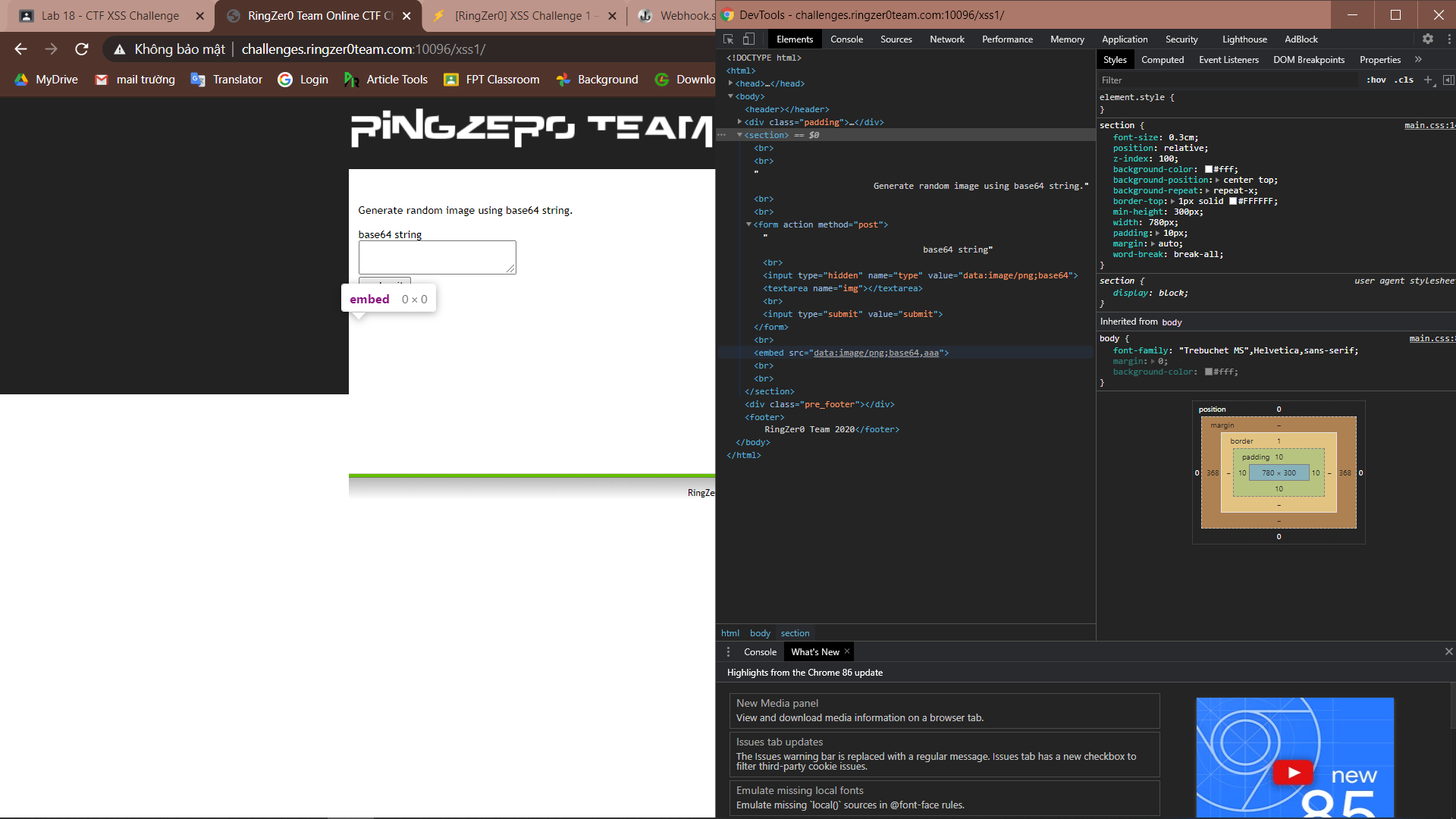
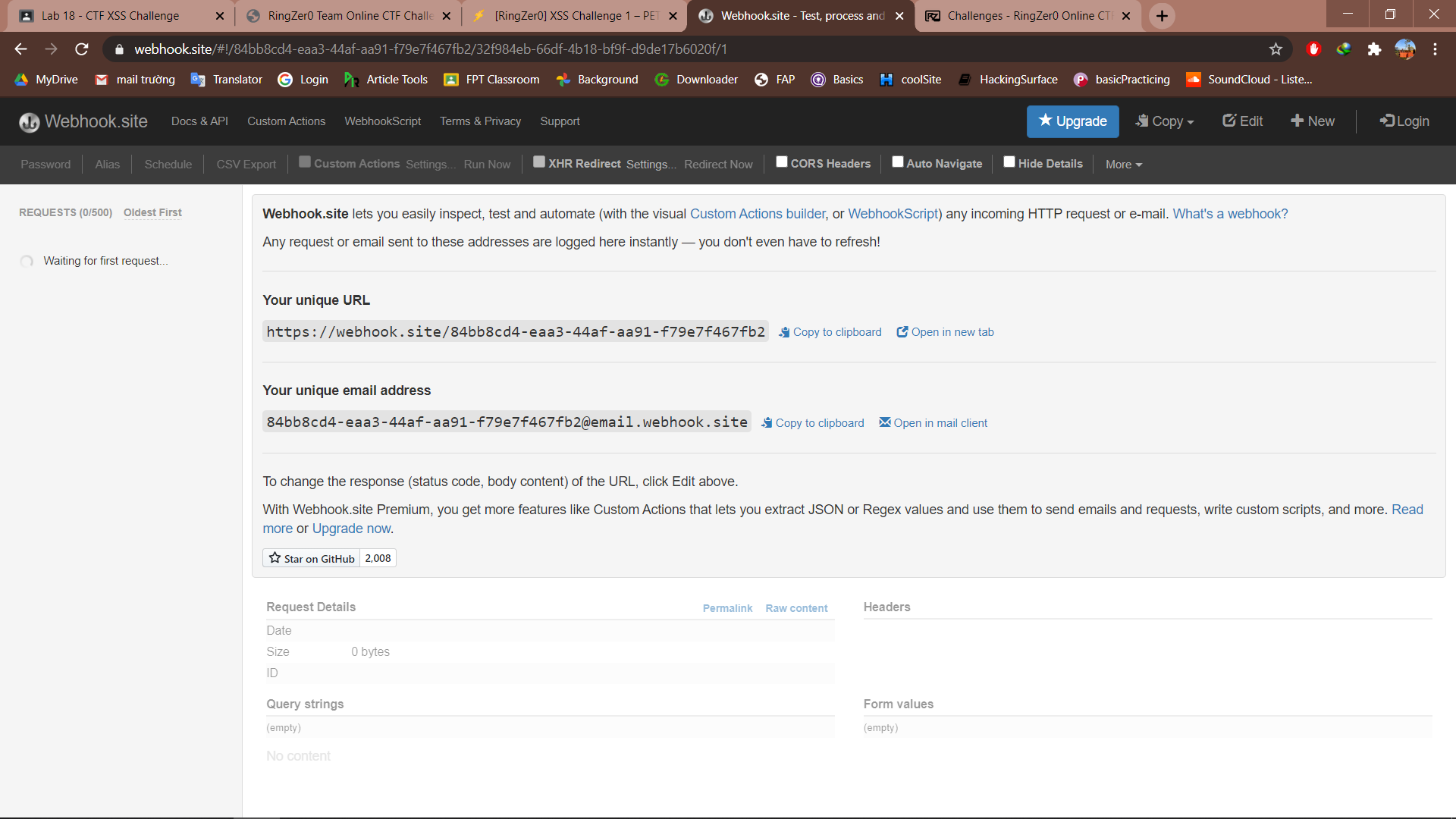
|  |  |
| --- | --- |
| Class & Module | IAW301  Lab 18: CTF XSS Challenge |
| Name | Nguyễn Đức Kiên |
| IC No. | HE141763 |
| Date & Time | October 22, 2020 |

#### Exercise 1.1 XSS Challenge 1

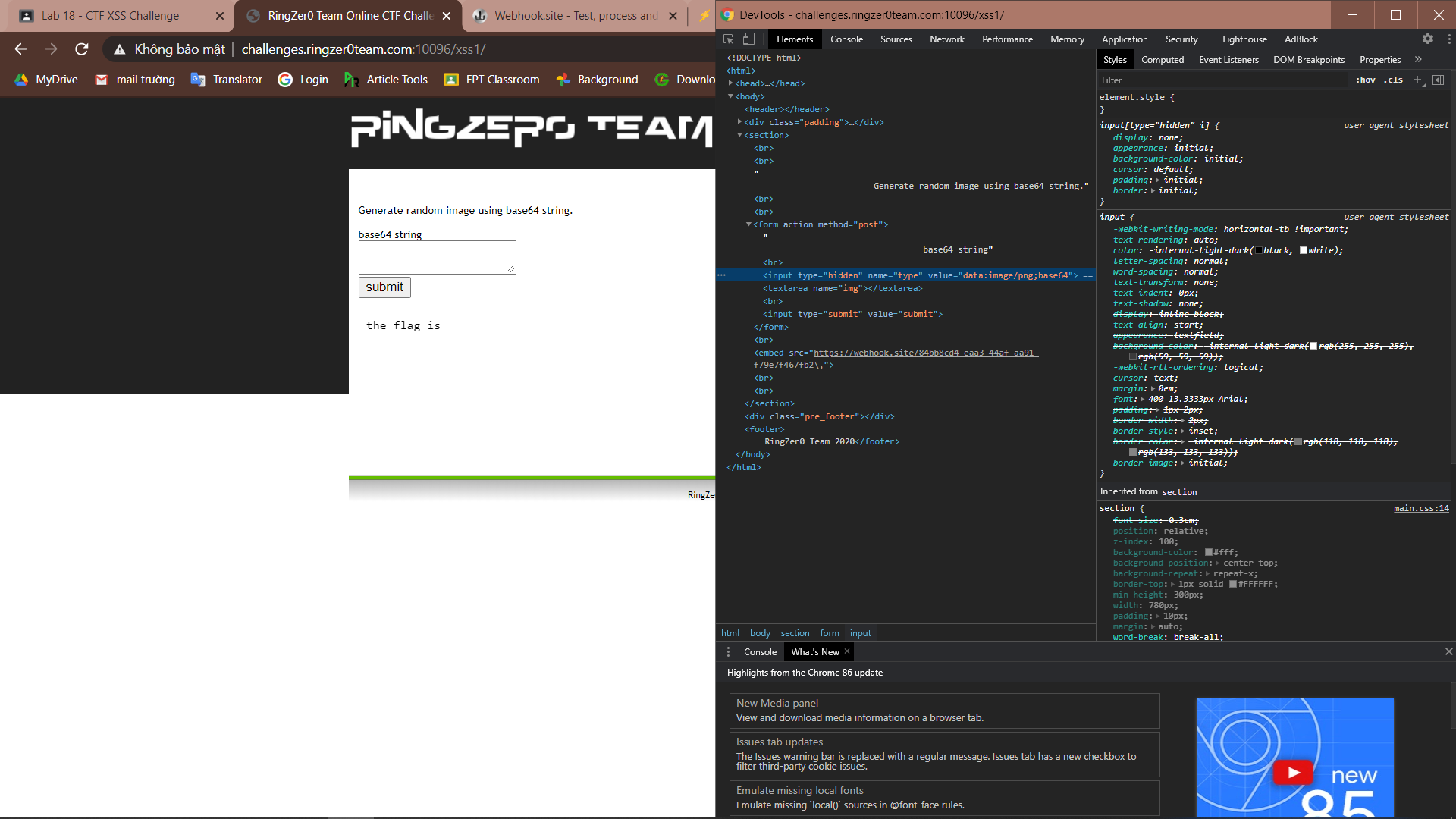
First in the website use F12 to inspect the page, noticed that there is an embed field which is hidden when we submit anything as input (here I used “aaa”).



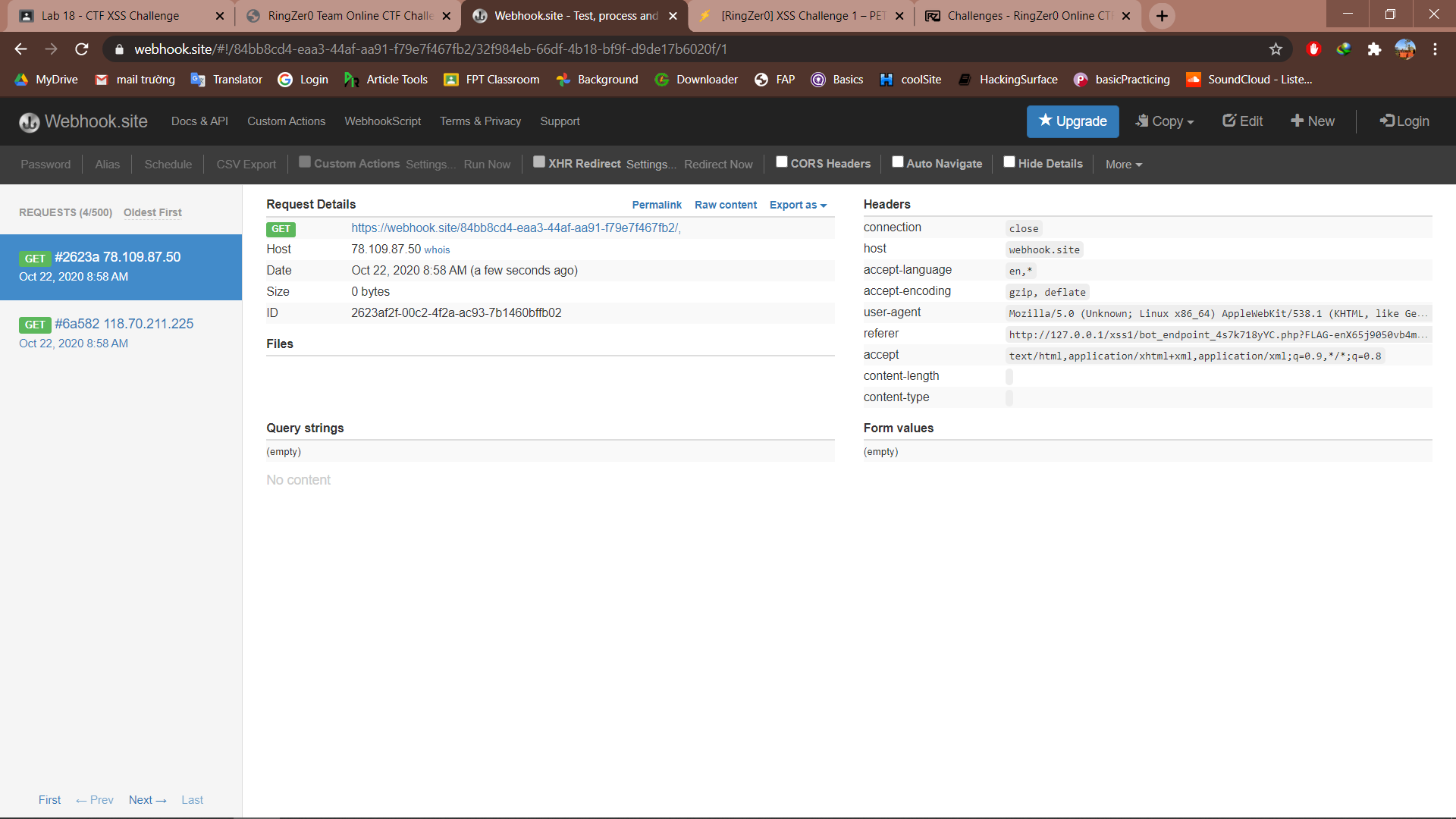
Go to webhook.site to create a site to catch respond



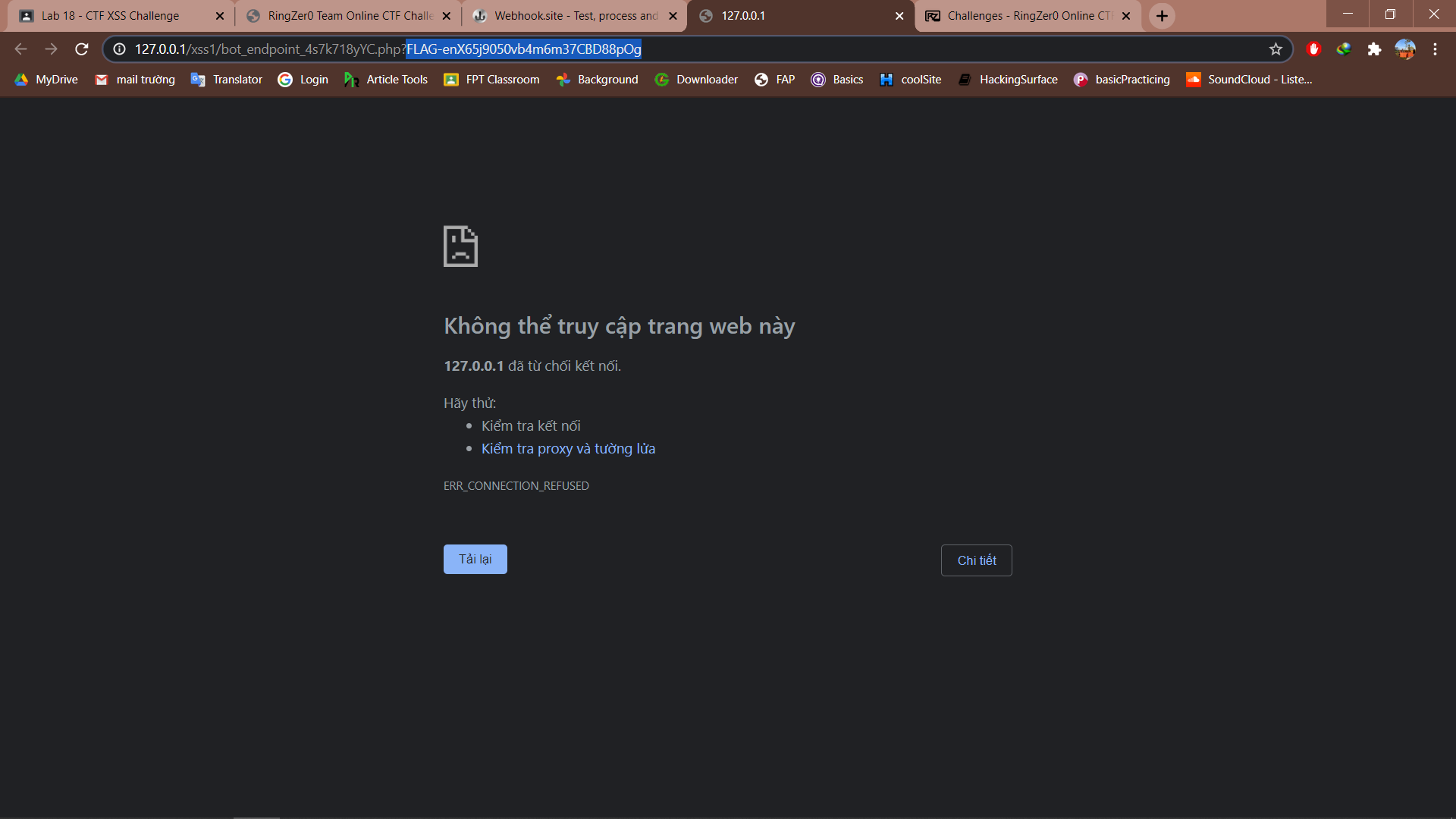
Copy the link and paste it into the value attribute, remember to add the “\” at the end to ignore the “,” which purpose is to append. Press submit and we have the output, the output content can be edited in webhook.



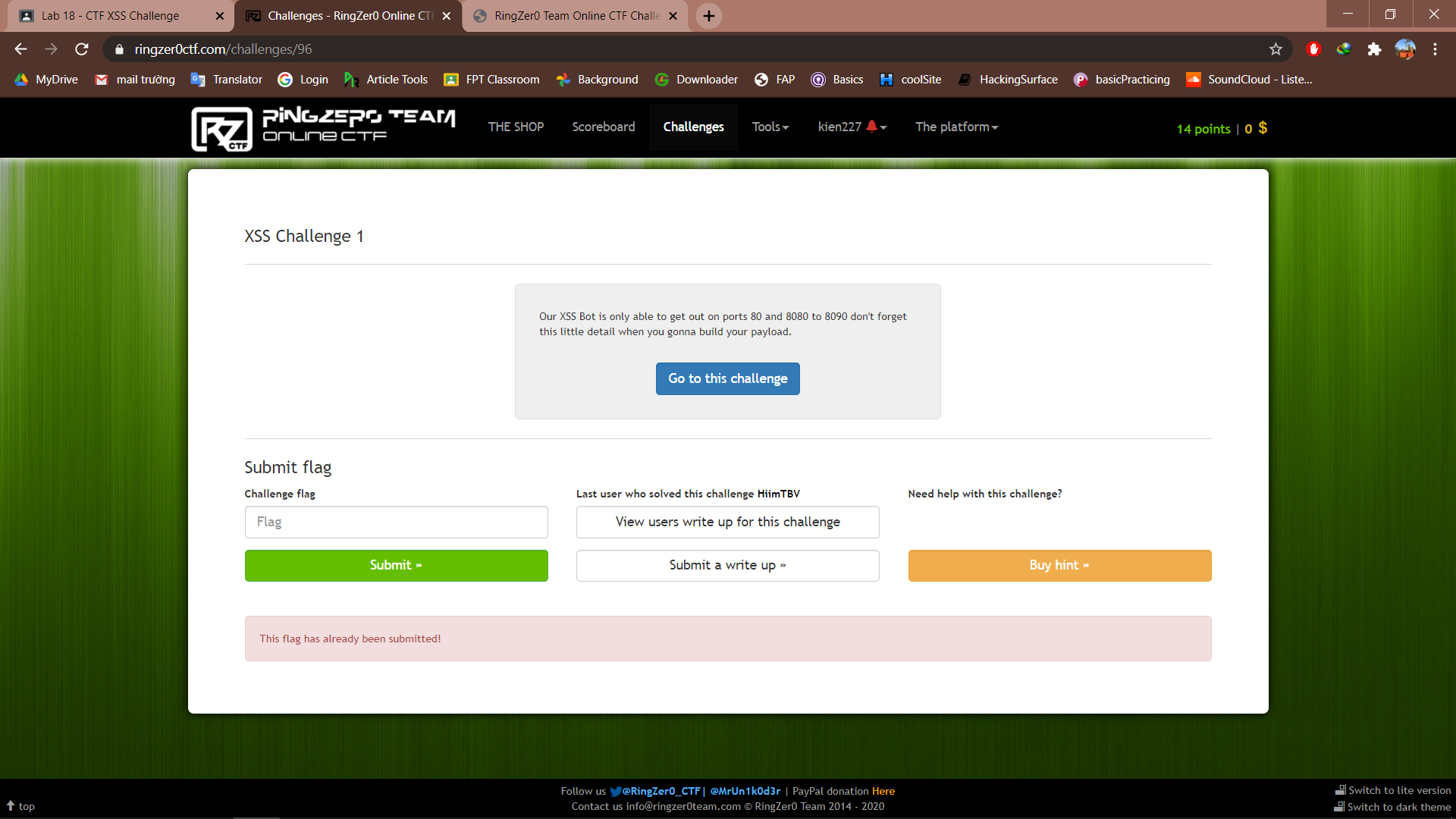
Noticed there are requests at webhook, we can start checking it out



First one was from something called “bot-endpoint” so we check this by copy the link and forward to the site. And we see the flag in the url.

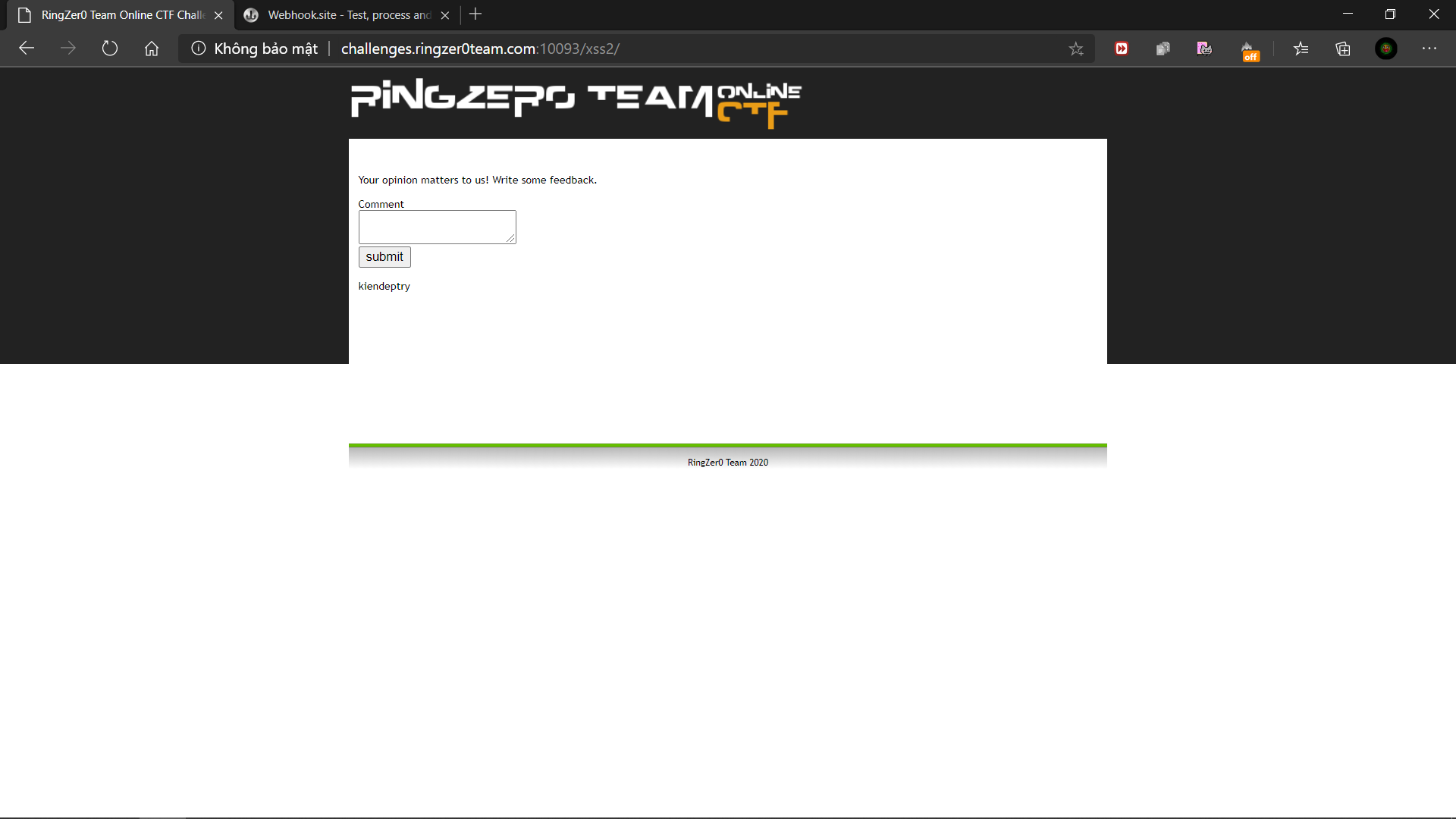


However I submitted the flag by accident

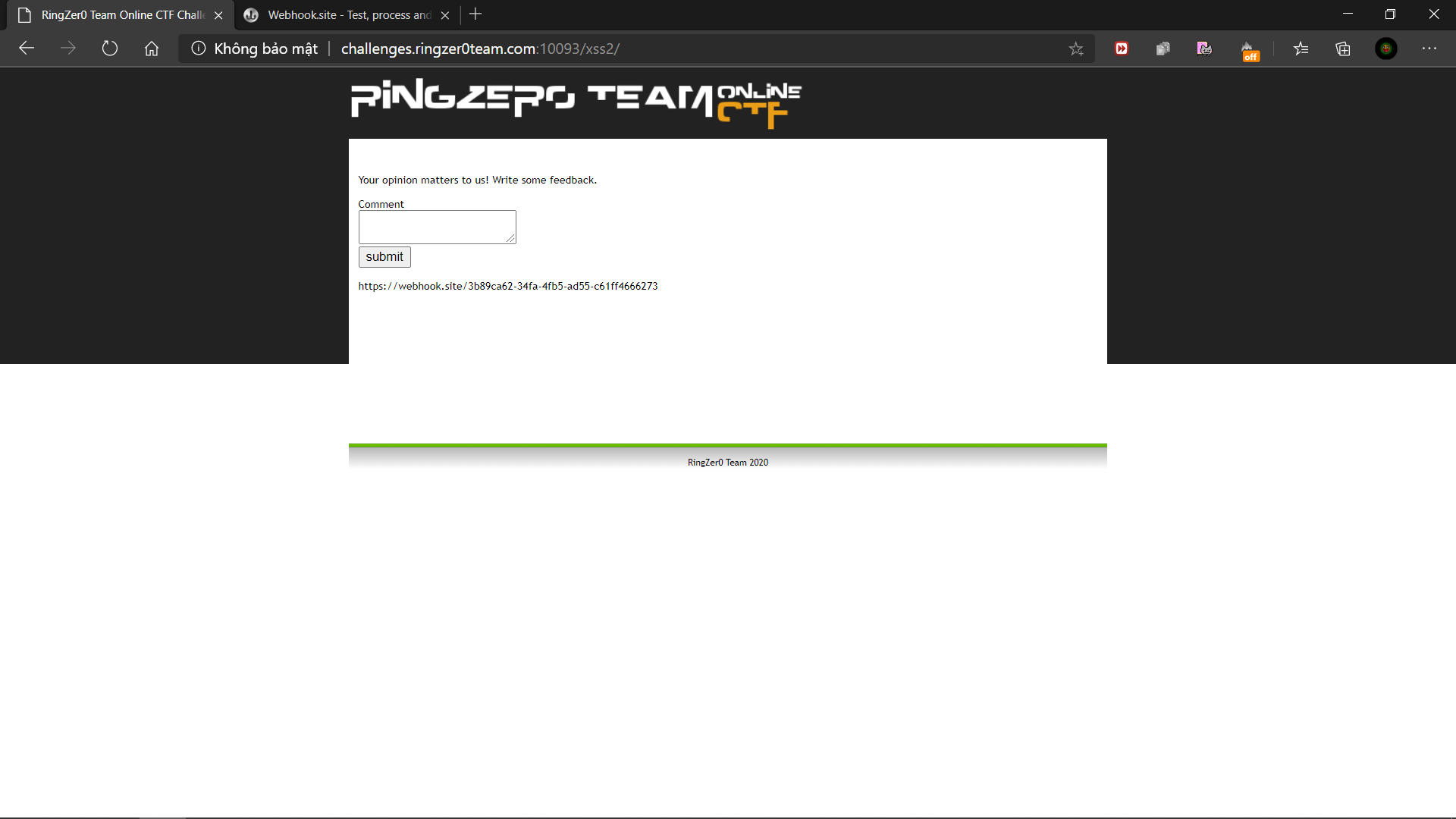


**Exercise 1.2 XSS Challenge 2**

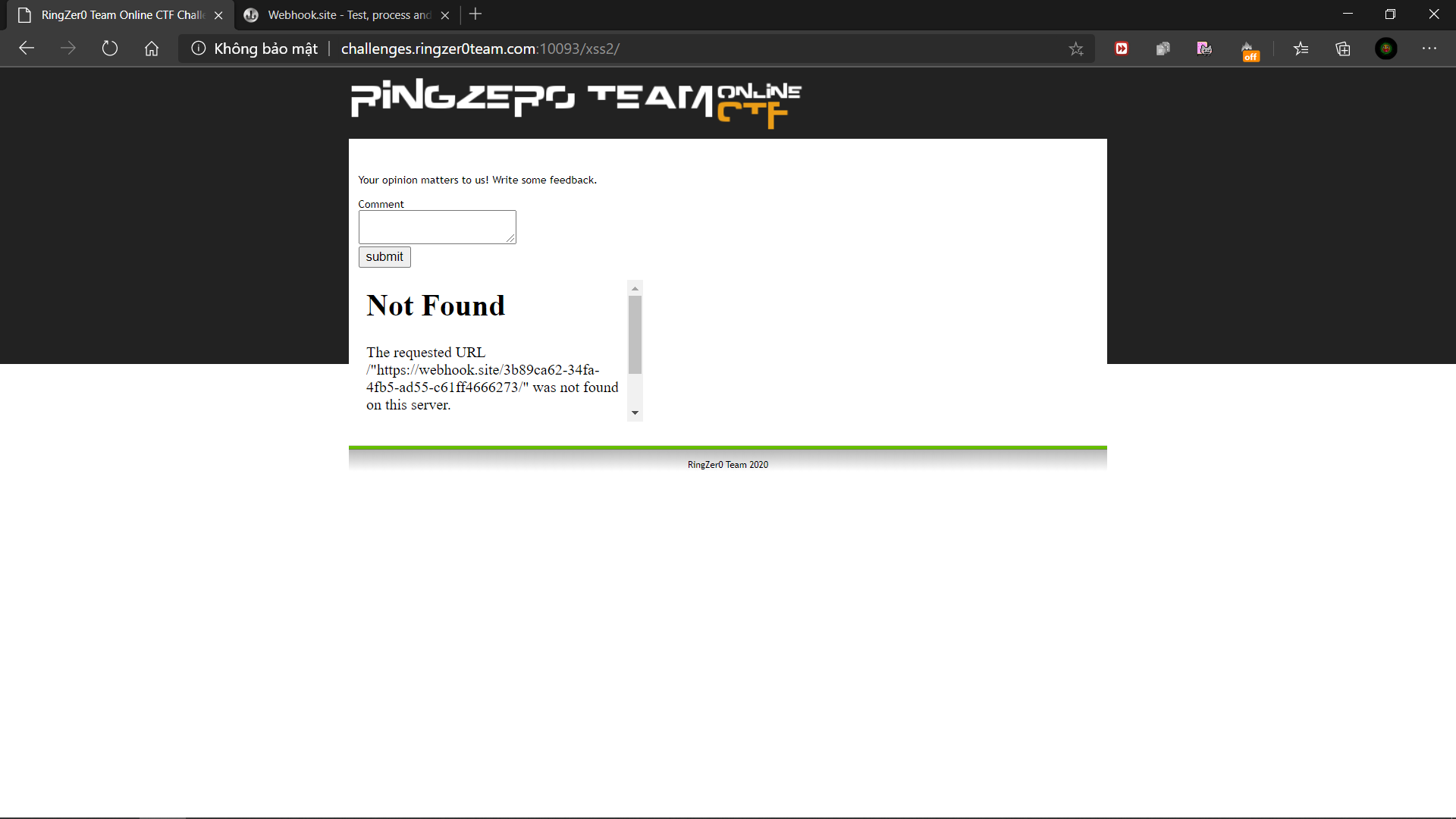
First better start by inputting something in the input field, as can be seen the input is shown under the submit button.



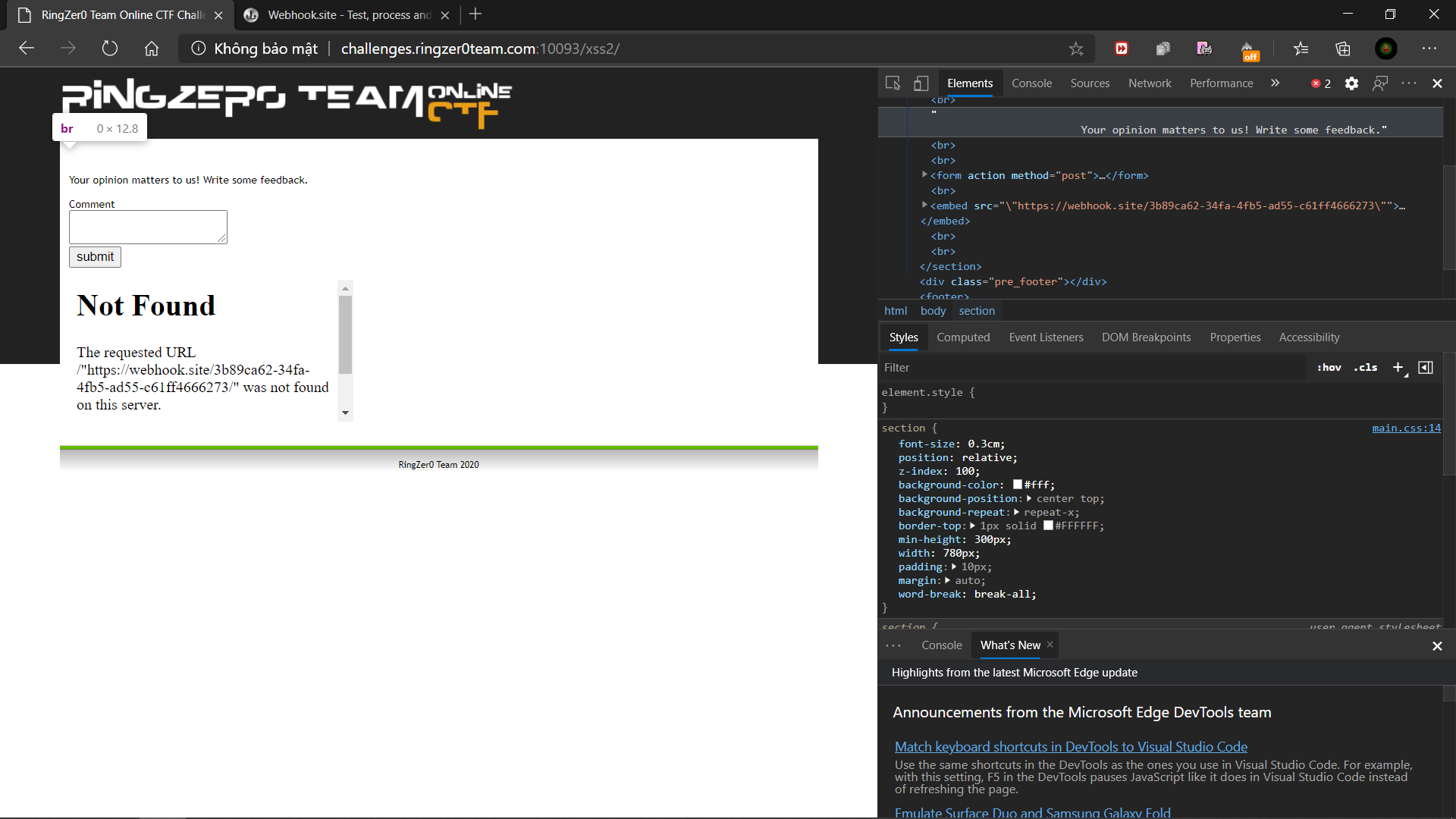
I have an instant idea of refering our webhook link in the comment, try this and see



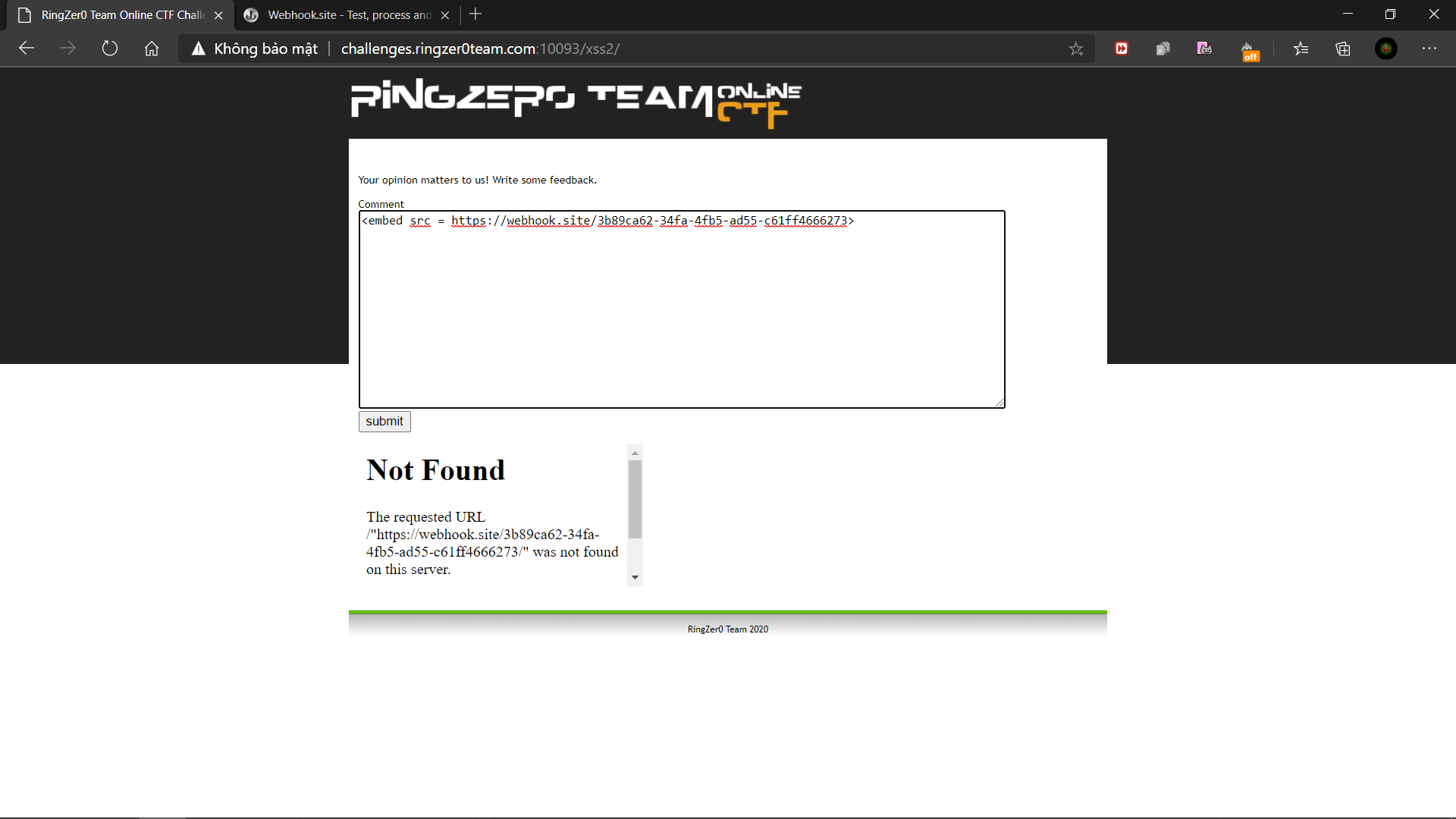
The link is shown as a plain text output and was not forwarded to the site, learnt from xss challenge 1 we can use the ‘embed src=”” to refer our link to the website, tried this and get the result.



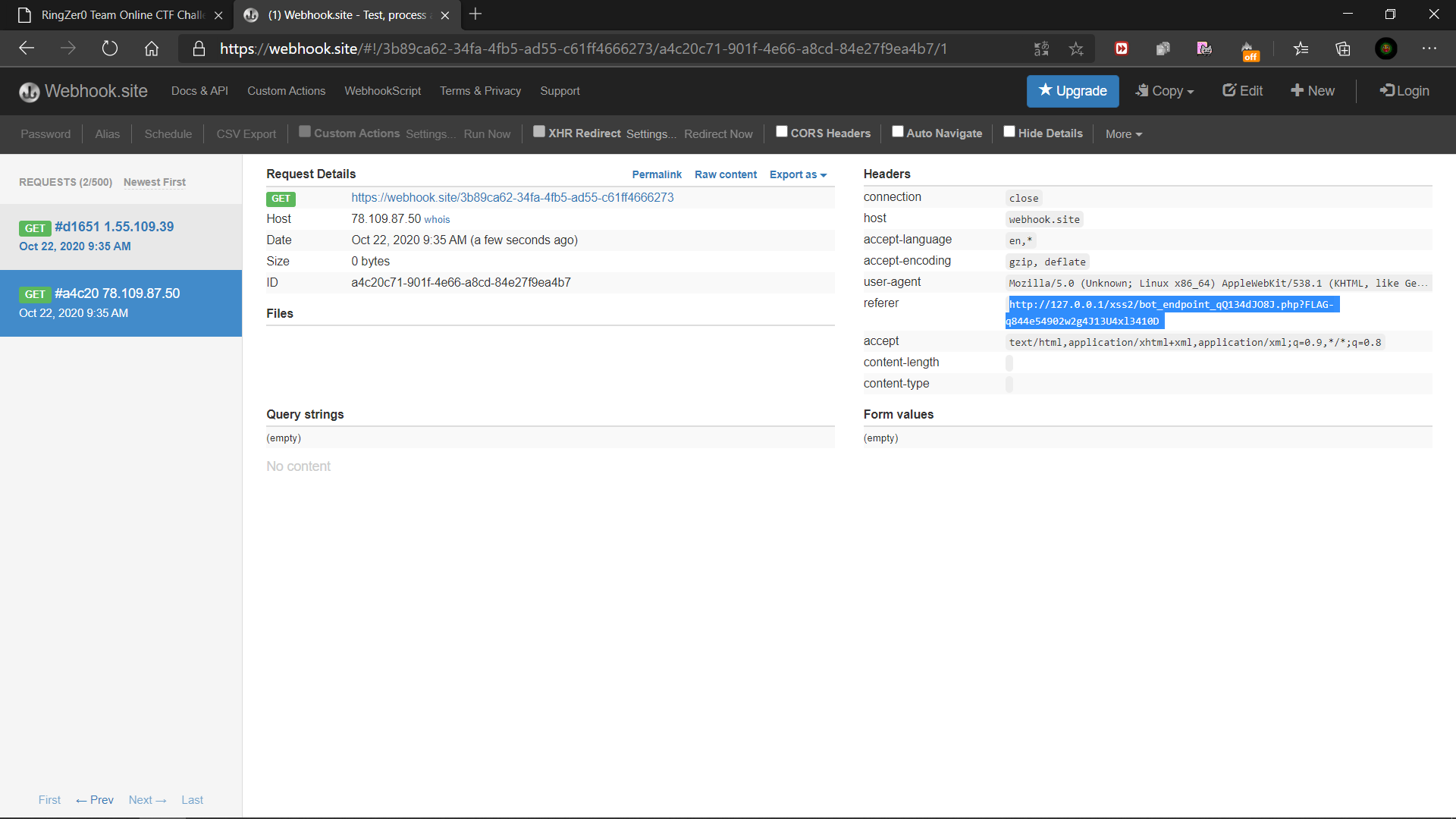
Turn on the inspect tab to see what is happening



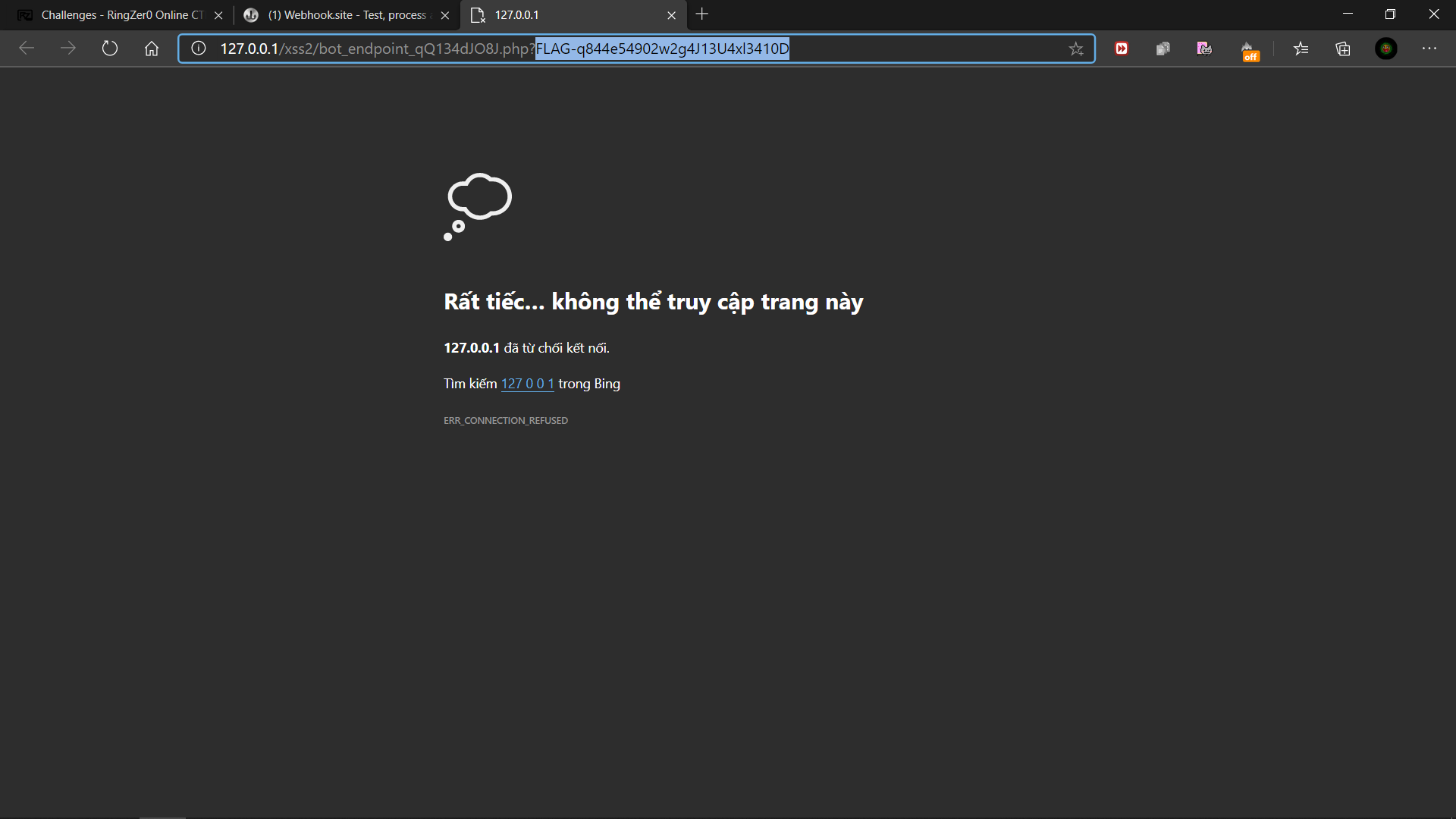
Noticed that we are having some extra “ at the start and the end of our link, so we can start by simply removing our own “ “ to see what happen



Pressed submit with no problem or error screen, swap to the webhook site to check, we see a request, isn’t it familiar with that “bot\_endpoint” thing.



Forward to the link we can see our flag in the url



Submit the flag and tada!

