A Cross-Site Request Forgery (CSRF) vulnerability was found in SourceCodester Best House Rental Management System v1.0. This could lead to an attacker tricking the administrator into adding/modifying/deleting valid tenant data via a crafted HTML page, as demonstrated by a Delete Tenant action at the /rental/ajax.php?action=delete_tenant URI.

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

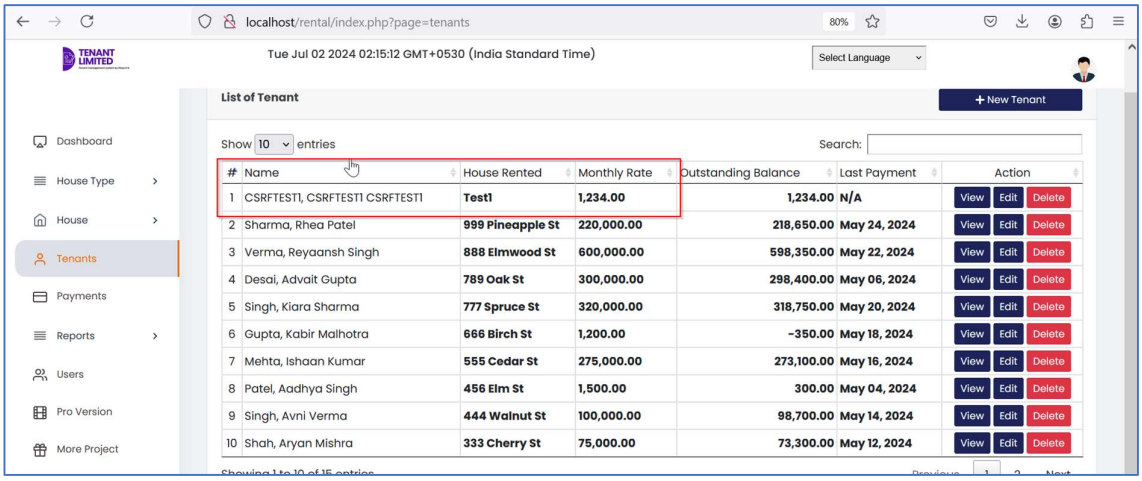
Affected Components:

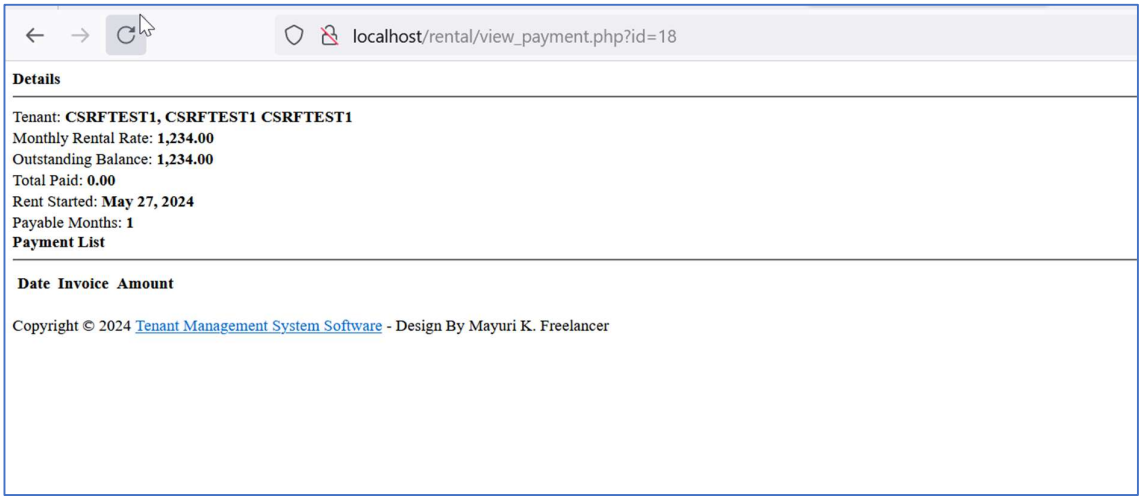
- **Affected File:** /rental/tenants.php
- **Application URL:** http://localhost/rental/ajax.php?action=delete_tenant

Steps:

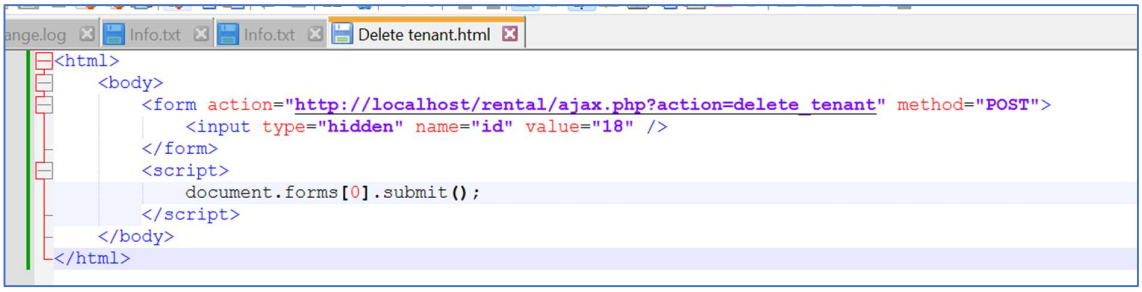
1. Login into the Best House Rental Management System and go to menu "Tenants" URL: http://localhost/rental/index.php?page=tenants

2. 1st entry is for "CSRFTEST1" tenant with ID="18". This is a tenant which was created to demonstrate CSRF attack

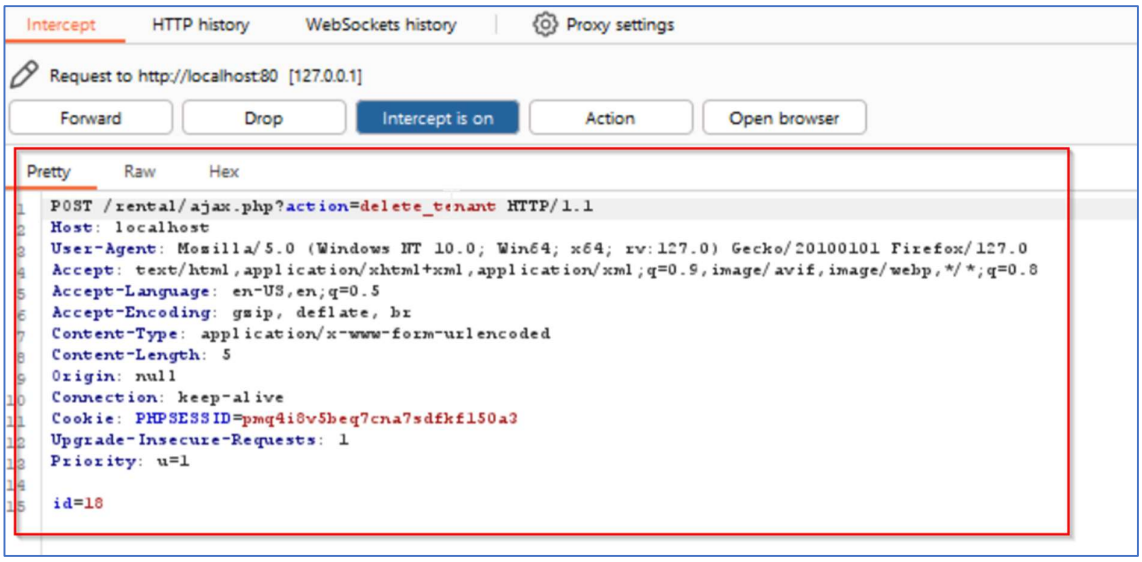


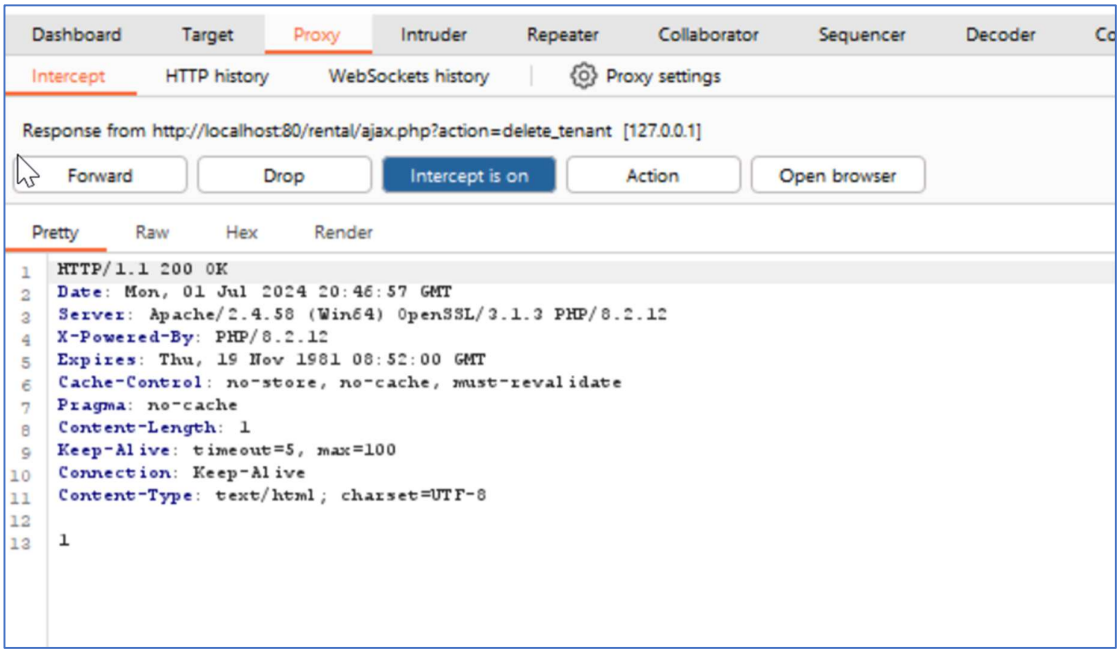


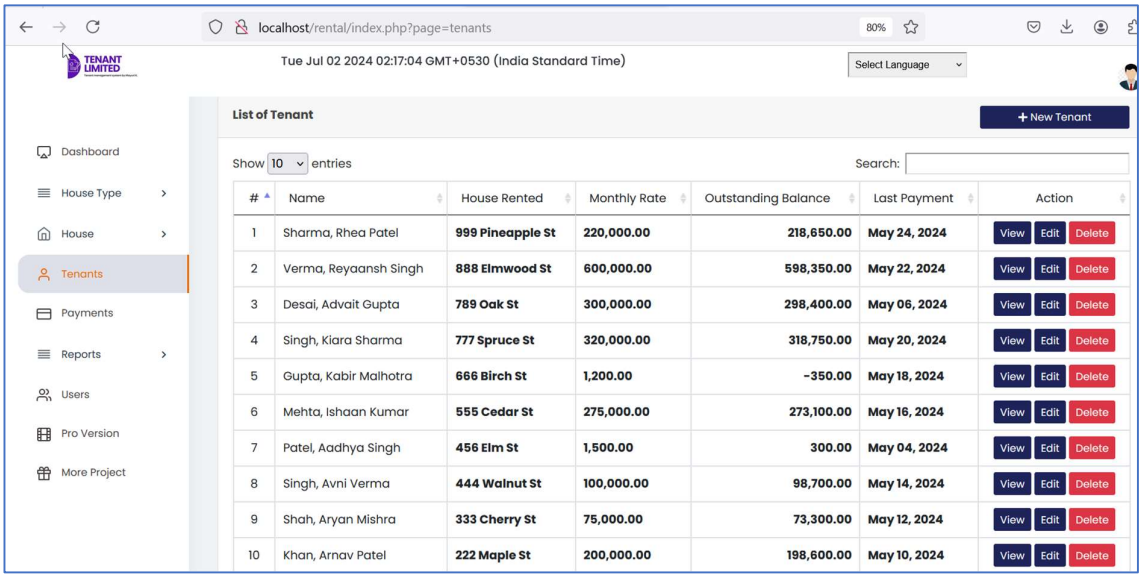
3. Now in new tab, open the CSRF POC with HTML script mentioned below:



4. As soon as the HTML page is opened, the request is sent to the server and the "CSRFTEST1" tenant with ID="18" gets deleted. This is because there is no Anti-CSRF protection in place.







Solution/Good Reads:

Implement Anti-CSRF Tokens.

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

https://portswigger.net/web-security/csrf/preventing