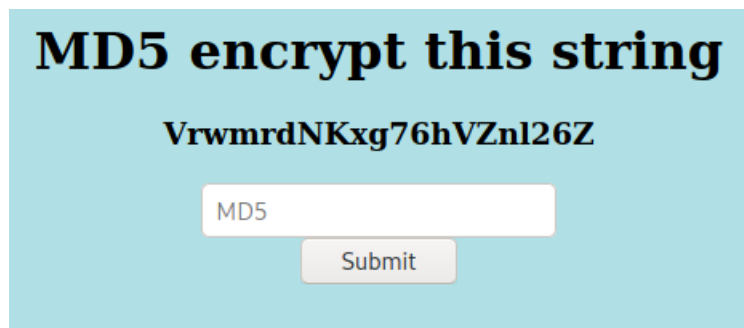


The website shows a string which explicitly mentioned to hash it using MD5 and submitting it.



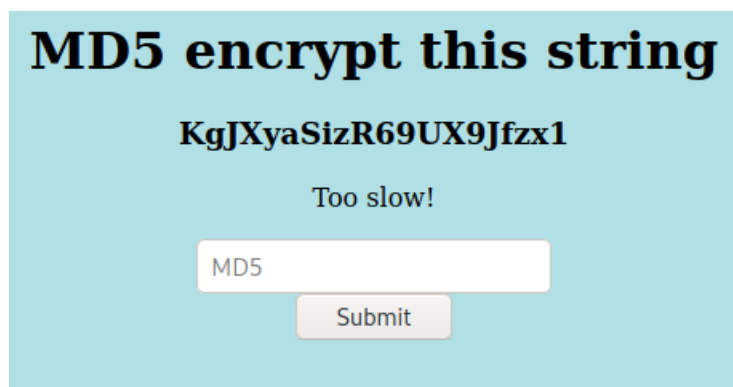
**MD5 encrypt this string**

**VrwmrdNKxg76hVZnl26Z**

MD5

Submit

When I try to do that manually, I was returned another string and was told that I was “Too slow!”.



**MD5 encrypt this string**

**KgJXyaSizR69UX9Jfzx1**

Too slow!

MD5

Submit

As such, I probably need to write a script to make the hash submission faster. Using Burp Suite, I can see how the request is like when the string is being loaded (GET method) and how to hash is being submitted (POST method):

```
1 GET / HTTP/1.1
2 Host: 167.99.90.58:31673
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=inl5vbm5gje39ceu3rb4hofd5
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
```

```
1 POST / HTTP/1.1
2 Host: 167.99.90.58:31673
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 12
9 Origin: http://167.99.90.58:31673
10 Connection: close
11 Referer: http://167.99.90.58:31673/
12 Cookie: PHPSESSID=inl5vbm5gje39ceu3rb4hofd5
13 Upgrade-Insecure-Requests: 1
14
15 hash=TESTING
```

So all we need to do is write a script which uses regex to grab the string in the first GET request, followed by hashing and submitting it using the “hash” parameter in the second POST request. Key thing to note is to ensure that the session is persistent between both requests.

```
root@kali:~/Downloads/Emdee_five_for_life# python3 script.py
The string is: pnMkPbQB8mIG60NyrPXo
The md5 hash is: 5225fc3fe1fa5343ab12e4e4d0c6af2c
Response:
<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'>pnMkPbQB8mIG60NyrPXo</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>
```

Using my script, I obtained the flag.