

Stored Cross Site Scripting (XSS) vulnerability was found in "manage\_houses.php" in SourceCodester House Rental Management System v1.0 allows remote attackers to execute arbitrary code via "House\_no" and "Description" POST parameter fields.

**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 Code File:** manage\_houses.php
- **Affected Parameter:** "House\_no" and "Description" POST parameters
- **Application URL:** [http://localhost/rental/index.php?page=manage\\_houses](http://localhost/rental/index.php?page=manage_houses)

**Steps:**

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

The screenshot displays the 'Tenant Management System' web application. The browser address bar shows the URL [localhost/rental/index.php?page=houses](http://localhost/rental/index.php?page=houses). The page header includes the 'TENANT LIMITED' logo, the date and time 'Mon Jul 01 2024 10:54:41 GMT-0700 (Pacific Daylight Time)', and a 'Select Language' dropdown. The left sidebar contains a menu with items: Dashboard, House Type, House, Add, Manage, Tenants, Payments, Reports, Users, and Pro Version. The 'Add' link is highlighted with a red box. The main content area is titled 'House Form' and contains a form with the following fields: 'House No' (text input), 'Category' (dropdown menu with 'Apartment' selected), 'Description' (text area), and 'Price' (text input with a currency icon). At the bottom of the form are 'Save' and 'Cancel' buttons. The footer text reads 'Copyright © 2024 Tenant Management System Software - Design By Mayuri K. Freelancer'.

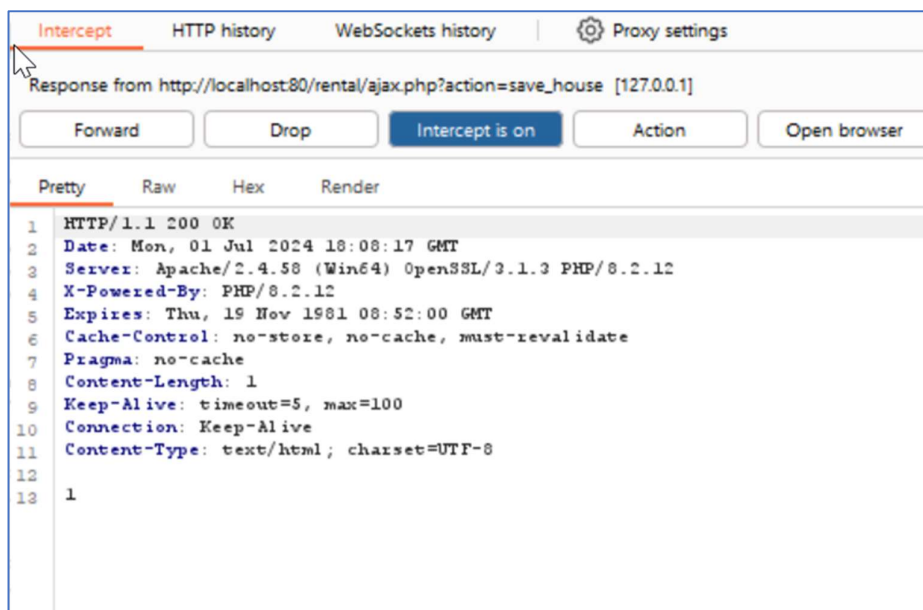
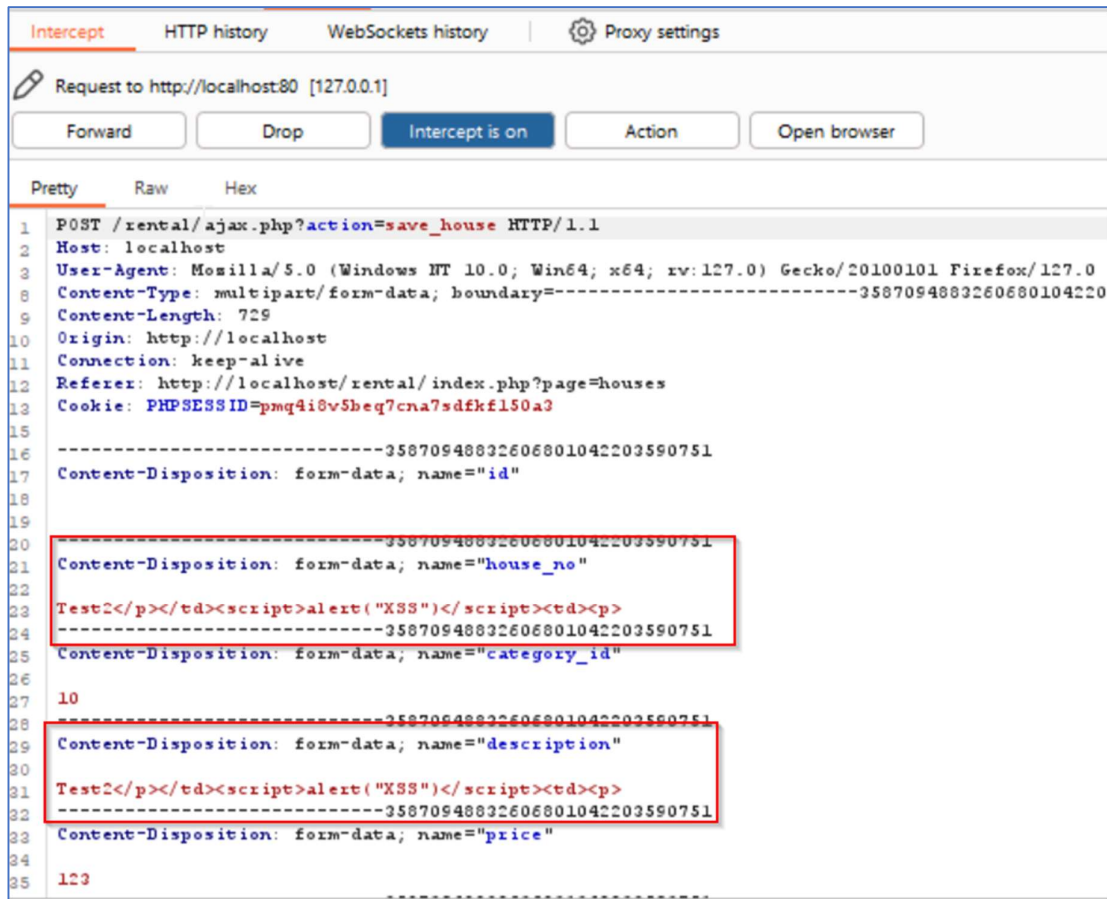
2. Insert the XSS script "`Test2</p></td><script>alert('XSS')</script><td><p>`" in the "House\_no" and "Description" fields as shown in the following screenshot. Click "Save".

The screenshot shows a web application interface for "TENANT LIMITED". The browser address bar displays "localhost/rental/index.php?page=houses". The page title is "Mon Jul 01 2024 10:56:01 GMT-0700 (Pacific Daylight Time)". A sidebar on the left contains navigation links: Dashboard, House Type, House, Add, Manage, Tenants, Payments, Reports, and Users. The main content area is titled "House Form" and contains the following fields:

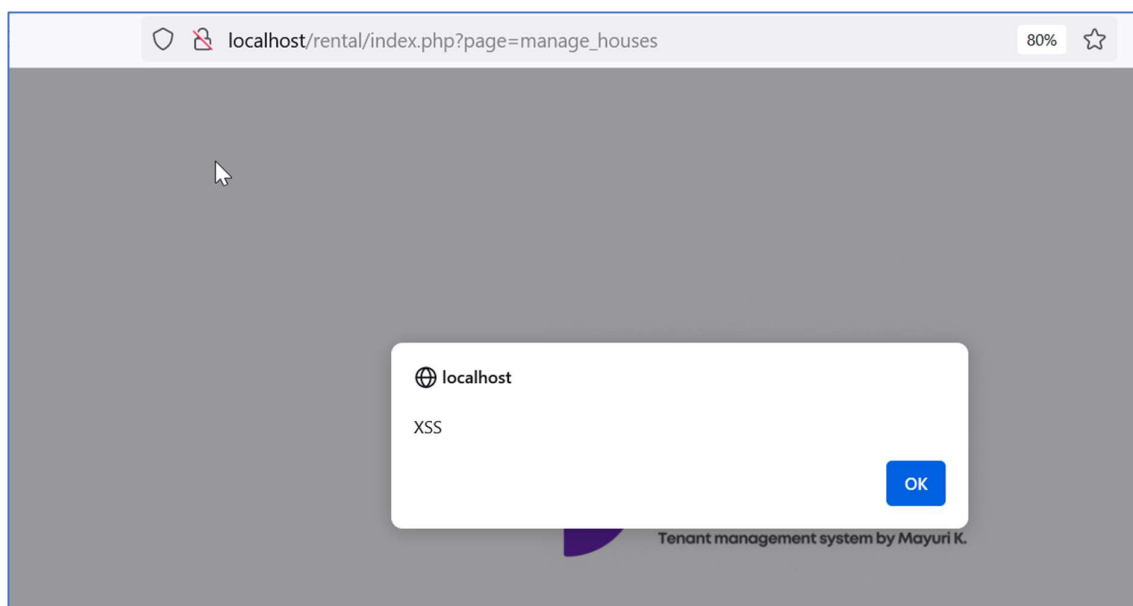
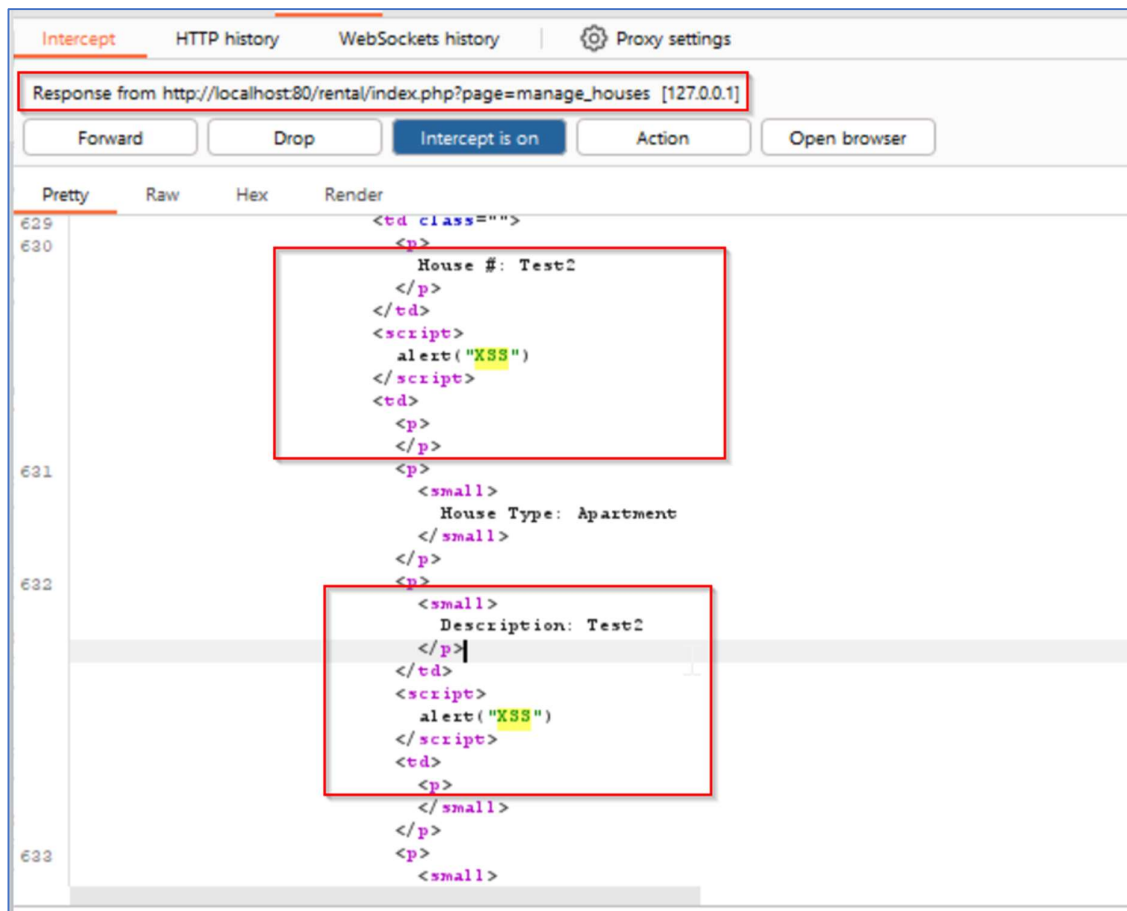
- House No:** A text input field containing the XSS payload: `Test2</p></td><script>alert('XSS')</script><td><p>`. This field is highlighted with a red rectangle.
- Category:** A dropdown menu with "Apartment" selected.
- Description:** A text area containing the same XSS payload as the House No field. This field is also highlighted with a red rectangle.
- Price:** A numeric input field with the value "123".

At the bottom of the form, there are two buttons: "Save" (highlighted with a red rectangle) and "Cancel". The footer of the page reads: "Copyright © 2024 Tenant Management System Software - Design By Mayuri K. Freelancer".

3. This will forward the request with XSS script to server. The request gets accepted and the House name entry with XSS script is stored in the application database.



4. Every time we access the House name list (URL: [http://localhost/rental/index.php?page=manage\\_houses](http://localhost/rental/index.php?page=manage_houses)), the XSS script will get executed.



**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](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)