SQL Injection was found in the /lms/remove_sent_message.php of the kashipara E-learning Management System project v1.0, Allows remote attackers to execute arbitrary SQL command to get unauthorized database access via the id parameter in a POST HTTP request.

- **Official Website URL**

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

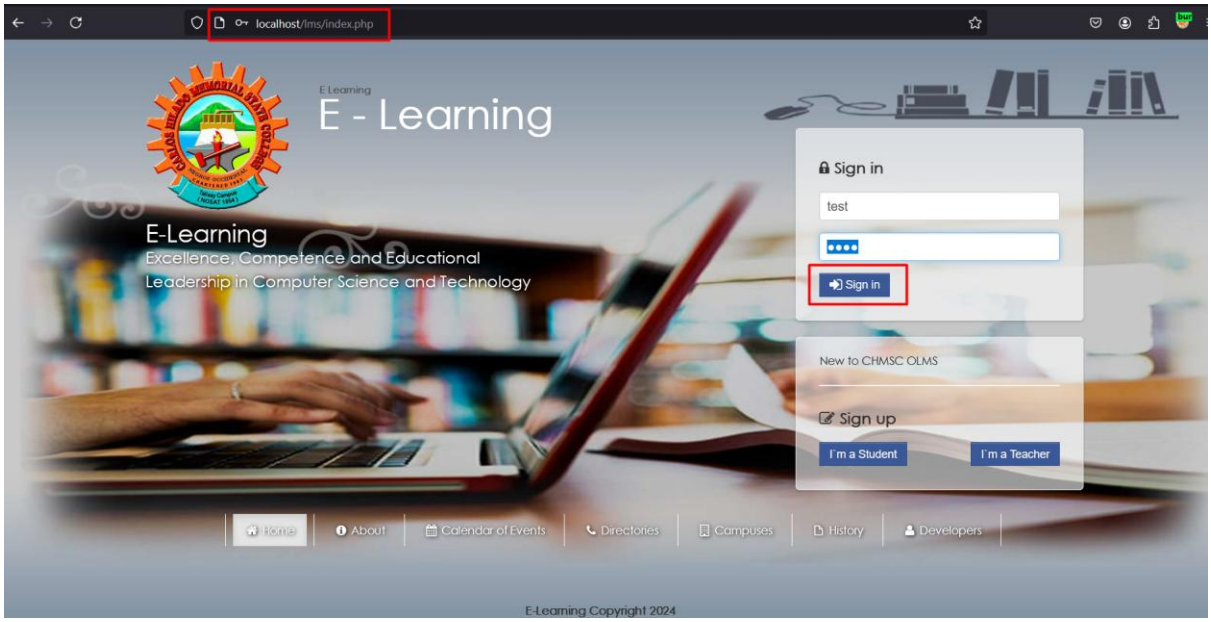
- **Affected Product Name**

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

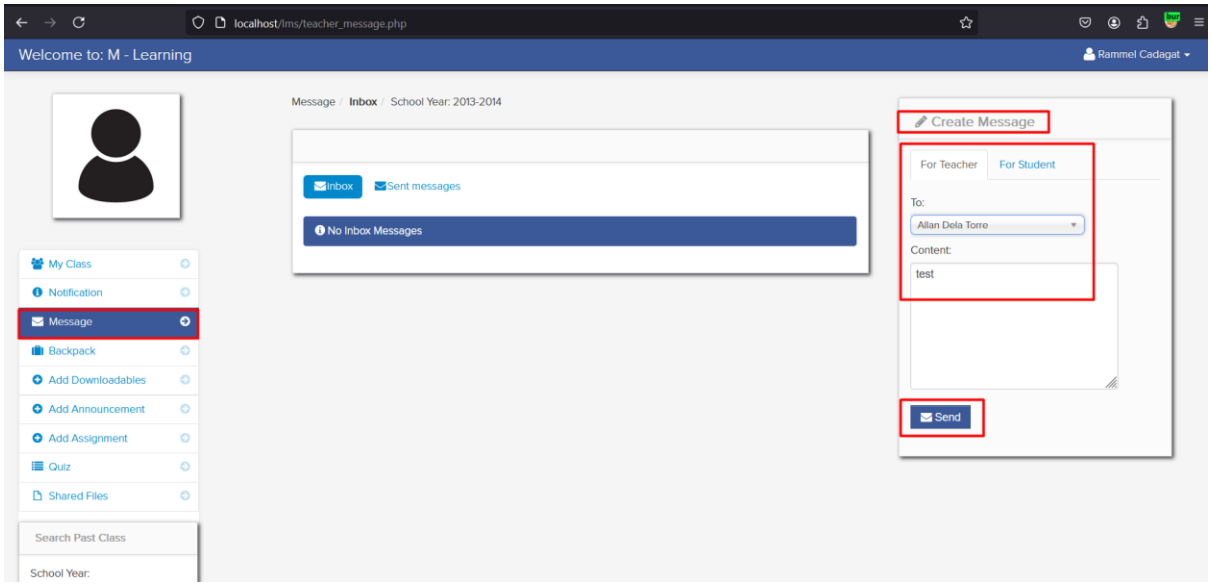
Affected Vendor	kashipara
Affected Code File	/lms/remove_sent_message.php
Affected Parameter	id
Method	POST
Type	time-based blind
Version	V1.0

Steps to Reproduce:

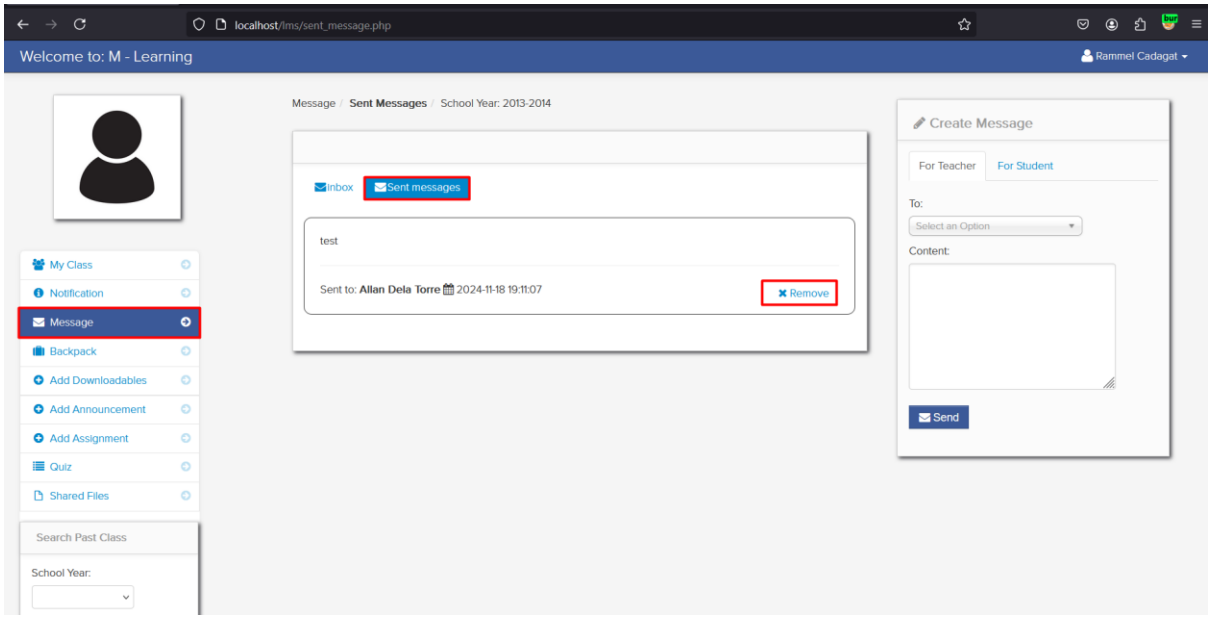
Step 1: Visit to login page and login with teacher credential.

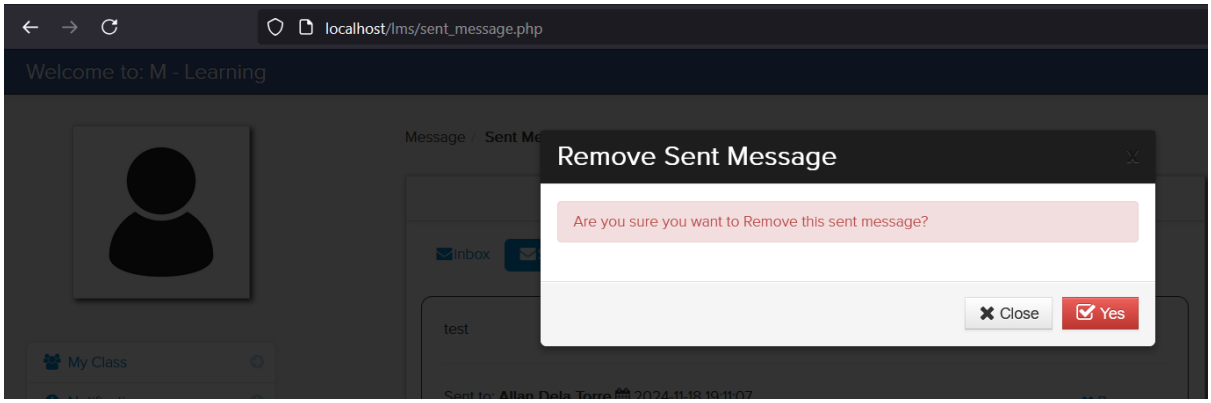


Step 2: Navigate the ‘Message’ page and create a new message and click on ‘send’ button.

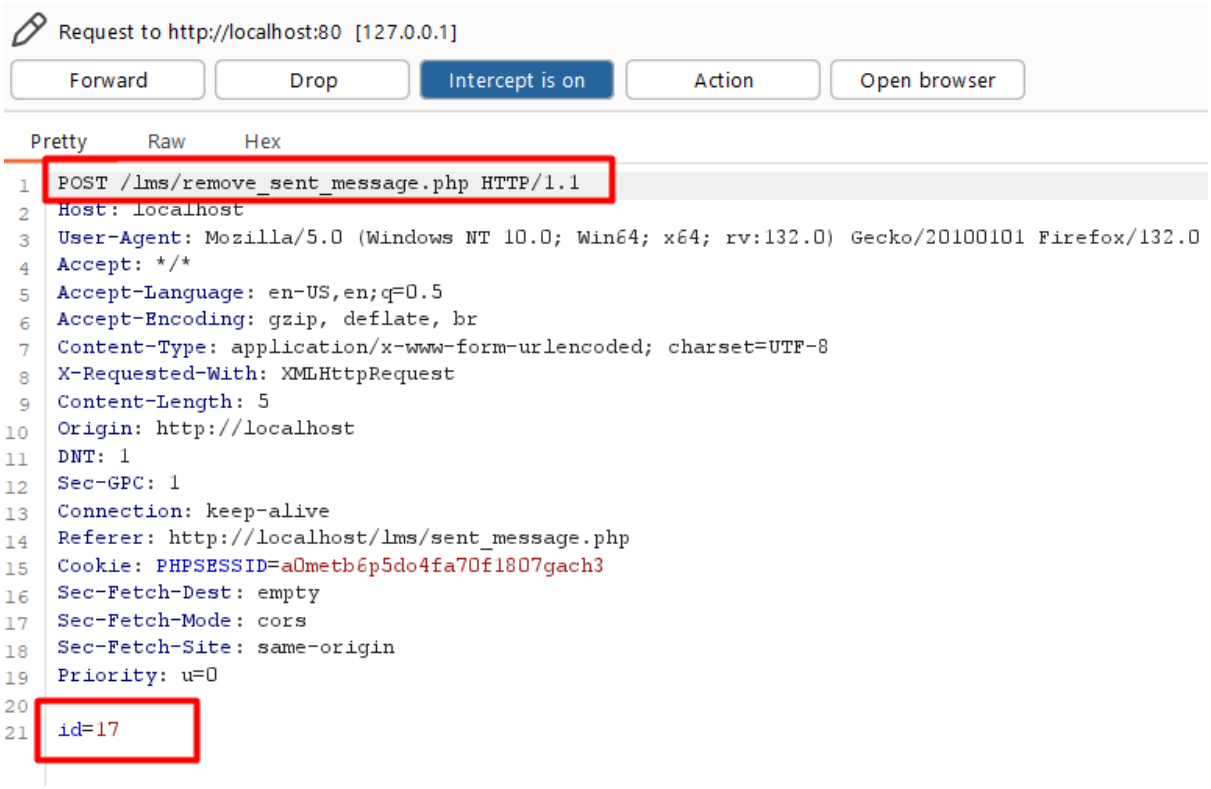


Step 3: Click on ‘Sent message’ tab and notice that send message is listed. Now enable intercept in bupsuite and click on ‘remove’ button.



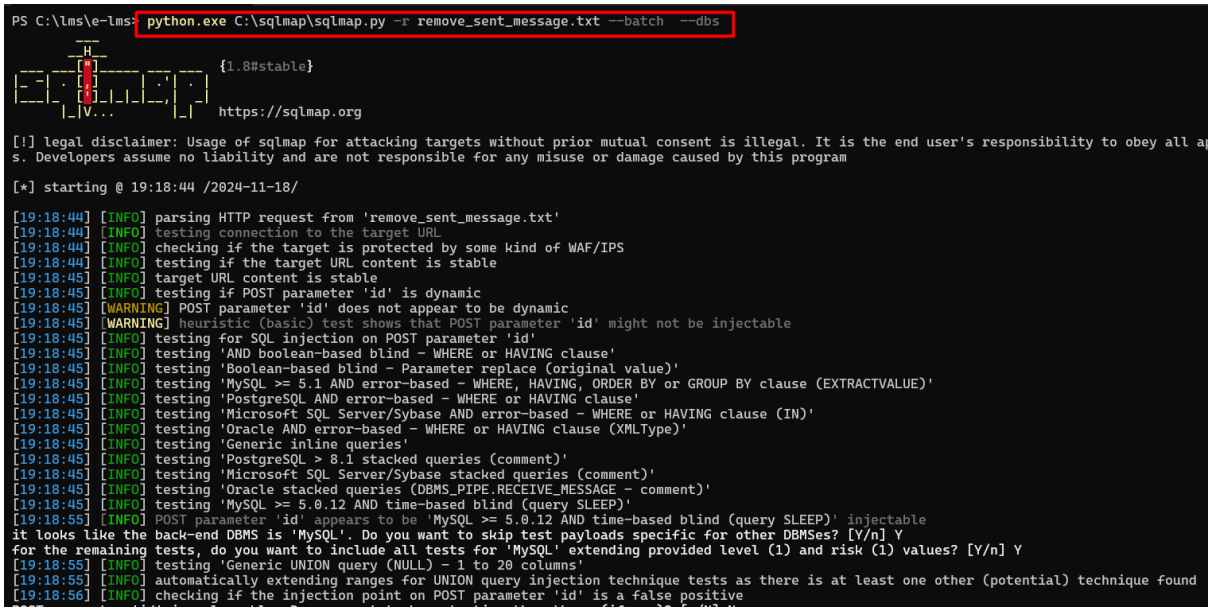


Step 4: Save the burpsuite request in a file.

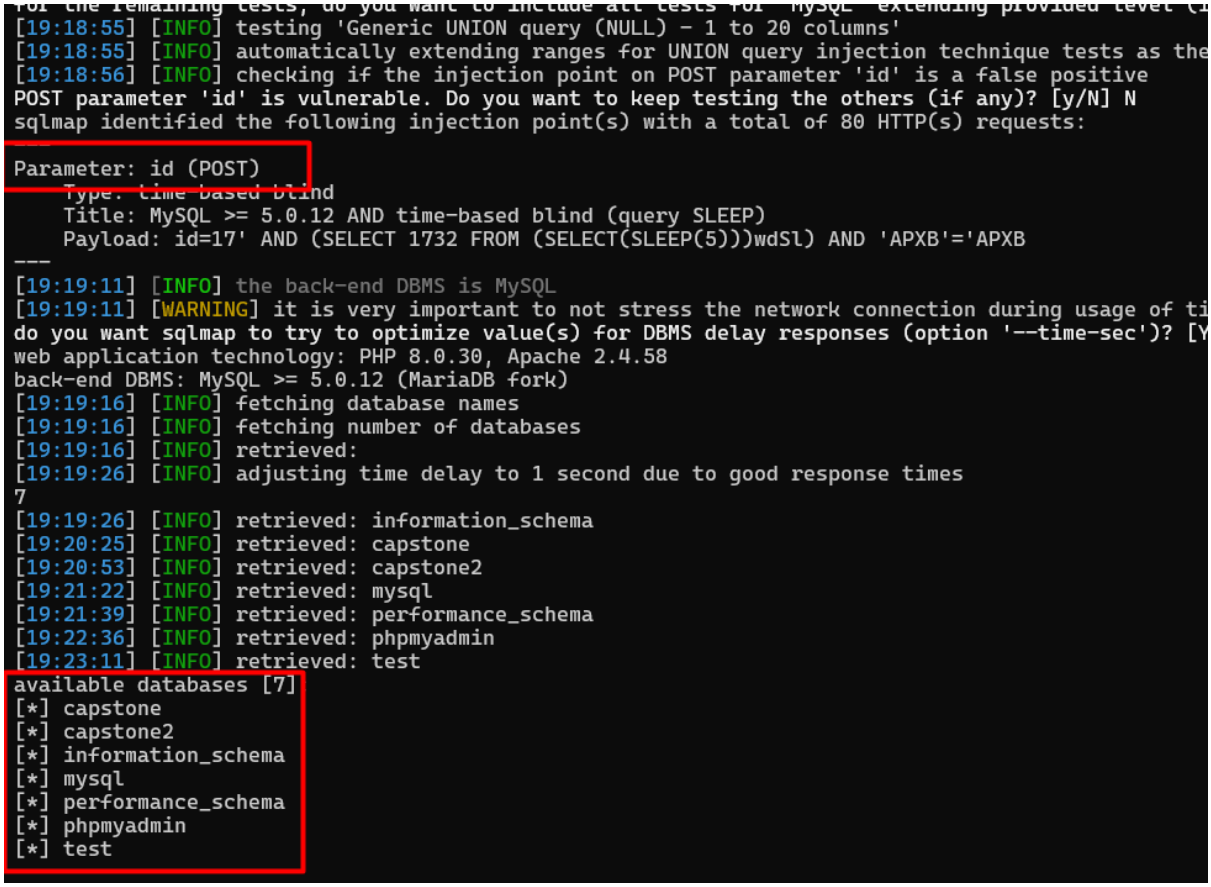


Step 5: Now run the sqlmap command against request saved in file.

- python.exe C:\sqlmap\sqlmap.py -r remove_sent_message.txt --batch --dbs



Step 6: Notice that 'id' parameter is detected vulnerable and all database is successfully retrieved.



Mitigation/recommendations

- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
- https://portswigger.net/web-security/sql-injection#how-to-prevent-sql-injection