in the search field. Escape special characters (<, >, ", ', etc.) before rendering on the page. Use frameworks/libraries with built-in XSS protection and apply Content Security Policy (CSP) to reduce XSS impact.