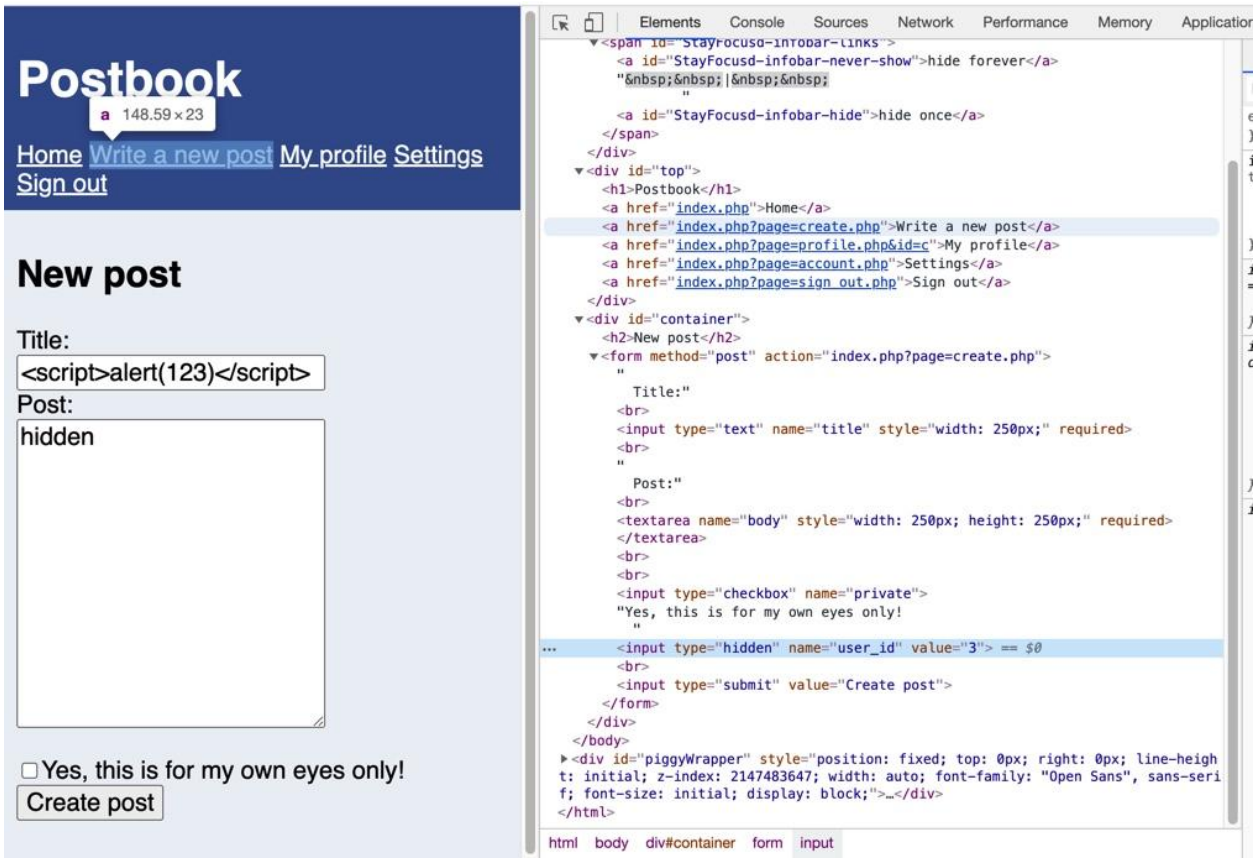
Flag 0: Try using the username provided by the hint. Then try to use common known passwords out there to log in to the site to get the flag.

Flag 1: The ID of each page is written on the web browser. See if you could edit the link.

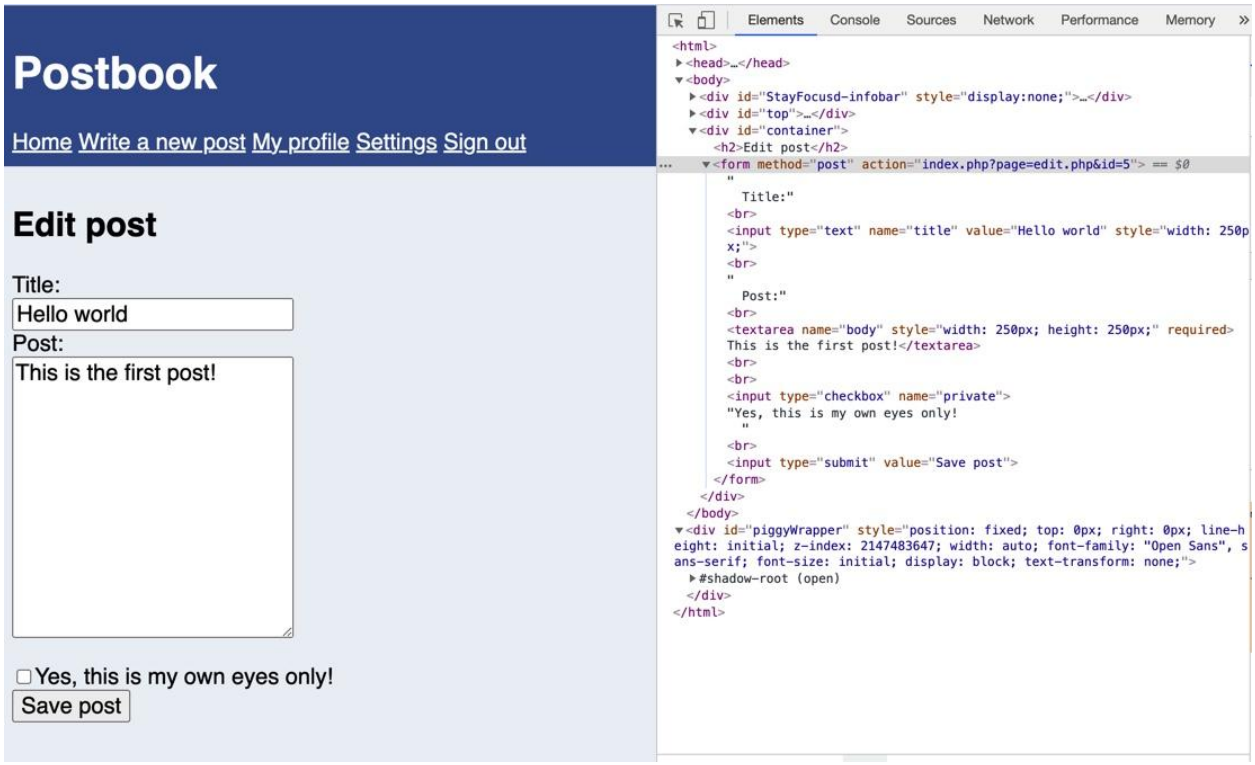
Flag 2: Try to find the hidden field in the inspect element and change the id of the user to post as someone else.



Flag 3: 189*5. Change the ID of the page to 945 like you did in Flag2

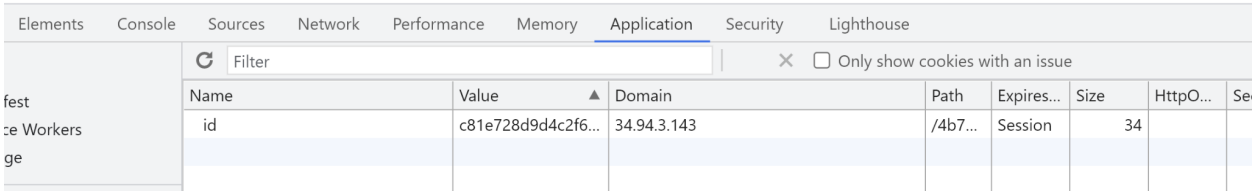
Flag 4:

- You can edit your own posts, what about someone else's?
- Change the ID number of the edit page of another user



Flag 5:

- The cookie allows you to stay signed in. Can you figure out how they work so you can sign in to the user with ID 1?
- Inspect the log-in page
- The cookie's ID is using MD5 Hash. Mine is reversed to 2
- I also use the MD5 Hash to reserve ID = 1 which gives me "`c4ca4238a0b923820dcc509a6f75849b`"
- Then I edit cookie's ID in application to ID = 1

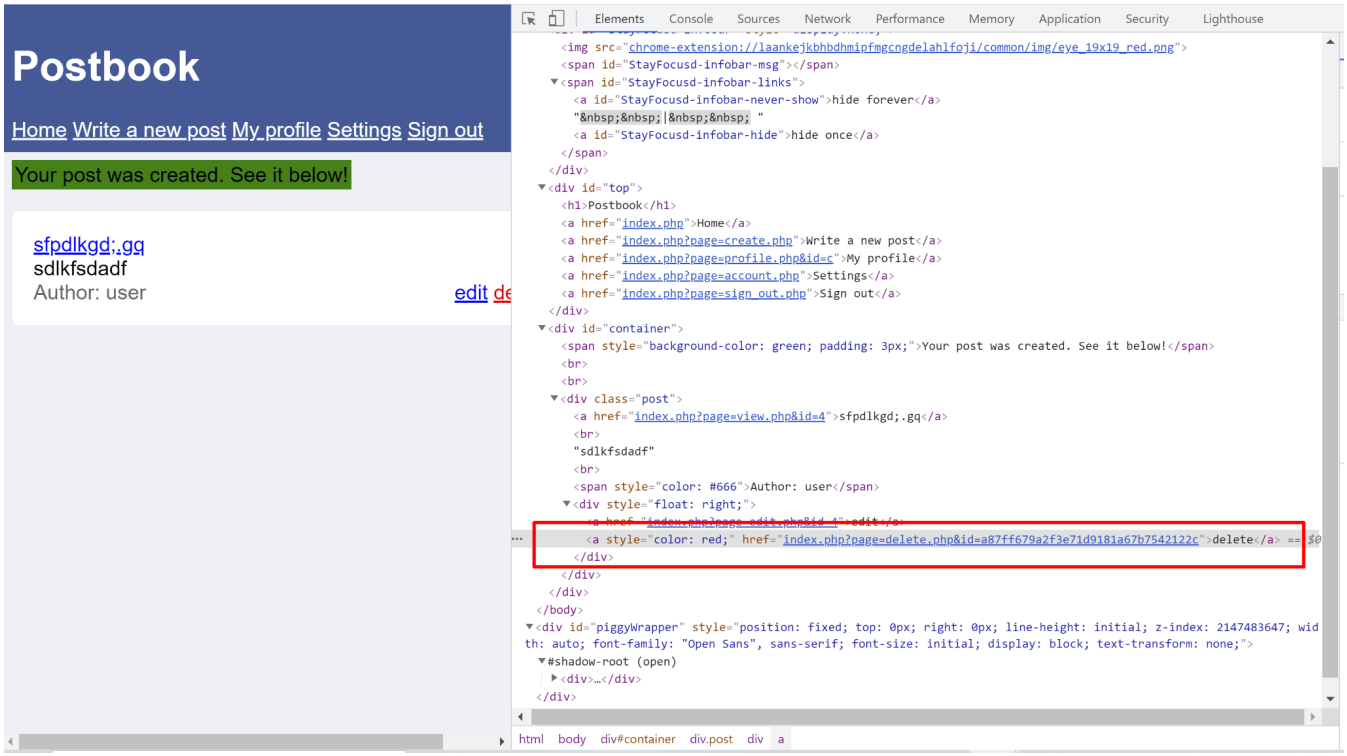


- Finally, I reload the page and I get the flag.

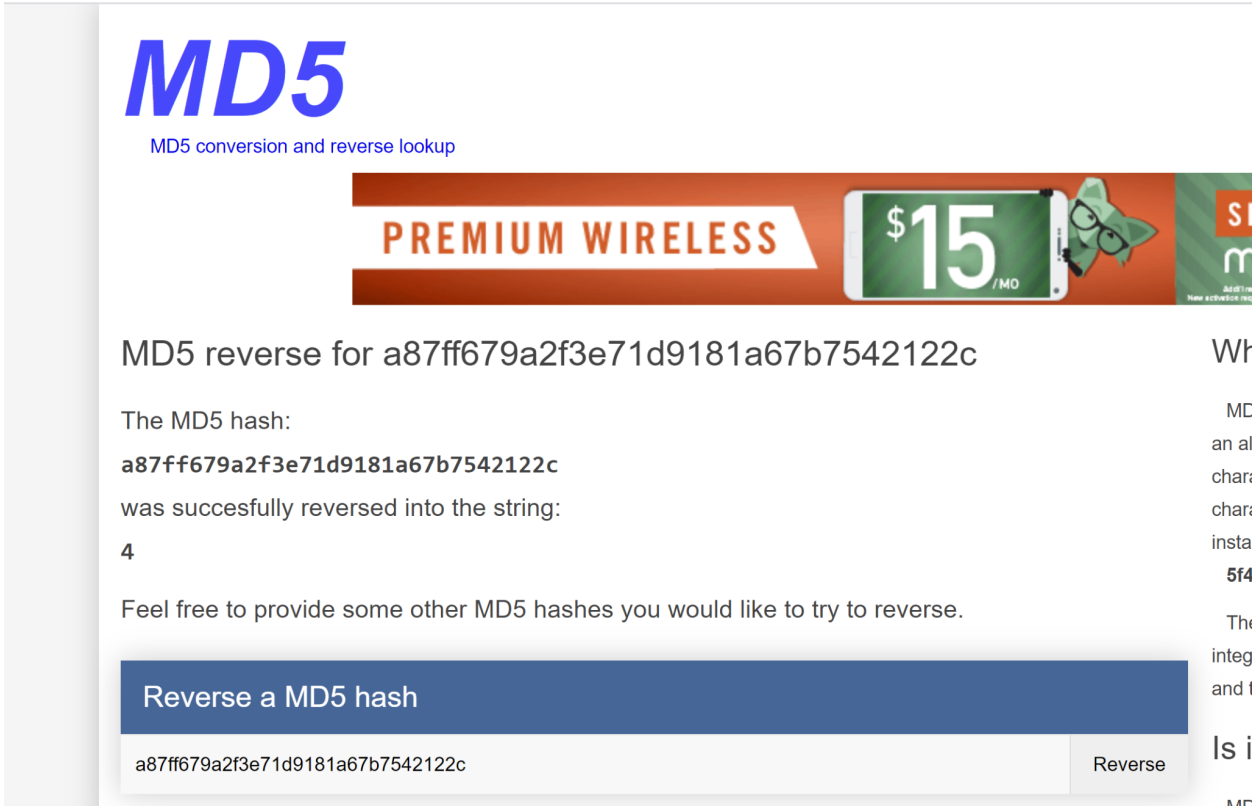
Flag 6:

- Deleting a post seems to take an ID that is not a number. Can you figure out what it is?

- ❖ Inspect the “delete button” element
- ❖ You will find that the ID for delete button is in Hash MD5



I got ID = 4 after I reversed the hash.



Then, I tried to hash the number “1” which is for admin page into MD5 Hash and then I edited the hash ID from 4 to 1.

MD5

MD5 conversion and reverse lookup

MD5 reverse for c4ca4238a0b923820dcc509a6f75849b

The MD5 hash:

c4ca4238a0b923820dcc509a6f75849b

was succesfully reversed into the string:

1

Feel free to provide some other MD5 hashes you would like to try to reverse.

Reverse a MD5 hash

c4ca4238a0b923820dcc509a6f75849b | Reverse

Finally, I refreshed the page and I received the sixth flag.