ST#IS#4899

TASK – 5

TARGET:

-> You need to complete 5 XSS (Cross Site Scripting) from the following platform.

-> https://xss-quiz.int21h.jp/

- You need to prove there is a XSS vulnerability in that particular web page.

NOTE:

- ❖ You need to complete challenges one after the other because after the completion of 1st challenge only you will enter into the 2nd challenge.
- ❖ Challenges 2 to 6 are considered as task-5.

SYNOPSIS:

XSS – cross site scripting:

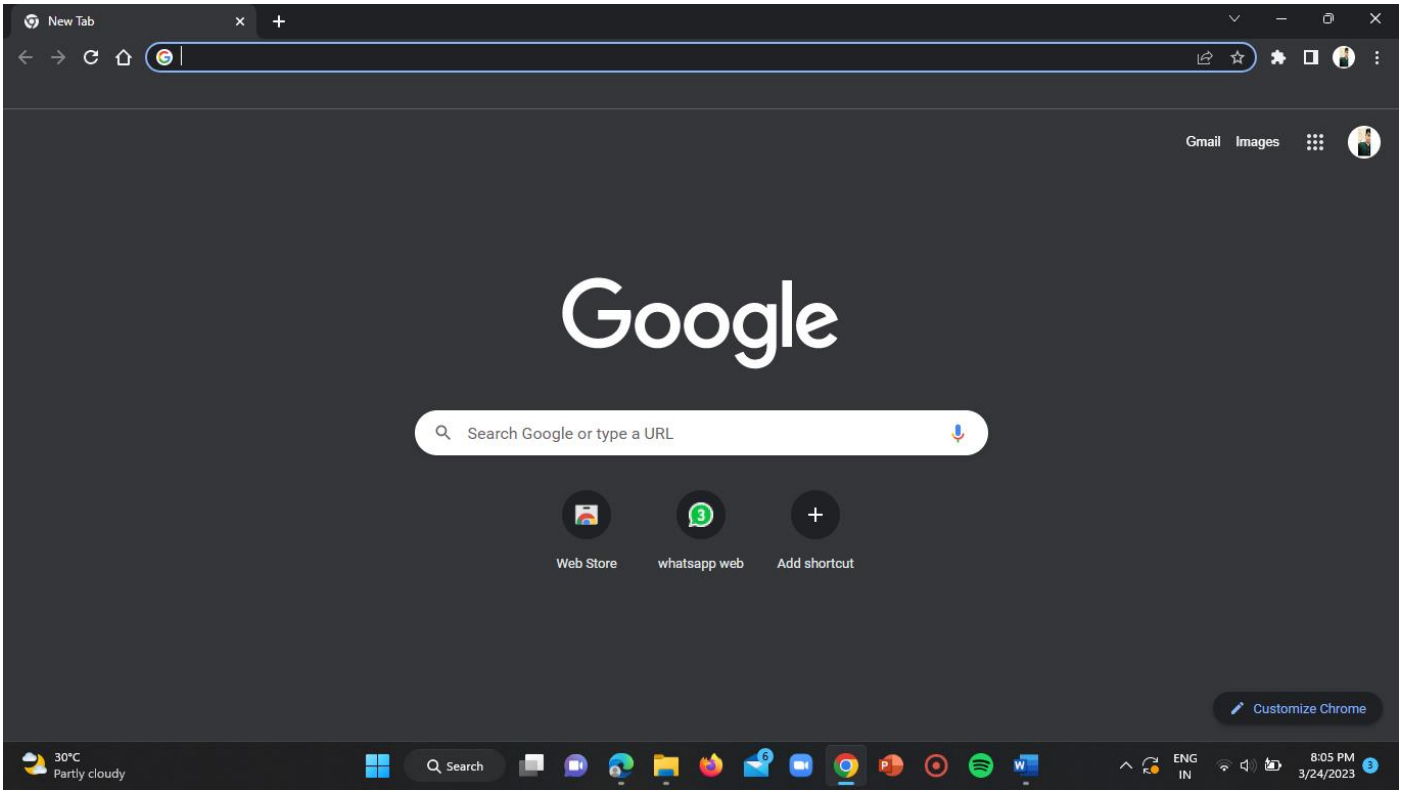
- ➢ Cross site scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise being and trusted websites.
- ➢ XSS attacks occur when:
- Data enters a web application through an untrusted source, most frequently a web request.
- Data is included in dynamic content that is sent to a web user without being validated for malicious content.
  - ➢ Example of XSS include running unverified code on social media platforms or online games.

SOLUTION:

Step-1:

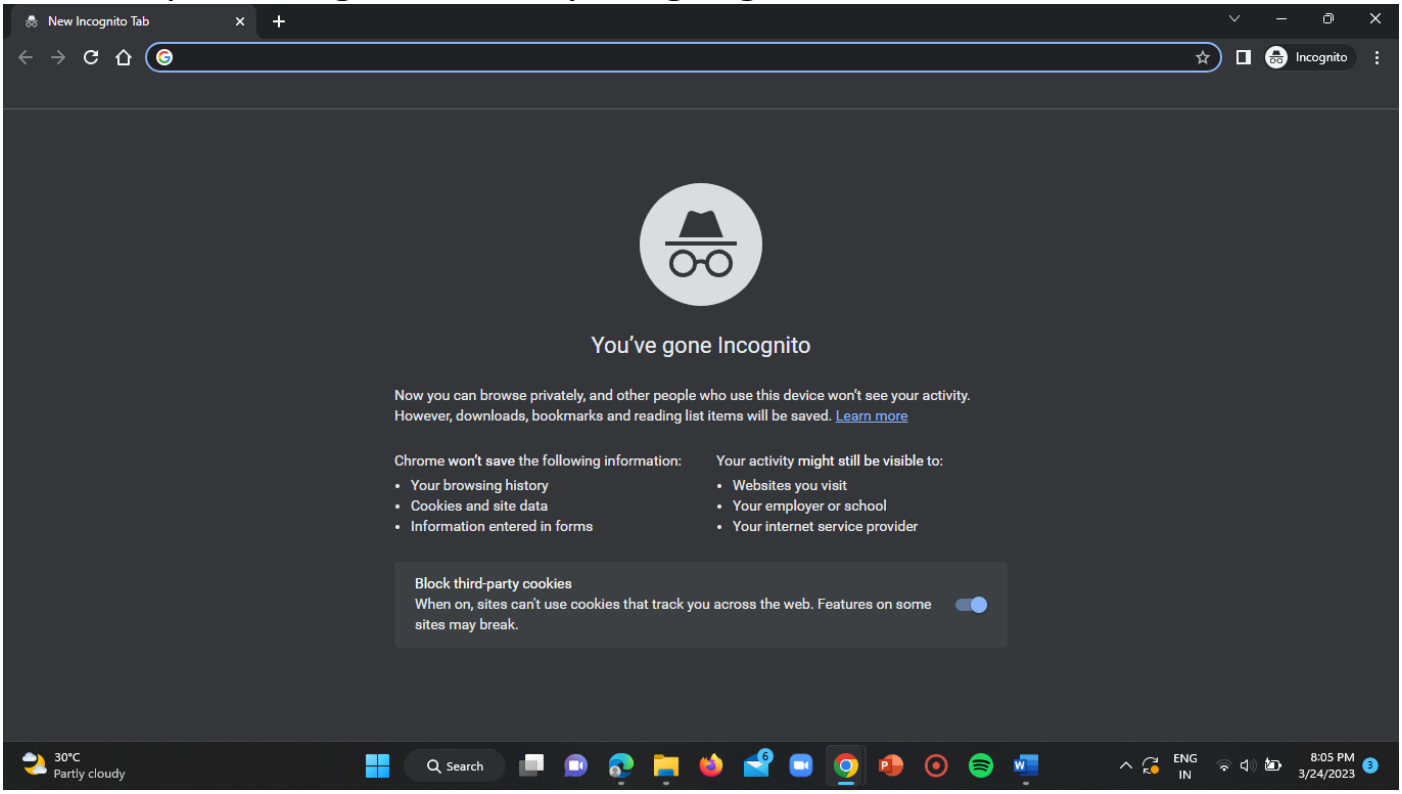
Open google chrome on your PC.

ST#IS#4899



Step-2:

Open incognito tab in your google browser.



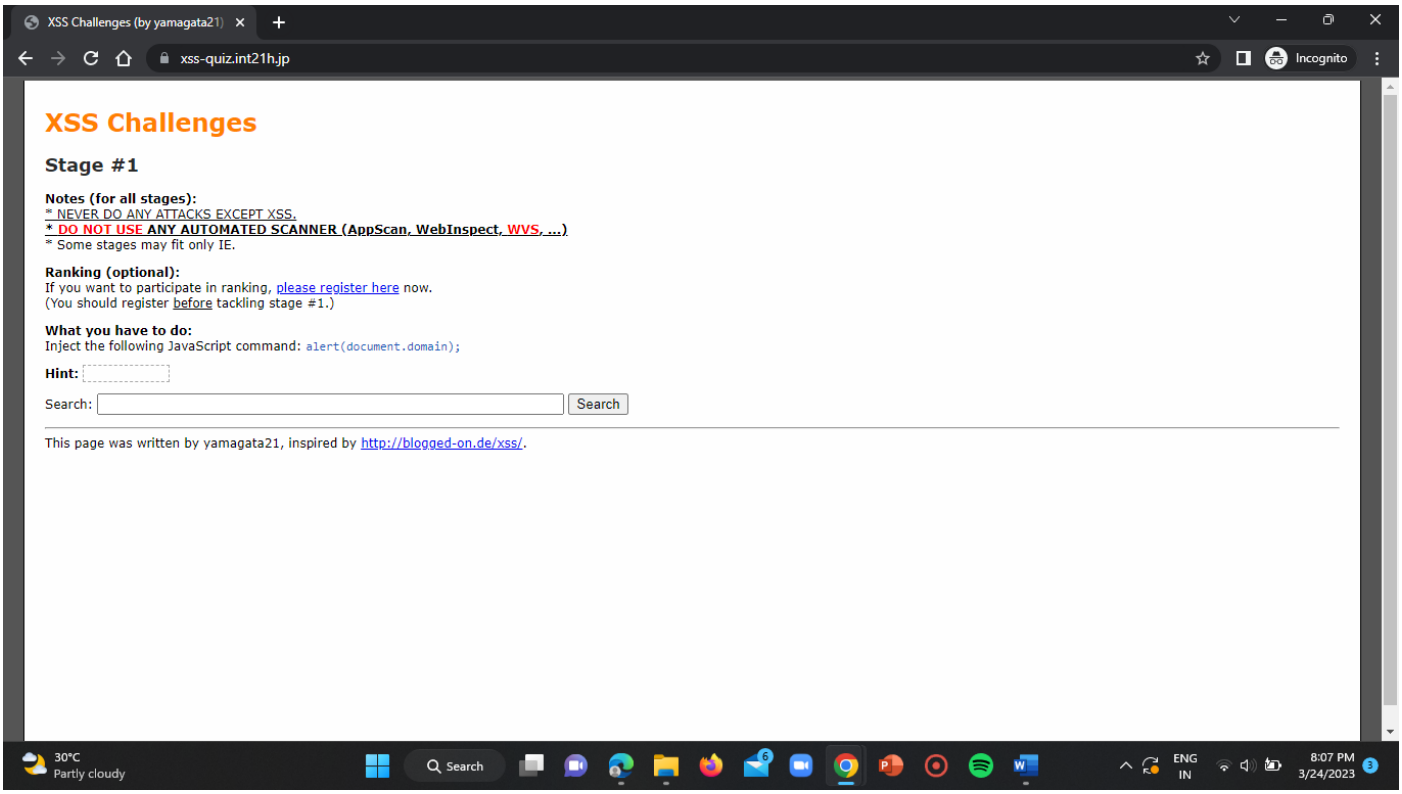
Challenge – 1:

Step-3:

Now go to above mentioned site i.e,

ST#IS#4899

https://xss-quiz.int21h.jp/



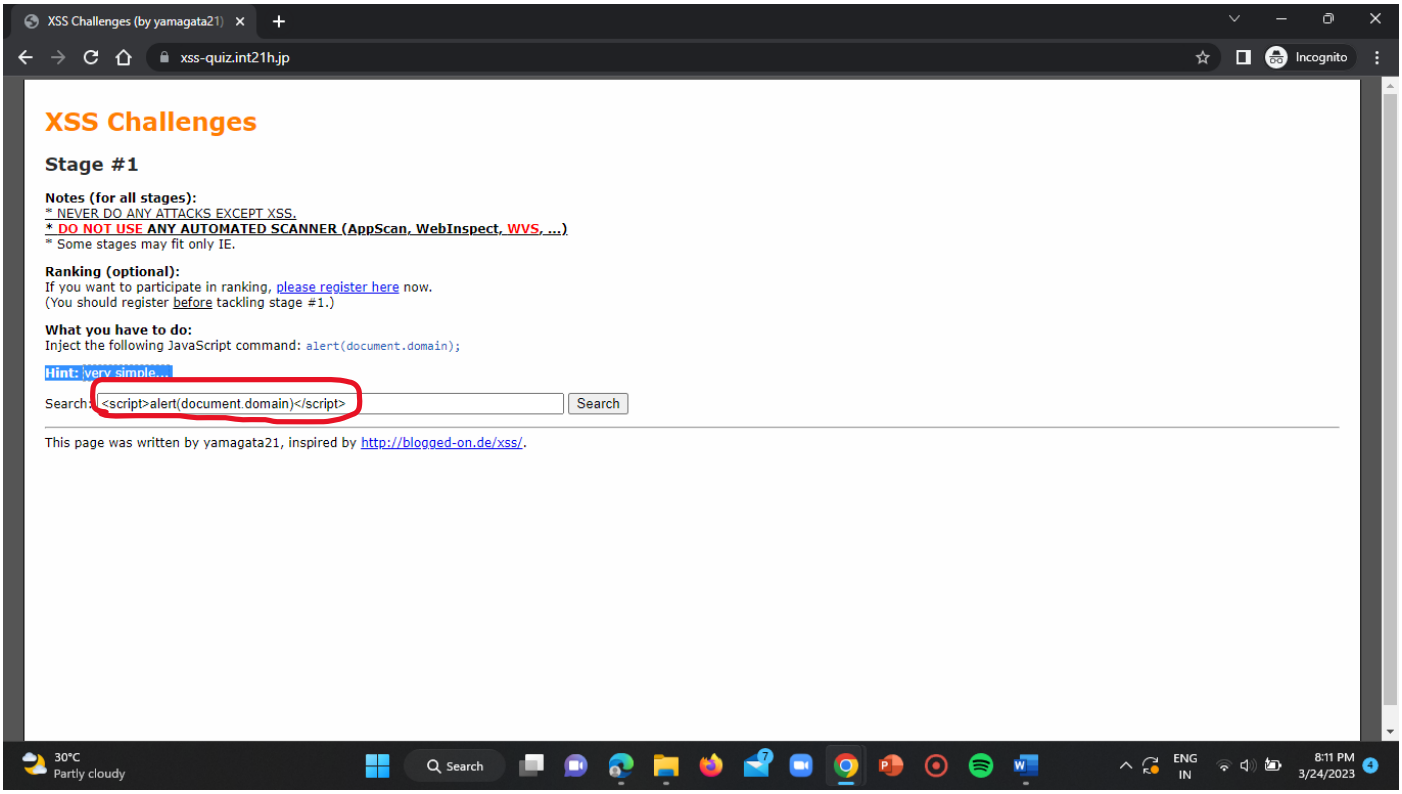
Step-4:

Now we can start the challenge 1 and we can use the hint given there (highlight that to see the hint). Now try to give the script to complete the challenge 1 in search field.

The script to use in this stage is:

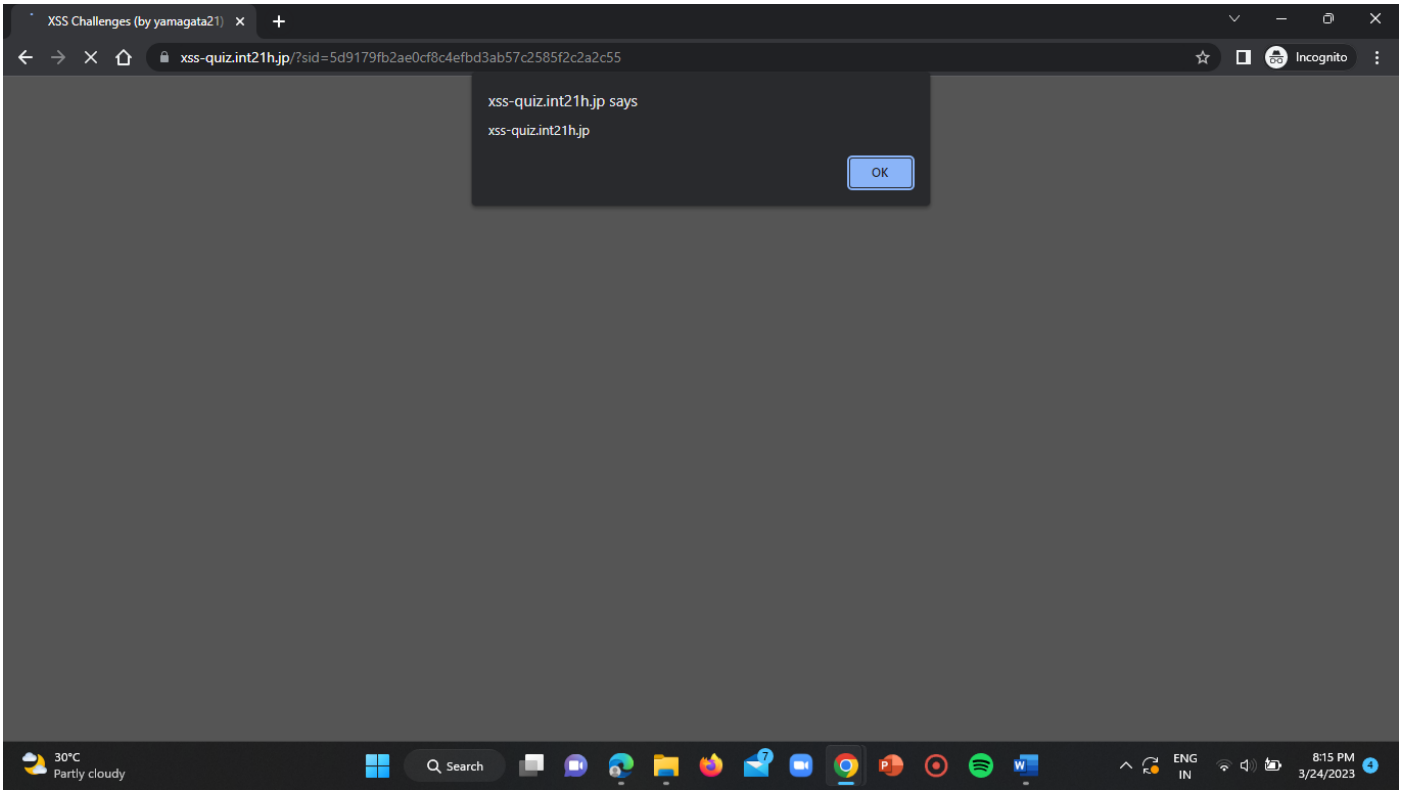
“ <script>alert(document.domain)</script> ”

ST#IS#4899



Step-5 :

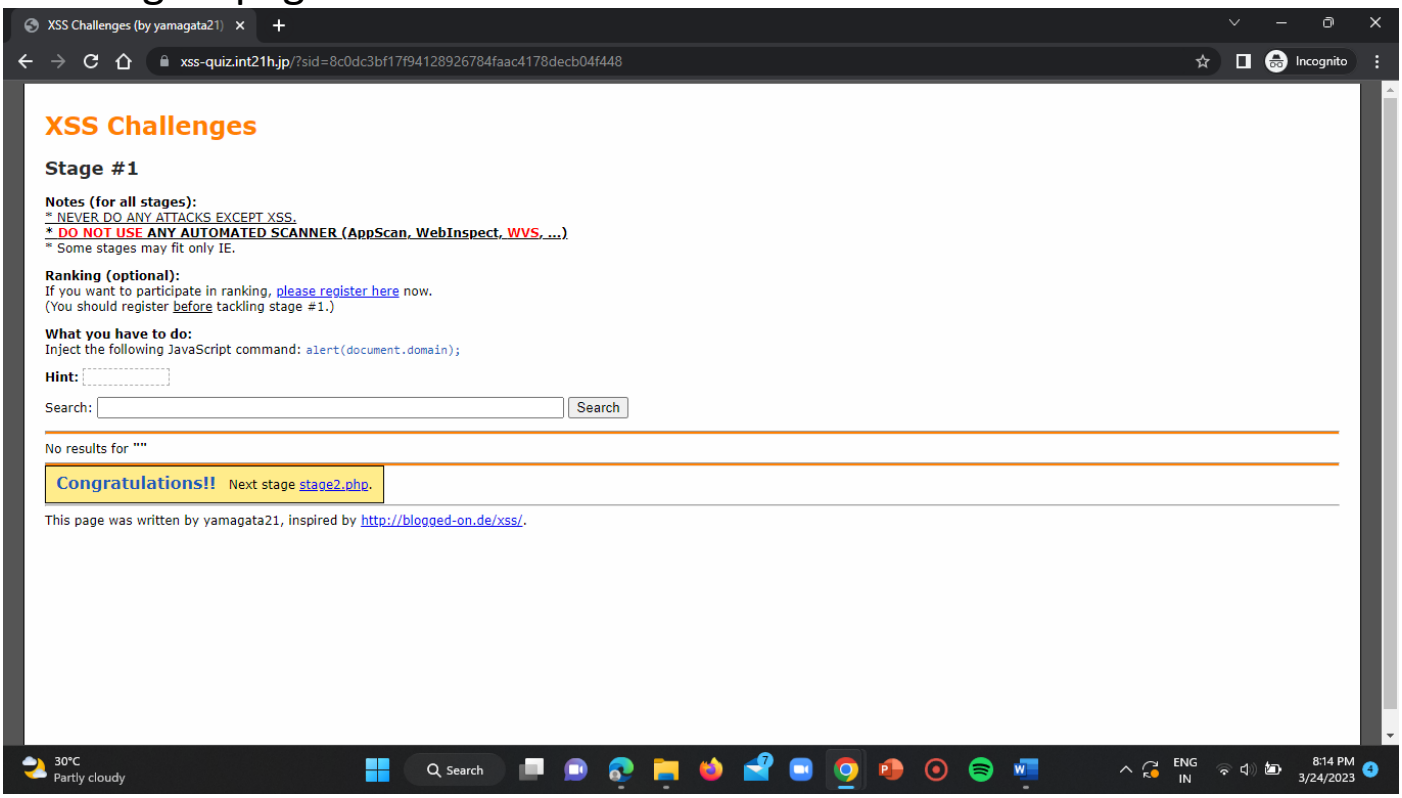
Click on enter and observe if any popup occurs. If there is any popup coming then click on yes.



Step-6:

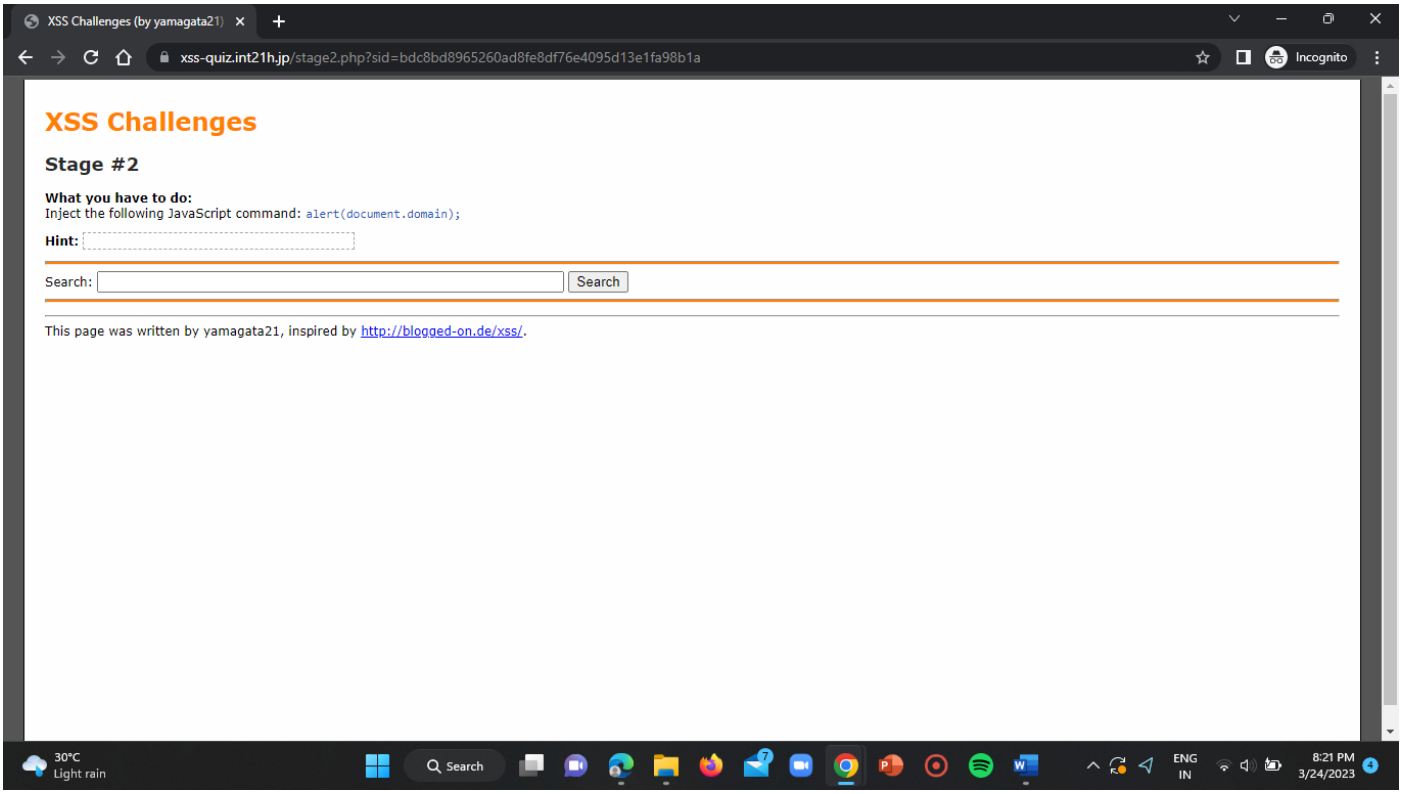
Now you will be displayed with a congratulations note which means you've completed the challenge now you are ready to move to challenge 2.

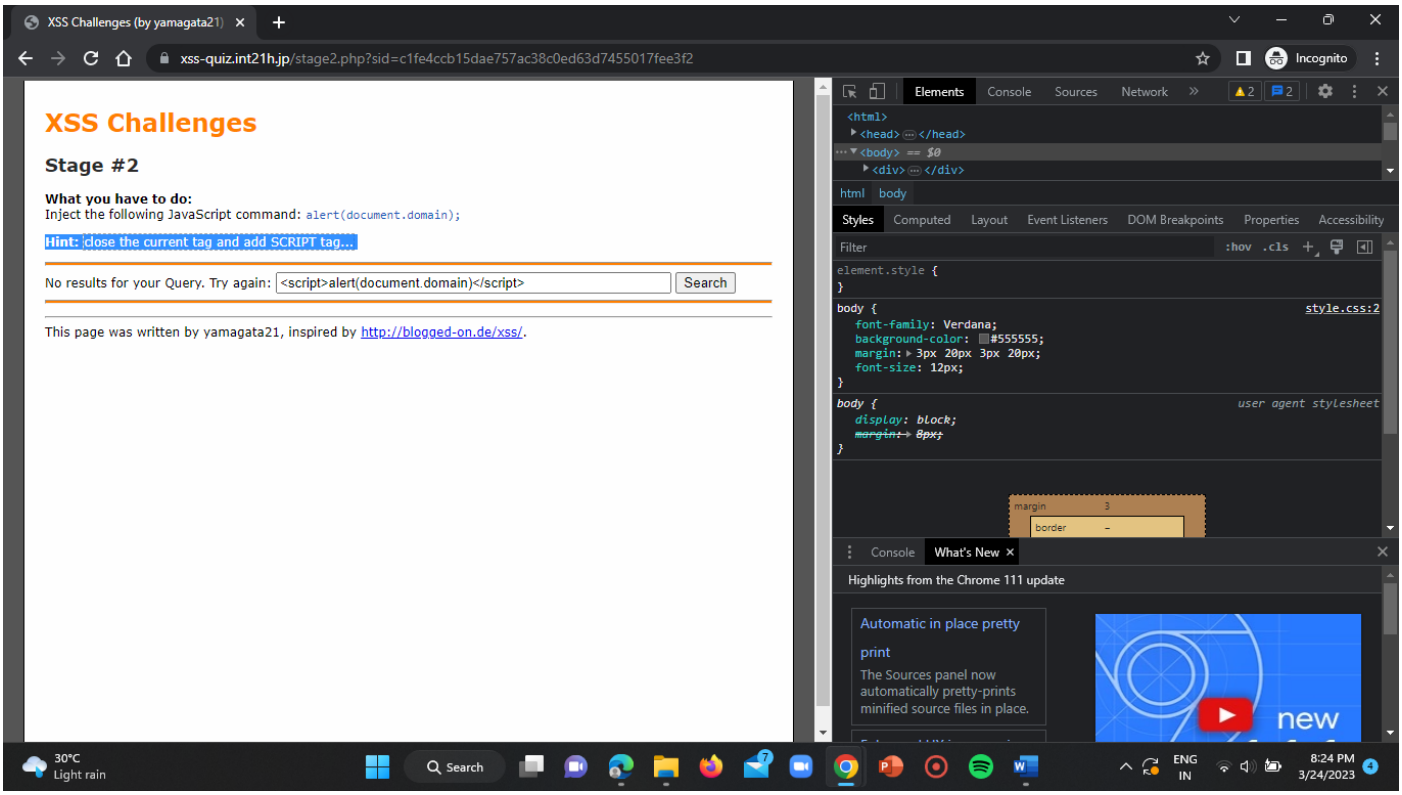
Then click on "stage2.php" then you will be redirected to the challenge 2 page.



Challenge – 2:

ST#IS#4899



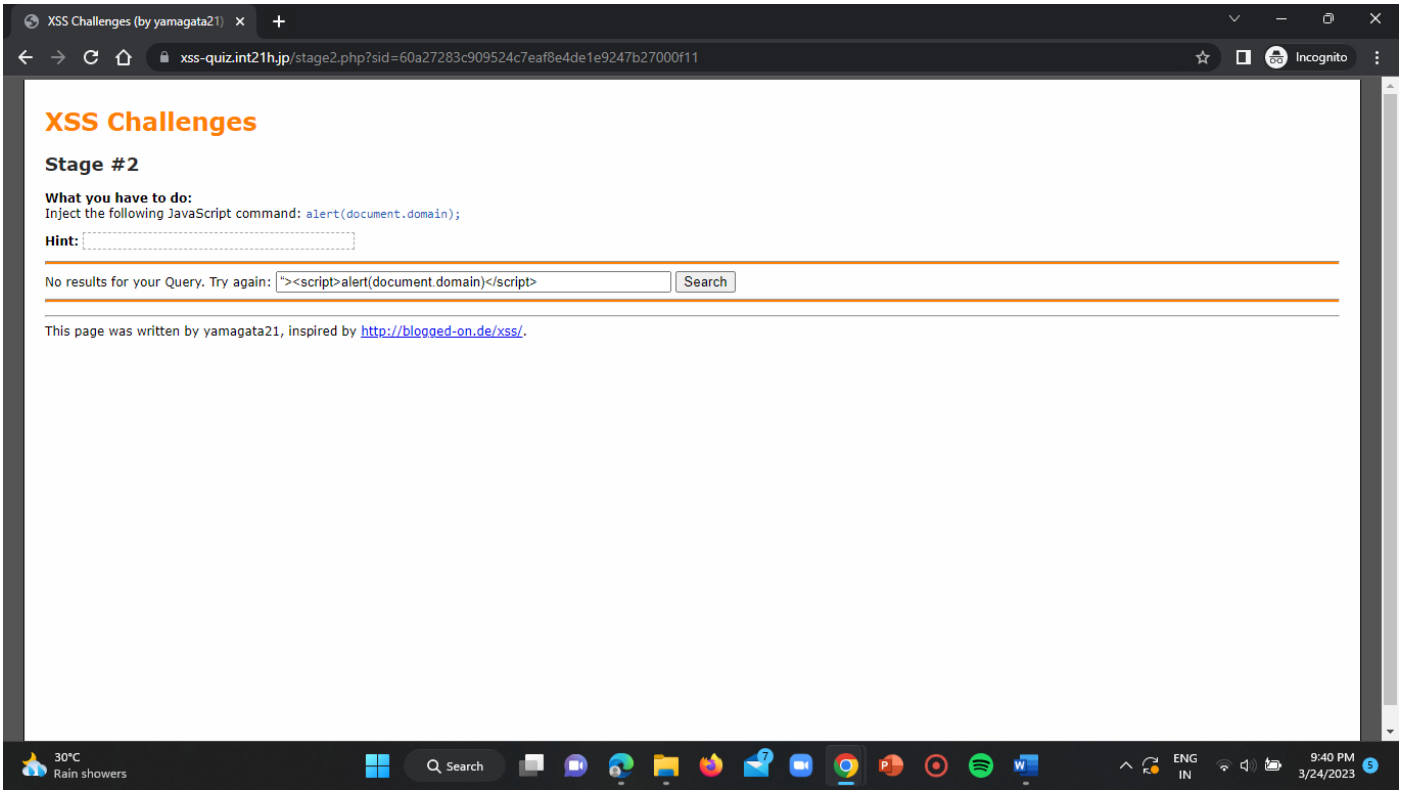


Here as we see in above picture, the input is taken as a string. So now we need to close the current tag and script tag (by adding “> at the start of the given script).

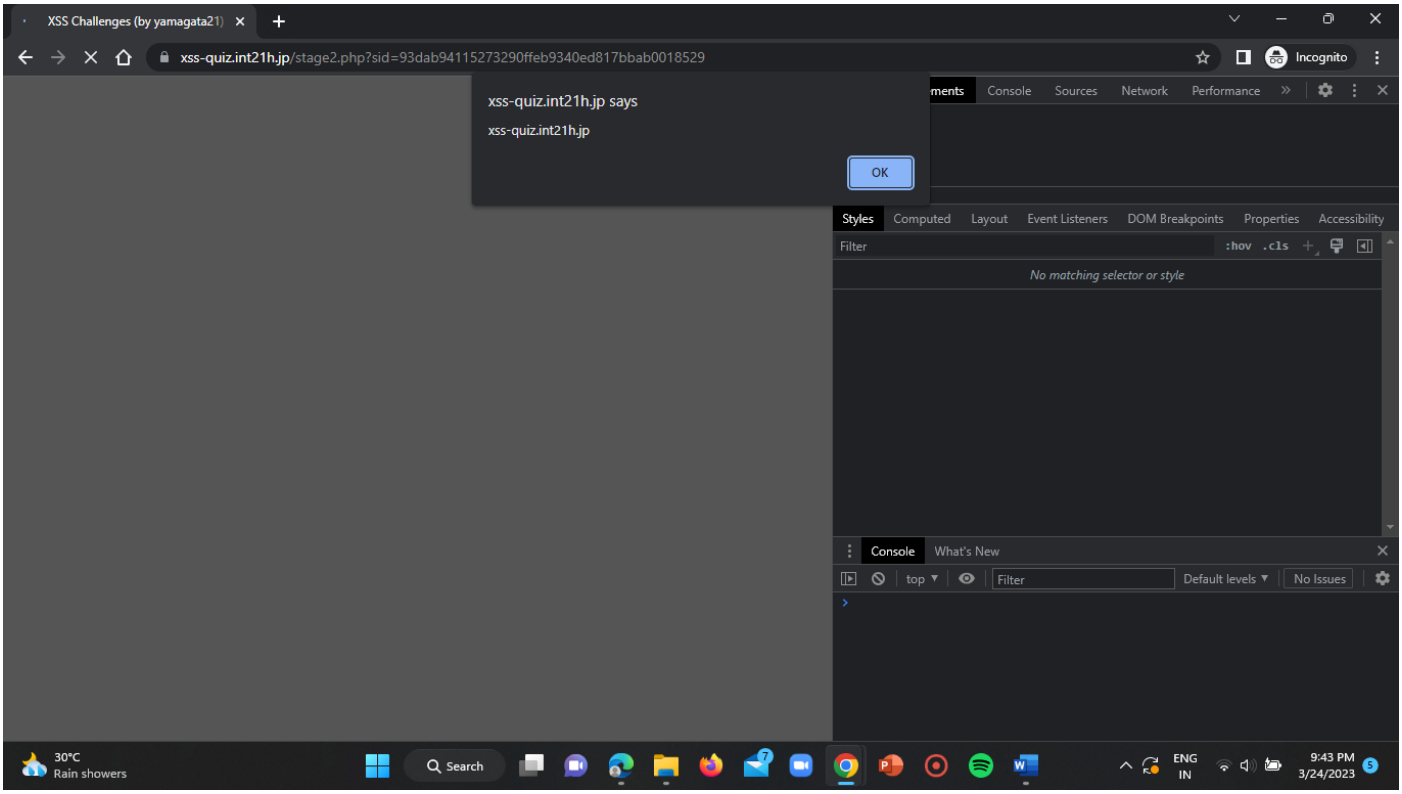
SCRIPT:

“ “><script>alert(document.domain)</script> ”

ST#IS#4899

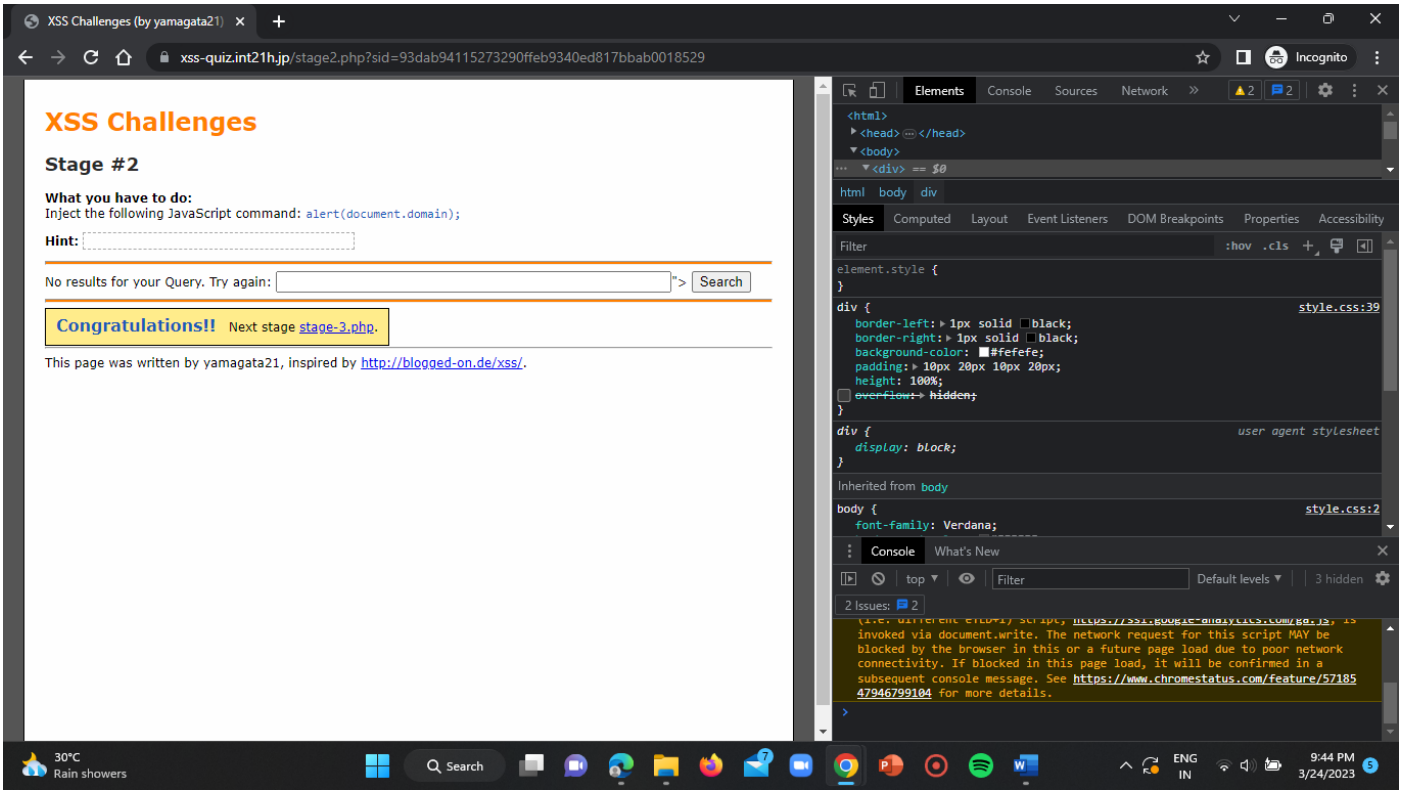


Click on enter.



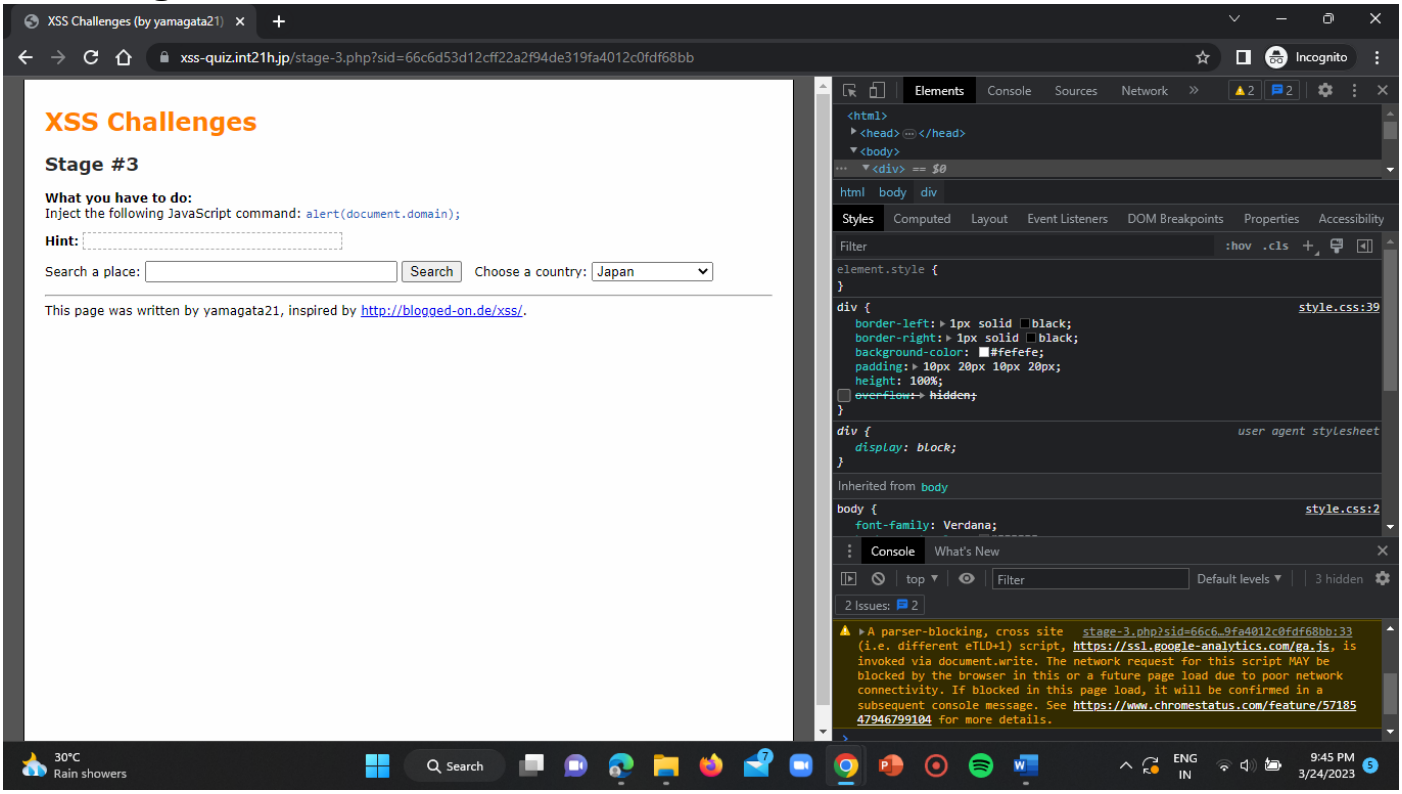
Click on OK.

ST#IS#4899

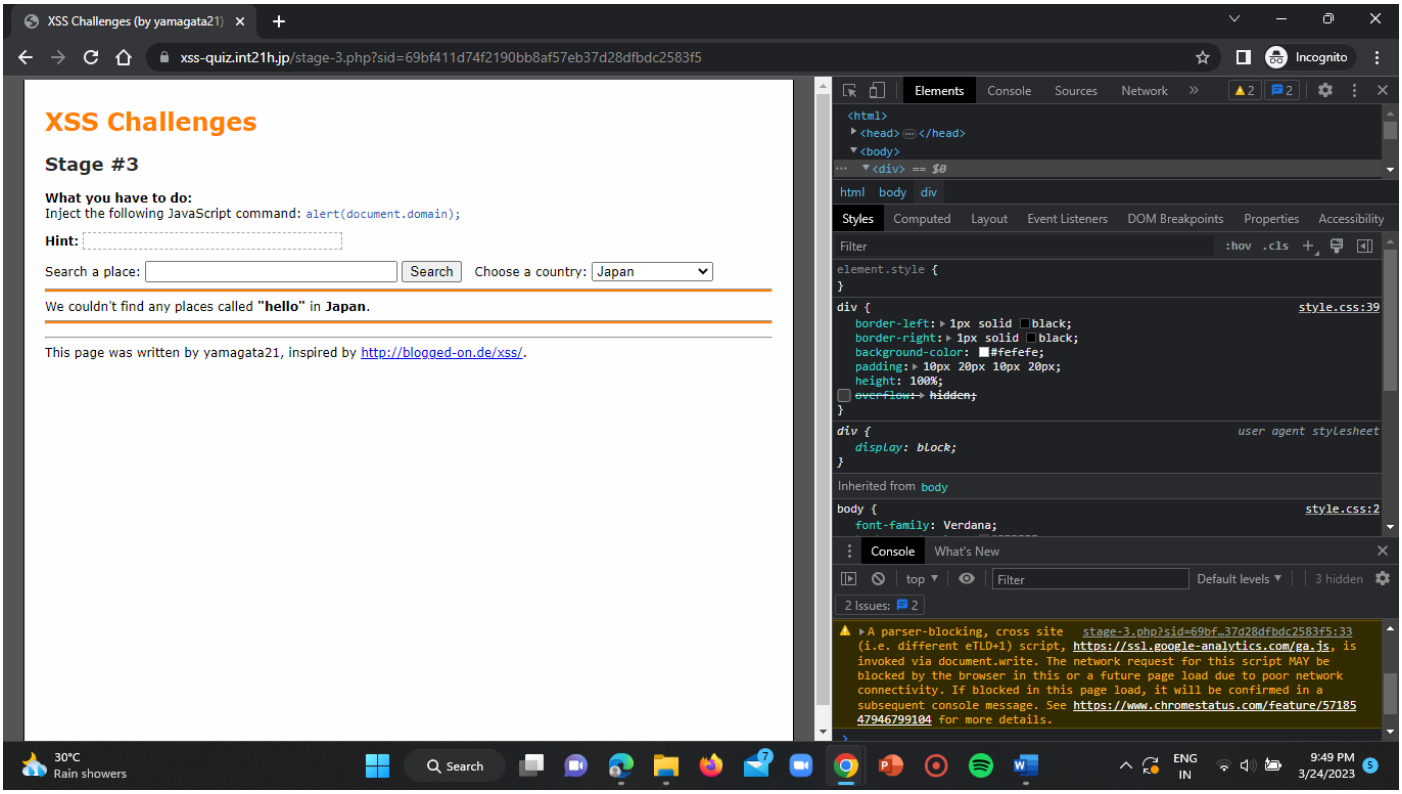


Click on stage-3.php .

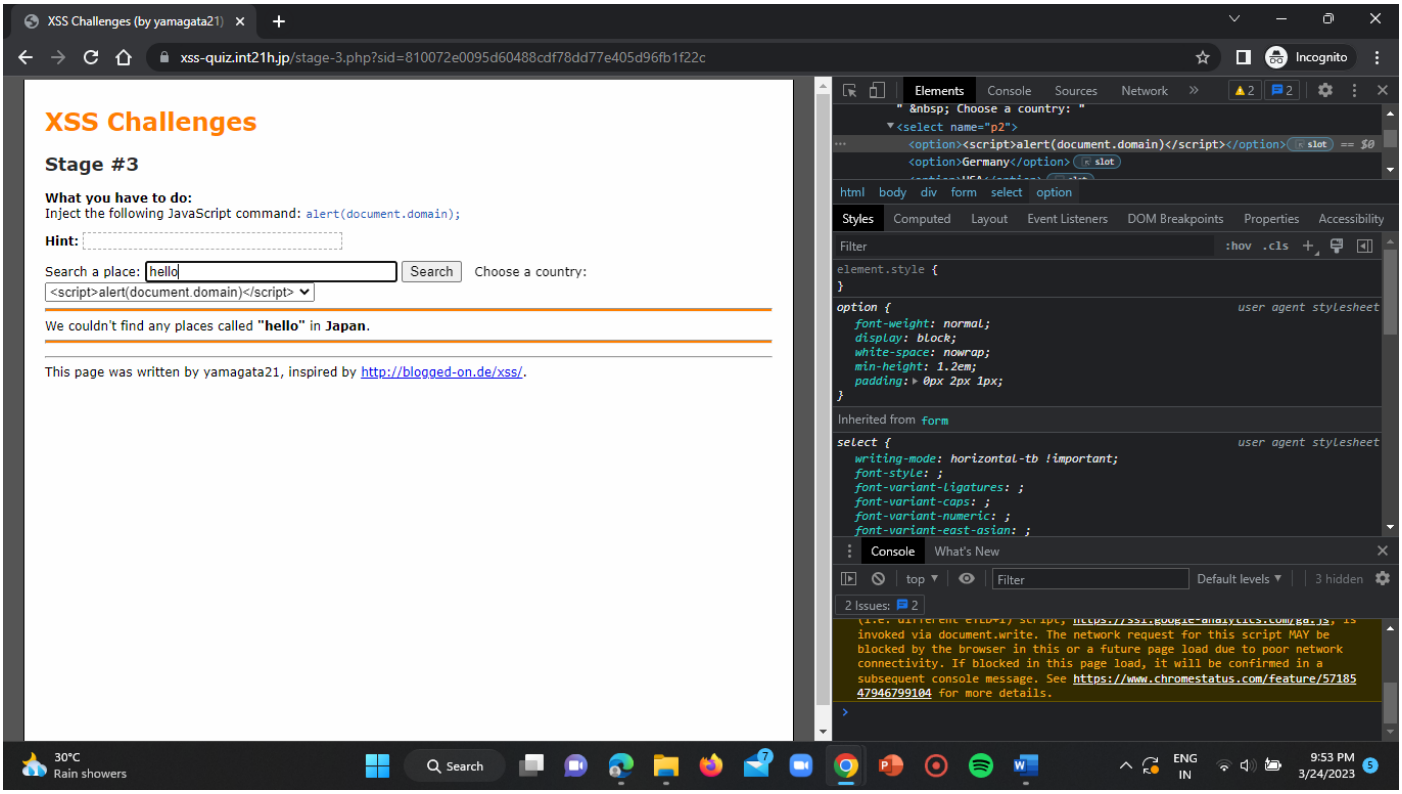
Challenge-3 :



ST#IS#4899

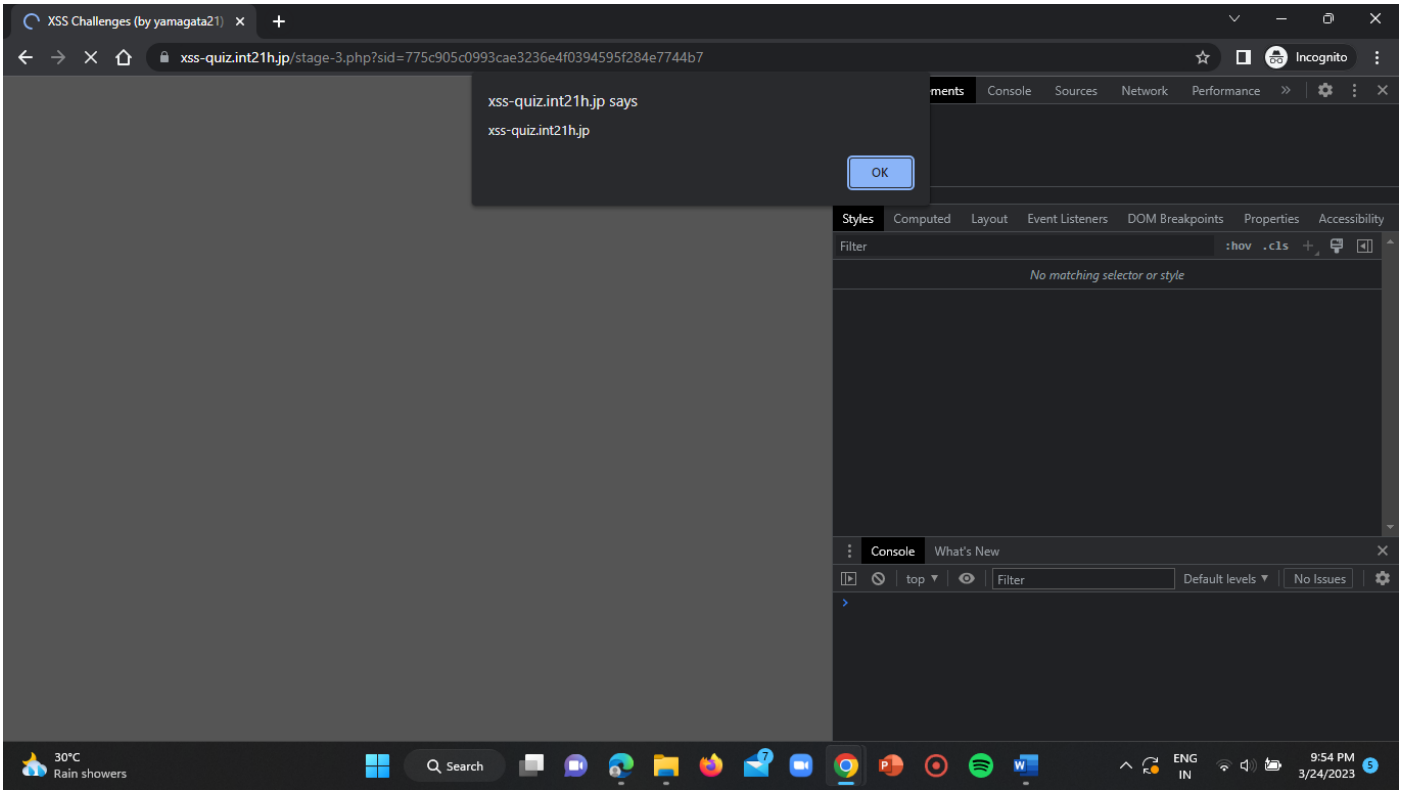


As we given hello it is saying that “we could not find any places called ‘hello’ in Japan”. As we can see that by searching something it is shifting to another field called “choose a country”, so let us change the script at “p2.Script(<script>alert(document.domain)</script>)”.

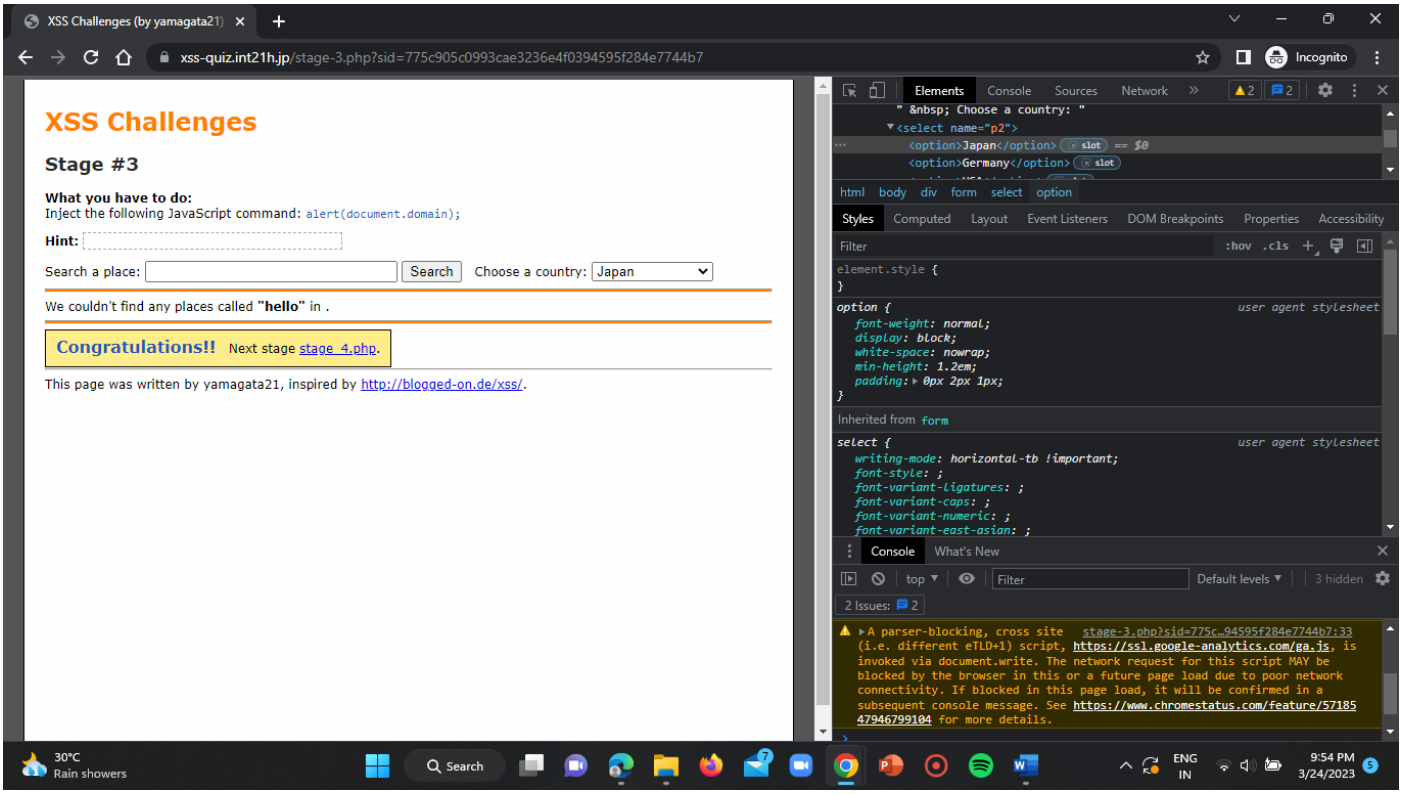


Click on enter.

ST#IS#4899

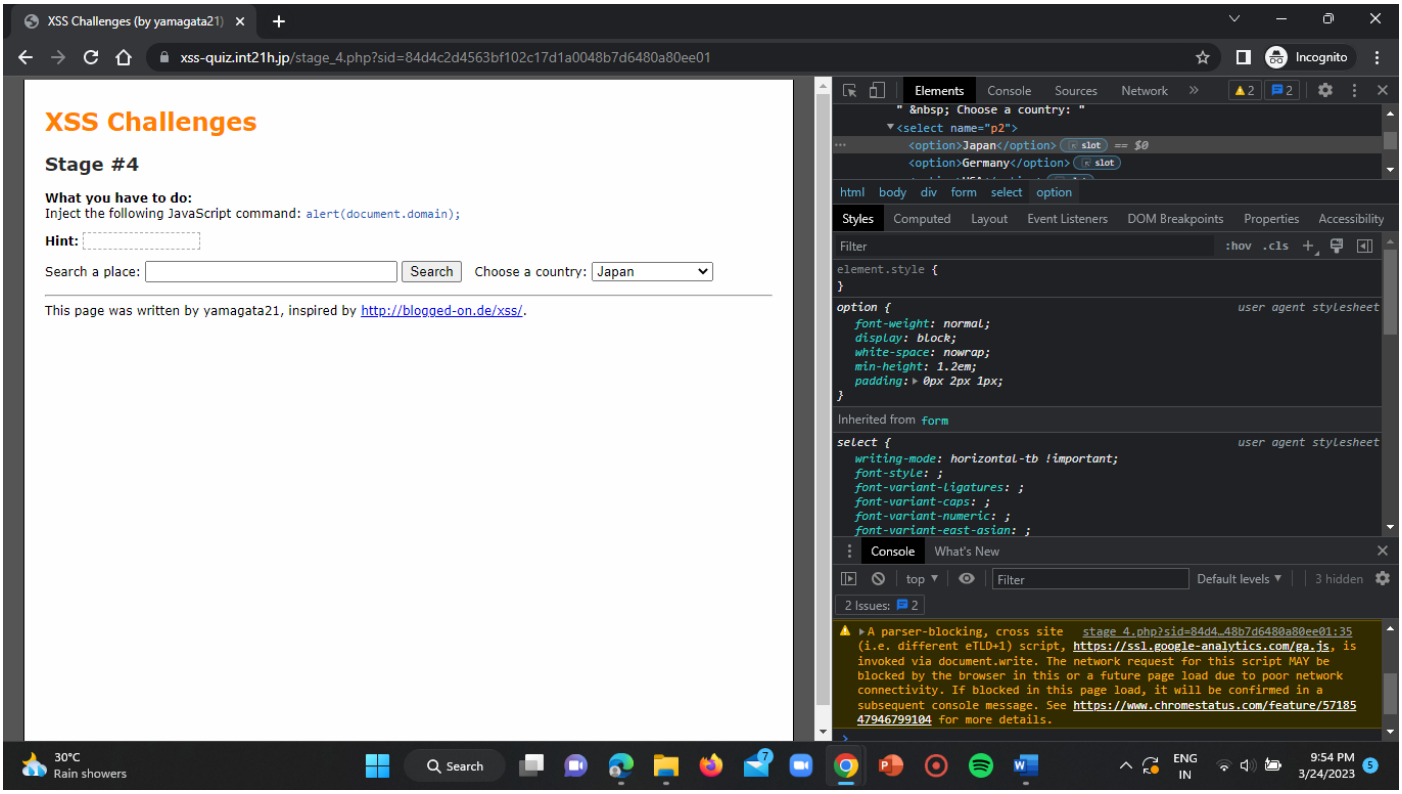


Click on OK.



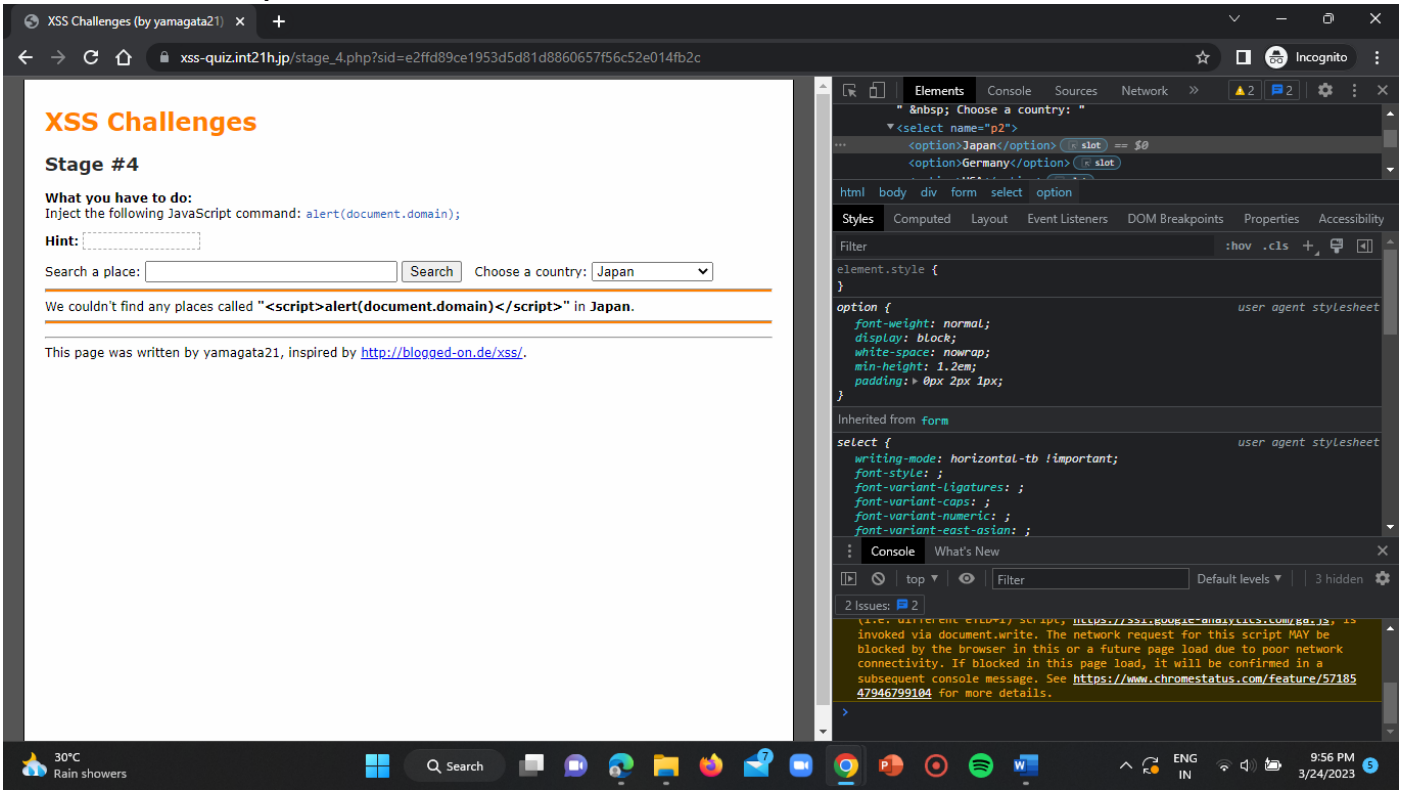
Now click on “stage-4.php”.

ST#IS#4899



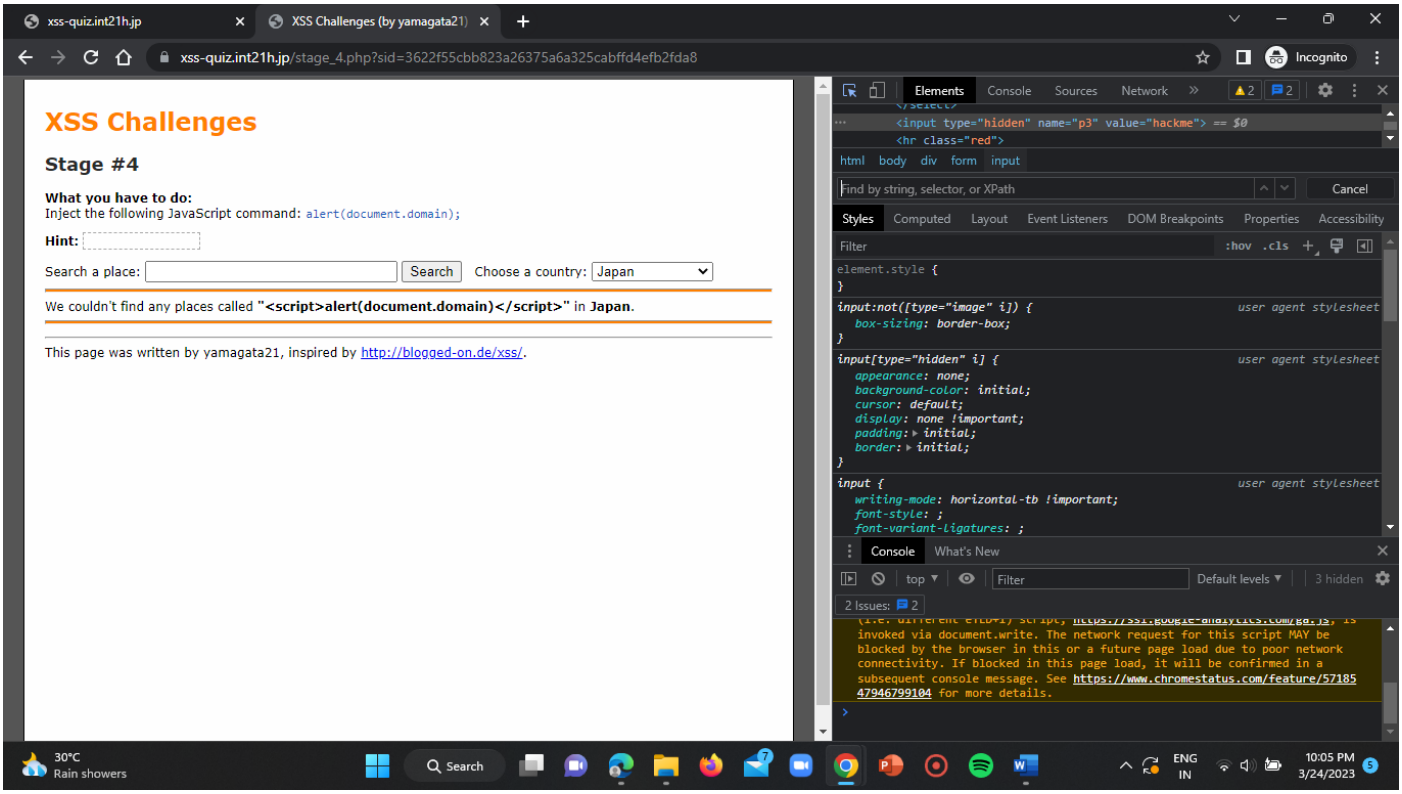
Challenge-4:

Paste the script in the search bar and click on enter.



The given script could not find any places. Now observe the inspect we can see the hidden value ‘hackme’. Replace that with “<script>alert(document.domain)</script>” and add ‘ “> ’ at the start of the script.

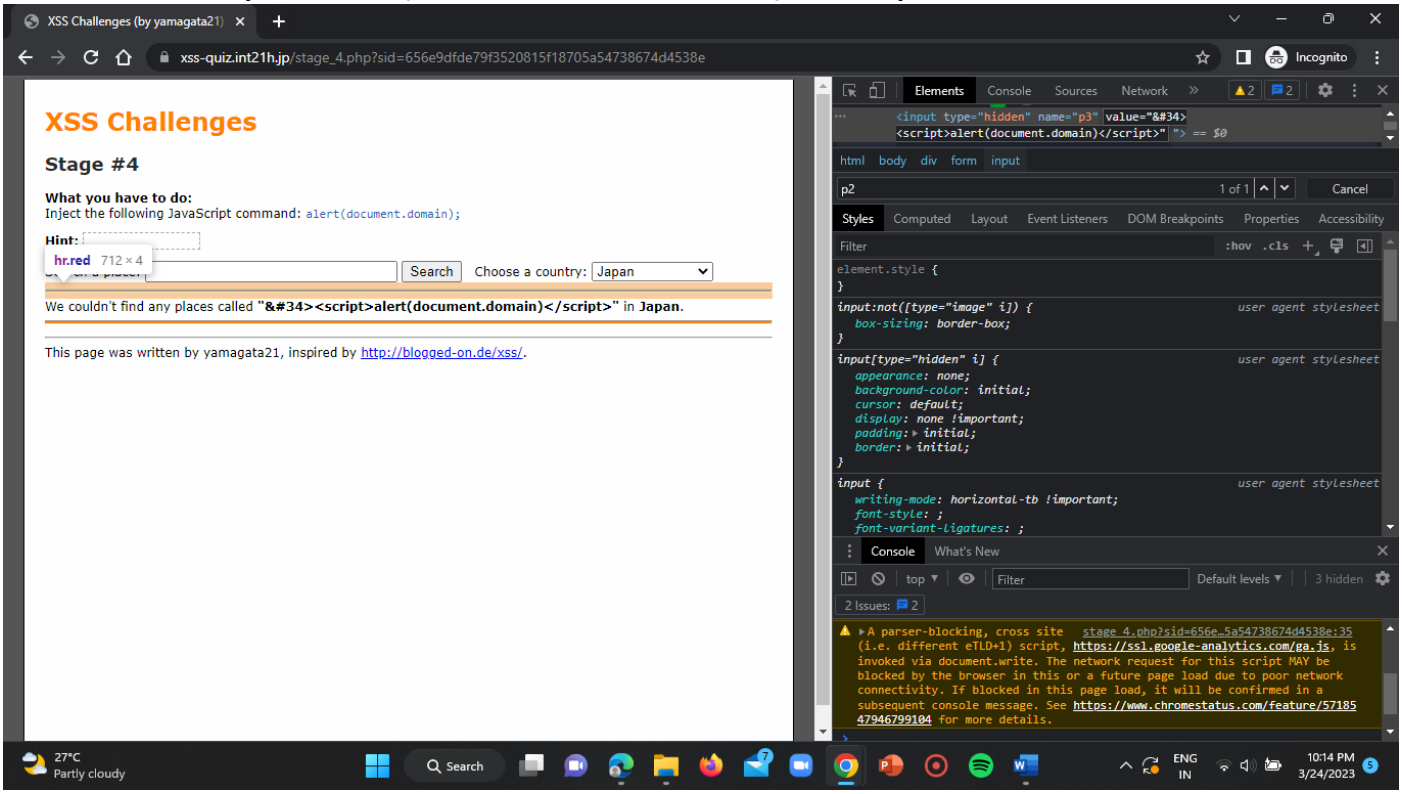
ST#IS#4899



After clicking on enter we observe that the script disappears due to more number of double quotes so add '&#34' to replace the double quotes.

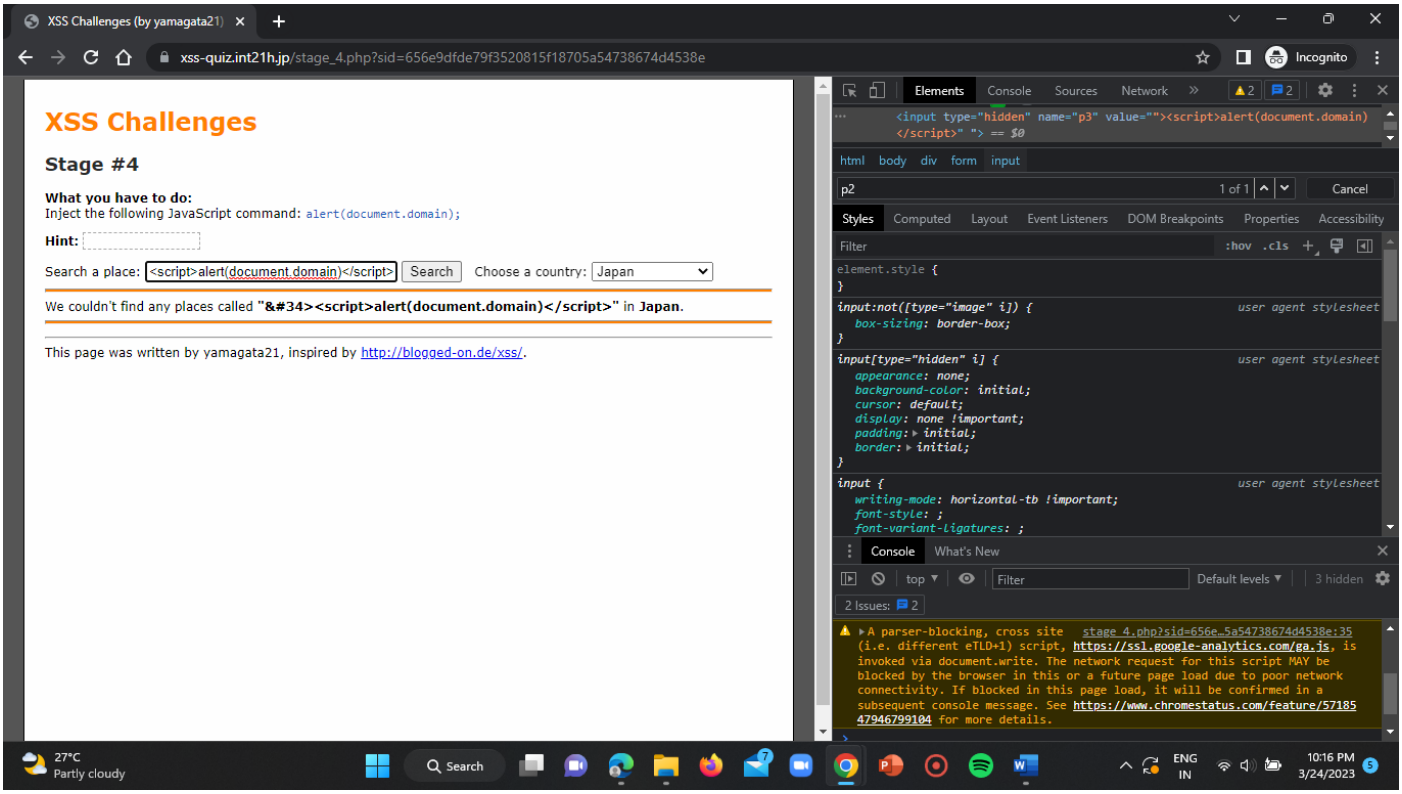
Now place the given script which is given below in inspect:

"&#34><script>alert(document.domain)</script>"

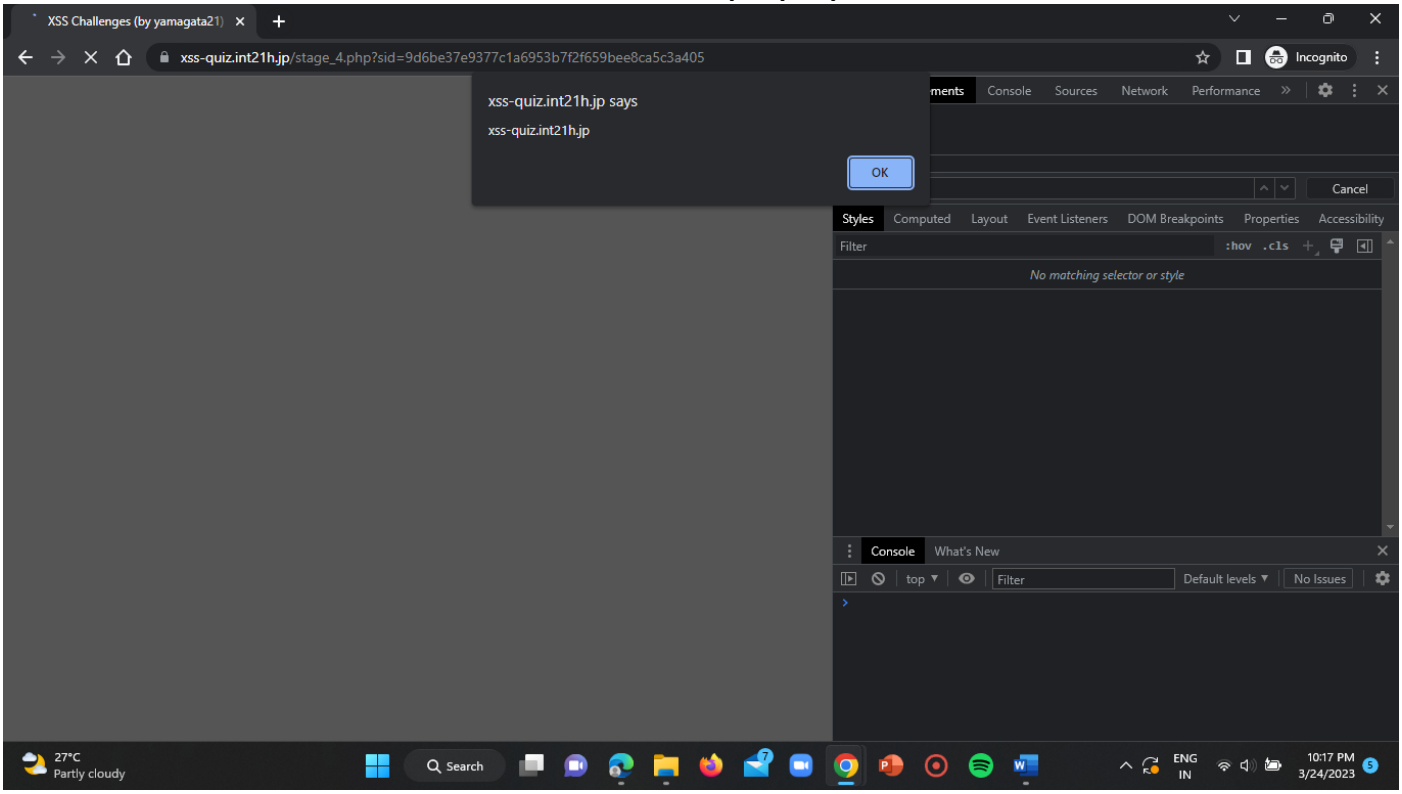


Now click on enter and give the given script in search bar on webpage.

ST#IS#4899

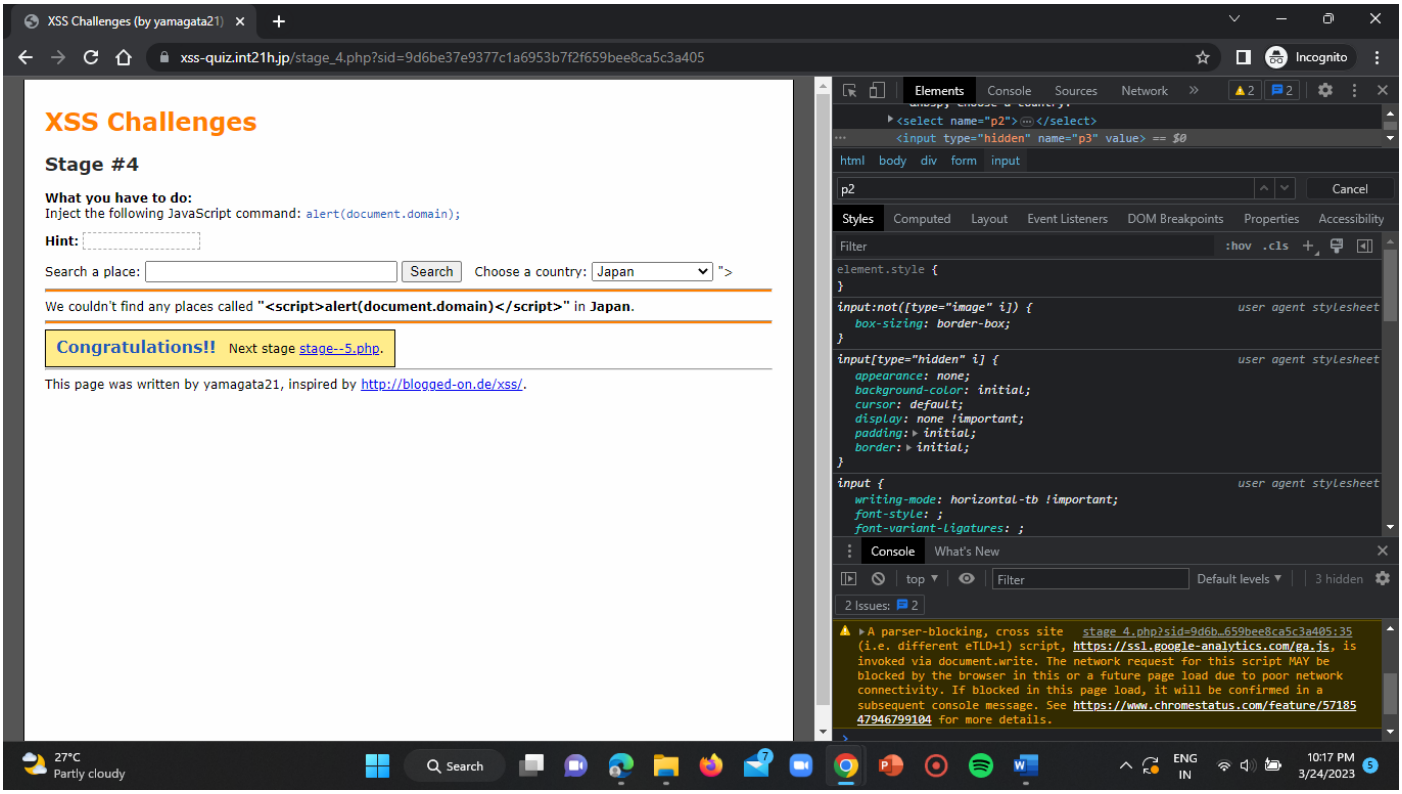


Click on enter and click on OK on the popup raised.

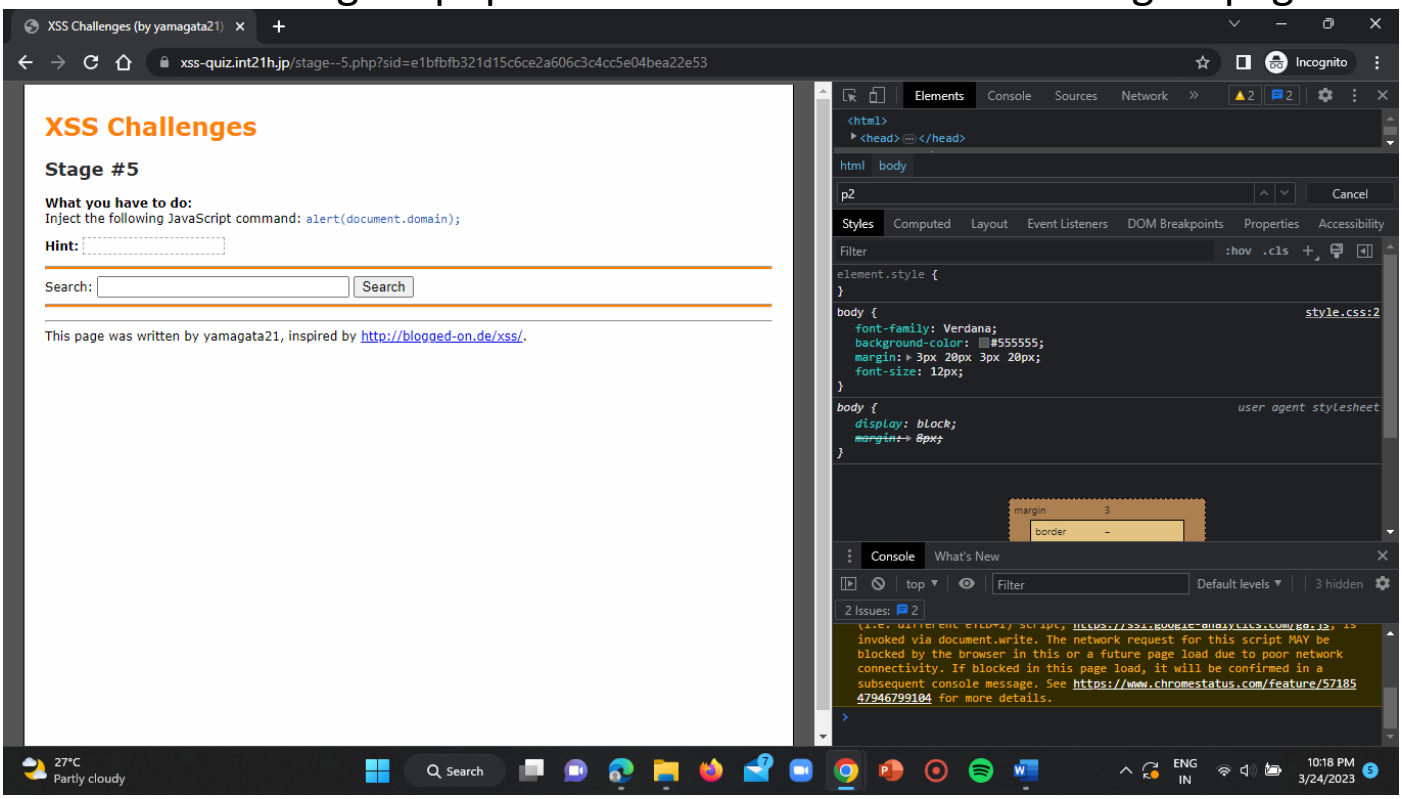


Click on OK.

ST#IS#4899

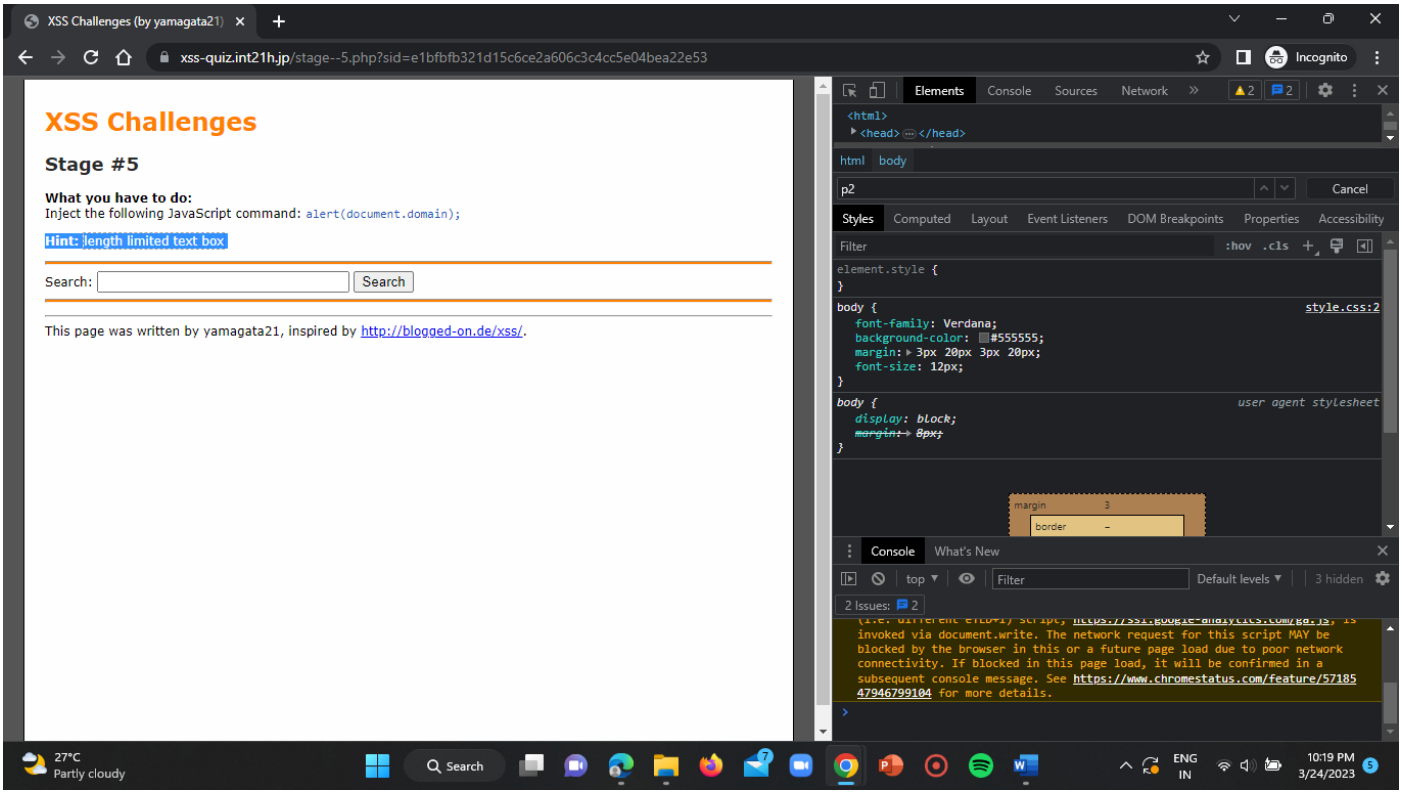


Now click on “stage-5.php” to be redirected to the challenge 5 page.



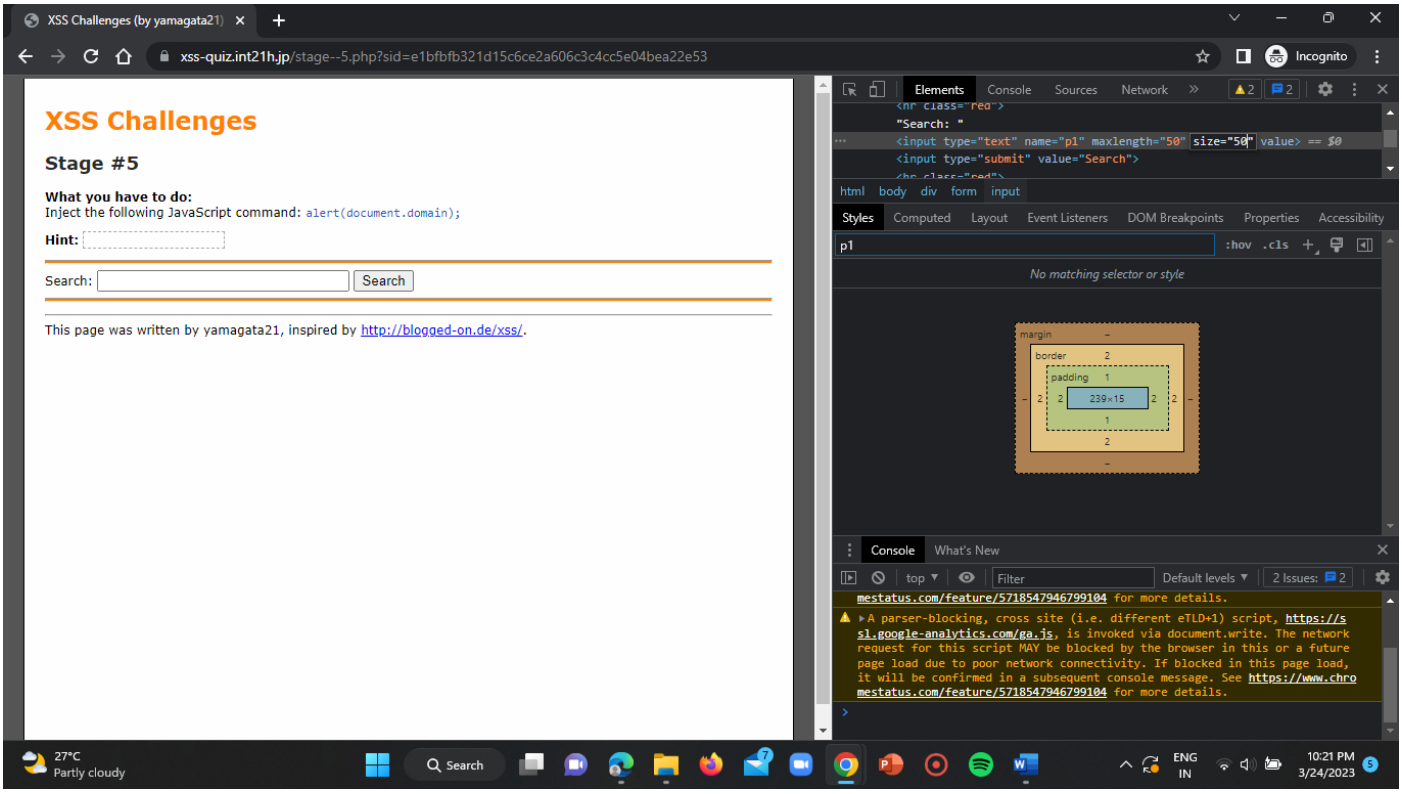
Challenge – 5:

ST#IS#4899



open the inspect.

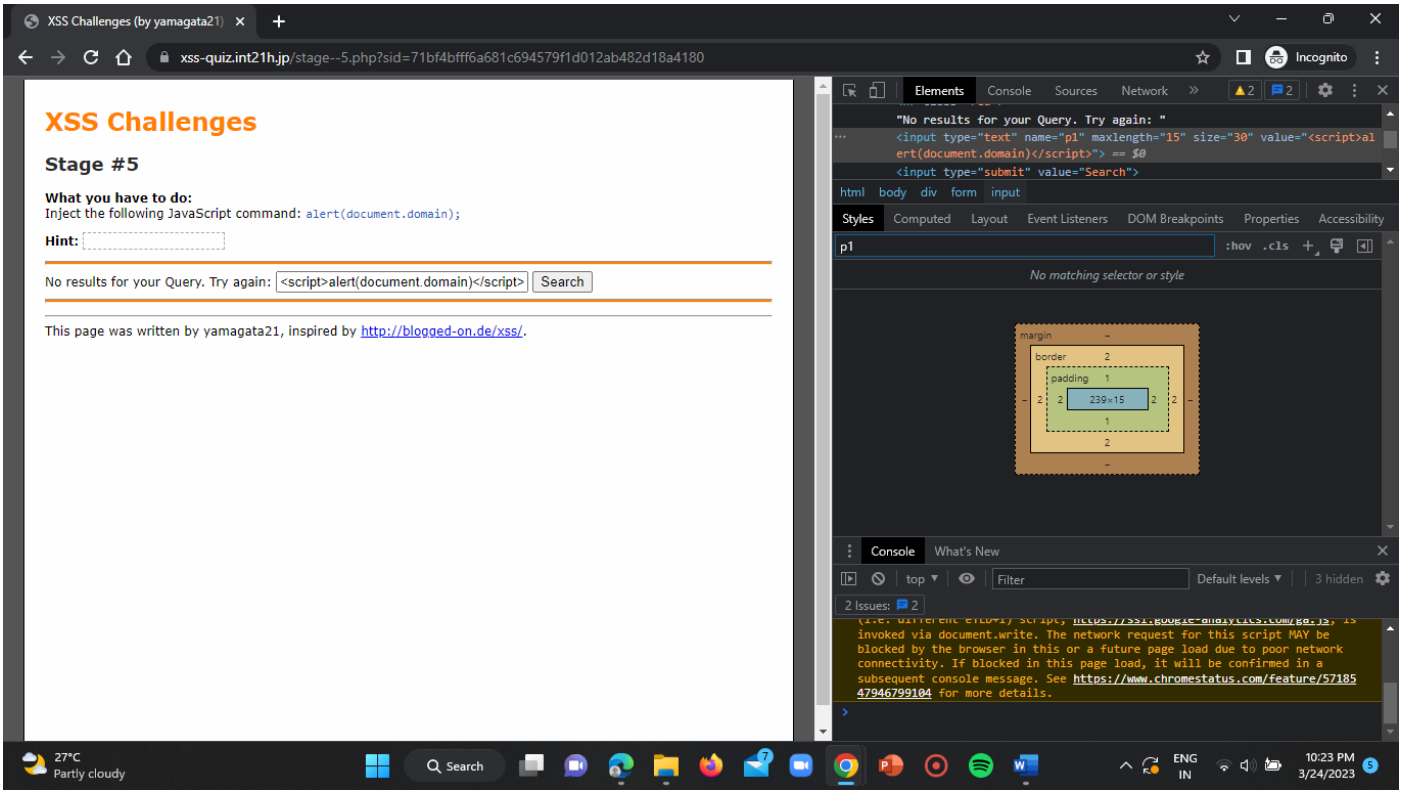
So now change the size and length to 50 or high.



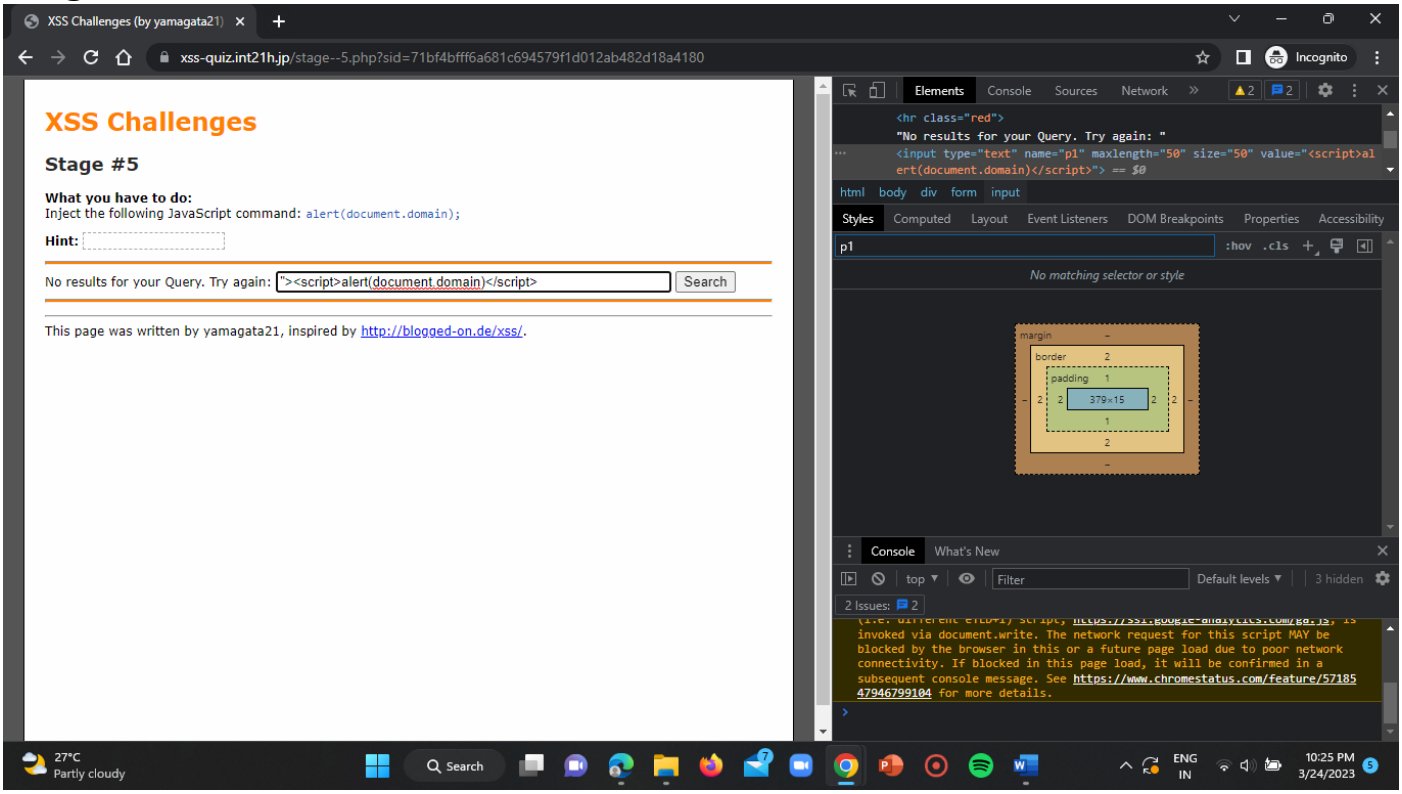
Now enter the script on search bar of the webpage.

Script: <script>alert(document.domain)</script>

ST#IS#4899

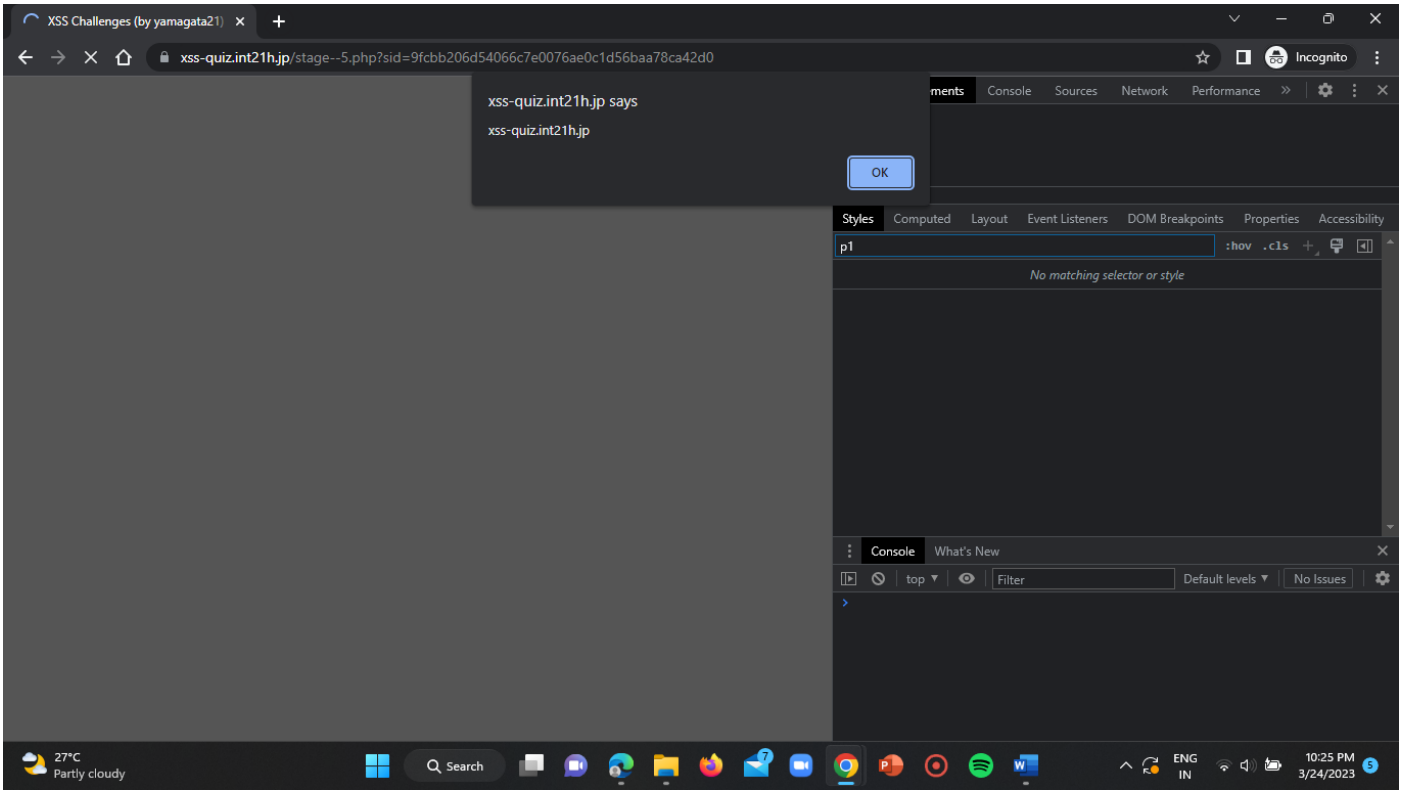


We get no results for our query. So, let us give a closing tag at the start of the script by adding " "> " at start. Do not forget to change the length and size.

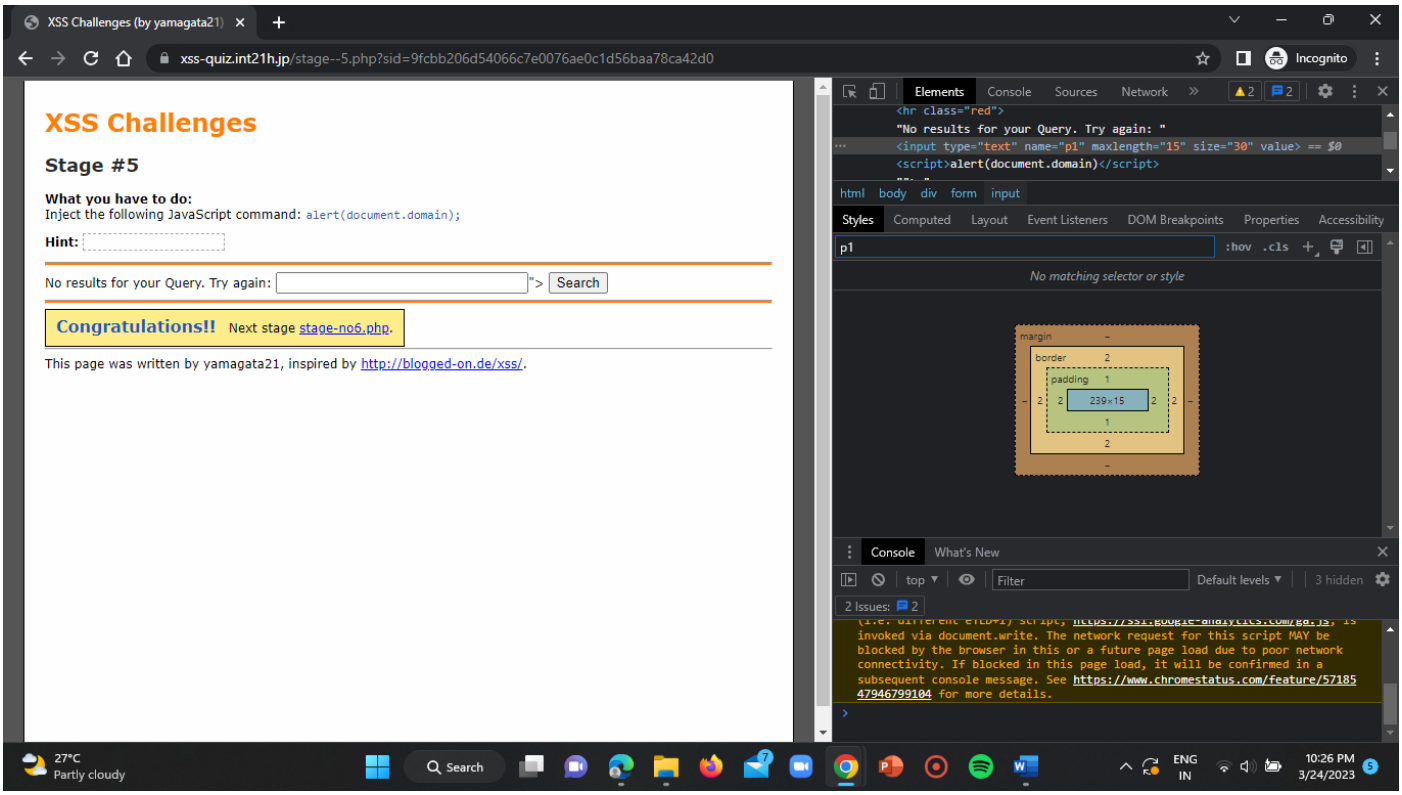


Click on enter.

ST#IS#4899

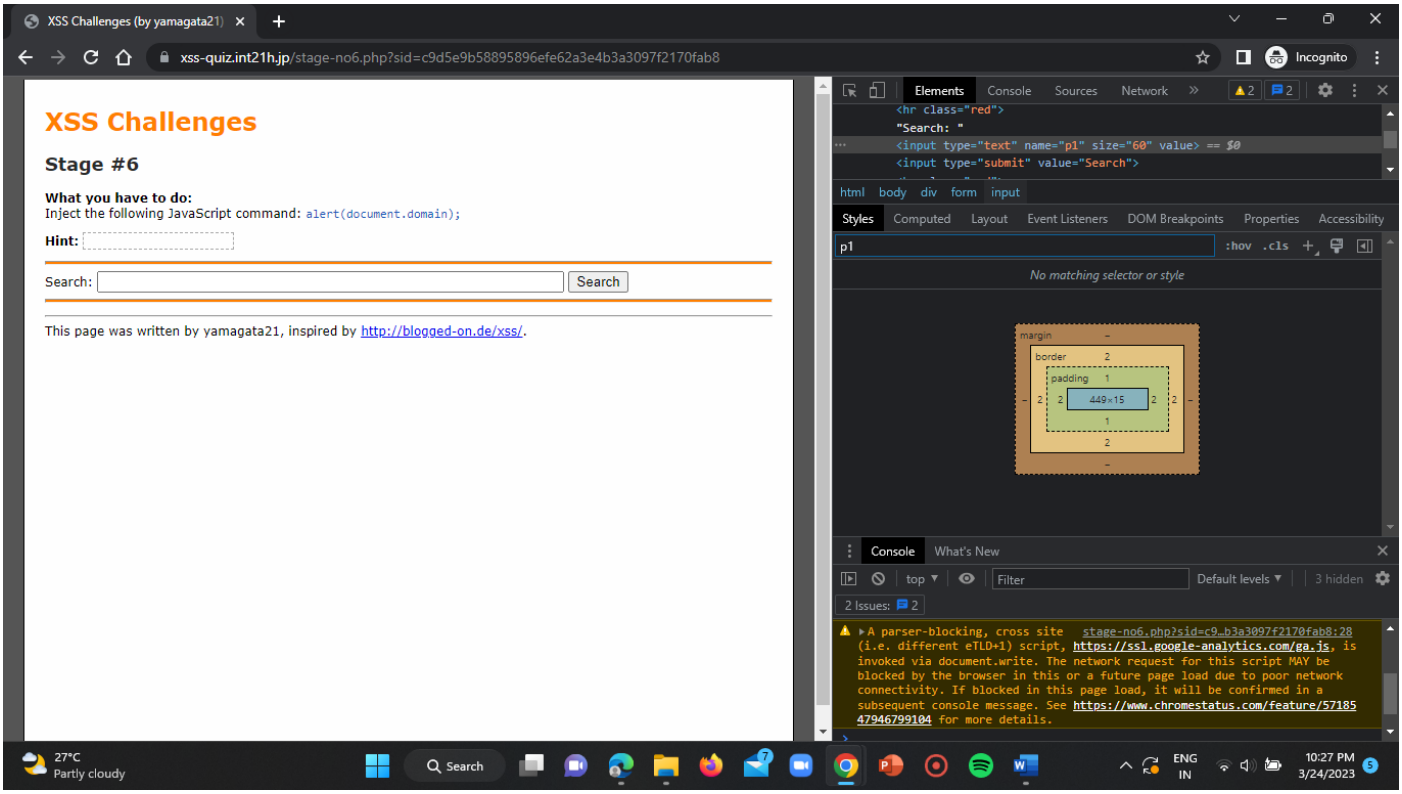


Click on OK.

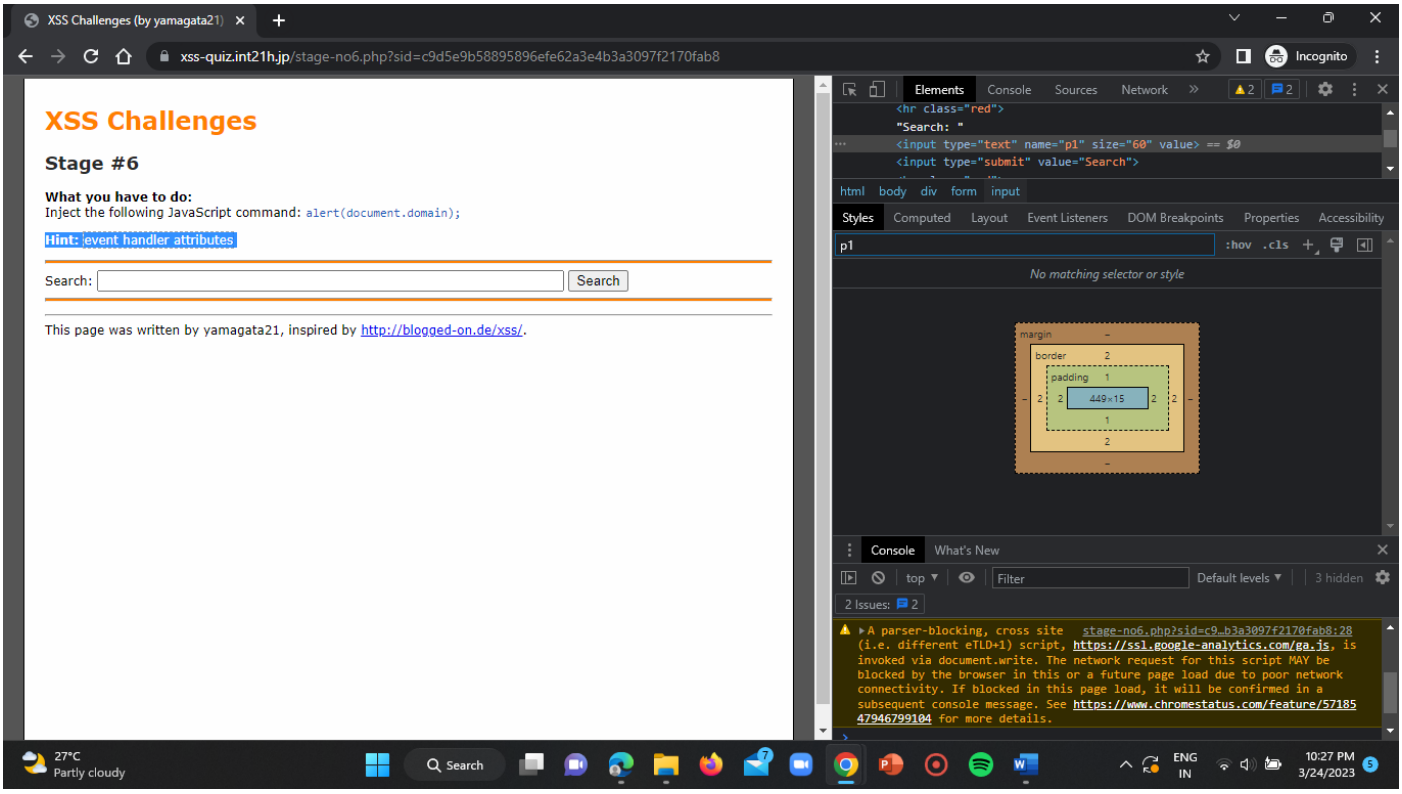


Now click on “stage-no6.php”. you will be redirected to the challenge 6 webpage.

ST#IS#4899



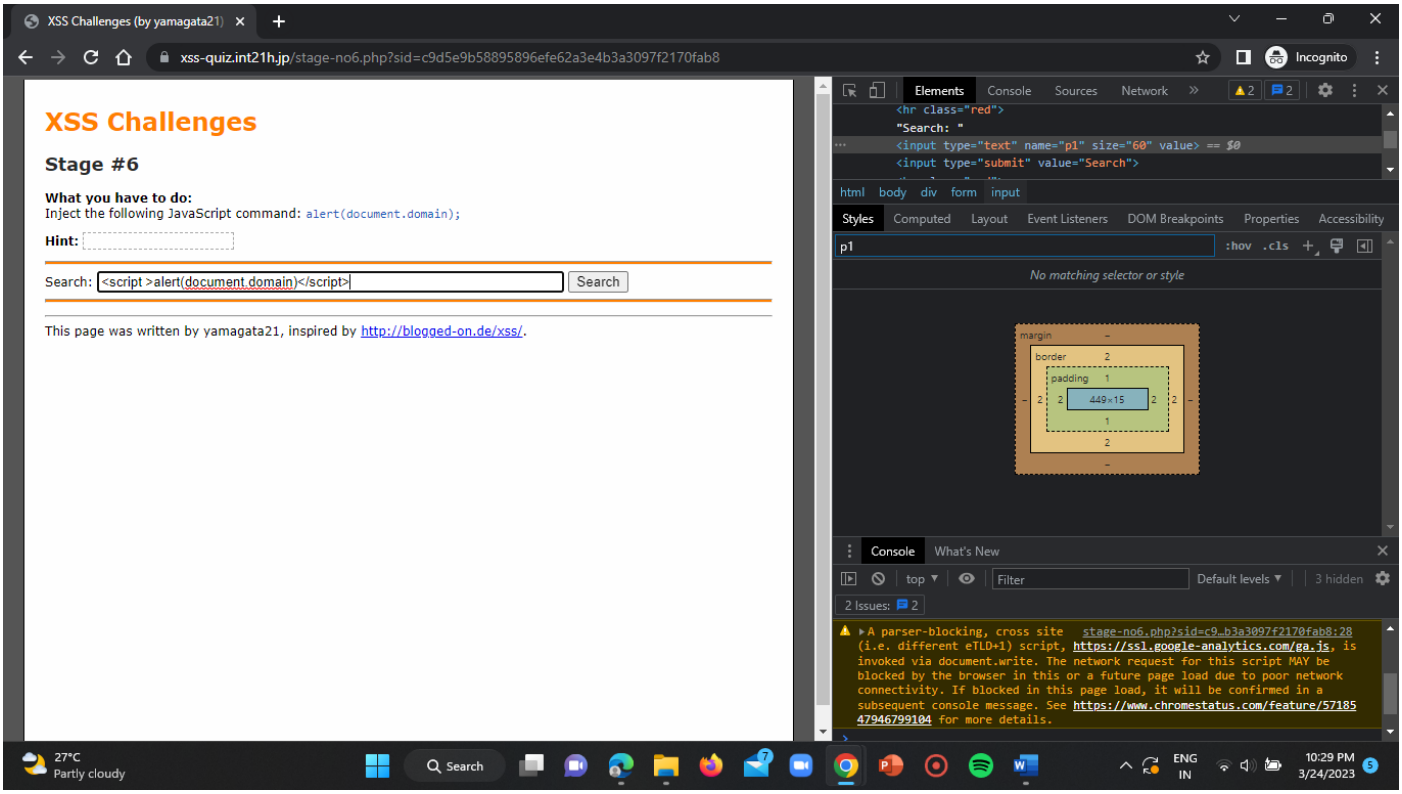
Challenge – 6:



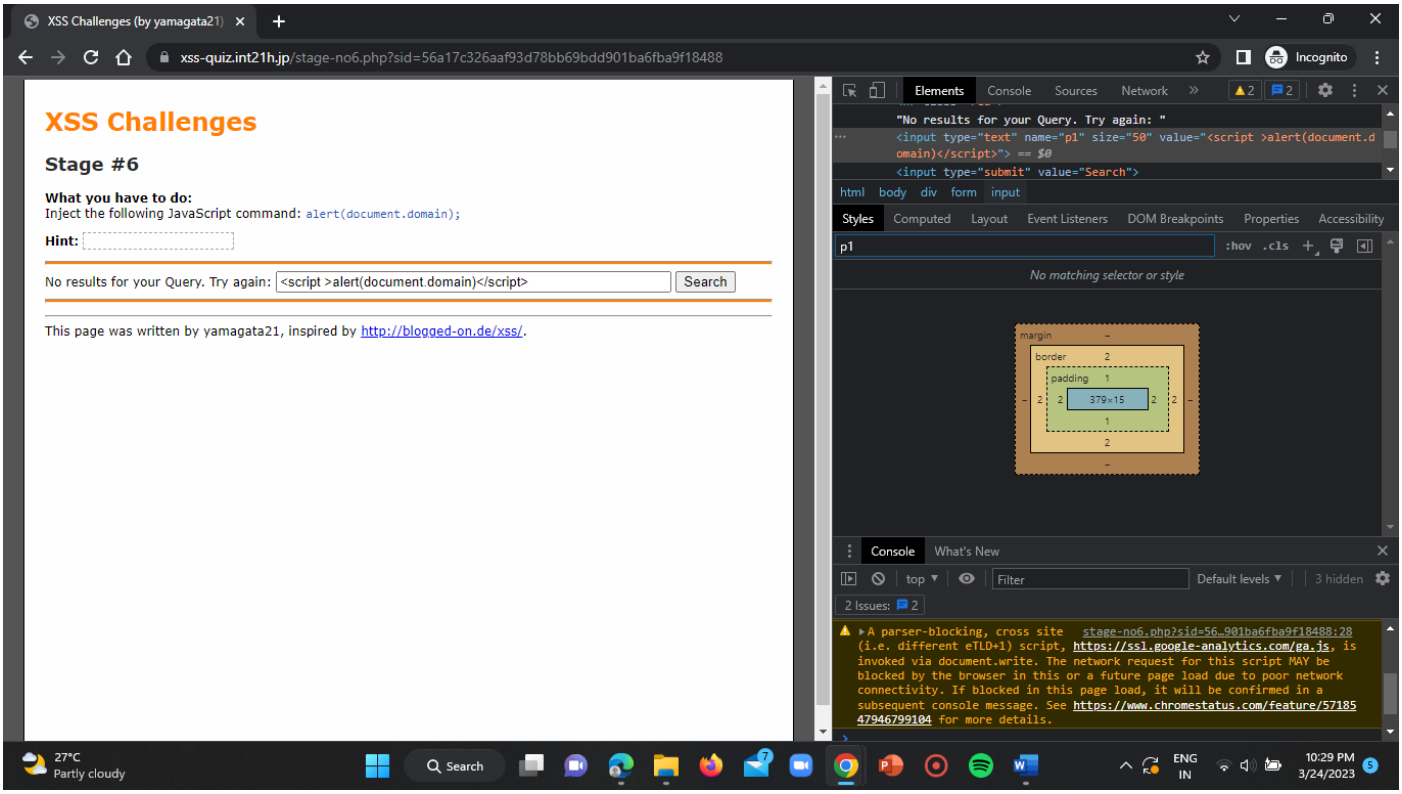
Now give a script in search bar.

Script: “<script >alert(document.domain)</script>”

ST#IS#4899

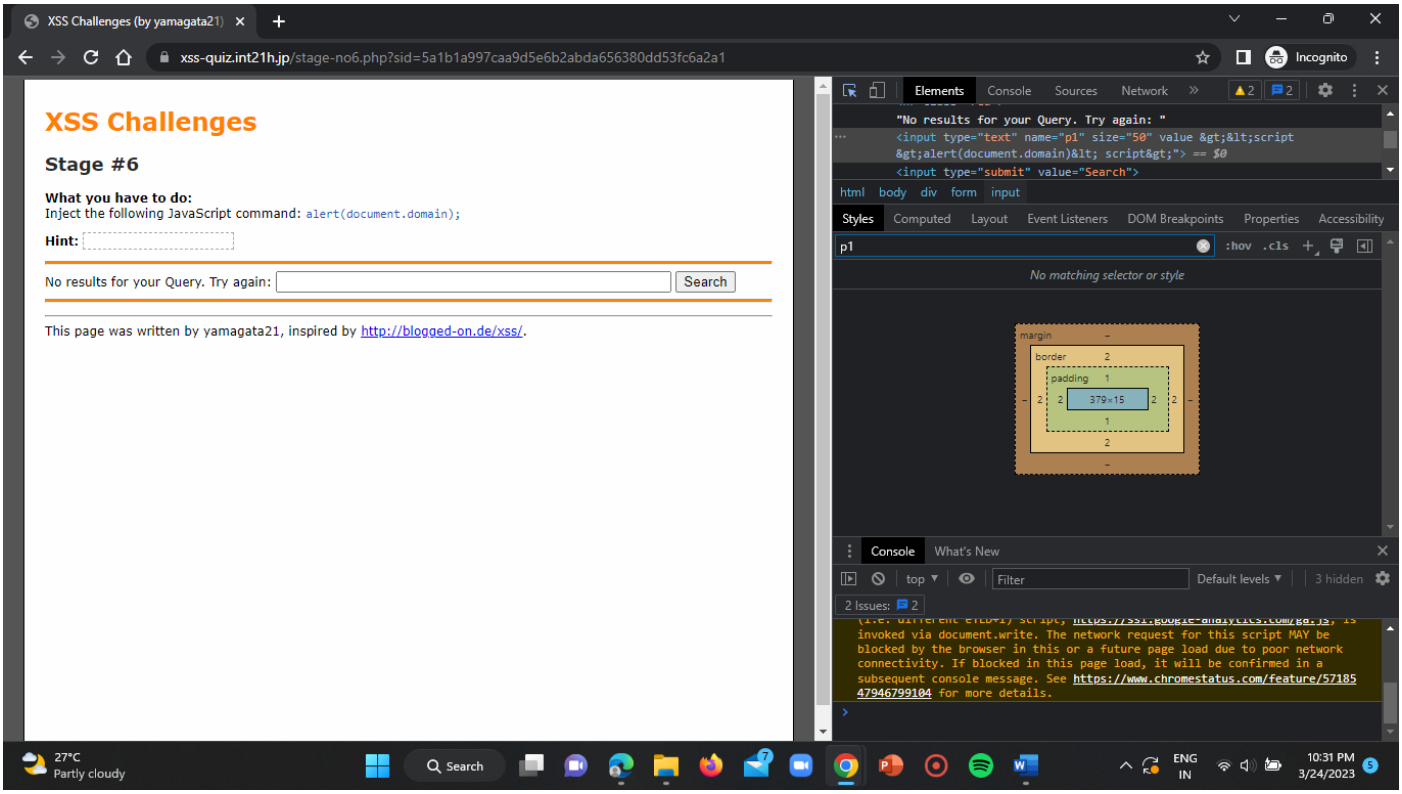


Click on enter.



We get no results for our query. So, add closing start at the start i.e “ “> ”.

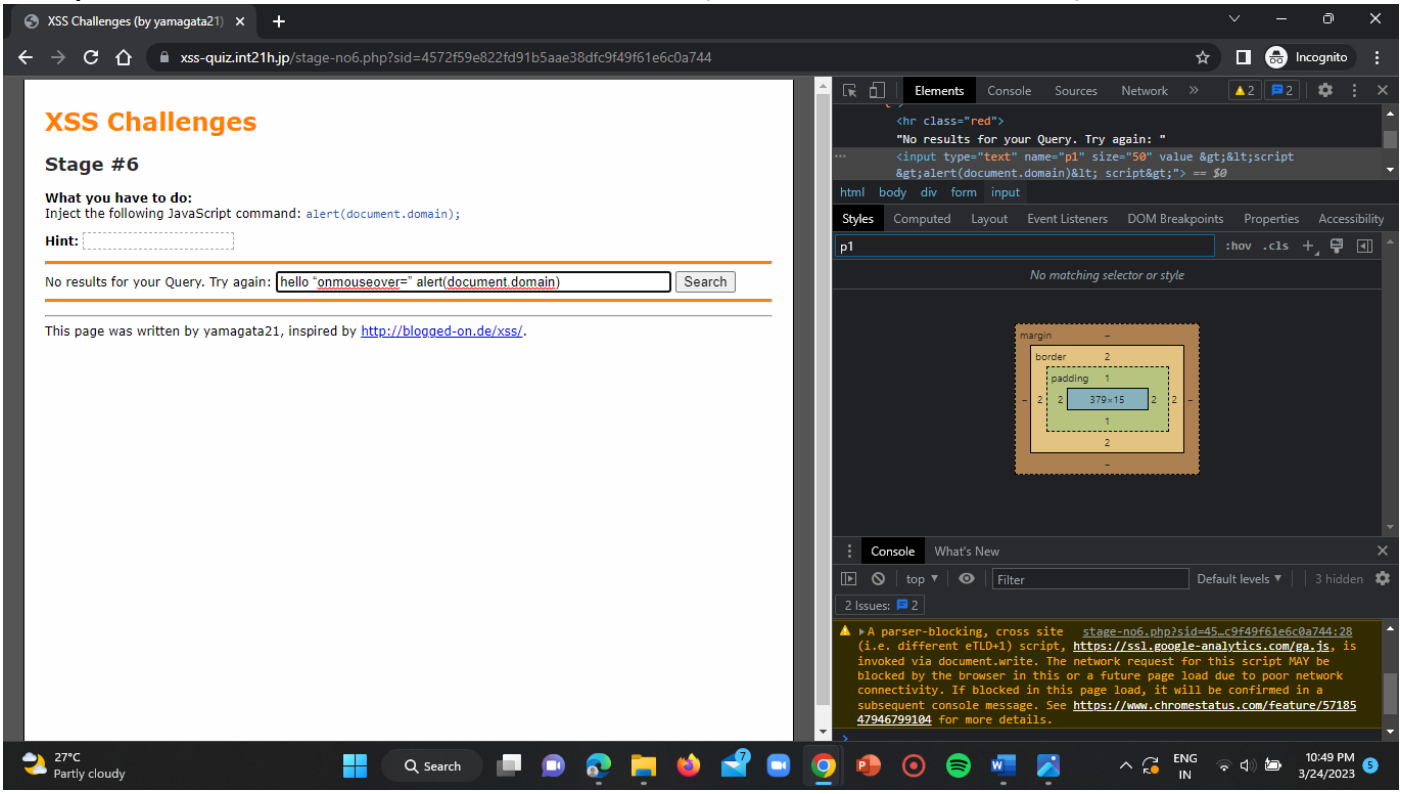
ST#IS#4899



Here we can observe that in inspect it is encoded but we get no results.

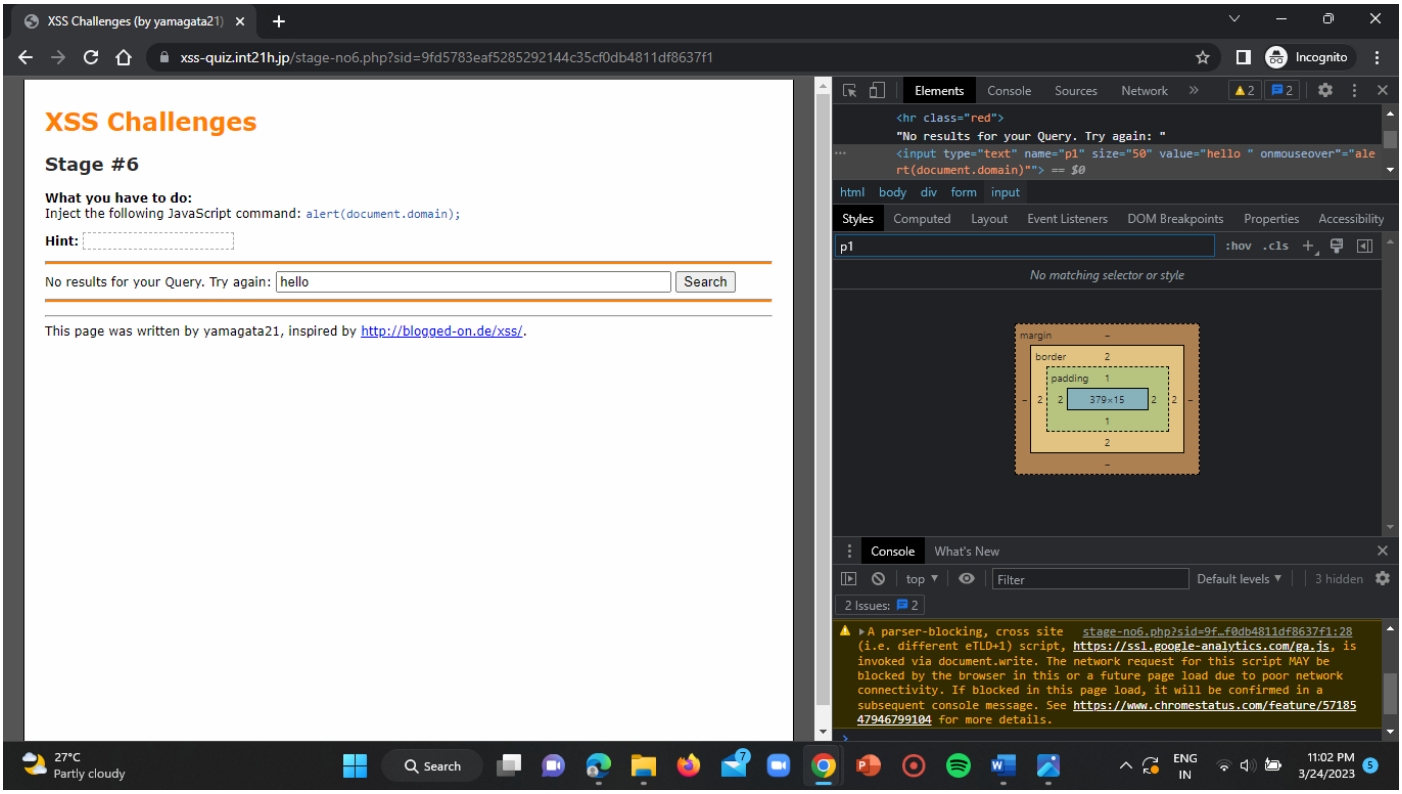
So, now try the given below script in the search bar.

Script: “hello “onmouseover=” alert(document.domain)”

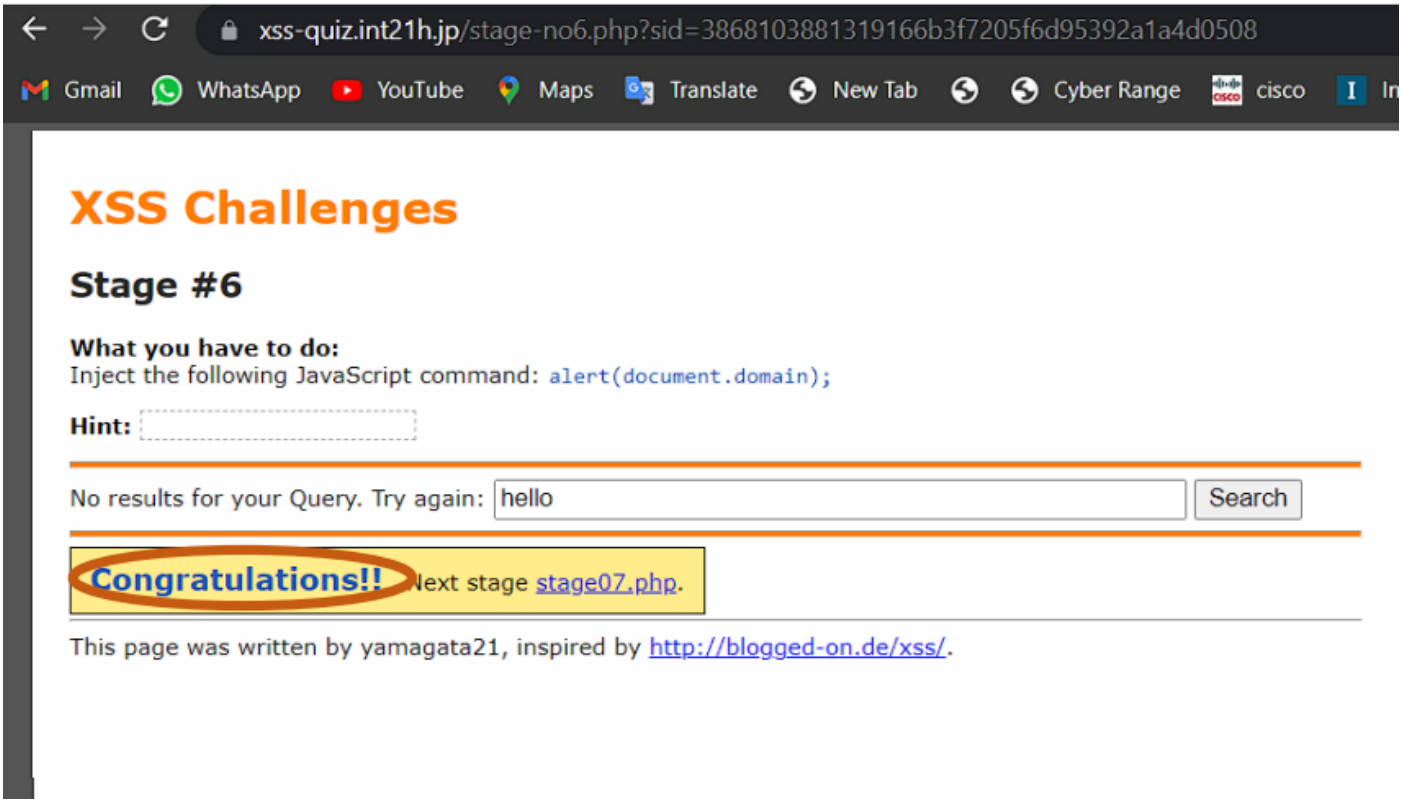


Click on enter.

ST#IS#4899



You will get a popup then click on OK.



Now you've successfully completed the challenge-6.

CONCLUSION:

I hereby conclude that by attempting this task I have learnt about some vulnerabilities using scripts. I also gained knowledge about XSS and we have three types of XSS attacks. They are “Reflected XSS, DOM based XSS attack, Stored XSS attack”.