002. Micro-CMS v1

Date : 07-02-2023

Time Taken : 20 Minutes

Platform : Hacker101

Player Name : Fr3y0

CTF Name : Micro-CMS v1

Full URL:- https://ctf.hacker101.com/ctf

IP: xx.xx.xx.xx

Host-name: NULL

Nmap Scan: NULL

System Information: Linux

So There Are 4 Flags !

Flag 1

- As this is some kind of form and it is taking response and shifts to one another page as shown in URL so I edit last page number and kaboom ! we got our flag (broken authentication) or just run dirb `ni6st@x:~$ dirb https://141ac3ff0aaf8130b4280eab22368ed6.ctf.hacker101.com/page/edit/

```
DIRB v2.22
By The Dark Raver
```

```
START_TIME: Tue Feb 6 22:27:58 2024
URL_BASE:
https://141ac3ff0aaf8130b4280eab22368ed6.ctf.hacker101.com/page/edit/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612
```

`---- Scanning URL:

- `https://141ac3ff0aaf8130b4280eab22368ed6.ctf.hacker101.com/page/edit/02 (CODE:200|SIZE:808)`
- `https://141ac3ff0aaf8130b4280eab22368ed6.ctf.hacker101.com/page/edit/06 (CODE:200|SIZE:682)`
- `https://141ac3ff0aaf8130b4280eab22368ed6.ctf.hacker101.com/page/edit/08 (CODE:200|SIZE:595)`
- `https://141ac3ff0aaf8130b4280eab22368ed6.ctf.hacker101.com/page/edit/1 (CODE:200|SIZE:625)`
- `https://141ac3ff0aaf8130b4280eab22368ed6.ctf.hacker101.com/page/edit/2 (CODE:200|SIZE:808)`
- `https://141ac3ff0aaf8130b4280eab22368ed6.ctf.hacker101.com/page/edit/6 (CODE:200|SIZE:682)`
- `https://141ac3ff0aaf8130b4280eab22368ed6.ctf.hacker101.com/page/edit/8 (CODE:200|SIZE:595)`
  `--> Testing: https://141ac3ff0aaf8130b4280eab22368ed6.ctf.hacker101.com/`

well I did get anything by dirb only code 200 so I stopped it

`

Flag 2 (SQLI)

Well I used simple payload for this As we can edit URL I just tried that in the main page
`https://fee969caffc1c920c10030c1a79cc9ab.ctf.hacker101.com/page/1'`

but did't found anything so let's move to the edit part !
And got it
`https://fee969caffc1c920c10030c1a79cc9ab.ctf.hacker101.com/page/edit/1'`

Flag 3 (XSS)

I love this XSS easy and simple so lets crate a page
I used this payload : `<script>alert(1)</script>` Universal Payload
and then we go back we got our flag

Flag 4 (XSS on button)

To be serious that button on the edit page was really bugging me since the start of this challenge so let's see what we can do
`https://fee969caffc1c920c10030c1a79cc9ab.ctf.hacker101.com/page/2`
let's edit this
`https://fee969caffc1c920c10030c1a79cc9ab.ctf.hacker101.com/page/edit/2`
now time to write our payload
Payload `<button onclick="alert(1)">Hacked by fr3y</button>`
That's it go to your Inspect section and you will have the flag or just view source of the page

<-- Go Home
Edit this page

Markdown Test

Just testing some markdown functionality.

 adorable kitten

Hacked by fr3y