Emdee five for life

🛡 ⬕ 139.59.162.63:31239

kyrepo/... ⊕ Reverse Shell Cheat Sh... ◉ Linux – Privilege Escala... ◉ Windows – Privilege Es... 👕 CyberChef

MD5 encrypt this string

uDOpk3cIITYkZGyacuvX

MD5

Submit

🛡 ⬕ 139.59.162.63:31239

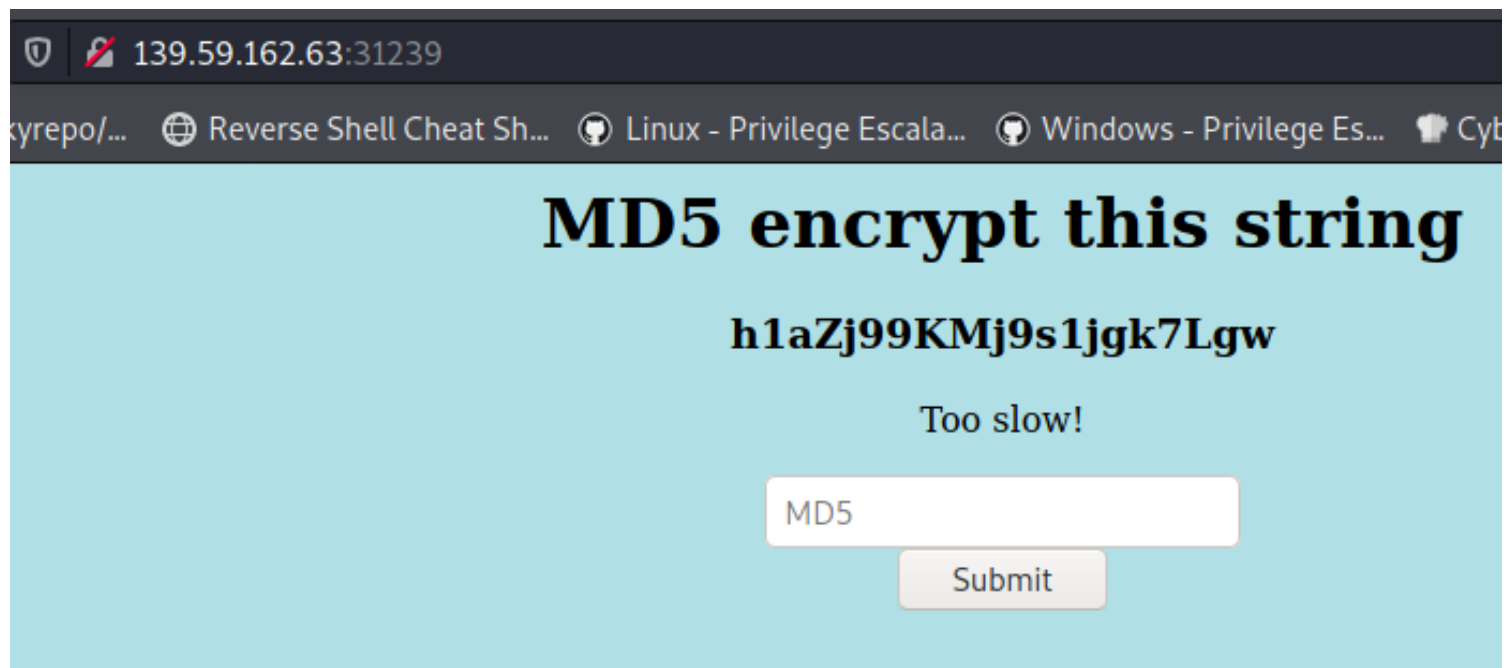kyrepo/... ⊕ Reverse Shell Cheat Sh... ◉ Linux – Privilege Escala... ◉ Windows – Privilege Es... 👕 Cyb

MD5 encrypt this string
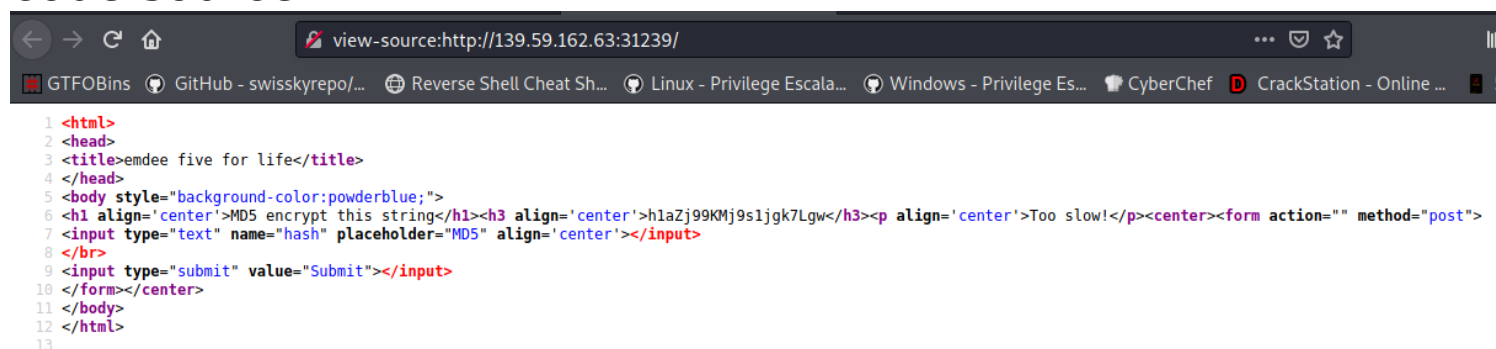
x7nFp19lx25UiBPet4pm

MD5

Submit

our only task is to submit the string after converting it to md5 hash ...but when i tried to submit i got this...

MD5 encrypt this string

h1aZj99KMj9s1jgk7Lgw

Too slow!

```
MD5
```

Submit

Let's automate this and build a python script for it and i will be using :
>>re module (For regex)
>>hashlib module (For md5)
>>requests module (For GET and post)

code source


```html
1  <html>
2  <head>
3  <title>emdee five for life</title>
4  </head>
5  <body style="background-color:powderblue;">
6  <h1 align='center'>MD5 encrypt this string</h1><h3 align='center'>h1aZj99KMj9s1jgk7Lgw</h3><p align='center'>Too slow!</p><center><form action="" method="post">
7  <input type="text" name="hash" placeholder="MD5" align='center'></input>
8  </br>
9  <input type="submit" value="Submit"></input>
10 </form></center>
11 </body>
12 </html>
13
```

Building the script

So with my crappy skills of regex let's start building the logic ...
<h3 align='center'>h1aZj99KMj9s1jgk7Lgw</h3>

This was achieved by using this ...
center'>+.*?</h3>

Now we will filter it more and will make the final script...

```python
1    import requests
2    import hashlib
3    import re
4
5    url = "http://139.59.162.63:31239/"
6
7    r = requests.session()
8    out = r.get(url)
9    out = re.search("<h3 align='center'>+.*?</h3>",out.text)
10   out=re.search("'>.*<",out[0])
11   out=re.search("[^|'|>|<]....................",out[0])
12
13   out=hashlib.md5(out[0].encode('utf-8')).hexdigest()
14
15   print("sending md5 :-{}".format(out))
16
17   data={'hash': out}
18   out = r.post(url = url, data = data)
19
20   print(out.text)
21
```

Now time to run the script and get the flag :)

```
┌──(root㉿kali)-[/Documents/htb/challenge/web/Emdee five for life]
└─# python3 emdee.py                                                                          130
sending md5 :-9cefad0e4bee9c9dfc5cc32c1a6a1a3b
<html>
<head>
<title>emdee five for life</title>
</head>
<body style="background-color:powderblue;">
<h1 align='center'>MD5 encrypt this string</h1><h3 align='center'>0N76noNyrxkW5BVVzExP</h3><p align='center'>HTB{N1c3_ScrIpt1nG_B0i!}</p><center><form action="" method="post">
<input type="text" name="hash" placeholder="MD5" align='center'></input>
</br>
<input type="submit" value="Submit"></input>
</form></center>
</body>
</html>
```