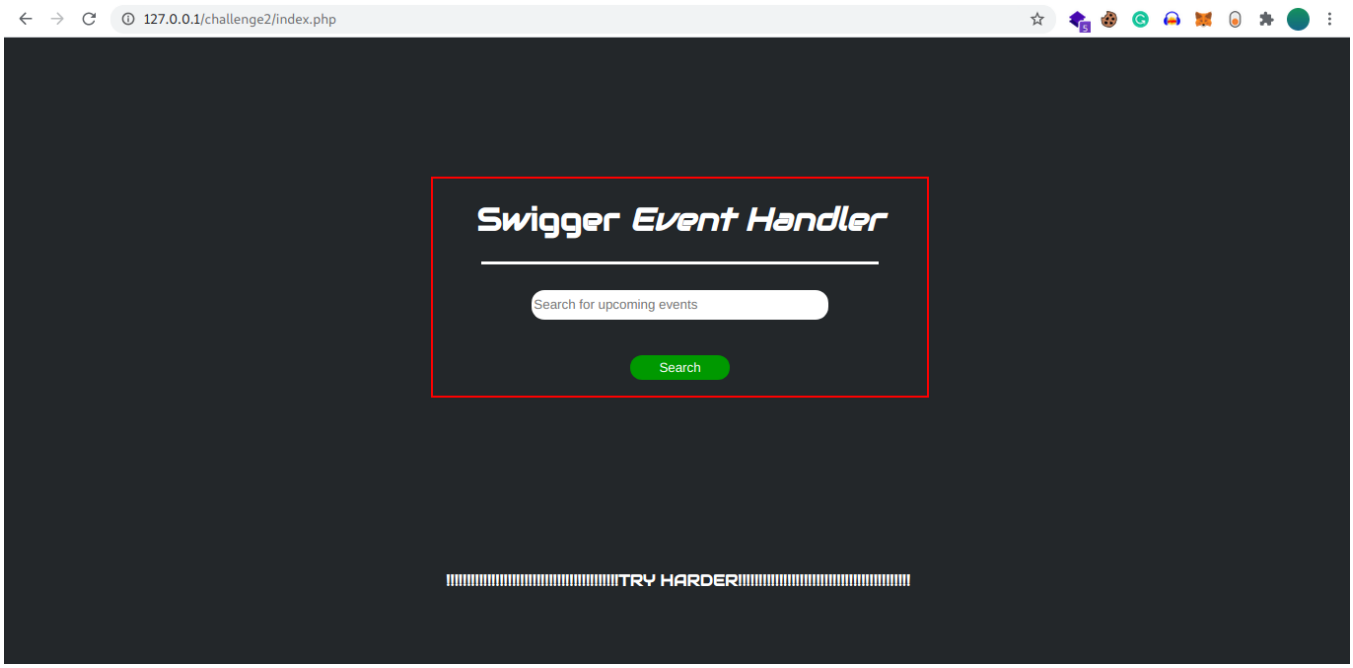
Swigger

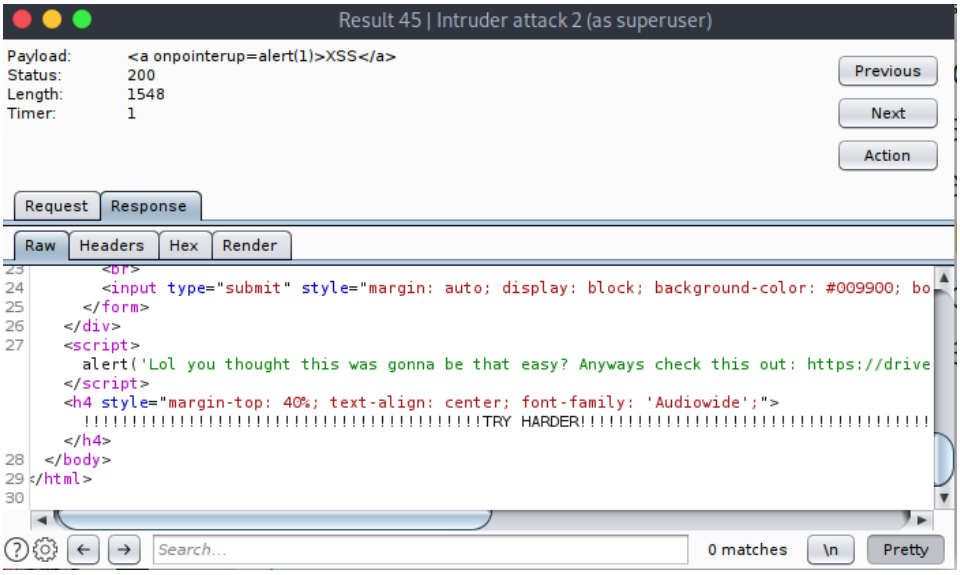


Upon opening the homepage we discover an input field with a title saying Swigger Event Handler.
Basically this challenge involves using the XSS Cheatsheet by Portswigger where they have a section specifically for event handlers.

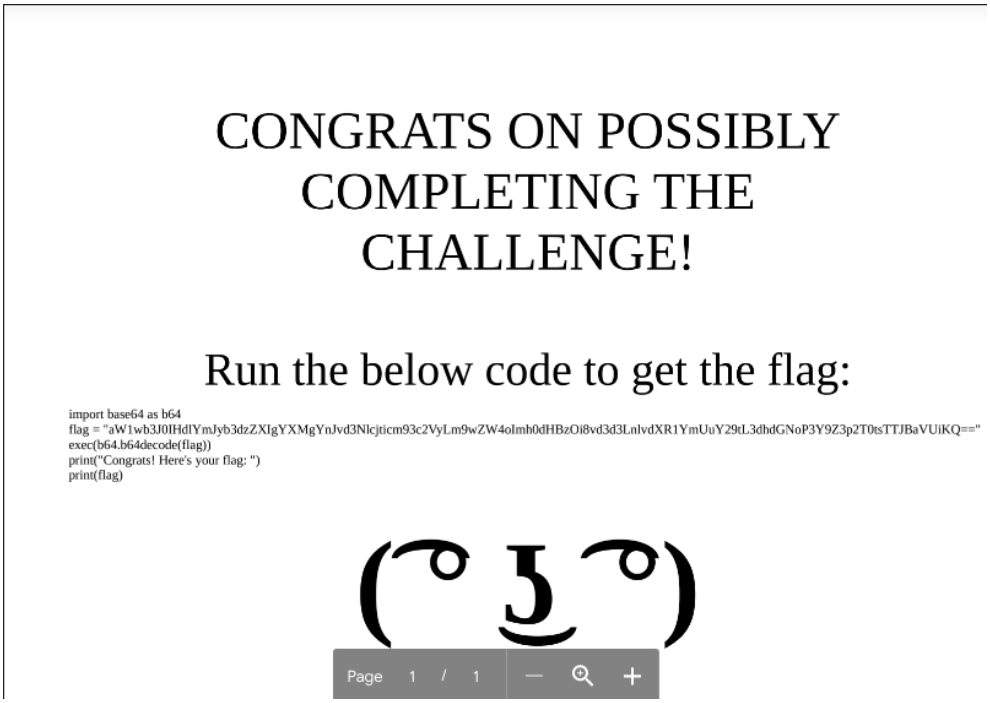
Once we get the payloads by copying it to clipboard, we will input some random text in the webpage and capture the request through Burpsuite.

Now we need to send the data to intruder and add the paste our payloads in the Payloads section. Make sure we are only fuzzing the specific parameter where your sample input was added.

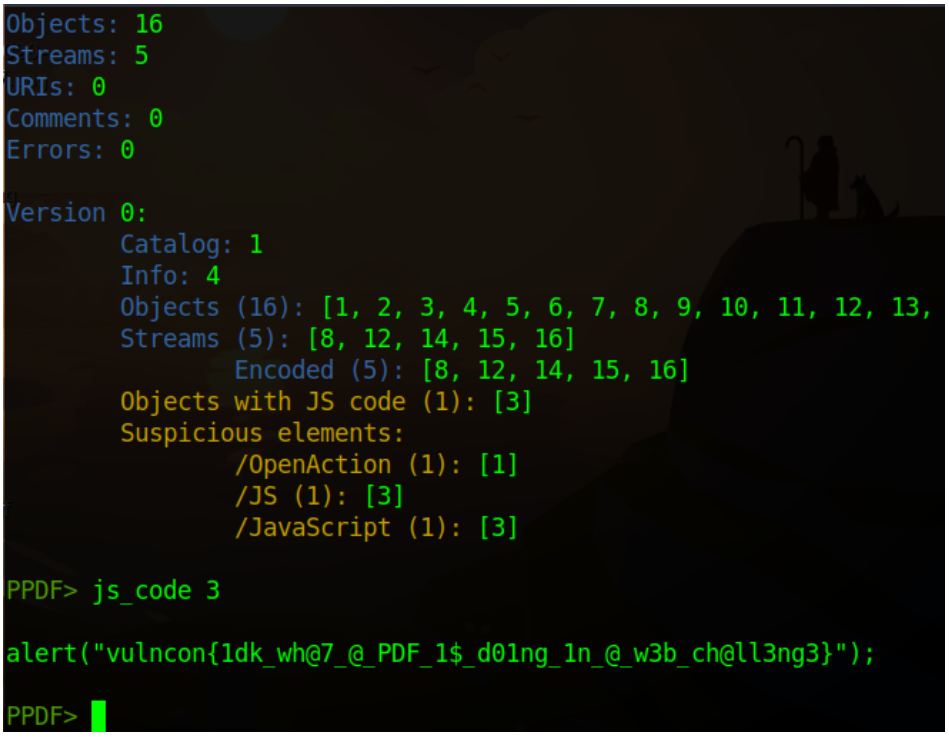
Once you start the attack you just need to pay attention the the length section of the intruder attack window and notice if there is a different length when compared with other requests made. Now just open the request by double clicking it and choose the response tab. Scroll down to the comment part of the code and you will notice a Google drive link mentioned like in the image below:



Once we head over to https://drive.google.com/file/d/1yd6HHon9Gtfxw0Hwuk6HHDRxiSTjnBif/view?usp=sharing we discover a PDF file. Let's download it to our machine and see what we have in it.



Basically what you see on this pdf file is just a rabbit hole. This PDF file has some javascript injected in it which we need to extract first. For this we can use https://github.com/jesparza/peepdf .
We will start up this tool using
python peepdf.py -i
Then we will open our pdf file using
open swigger.pdf
Now we will try to extract the javascript object using
js_code 3
The 3 above is the object id which can be different for others.



And there we have our flag:

vulncon{1dk_wh@7_@_PDF_1$_d01ng_1n_@_w3b_ch@ll3ng3}