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)

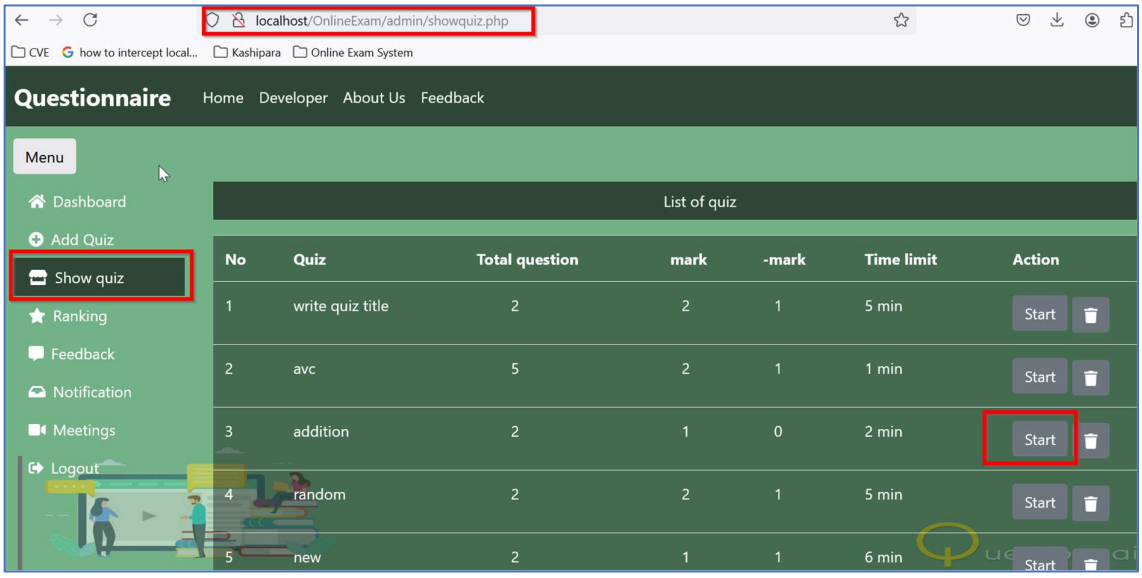
Version: 1.0

Affected Components:

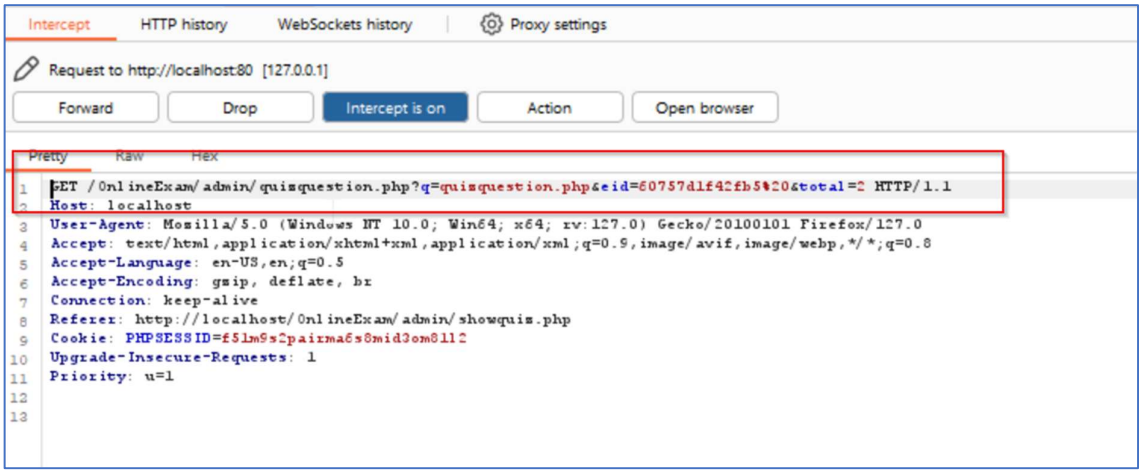
- **Affected Code File:** /admin/quizquestion.php
- **Affected Parameter:** "eid" parameter
- **Application URL:** http://localhost/OnlineExam/admin/quizquestion.php?q=quizquestion.php&eid=60757d1f42fb5&total=2

Steps:

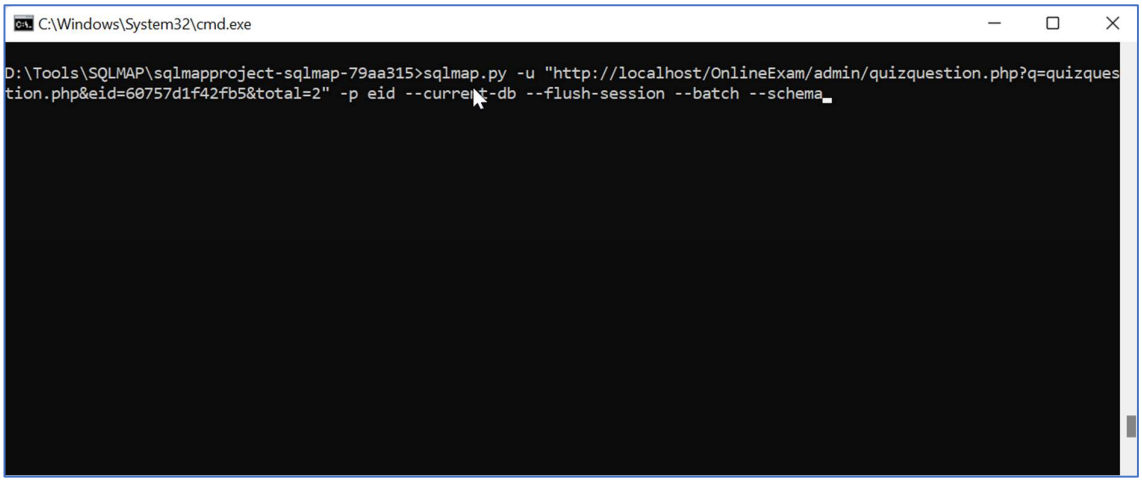
1. Login as an admin in the Online Exam System v1.0 and access the “Show Quiz” menu. (URL: http://localhost/OnlineExam/admin/showquiz.php)
2. Select any one of the quizzes and click on “Start” button.



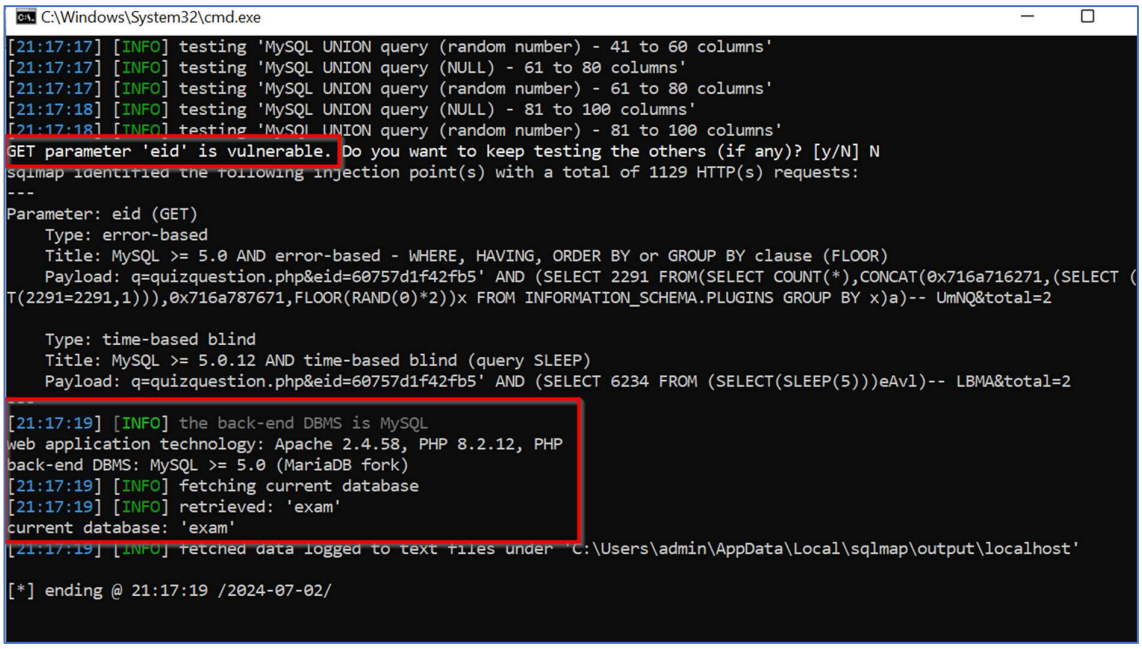
3. Capture the HTTP request going towards server in Burp Suite. In this HTTP GET request parameter "**eid**" is vulnerable to SQL injection. This is demonstrated in next steps.

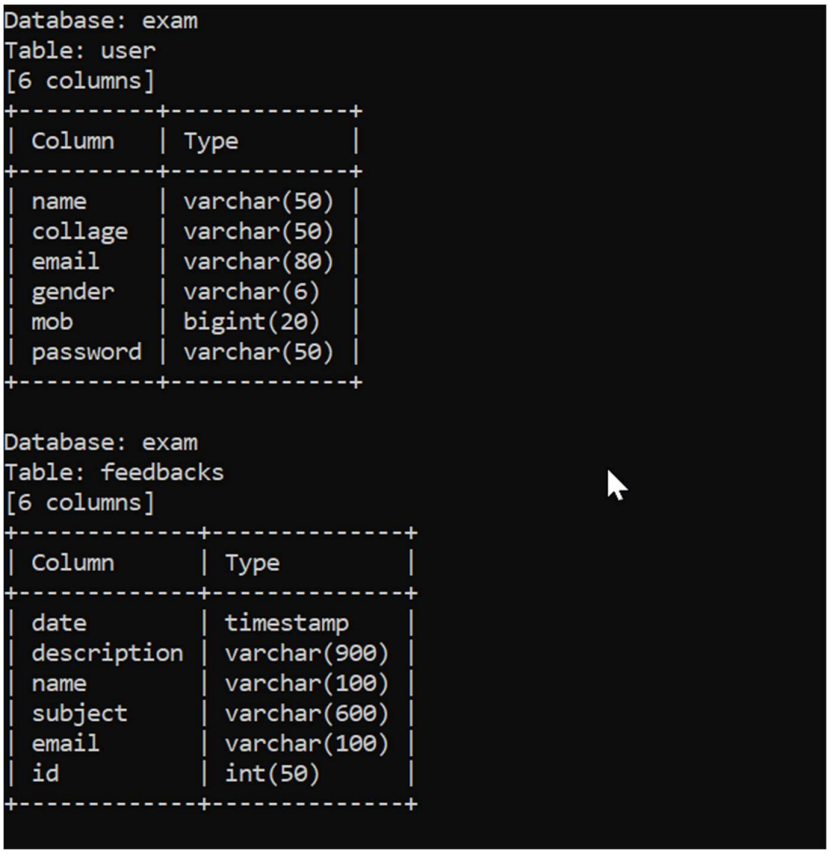


4. We will run SQLMAP against the GET Request as shown in the following screenshot.



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





Solution/Good Reads:

User parameterized SQL queries instead of the dynamic SQL queries.

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