

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.

The image shows a screenshot of a web browser displaying the 'Postbook' application. The application has a dark blue header with the 'Postbook' logo and navigation links: Home, Write a new post, My profile, Settings, and Sign out. The main content area is titled 'New post' and contains a form with a 'Title' field (containing a JavaScript alert), a 'Post' text area (containing the word 'hidden'), a checkbox labeled 'Yes, this is for my own eyes only', and a 'Create post' button. To the right, the browser's developer tools are open, showing the 'Elements' panel. The selected element is a form with the method 'post' and action 'index.php?page=create.php'. The form contains a hidden input field with the name 'user_id' and value '3'. The browser's address bar shows the URL 'http://localhost:3000/index.php?page=create.php'.

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

Postbook

[Home](#)
[Write a new post](#)
[My profile](#)
[Settings](#)
[Sign out](#)

Edit post

Title:

Post:

This is the first post!

☐ Yes, this is my own eyes only!

Elements
Console
Sources
Network
Performance
Memory

```

<html>
  <head>...</head>
  <body>
    <div id="StayFocusd-infobar" style="display:none;">...</div>
    <div id="top">...</div>
    <div id="container">
      <h2>Edit post</h2>
      ...
      <form method="post" action="index.php?page=edit.php&id=5"> == $0
        "
        Title:"
        <br>
        <input type="text" name="title" value="Hello world" style="width: 250p
        x;">
        <br>
        "
        Post:"
        <div id="body" style="width: 250px; height: 250px;" required>
          This is the first post!</div>
        <br>
        <br>
        <input type="checkbox" name="private">
        "Yes, this is my own eyes only!"
        "
        <br>
        <input type="submit" value="Save post">
      </form>
    </div>
  </body>
</html>

```

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

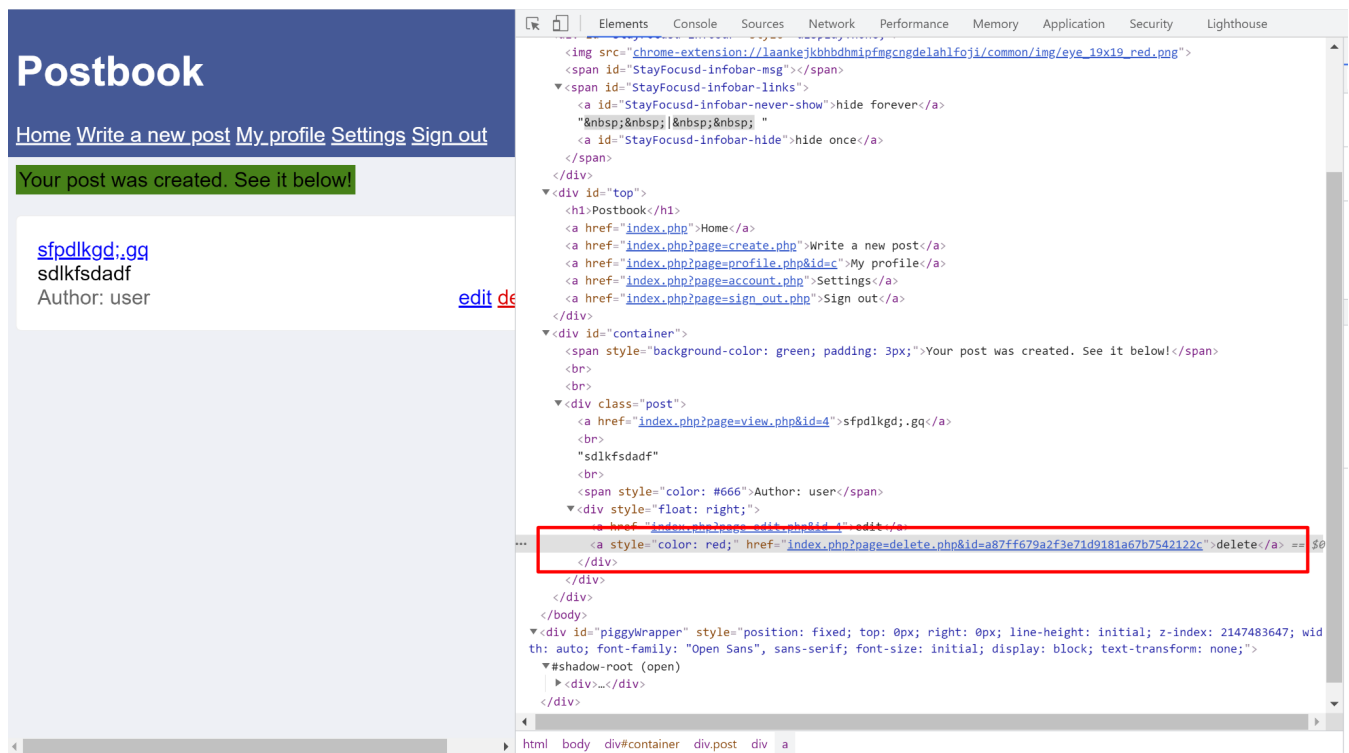
Elements	Console	Sources	Network	Performance	Memory	Application	Security	Lighthouse
<div> <div>Filter</div> <div> <input type="checkbox"/> Only show cookies with an issue </div> </div>								
fest ce Workers ge	Name		Value	Domain		Path	Expires...	Size
	id		c81e728d9d4c2f6...	34.94.3.143		/4b7...	Session	34

- ❖ 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.

MD5

MD5 conversion and reverse lookup

PREMIUM WIRELESS



MD5 reverse for a87ff679a2f3e71d9181a67b7542122c

The MD5 hash:

a87ff679a2f3e71d9181a67b7542122c

was successfully reversed into the string:

4

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

Reverse a MD5 hash

a87ff679a2f3e71d9181a67b7542122c

Reverse

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

PREMIUM WIRELESS



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

PREMIUM WIRELESS



SHOP NOW

mintmobile

Add'l restrictions apply. Taxes & fees extra.
New activation req'd. Min. 2 mo. purchase. See mintmobile.com.

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

Postbook

[Home](#) [Write a new post](#) [My profile](#) [Settings](#) [Sign out](#)

Welcome!

With this amazing tool you can write and publish your own posts. It'll allow you to write public and private posts. Public posts can be read by anyone that signs up. Private posts can only be read by you. See it as your own diary. We'll make sure that your private posts are safe with us.

Post timeline

^FLAG^

\$FLAGS\$

^FLAG^

\$FLAGS\$

What's on your mind?

☐ For my own eyes only

Create post

[xfdzfd](#)
sdfdsfdsg
Author: user

[edit](#) [delete](#)