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)

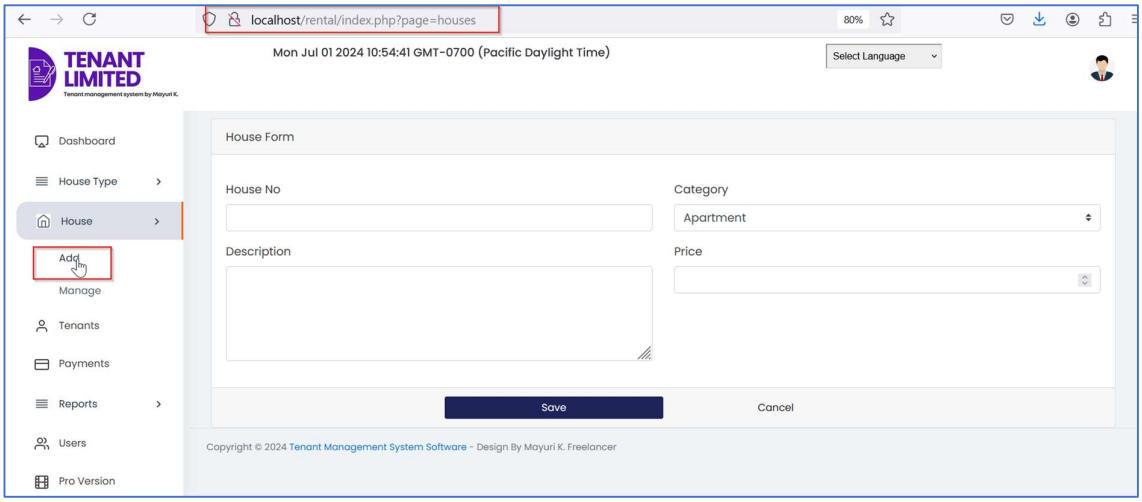
Version: 1.0

Affected Components:

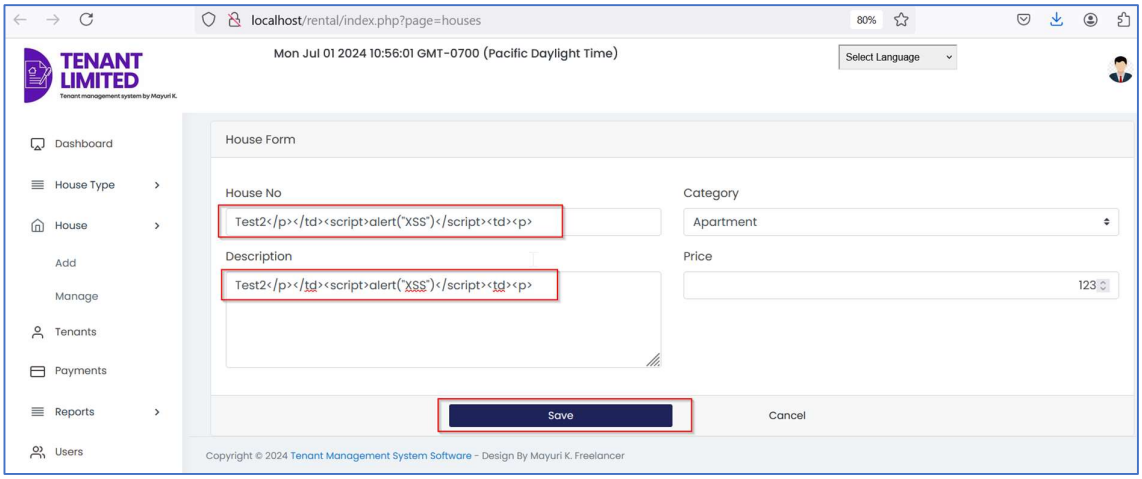
- **Affected Code File:** manage_houses.php
- **Affected Parameter:** "House_no" and "Description" POST parameters
- **Application URL:** http://localhost/rental/index.php?page=manage_houses

Steps:

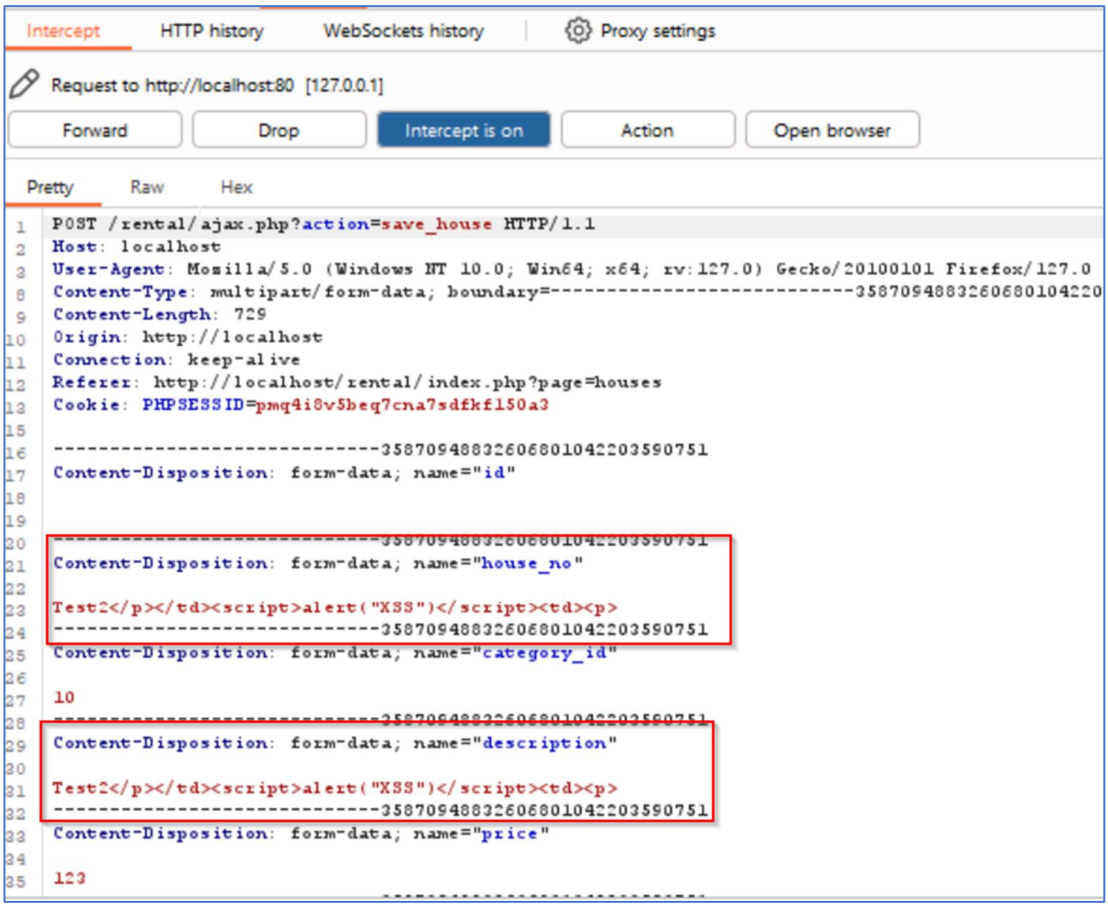
1. Login into the Best House Rental Management System and go to menu "House" -> "Add". URL: http://localhost/rental/index.php?page=houses

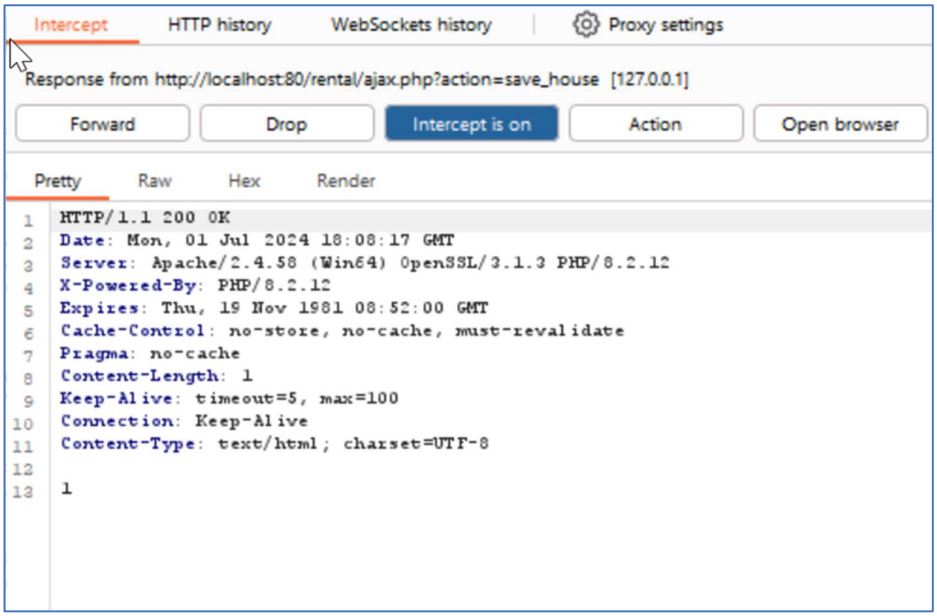


2. Insert the XSS script "***Test2 </td><script>alert("XSS")</script><td> ***" in the "**House_no**" and "**Description**" fields as shown in the following screenshot. Click "Save".

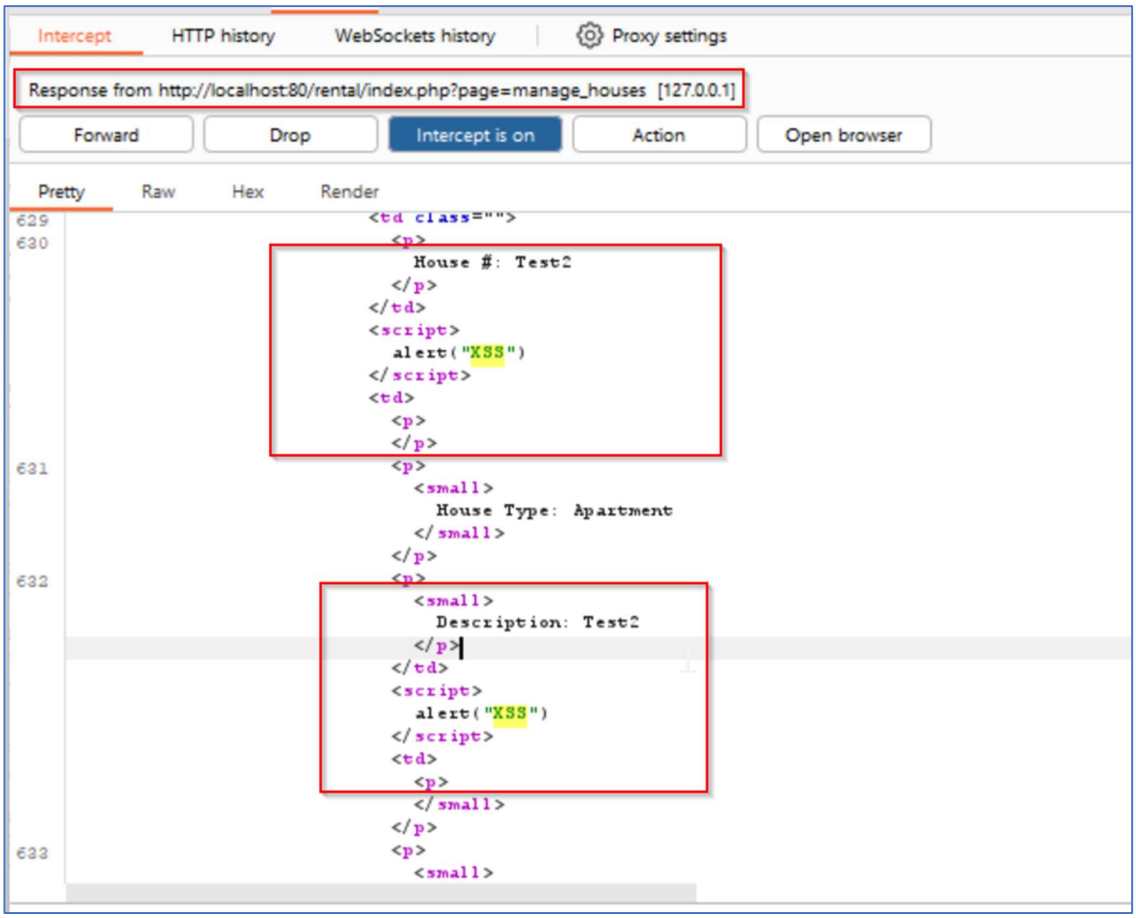


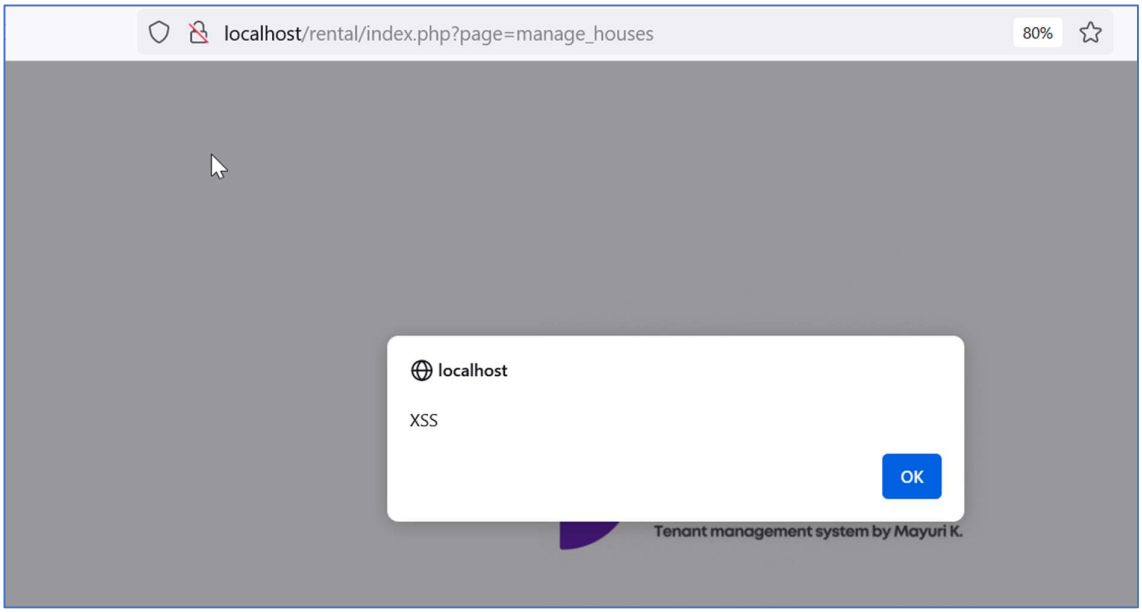
3. This will forward the request with XSS script to server. The request gets accepted and the House name entry with XSS script is stored in the application database.





4. Every time we access the House name list (URL: http://localhost/rental/index.php?page=manage_houses), 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