Stored Cross-Site Scripting (XSS) vulnerability was found in the /lms/admin/calendar_of_events.php page of the KASHIPARA E-learning Management System project v1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the date_start, date_end **and** title parameters in a POST HTTP request.

- **Official Website URL**

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

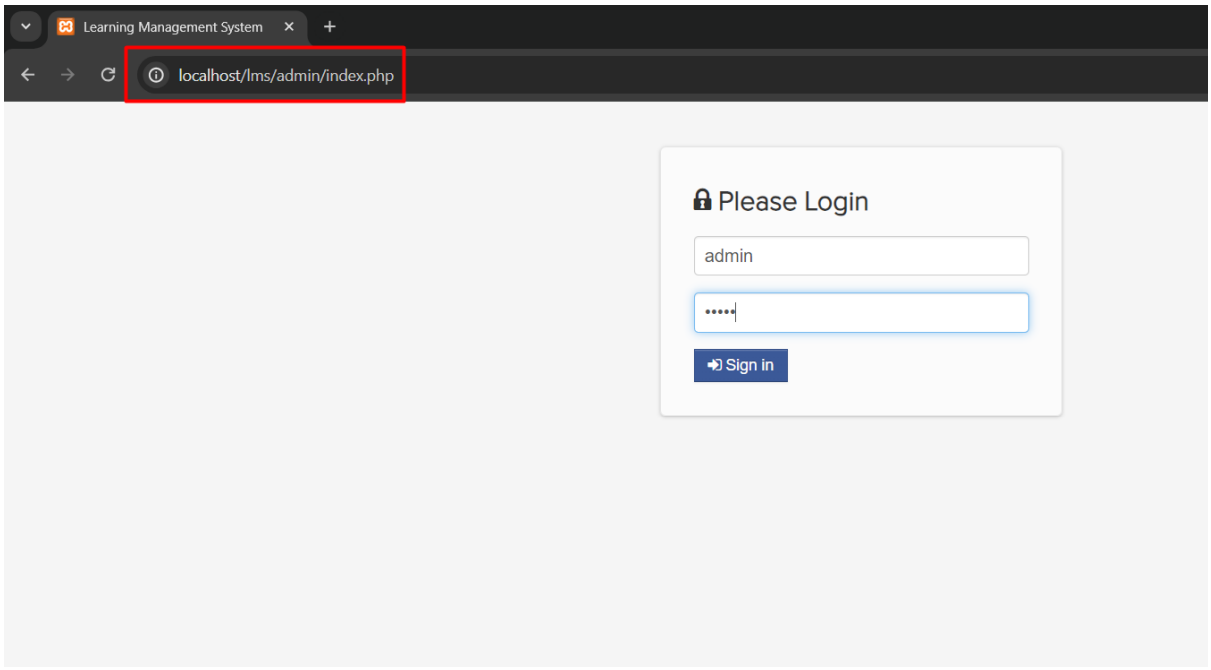
- **Affected Product Name**

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

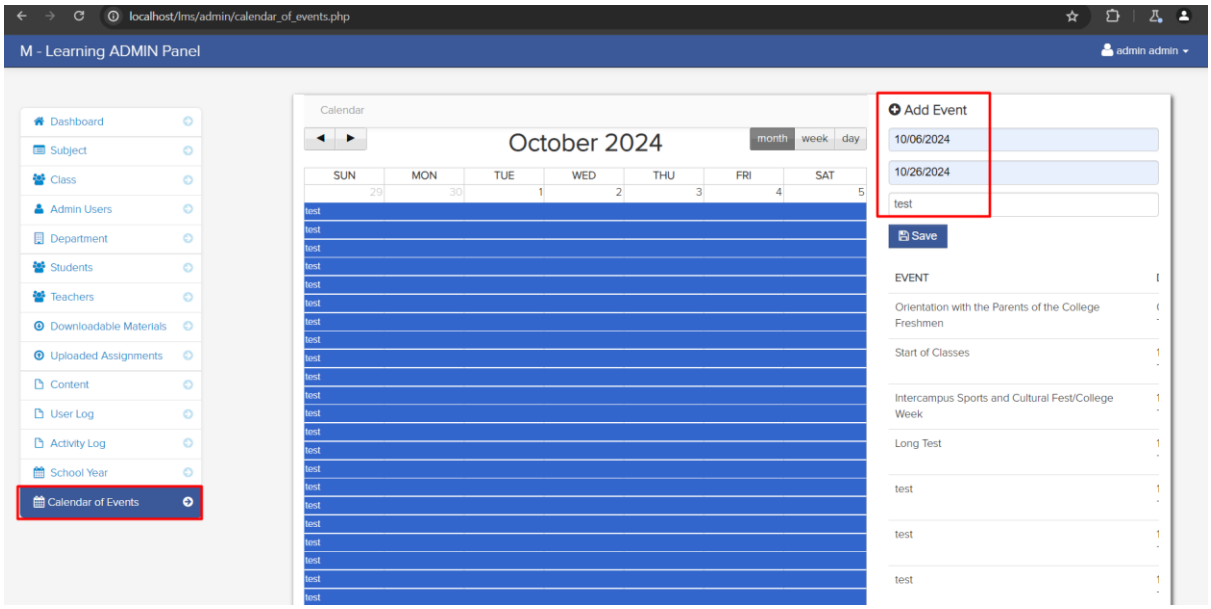
Affected Vendor	kashipara
Affected Code File	/lms/admin/calendar_of_events.php
Affected Parameter	date_start, date_end, title
Method	POST
Type	Stored Cross Site Scripting
Version	V1.0

Steps to Reproduce:

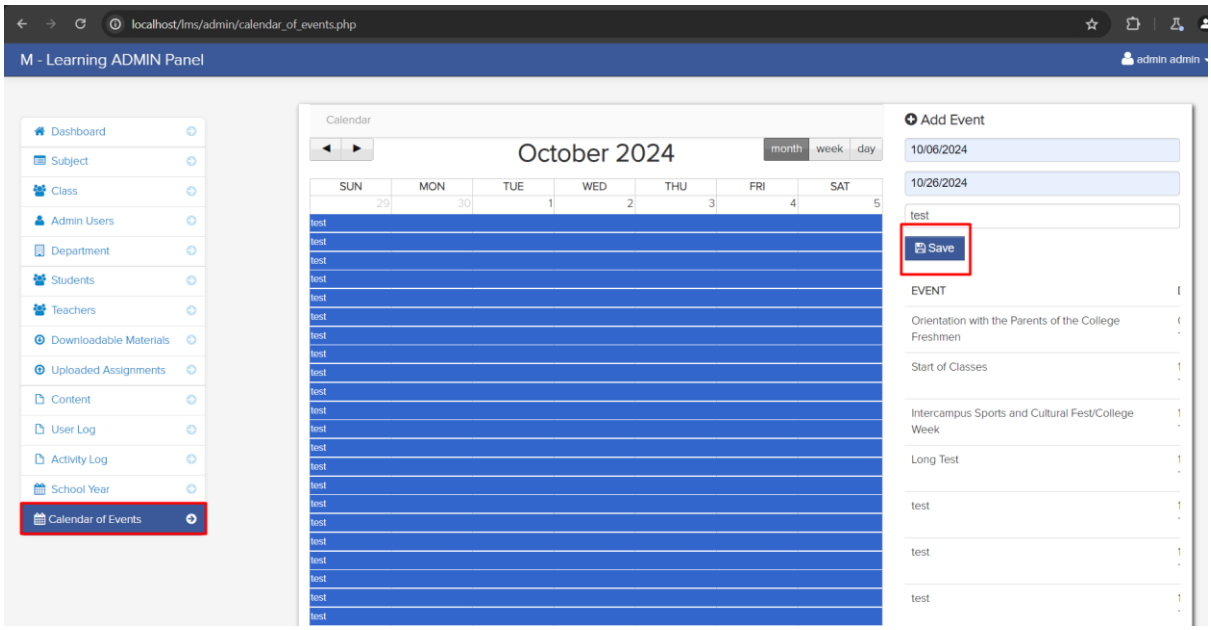
Step 1: Navigate admin login page and login with admin user credential at http://localhost/lms/admin/index.php



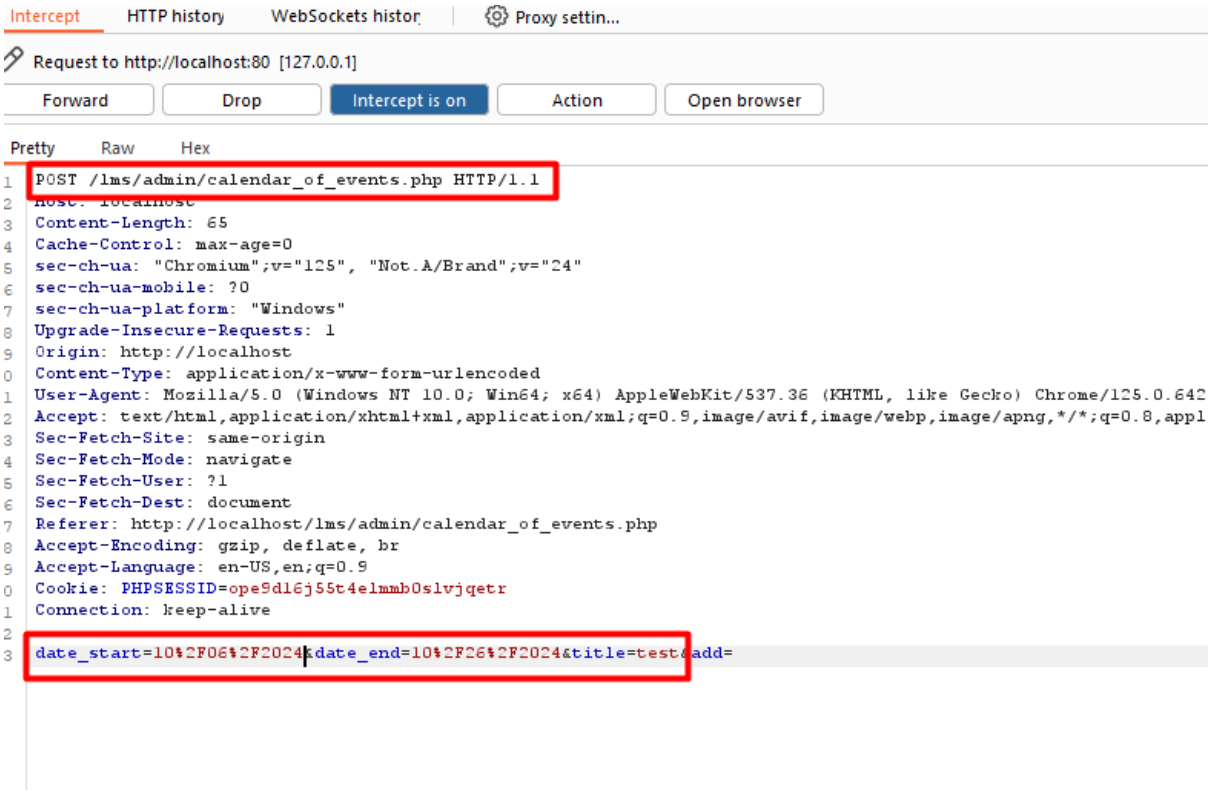
Step 2: Navigate the ‘Calendar of Events’ and fill the data in ‘Add Event’.



Step 3: Now enable burpsuite intercept and click on ‘Save’ button.

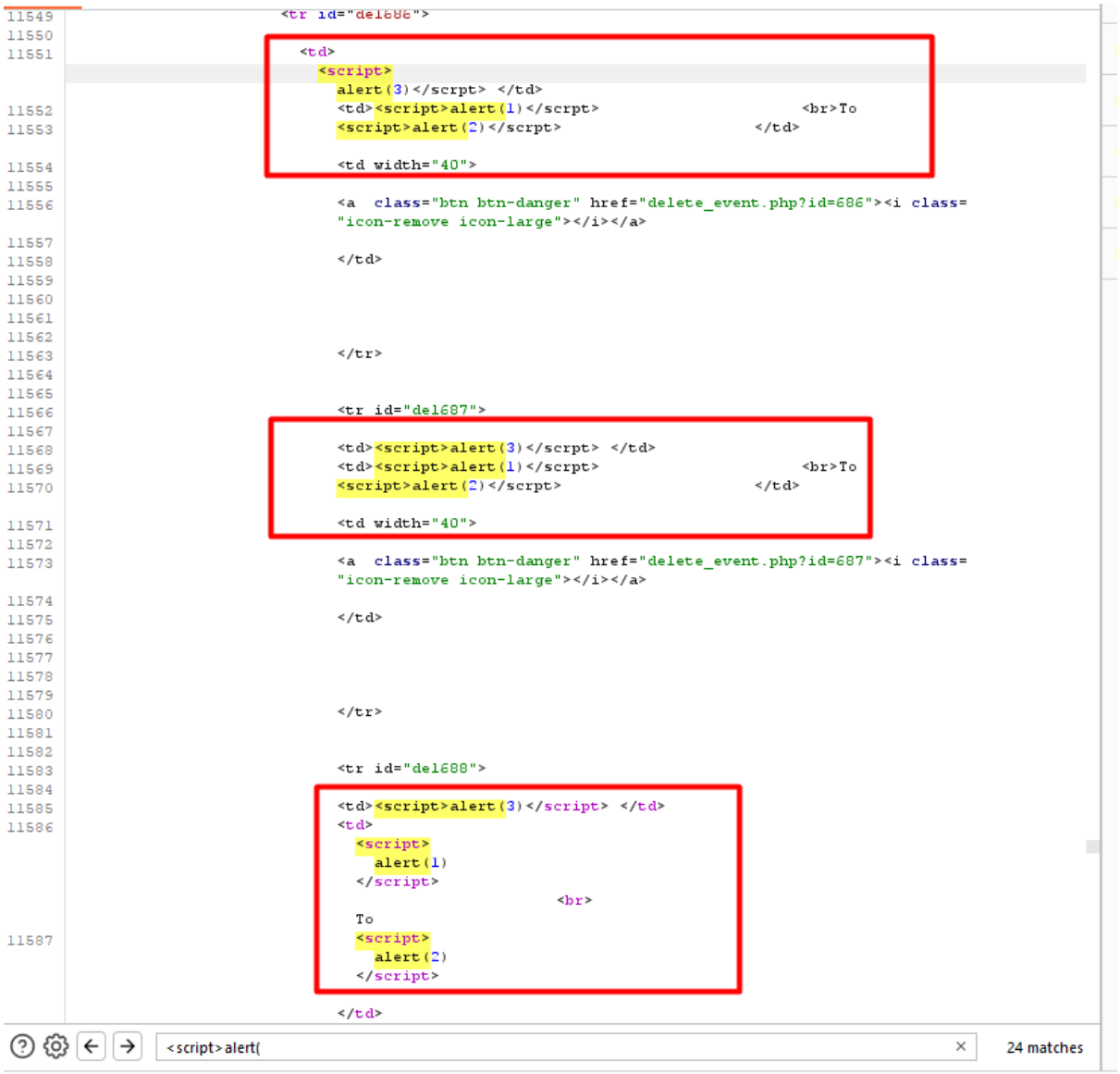


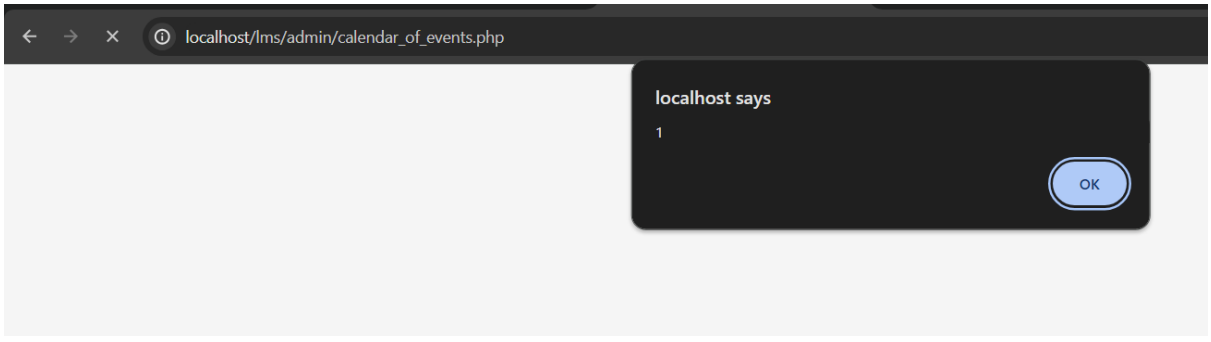
Step 4: Now observe the parameters ‘date_start, date_end **and** title’

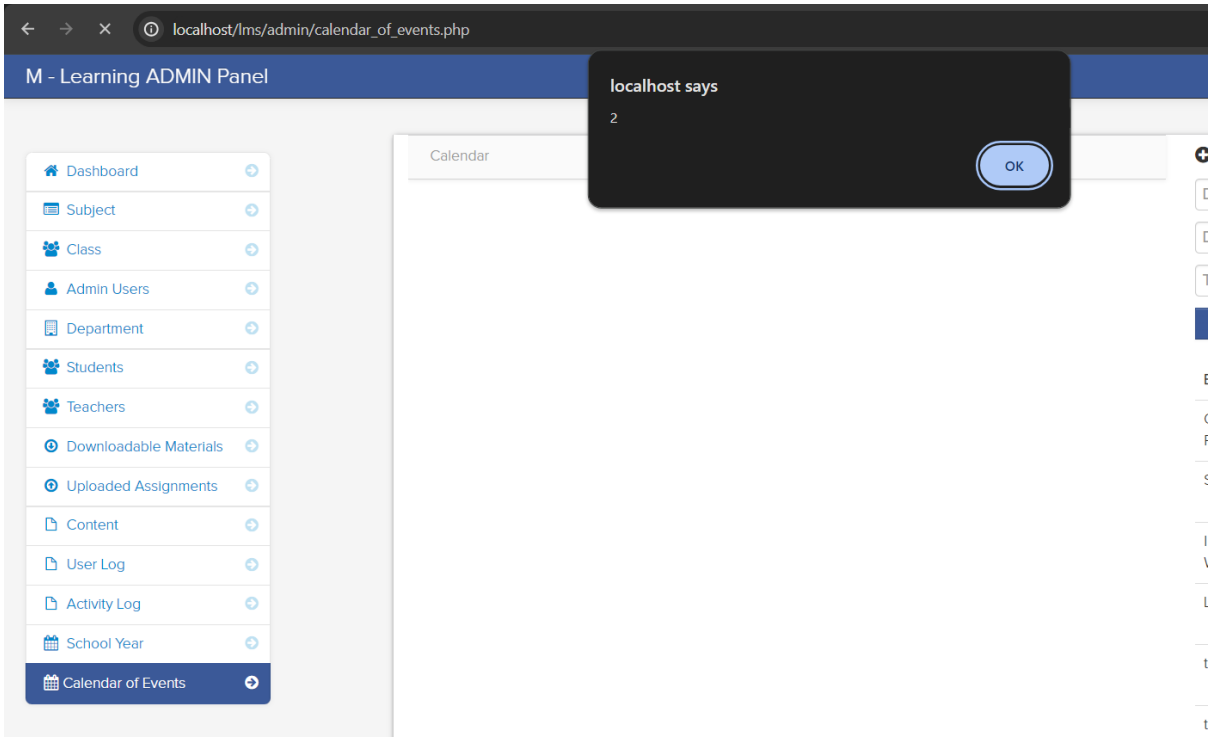


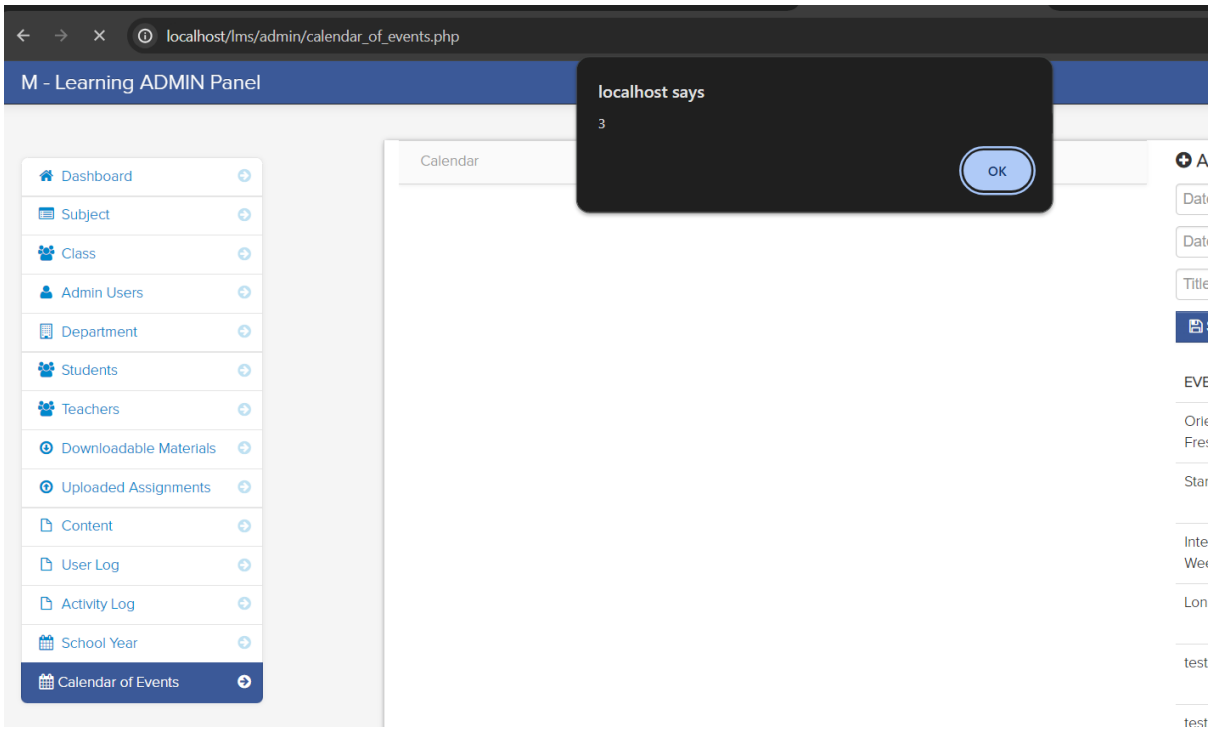
Step 5: Change the parameters values ‘data_start, date_end and title’ with xss payload <script>alert(1)</script> and forward the request.

Step 6: Notice that 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