

Stored Cross-Site Scripting (XSS) vulnerability was found in the /lms/admin/department.php page of the KASHIPARA E-learning Management System project v1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the d and pi parameter in a POST HTTP request.

➤ **Official Website URL**

<https://www.kashipara.com/project/php/13138/e-learning-management-system-php-project-source-code>

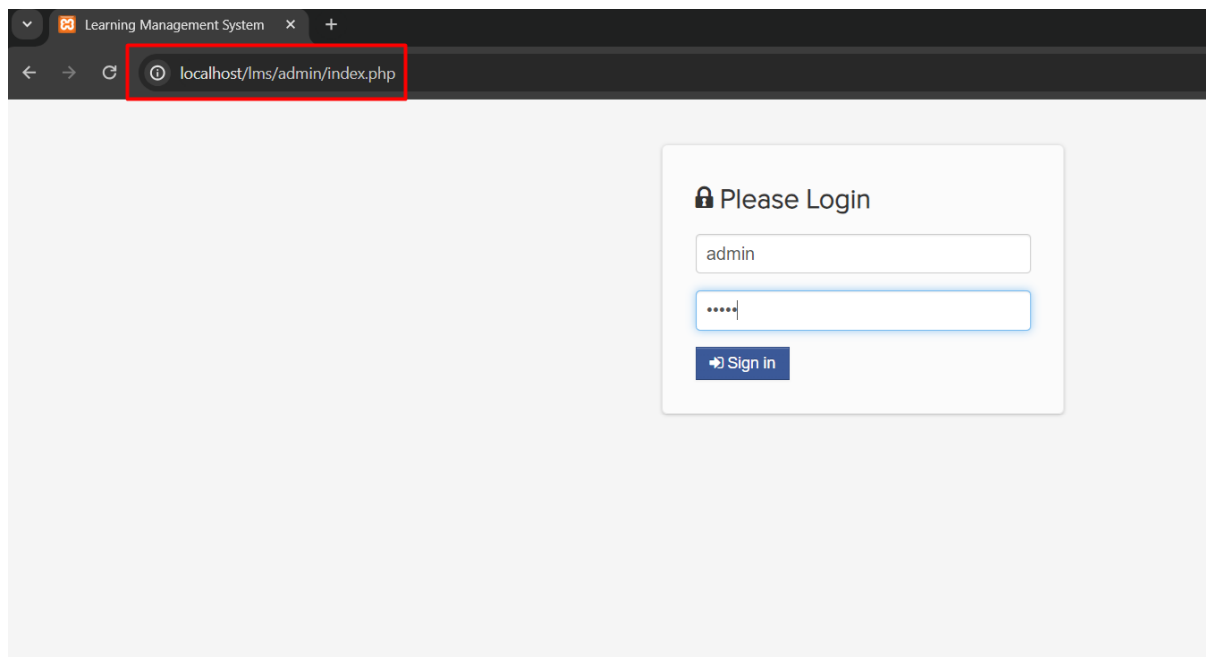
➤ **Affected Product Name**

E-learning Management System project in PHP with source code and document

Affected Vendor	kashipara
Affected Code File	/lms/admin/department.php
Affected Parameter	d, pi
Method	POST
Type	Stored Cross Site Scripting
Version	V1.0

Steps to Reproduce:

Step 1: Navigate admin login page and login with admin user credential at <http://localhost/lms/admin/index.php>



Step 2: Navigate the 'Department' page and fill the payloads `<script>alert(5)</script>` in the fields.

The screenshot shows the 'M - Learning ADMIN Panel' interface. On the left is a sidebar menu with options: Dashboard, Subject, Class, Admin Users, Department (highlighted), Students, Teachers, Downloadable Materials, Uploaded Assignments, Content, User Log, Activity Log, School Year, and Calendar of Events. The main content area is divided into two panels. The left panel, titled 'Add Department', contains two text input fields, both of which are highlighted with a red rectangle and contain the payload `<script>alert(5)</script>` and `<script>alert(6)</script>` respectively. Below the fields is a blue button with a plus icon. The right panel, titled 'Department List', shows a table with columns 'DEPARTMENT' and 'PERSON IN-CHARGE'. It lists four departments: 'Dr. Antonio Deraja' (College of Industrial Technology), 'School of Arts and Science' (DR.), 'College of Education' (null), and 'Sample Department' (DR. John Smith). Each row has a green edit icon. The table is paginated, showing 1 to 4 of 4 entries. The bottom right corner of the page says 'Programmed by: @lopalopa2007'.

localhost/lms/admin/department.php

M - Learning ADMIN Panel

admin admin

Dashboard

Subject

Class

Admin Users

Department

Students

Teachers

Downloadable Materials

Uploaded Assignments

Content

User Log

Activity Log

School Year

Calendar of Events

Add Department

`<script>alert(5)</script>`

`<script>alert(6)</script>`

Department List

10 records per page

Search:

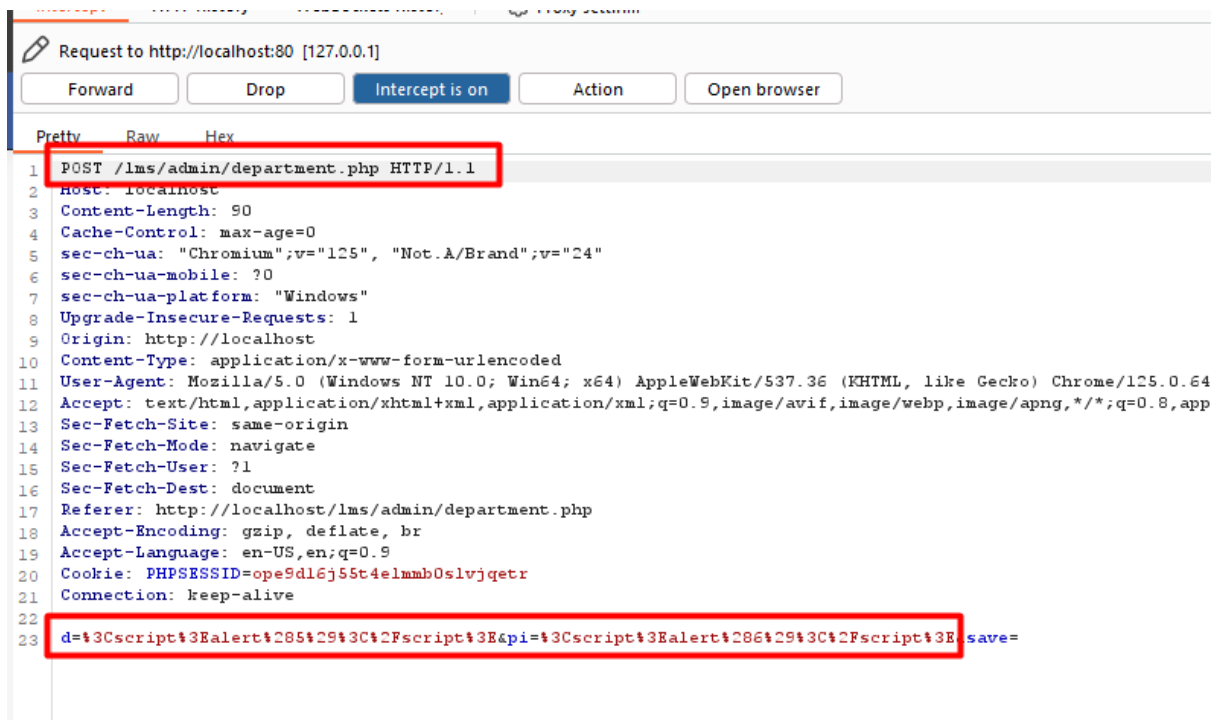
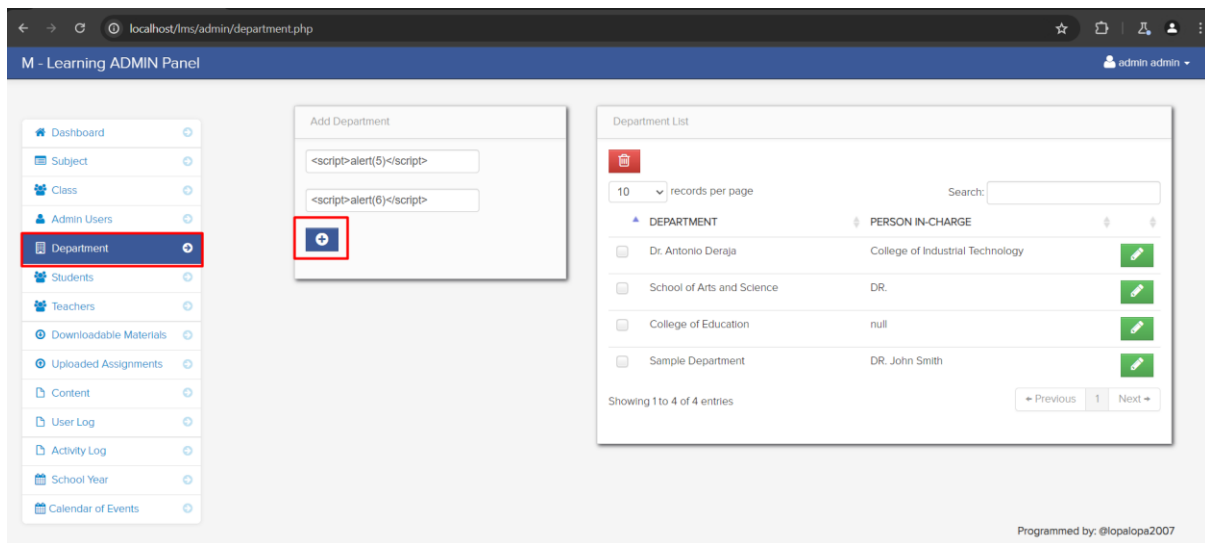
DEPARTMENT	PERSON IN-CHARGE	
Dr. Antonio Deraja	College of Industrial Technology	
School of Arts and Science	DR.	
College of Education	null	
Sample Department	DR. John Smith	

Showing 1 to 4 of 4 entries

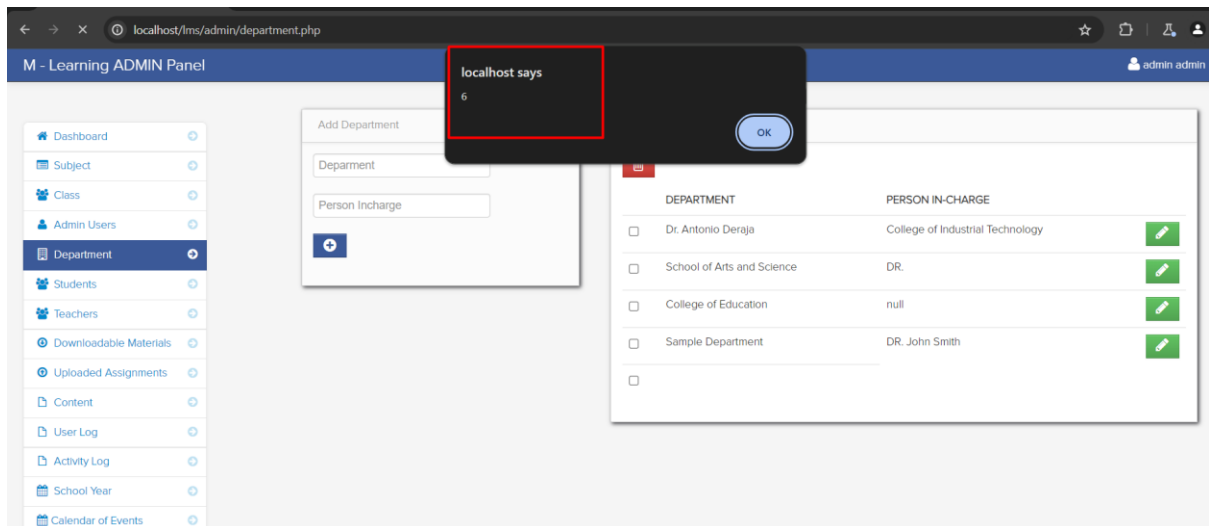
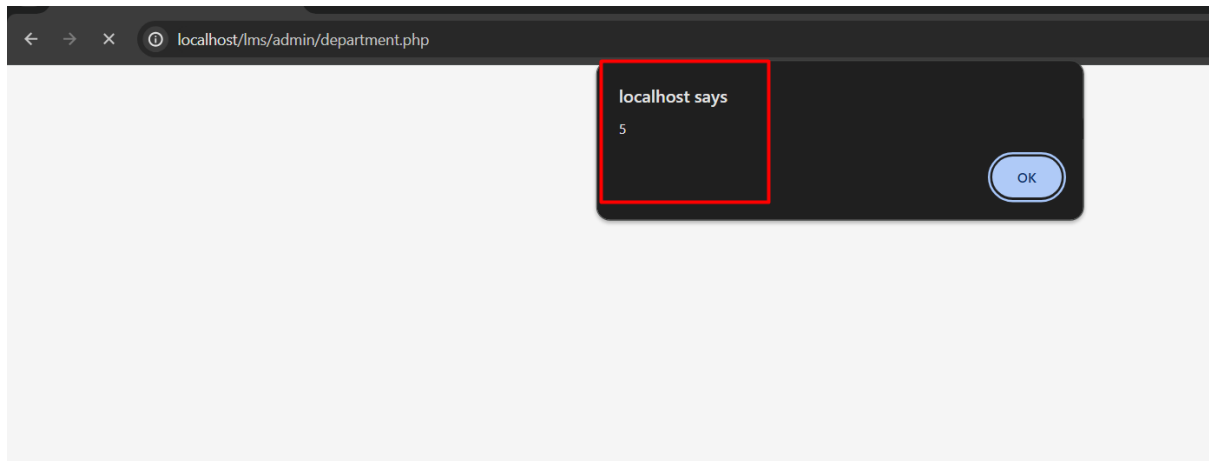
Previous 1 Next

Programmed by: @lopalopa2007

Step 3: After filling fields with payloads `<script>alert(5)</script>` click on add button.



Step 4: Now notice the given XSS payload executed and stored on web server.



Mitigation/recommendations

- <https://portswigger.net/web-security/cross-site-scripting>
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html