SQL Injection was found in the /lms/login.php page 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 username and password 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/login.php
Affected Parameter	username, password
Method	POST
Type	time-based blind
Version	V1.0

Steps to Reproduce:

Step 1: Visit to e-learning home page to login and give username and password abc at
http://localhost/lms/
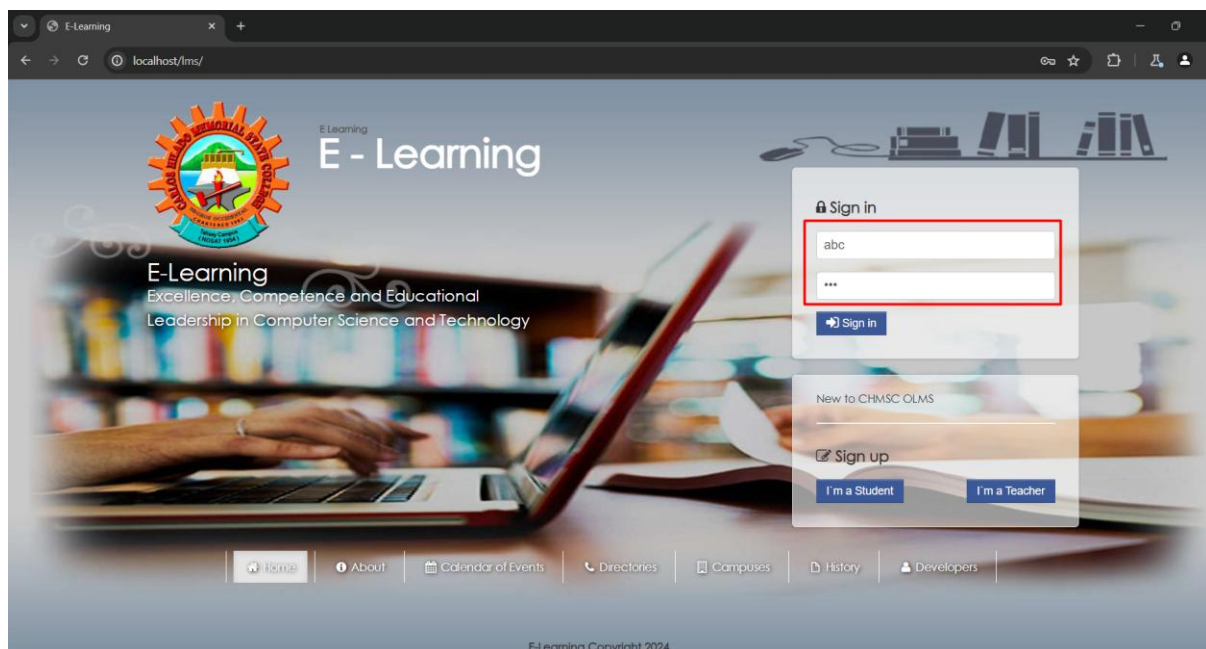
Step 2: Enable intercept in burpsuite and click on 'Sign in' button.
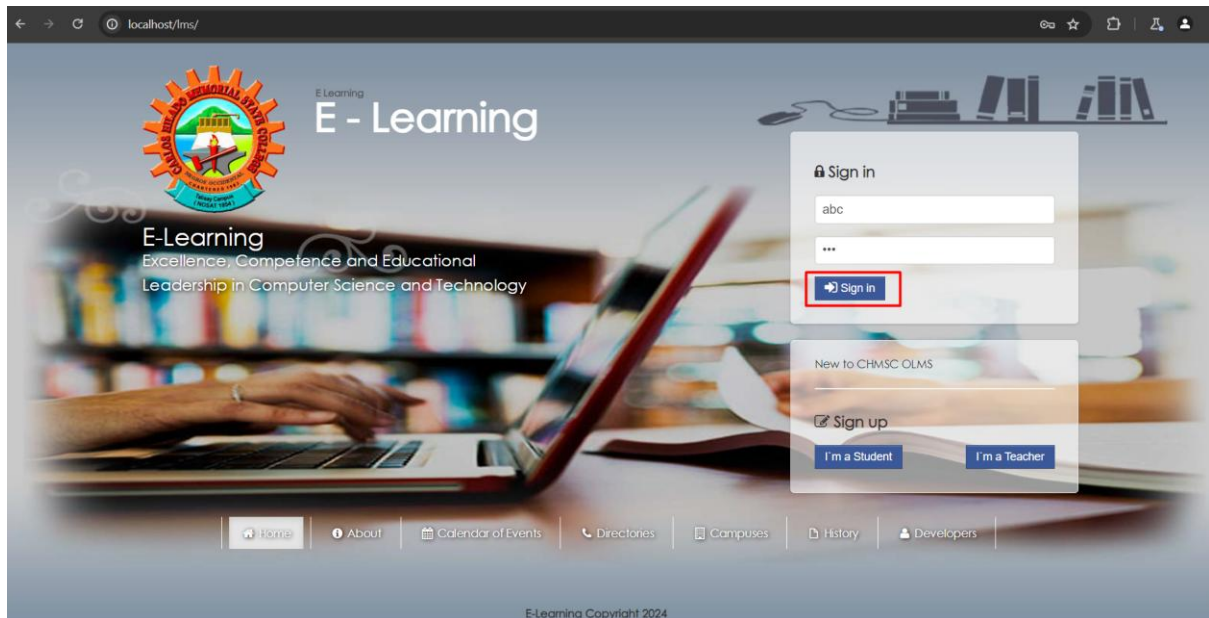
Step 3: Save the burpsuite request in a file.
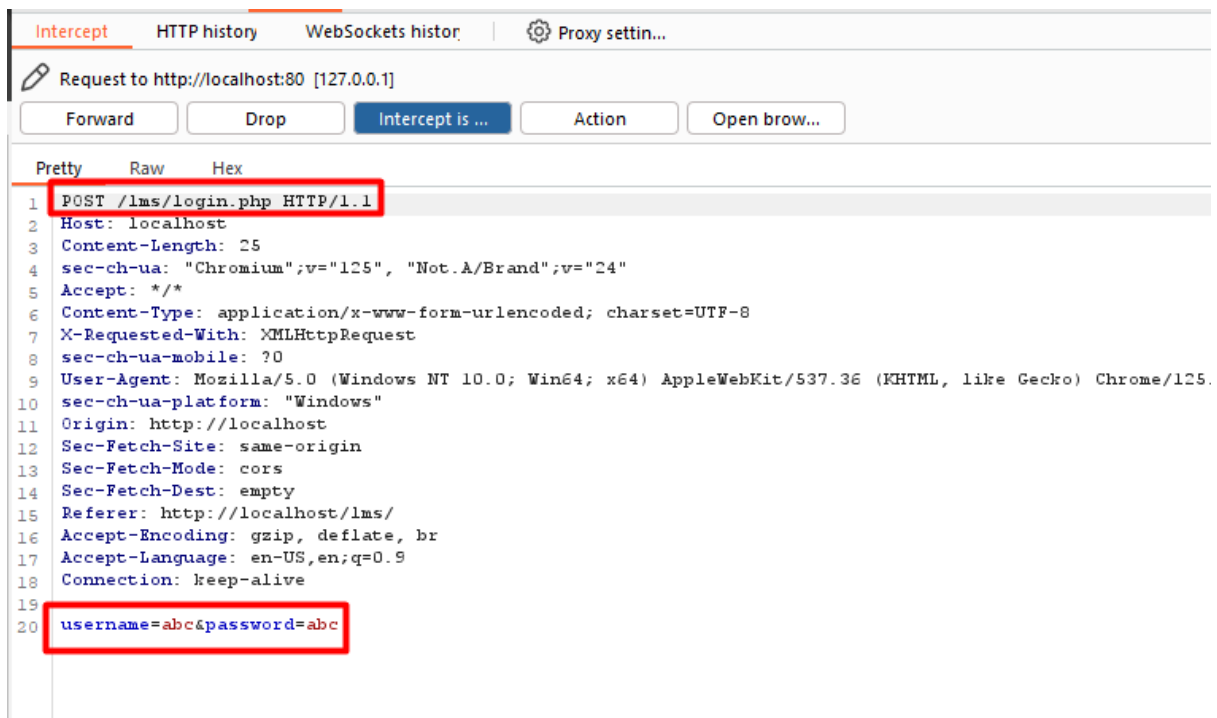
Step 4: Now run the sqlmap command against the burpsuite request saved in file.

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

Step 5: Now notice that 'username' parameter is detected vulnerable and all database is successfully retrieved.

Parameter: password

Step 6: Now run the sqlmap against 'password' parameter by using switch -p

- python.exe C:\sqlmap\sqlmap.py -r login.txt -p "password" --batch --dbs

Step 8: Now notice that 'password' 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