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

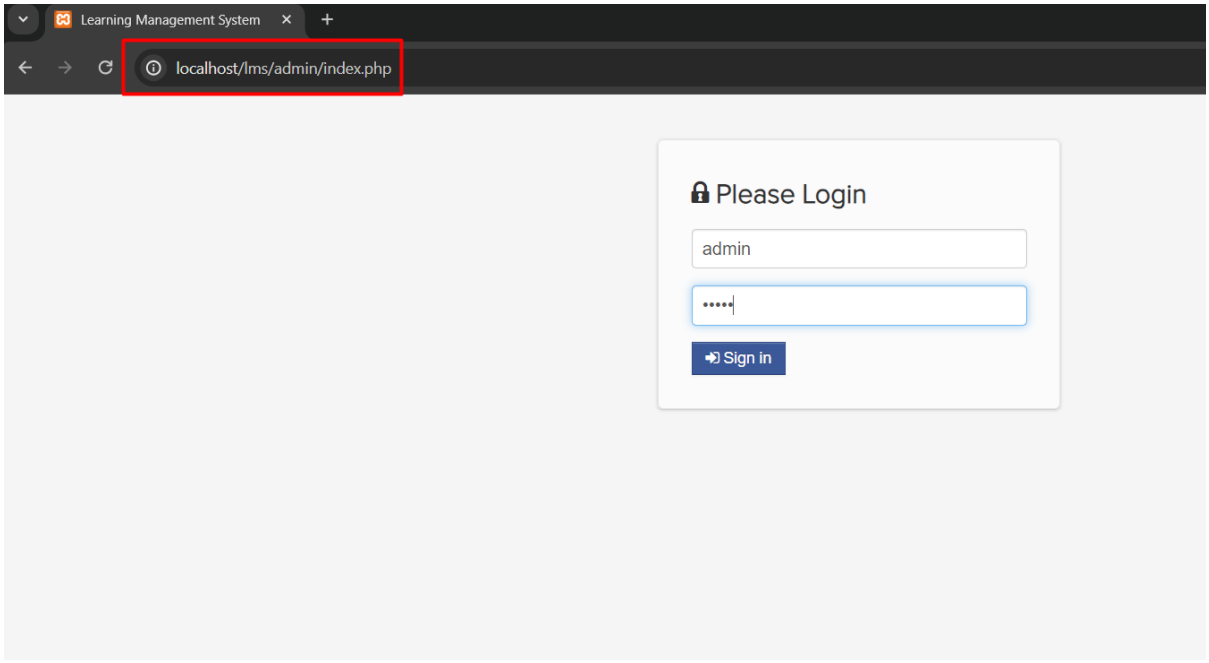
- **Affected Product Name**

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

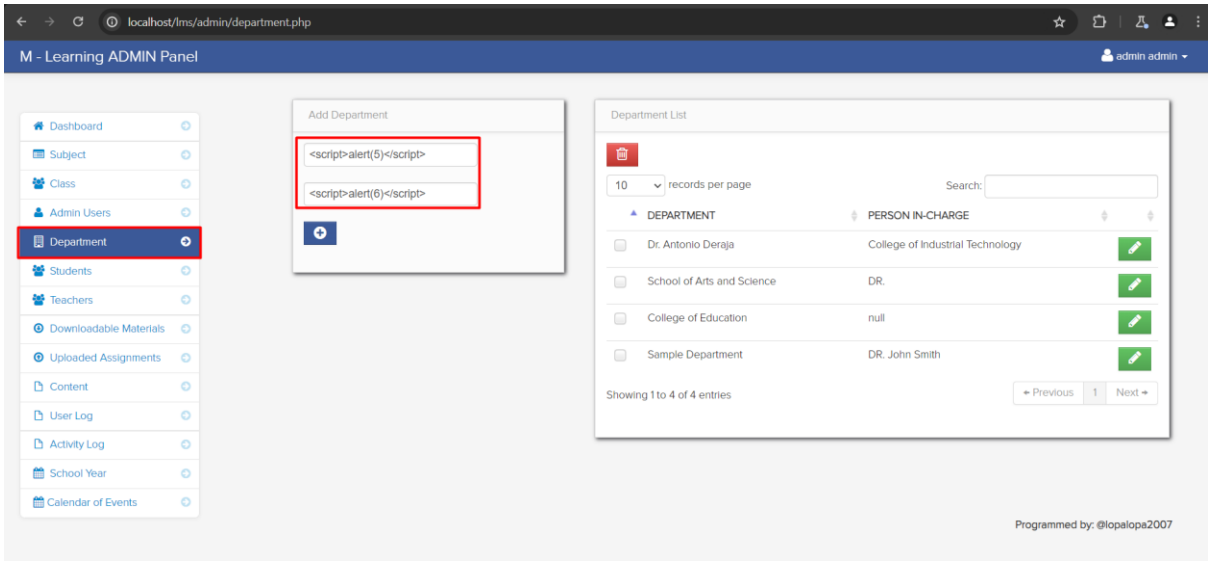
Affected Vendor	kashipara
Affected Code File	/lms/admin/department.php
Affected Parameter	d, pi
Method	POST
Type	Stored Cross Site Scripting
Version	V1.0

Steps to Reproduce:

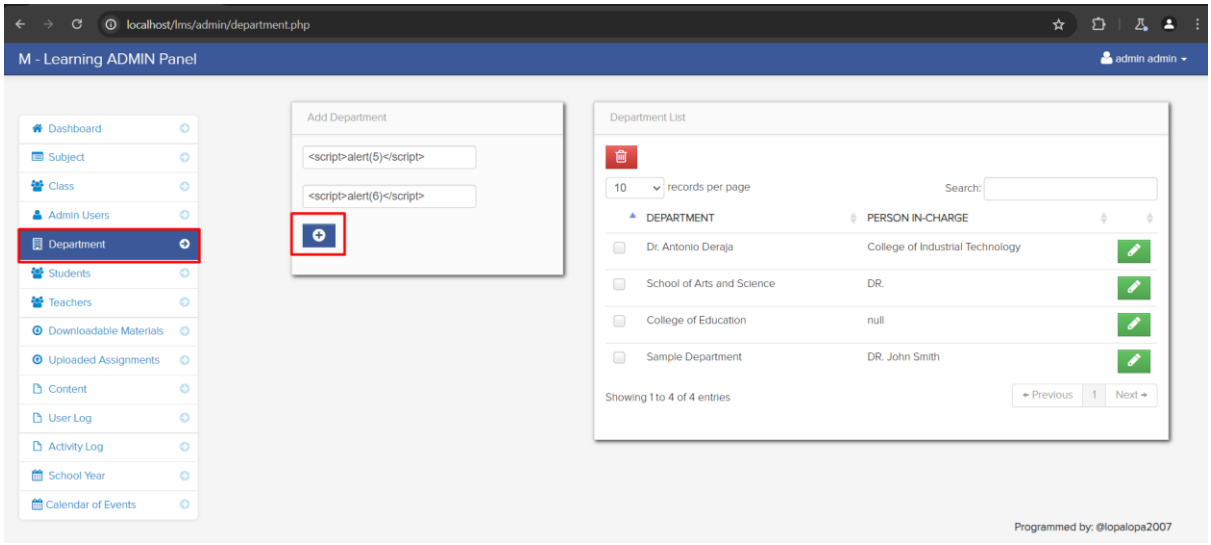
Step 1: Navigate admin login page and login with admin user credential at http://localhost/lms/admin/index.php

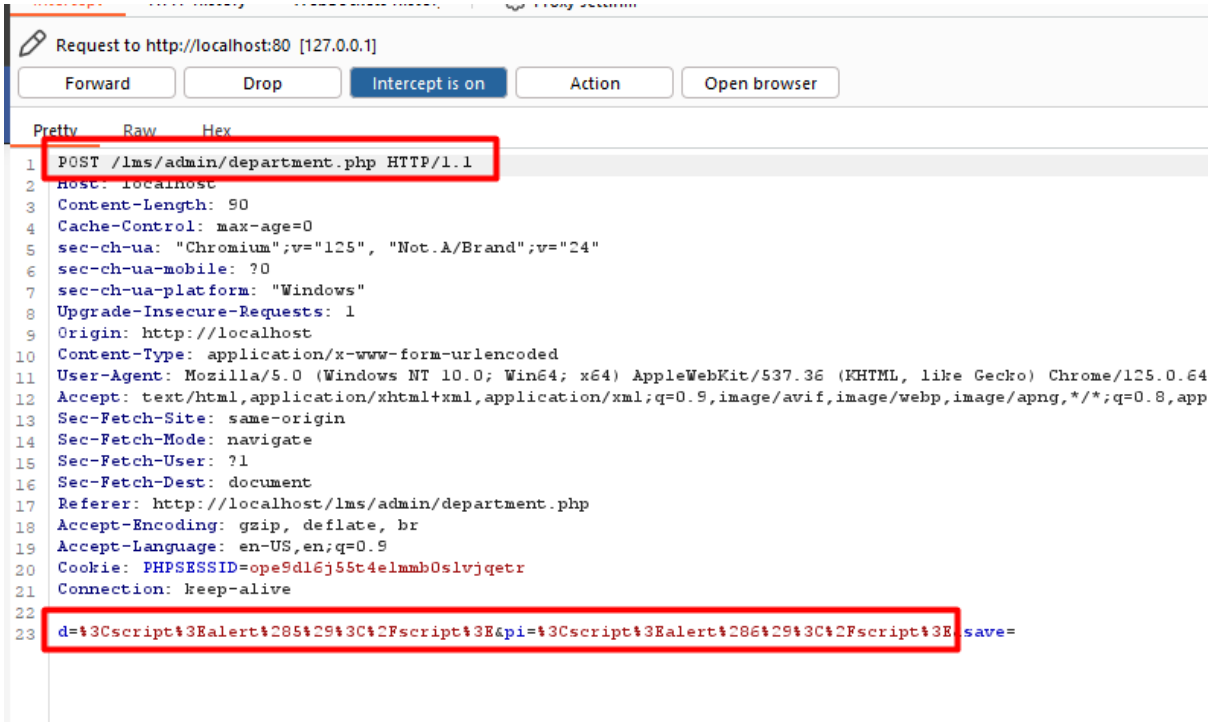


Step 2: Navigate the ‘Department’ page and fill the payloads <script>alert(5)</script> in the fields.

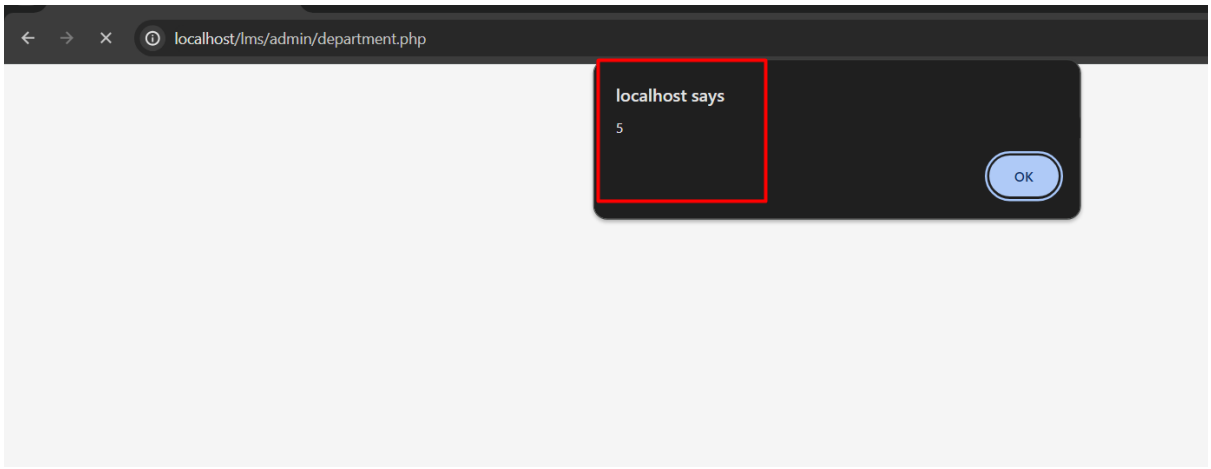


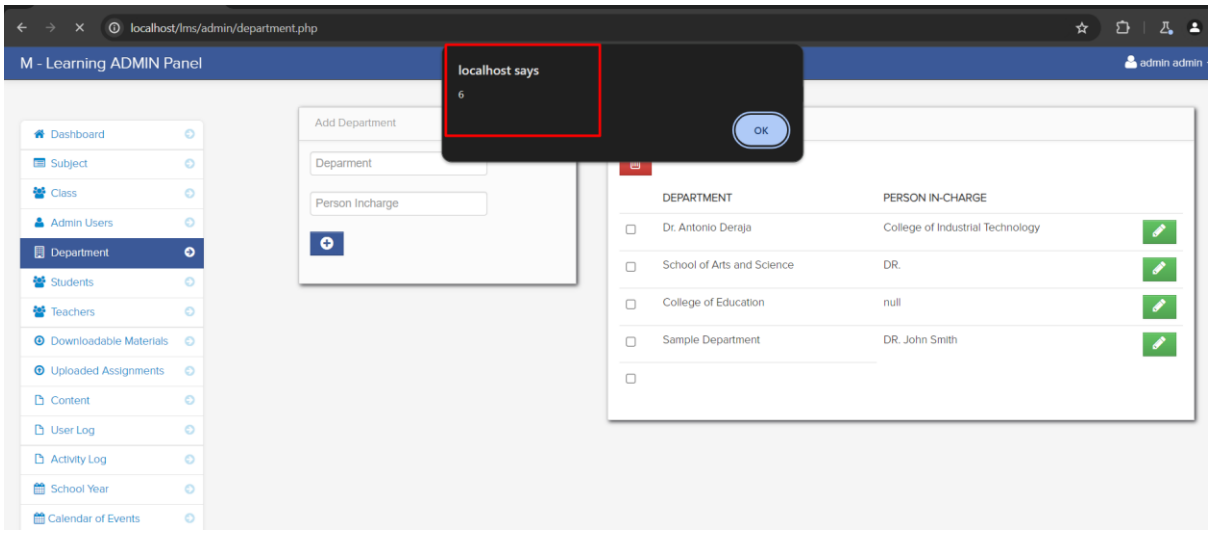
Step 3: After filling fields with payloads <script>alert(5)</script> click on add button.





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