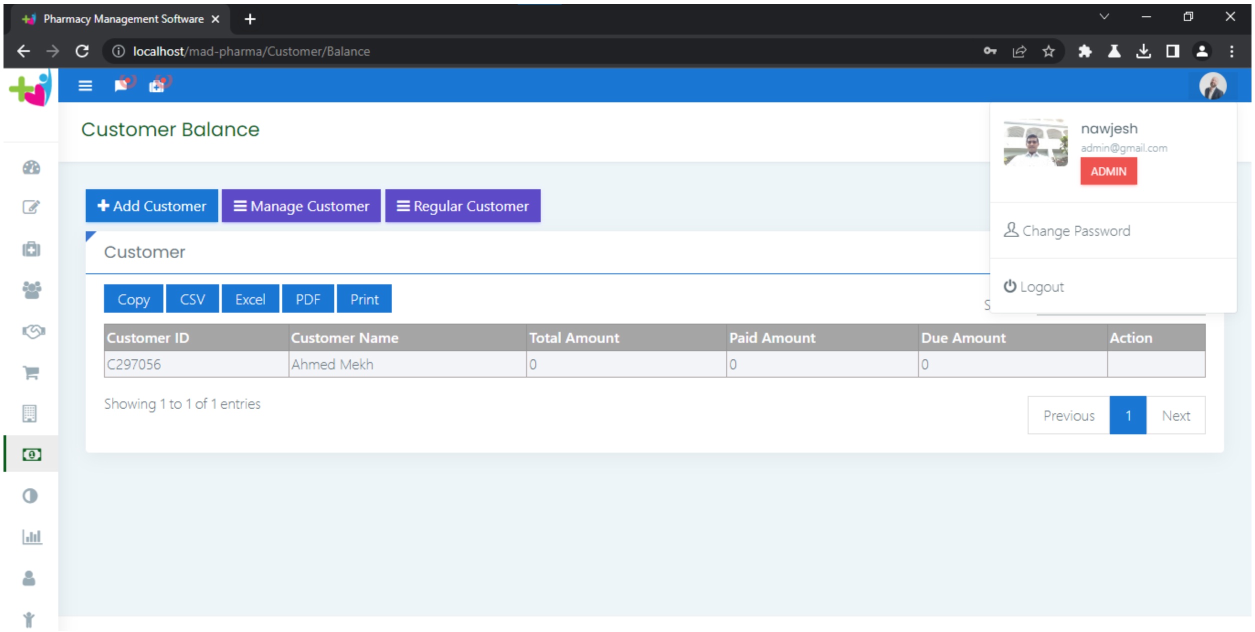
Assignment 1 Ahmed Khaled Saad Ali 1809799

1. Vulnerability

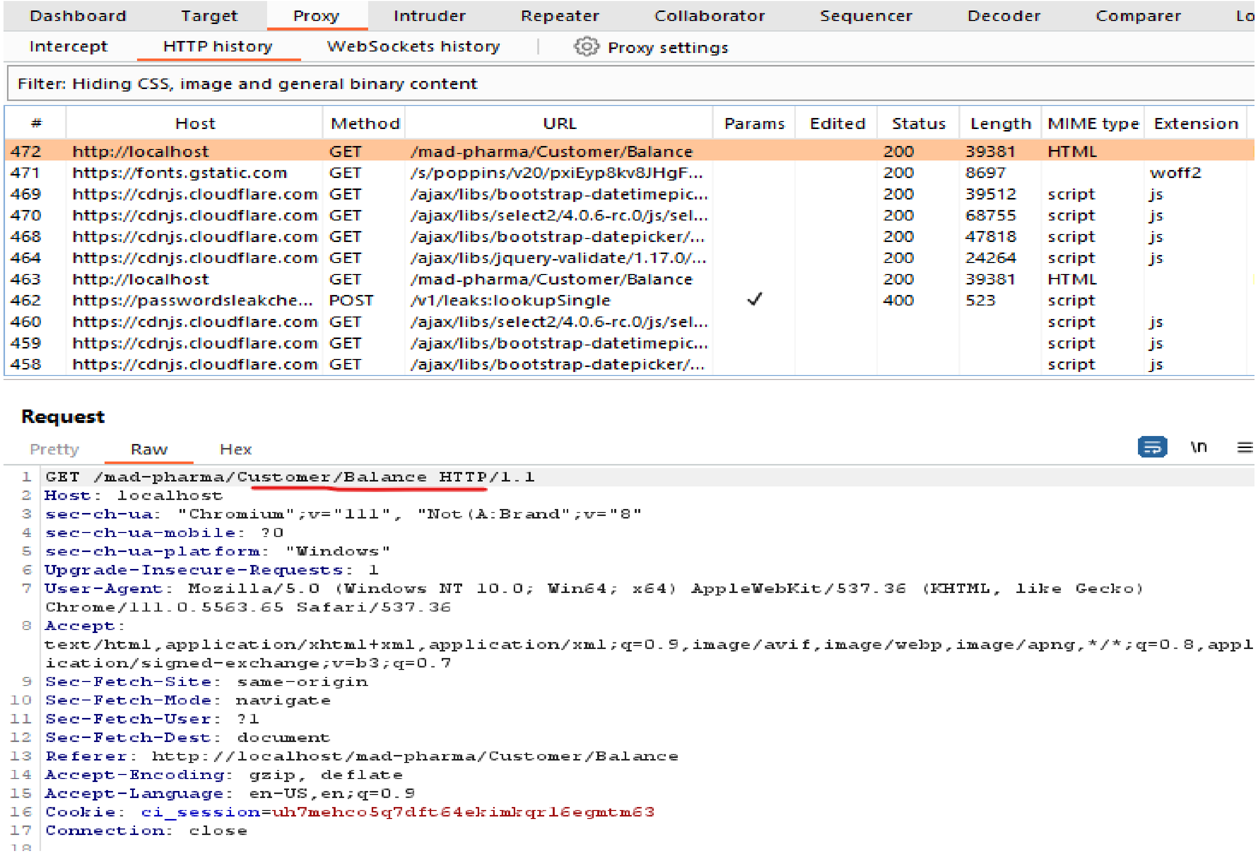
Customer Balance page in Admin Account



Customer ID	Customer Name	Total Amount	Paid Amount	Due Amount	Action
C297056	Ahmed Mekh	0	0	0	

Showing 1 to 1 of 1 entries

Get Request of Customer Balance

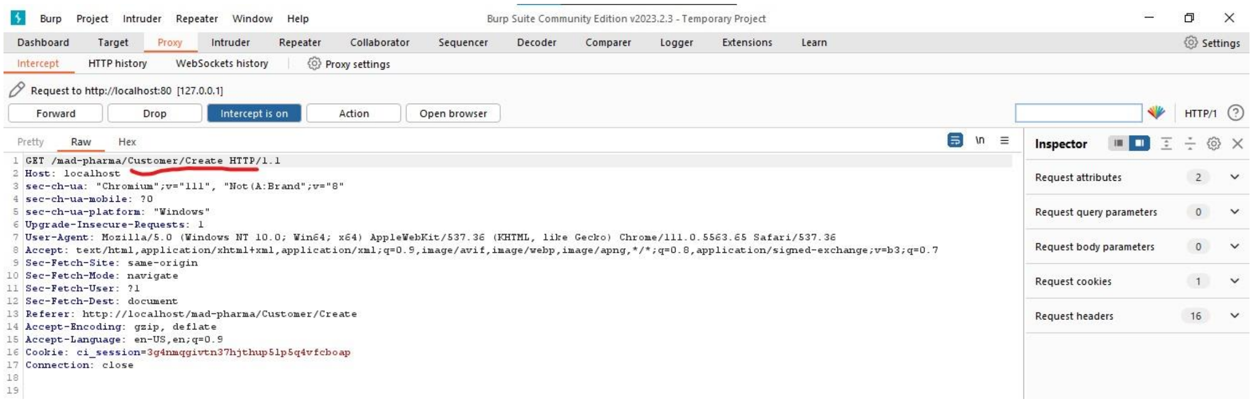


Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
472	http://localhost	GET	/mad-pharma/Customer/Balance			200	39381	HTML	
471	https://fonts.gstatic.com	GET	/s/poppins/v20/pxiEyp8kv8JHgF...			200	8697		woff2
469	https://cdnjs.cloudflare.com	GET	/ajax/libs/bootstrap-datetimepic...			200	39512	script	js
470	https://cdnjs.cloudflare.com	GET	/ajax/libs/select2/4.0.6-rc.0/js/sel...			200	68755	script	js
468	https://cdnjs.cloudflare.com	GET	/ajax/libs/bootstrap-datepicker/...			200	47818	script	js
464	https://cdnjs.cloudflare.com	GET	/ajax/libs/jquery-validate/1.17.0/...			200	24264	script	js
463	http://localhost	GET	/mad-pharma/Customer/Balance			200	39381	HTML	
462	https://passwordsleakche...	POST	/v1/leaks:lookupSingle	✓		400	523	script	
460	https://cdnjs.cloudflare.com	GET	/ajax/libs/select2/4.0.6-rc.0/js/sel...					script	js
459	https://cdnjs.cloudflare.com	GET	/ajax/libs/bootstrap-datetimepic...					script	js
458	https://cdnjs.cloudflare.com	GET	/ajax/libs/bootstrap-datepicker/...					script	js

```
GET /mad-pharma/Customer/Balance HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/111.0.5563.65 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
ication/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/mad-pharma/Customer/Balance
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ci_session=uh7mehco5q7dft64ekimkqrl6egmtm63
Connection: close
```

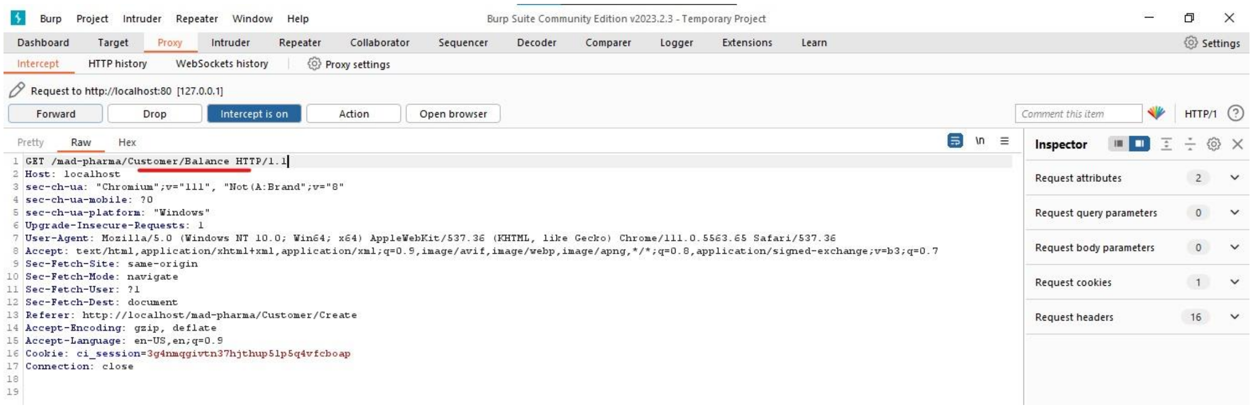
Customer Create in Salesman Account



```
GET /mad-pharma/Customer/Create HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/mad-pharma/Customer/Create
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ci_session=3g4nmqgivtn37hjthup5lp5q4vfcboap
Connection: close


```

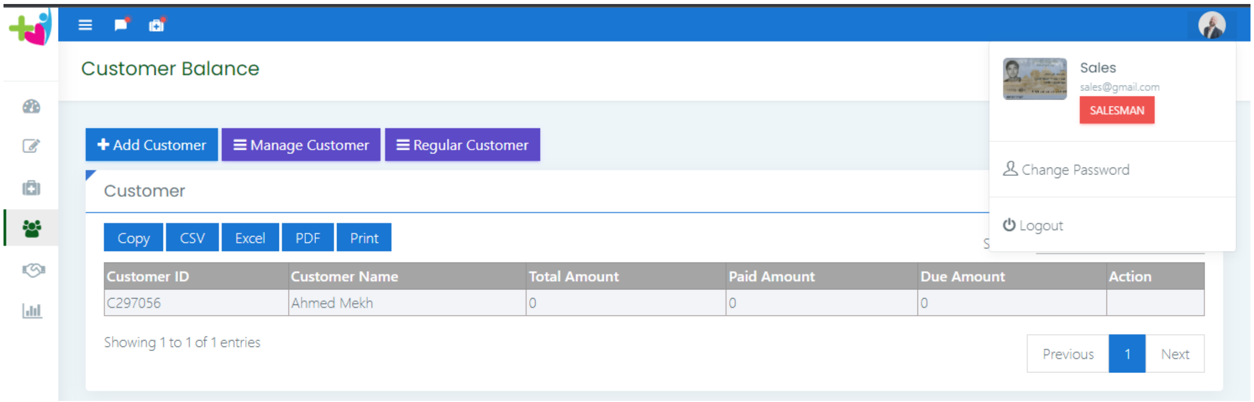
Entered Get Request of Customer Balance(admin-only feature) instead in Salesman account



```
GET /mad-pharma/Customer/Balance HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/mad-pharma/Customer/Create
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ci_session=3g4nmqgivtn37hjthup5lp5q4vfcboap
Connection: close


```

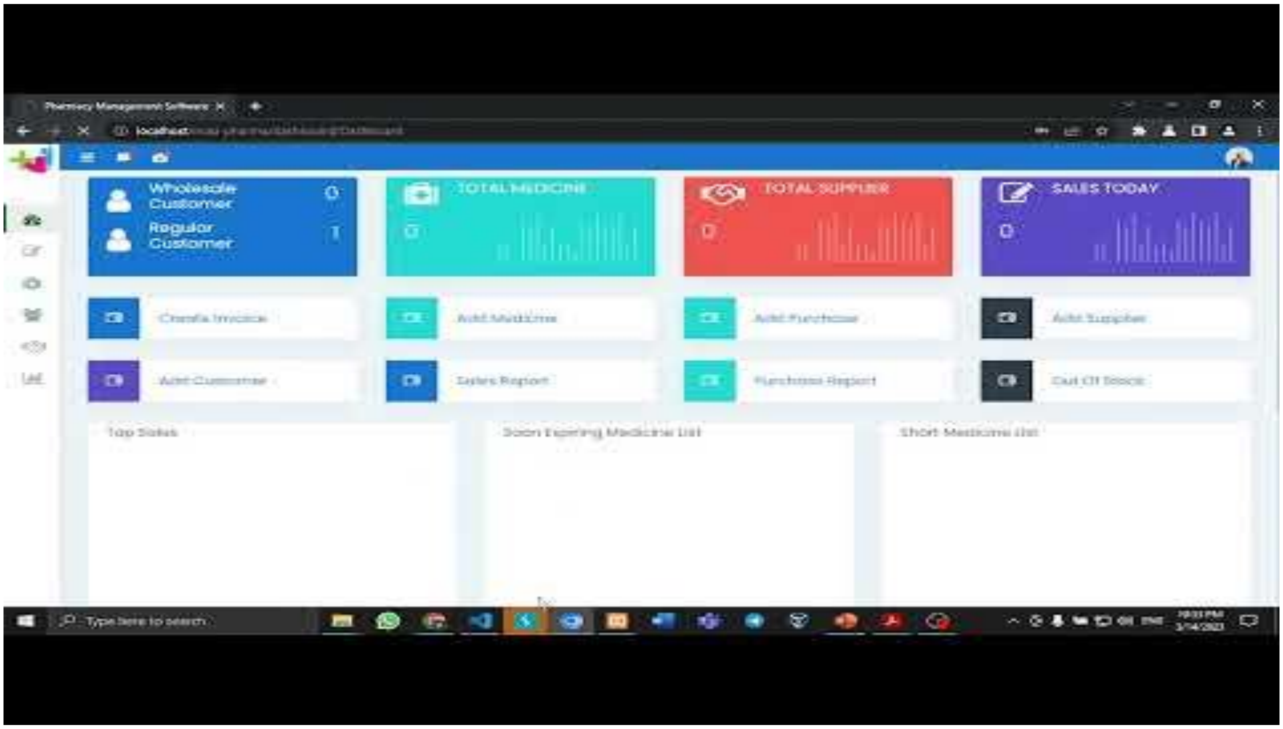
Top right it's a Salesman account, but we are in Customer Balance Page



Customer ID	Customer Name	Total Amount	Paid Amount	Due Amount	Action
C297056	Ahmed Mekh	0	0	0	

Showing 1 to 1 of 1 entries

Demo Video for Vulnerability, Click it



2. Vulnerability fixing

We will go to “Customer_Balance.php” and find out there is no condition to load this page, so we need to add an If condition that permits only Managers & Admins to load such page.
“Customer_Balance.php” file location is: mad-pharma\application\views\backend

```
<?php
if($this->session->userdata('user_type') =='ADMIN' ||
$this->session->userdata('user_type') =='MANAGER')
{
    $this->load->view('backend/header');
    $this->load->view('backend/sidebar');
}else{
    redirect('dashboard/Dashboard');
}
?>
```

So, when we try again through Burp to manipulate GET request for “Salesman” to enter “Customer Balance” page it will redirect us to “Dashboard” page, this will be observed in the “Video below”.
Also, we will make sure that “Admin” can still access “Customer Balance” page normally.

Click it.