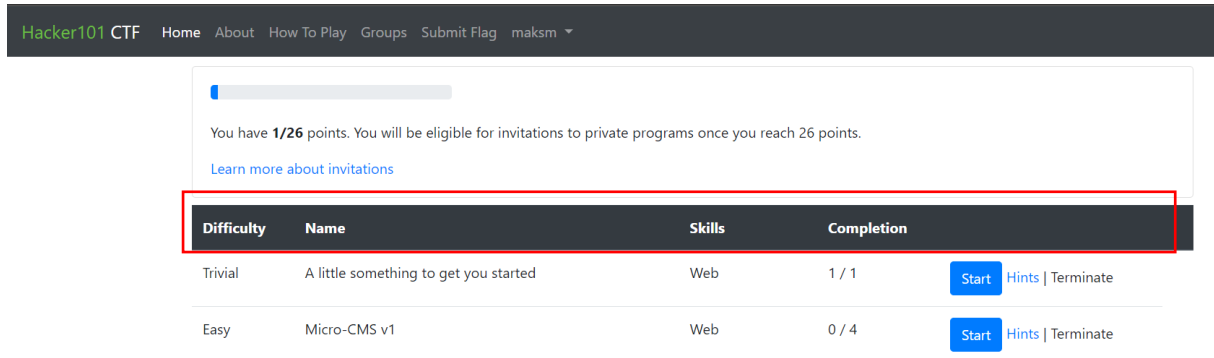


# Hacker101 CTF – Micro-CMS v1 (Easy)

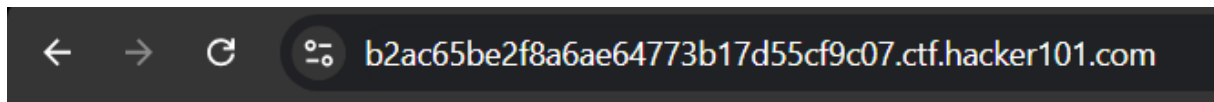
Hacker101 CTF challenges can be found here: <https://ctf.hacker101.com/ctf> The flags are hidden so you can have a go at doing this yourself!



The screenshot shows the Hacker101 CTF dashboard. At the top, there's a navigation bar with links: Home, About, How To Play, Groups, Submit Flag, and a user profile 'maksim'. Below this, a progress bar indicates 'You have 1/26 points. You will be eligible for invitations to private programs once you reach 26 points.' with a link 'Learn more about invitations'. A table of challenges is displayed below, with the first two rows highlighted by a red box.

Difficulty	Name	Skills	Completion	
Trivial	A little something to get you started	Web	1 / 1	<a href="#">Start</a> <a href="#">Hints</a>   <a href="#">Terminate</a>
Easy	Micro-CMS v1	Web	0 / 4	<a href="#">Start</a> <a href="#">Hints</a>   <a href="#">Terminate</a>

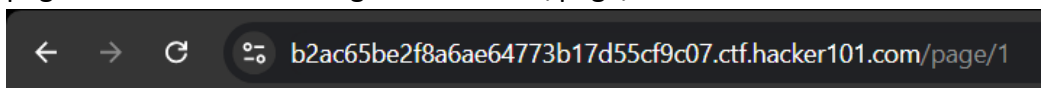
This challenge has 4 flags to capture. Upon starting the level, I am introduced to a page with 4 links:



- [Testing](#)
- [Markdown Test](#)

[Create a new page](#)

I clicked on the testing link. I was directed to the page below. I have an option to edit the page. I also noticed a change in the url to /page/1



[<-- Go Home](#)  
[Edit this page](#)

## Testing

## Woo

Testing out this new micro-CMS!

I clicked on Edit this page. I am introduced to fields where I can edit the page. I ed



[<-- Go Home](#)

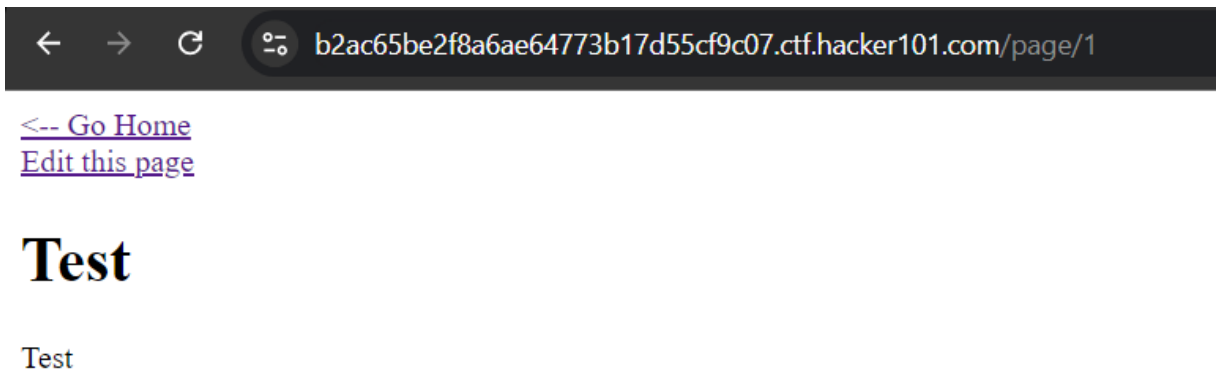
## Edit Page

Title:

#Woo  
Testing out this new micro-CMS!

[<u>Markdown</u>](#) is supported, but scripts are not

I tested the page by editing the fields and pressing the save button to see the changes.



[<-- Go Home](#)  
[<u>Edit this page</u>](#)

## Test

Test


The change worked and redirected me back to the page. The fields were also updated to how I made the changes in Edit this page. I pressed to Go Home at the top to test more links out. I pressed the Markdown Test link, and it navigated me to the page below.

← → ↻ 🔍 b2ac65be2f8a6ae64773b17d55cf9c07.ctf.hacker101.com/page/2

[<-- Go Home](#)  
[Edit this page](#)

# Markdown Test

Just testing some markdown functionality.

 adorable kitten

Some button

The image does not load, and the button does not do anything. I also pressed Edit this page to see the contents.

← → ↻ 🔍 b2ac65be2f8a6ae64773b17d55cf9c07.ctf.hacker101.com/page/edit/2

[<-- Go Home](#)

## Edit Page

Title:

Just testing some markdown functionality.

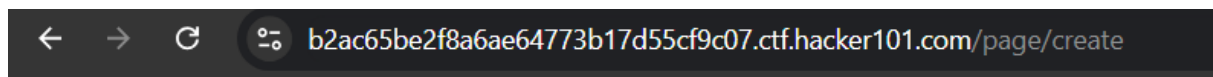
![adorable kitten]  
(<https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e/t/56c2a04520c64707756f4267/1493764650017/>)

<button>Some button</button>

Save

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

I went back Home again and pressed on Create a new page link.



[<-- Go Home](#)

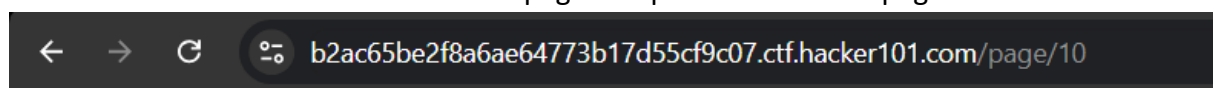
## Create Page

Title:

Create

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

I entered text in the fields to create the page and pressed create. A page was created:



[<-- Go Home](#)

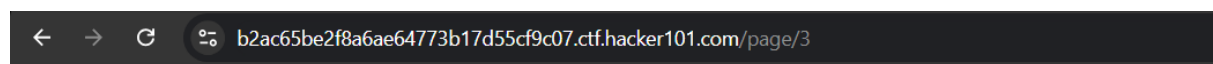
[Edit this page](#)

# fsdf

sfsdfs

I noticed the url having the extension /page/10. The previous pages had 1 and 2, so I checked for pages 3-9 to see if I can access them by modifying the url.

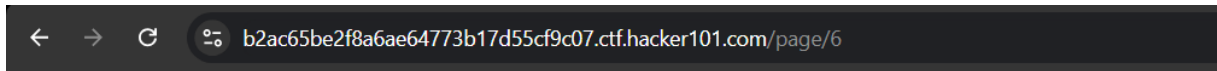
All pages besides number 6 had this text:



## Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

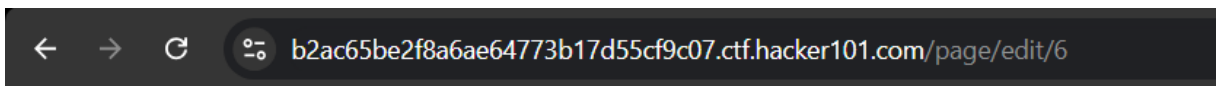
Number 6 had the forbidden text resulting in potential access to the server:



## Forbidden

You don't have the permission to access the requested resource. It is either read-protected or not readable by the server.

Pages can be edited through the url /page/edit/ so I tried to edit page 6 and managed to find the first flag:



[<-- Go Home](#)

## Edit Page

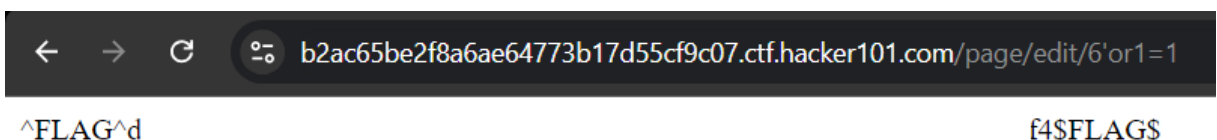
Title:

My secret is  
^FLAG^e

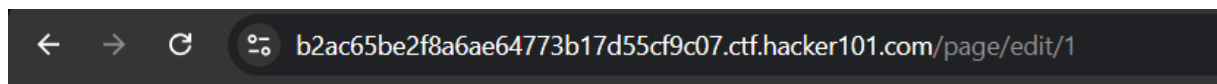
I\$FLAG\$

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

I did a simple sql injection by adding ' to the end of the urls. For /page/edit/"number", I found another flag. I then added 'or1=1 injection and the same flag appeared.



Since I can input and submit fields to either create a page or edit it, I tried an XSS script to see if the fields can be exploited.



[<-- Go Home](#)

## Edit Page

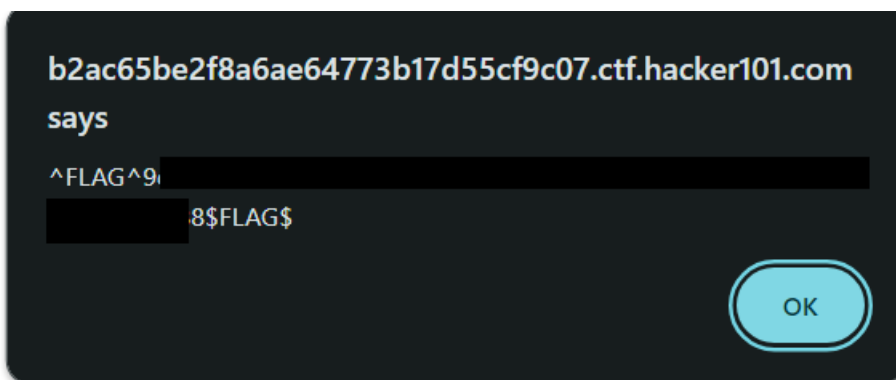
Title:

<script>alert('XSS')</script>

Save

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

The page saved and when I pressed to go home, I received an alert with the flag.



Lastly, I returned to the page containing the button that has no functionality. The page mentions that Markdown is supported but scripts aren't. I edited the page and added

payloads to bypass the markdown filter and execute XSS:

[←](#) [→](#) [↻](#) [🔍](#) b2ac65be2f8a6ae64773b17d55cf9c07.ctf.hacker101.com/page/edit/2

[<-- Go Home](#)

## 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>

Save

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

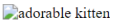
I tried many payloads and saved the page and clicked the button to see if the script responded successfully. The payload in the image above worked and provided an alert. I then inspected the button using inspect element on the browser and I found the flag in the source code:

[←](#) [→](#) [↻](#) [🔍](#) b2ac65be2f8a6ae64773b17d55cf9c07.ctf.hacker101.com/page/2

[<-- Go Home](#)  
[Edit this page](#)

## Markdown Test

Just testing some markdown functionality.

Elements Console Sources Network Performance Memory Application Security Lighthouse

```
<!DOCTYPE html>
<html>
  <head>
    </head>
  <body>
    <a href="/"><-- Go Home</a>
    <br>
    <a href="/edit/2">Edit this page</a>
    <h1>Markdown Test</h1>
    <p>Just testing some markdown functionality.</p>
    <p></p>
    <p>
      <button flag="FLAG"
      button</button> == $0
    </p>
  </body>
</html>
```