Domonic_Themonics : Web Exploitation

Creator: Eddie Points: N/A

Description

This is a faulty react website that embeds the flag in the DOM through overloading the console with excessive divs.The competitor has to know how to query the DOM.

Github Path: Hack-O-Ween/Domonic_Themonics/

Prompt

There's this new website out now that I have been looking at. I looked on reddit and it seems to be a crappy site that doesn't work. But..There was a weird thing that someone noticed. There are invisible attributes of the site. Can you see if there's something important inside the site?

<link>

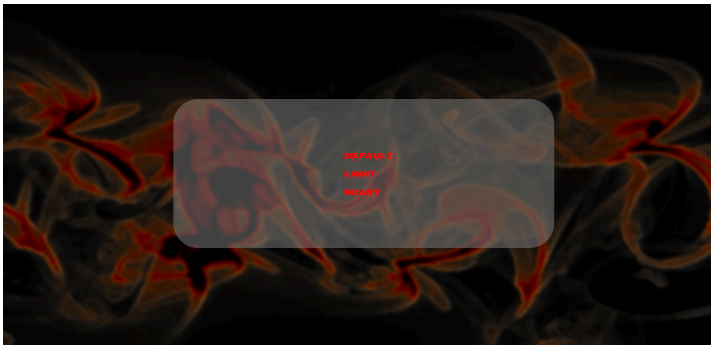
Hints

1. I wonder if there's a way to see what elements make up the page?
2. Is there a way you can search for certain elements in the DOM?
3. Hmm…I wonder if they used an id or class name when making this website

Solution

1. Upon loading into the website, the user can open the inspect

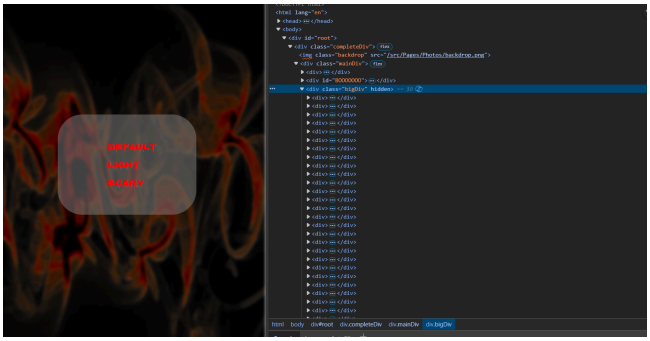
console to input commands. This is because the website does nothing and does not change when the text is selected.

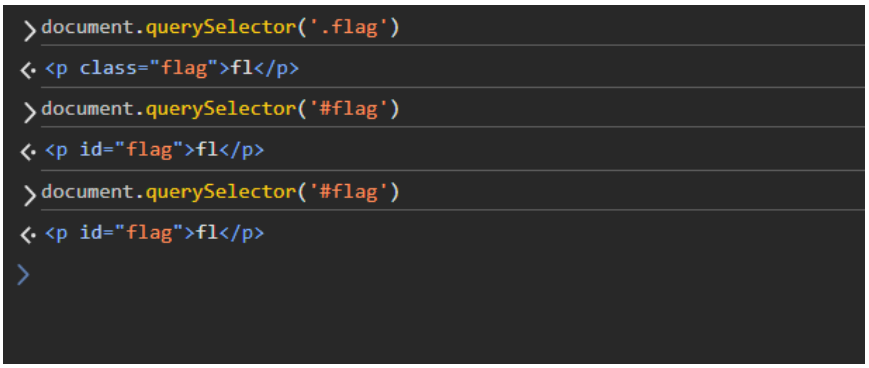


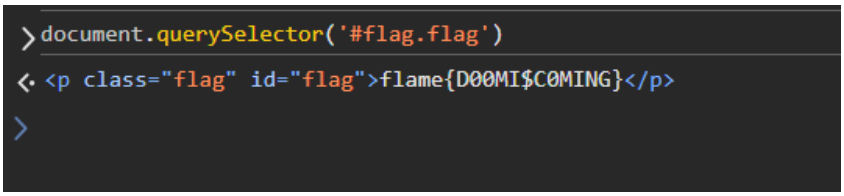
2. The DOM code that is displayed will be too long to individually go through, so the competitor will use the document.selectQuery() command and will do

> document.querySelector('.flag#flag')

I have made it so only that command returns the div with the flag. If you query for just the id or just the class then you will not get the flag.







3. They will do the command on the Scary theme and get the flag. The other text “Default and Light” will change the DOM and the div with the flag will no longer be there.

Flag

flame{DO0MI$C0MING}