

Stored Cross-Site Scripting (XSS) vulnerability was found in the /lms/admin/admin\_user.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 username parameter in a POST HTTP request.

➤ **Official Website URL**

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

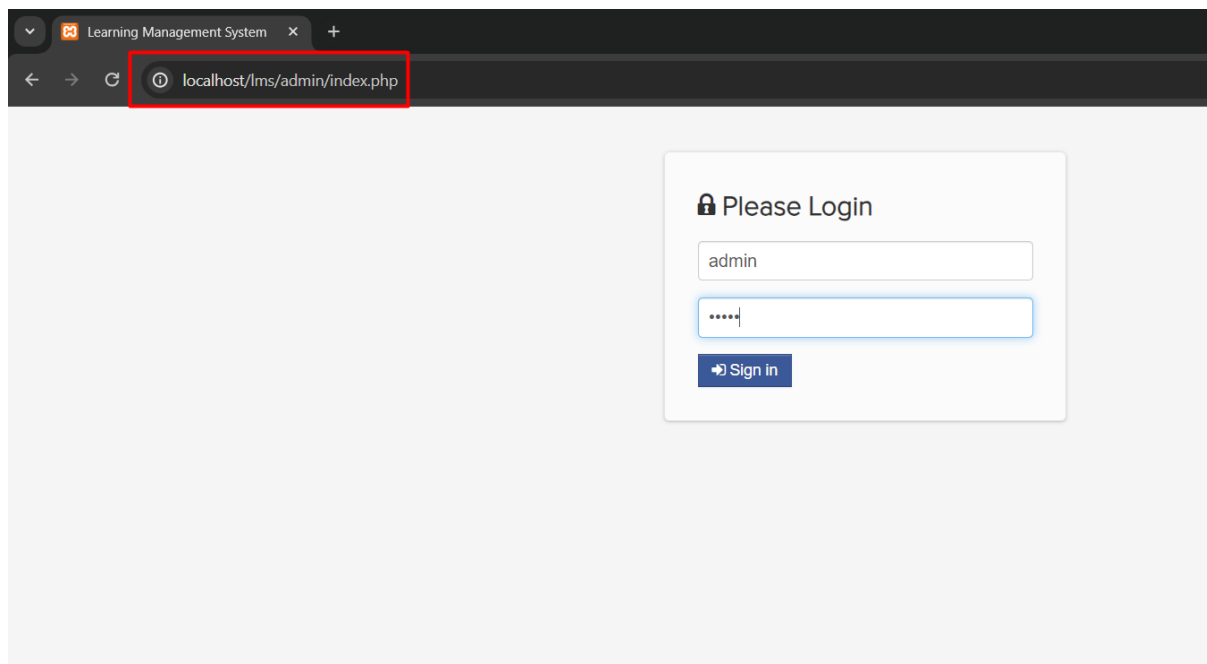
➤ **Affected Product Name**

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

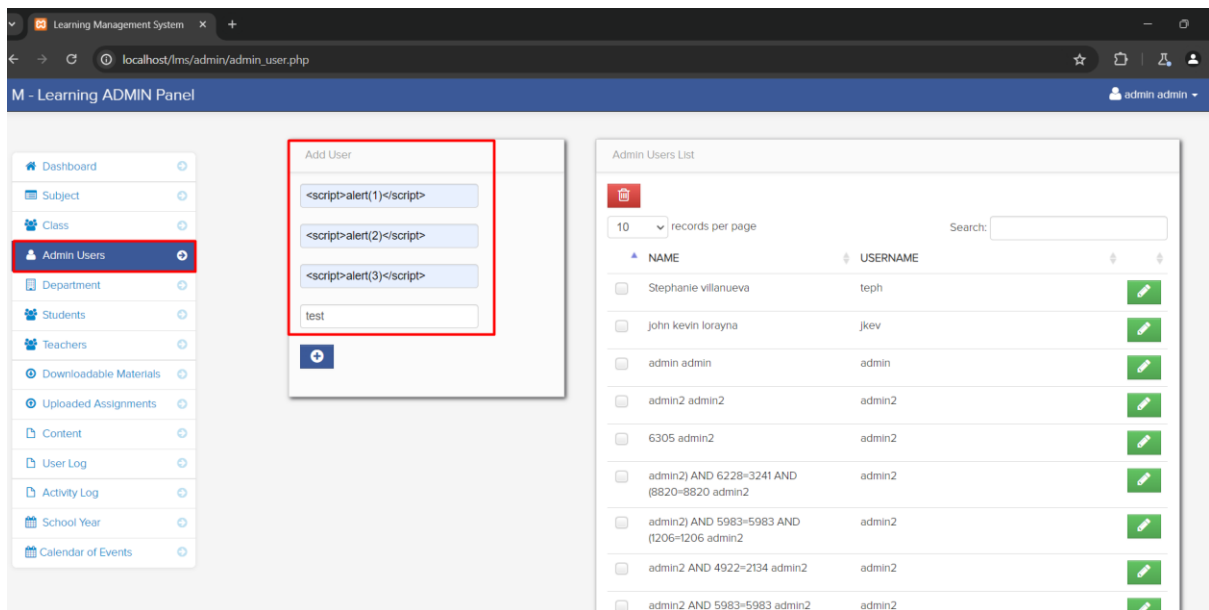
<b>Affected Vendor</b>	kashipara
<b>Affected Code File</b>	/lms/admin/admin_user.php
<b>Affected Parameter</b>	firstname, username
<b>Method</b>	POST
<b>Type</b>	Stored Cross Site Scripting
<b>Version</b>	V1.0

## Steps to Reproduce:

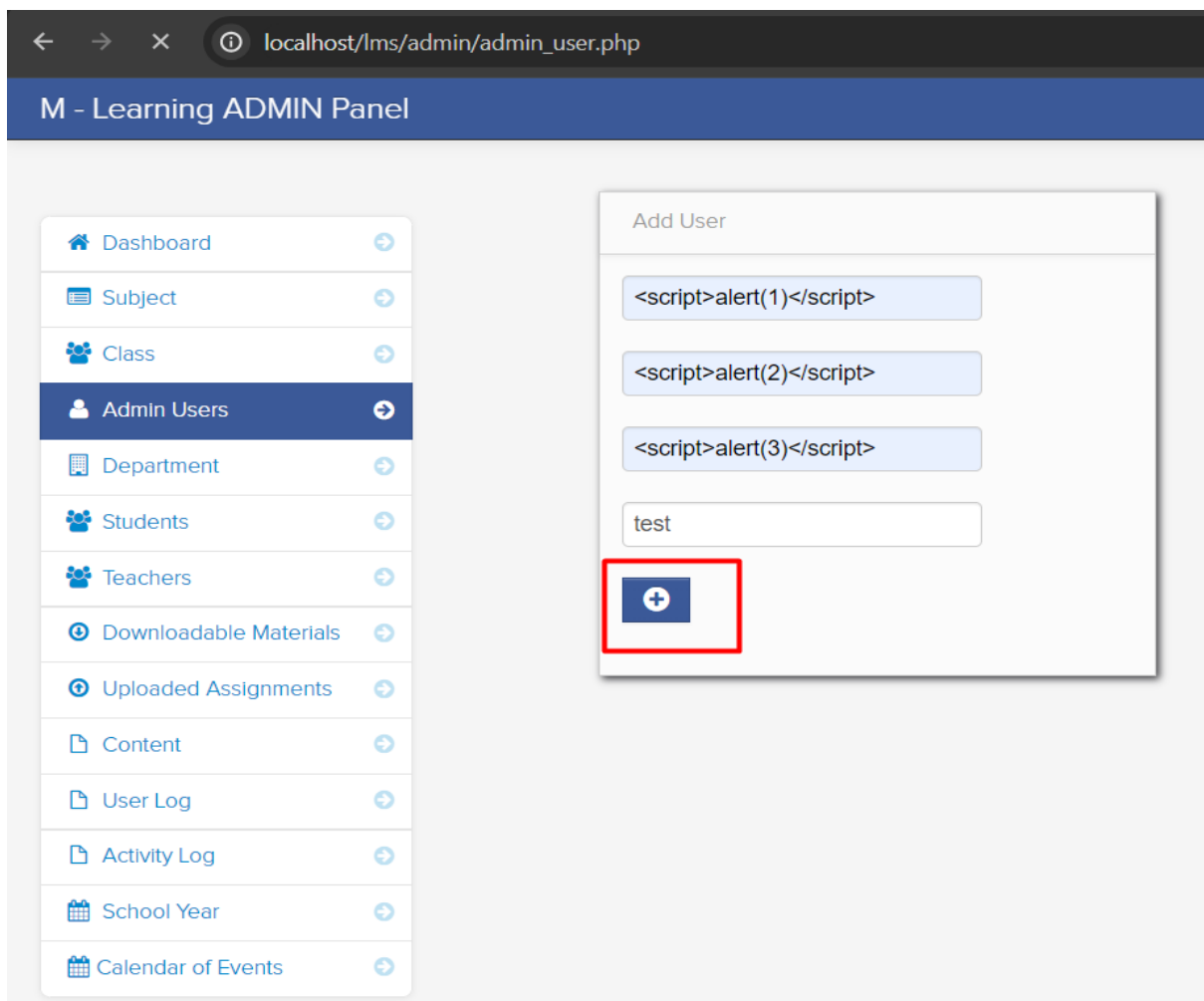
**Step 1:** Navigate admin login page and login with admin user credential at <http://localhost/lms/admin/index.php>

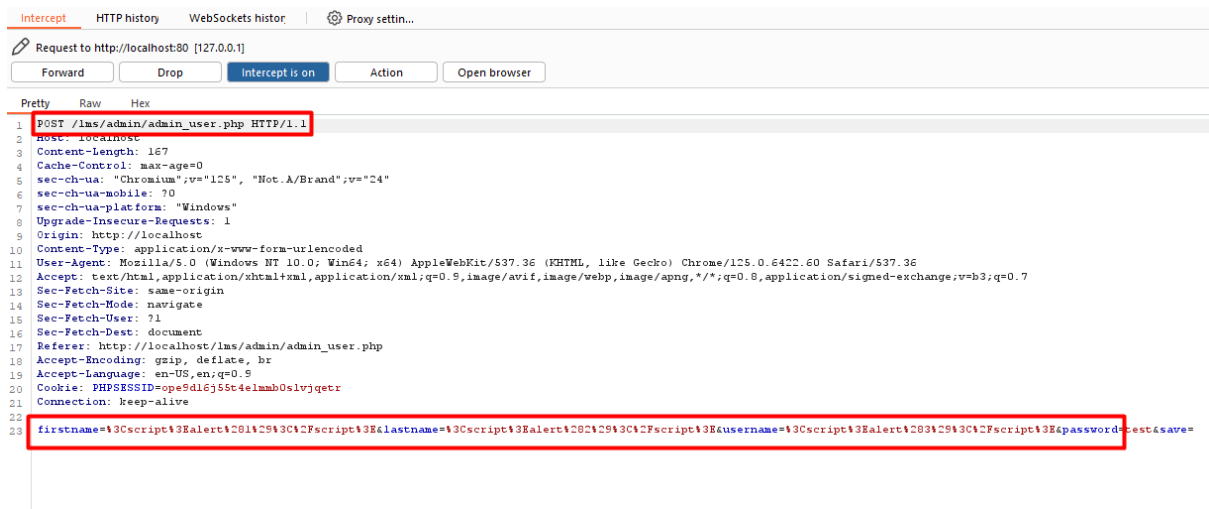


**Step 2:** Navigate the 'Admin Users' page and fill the payloads `<script>alert(1)</script>` fields.

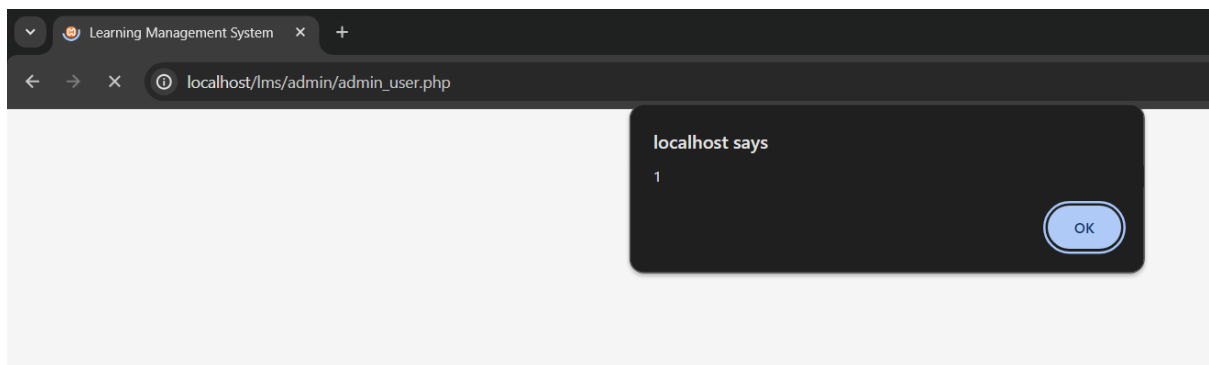


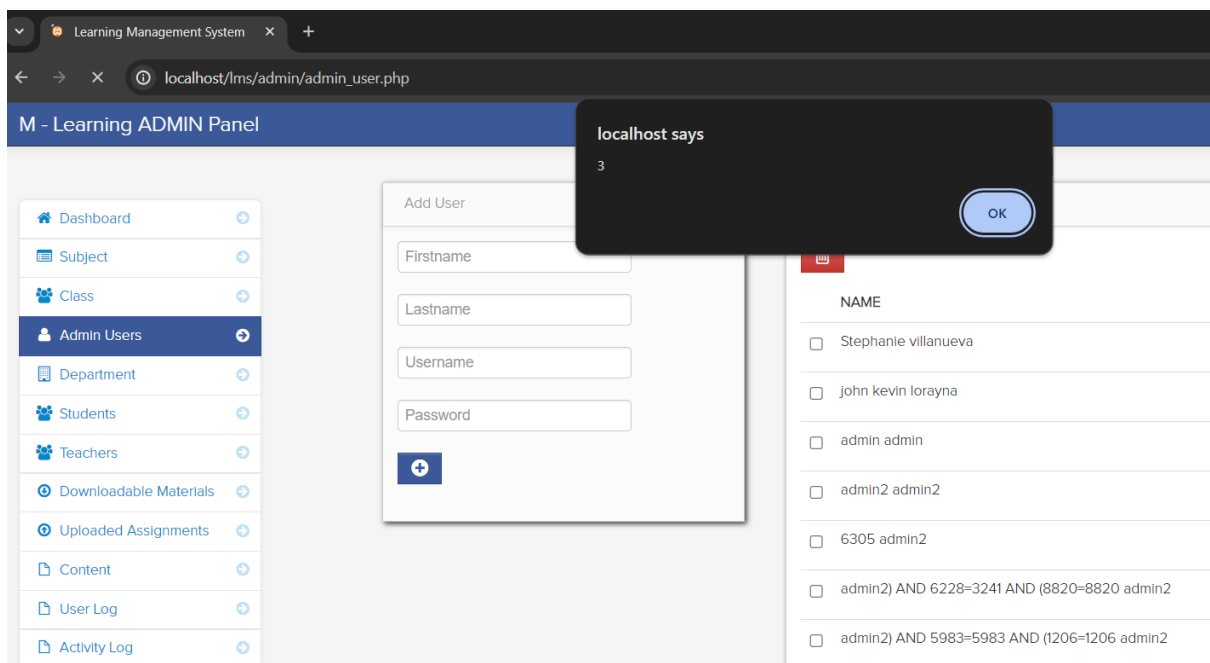
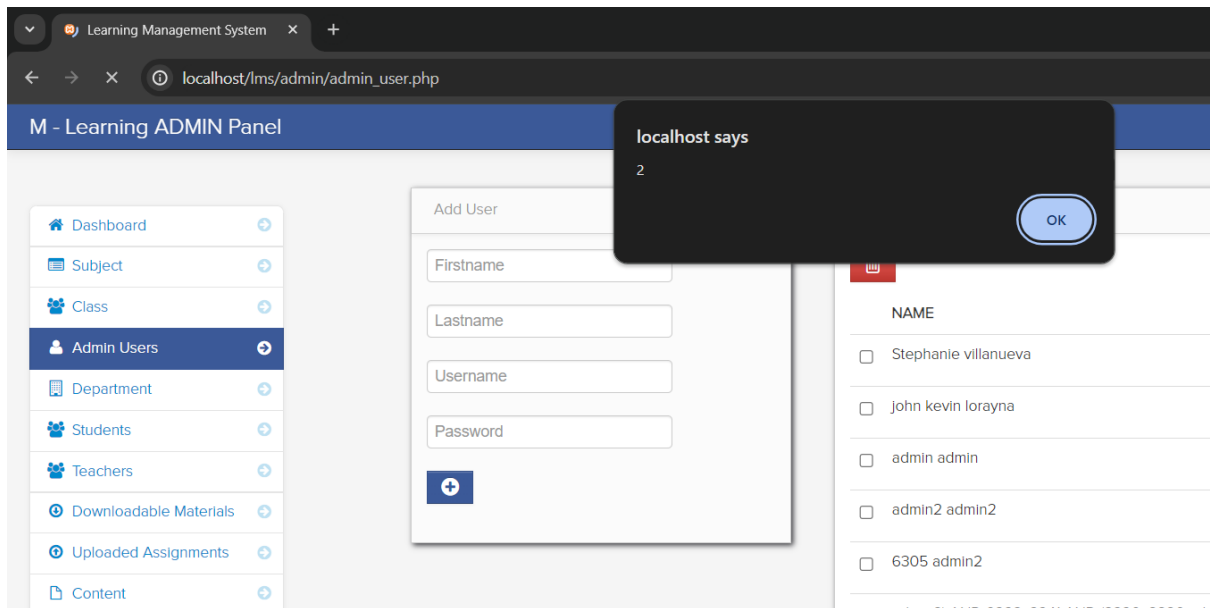
**Step 3:** After filling fields with payloads click on add button.





**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](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)

