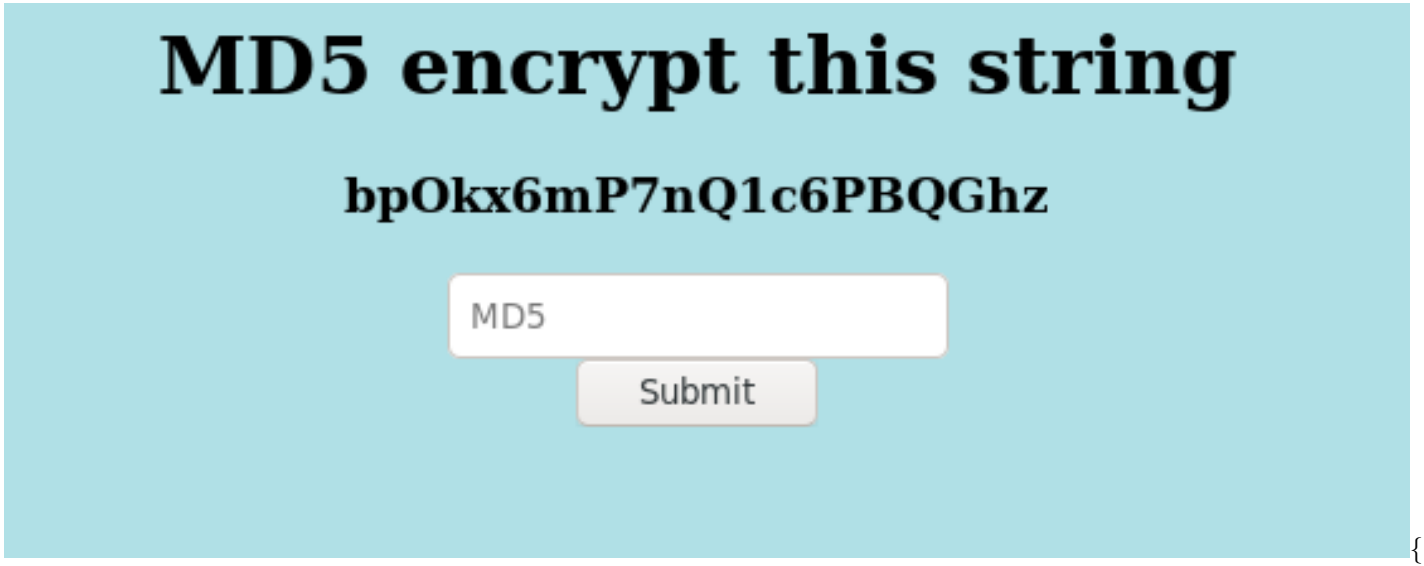
Emdee five for life Writeup HackTheBox Web Challenge

2019-12-01

La descripción del reto es la siguiente:

`Can you encrypt fast enough?`

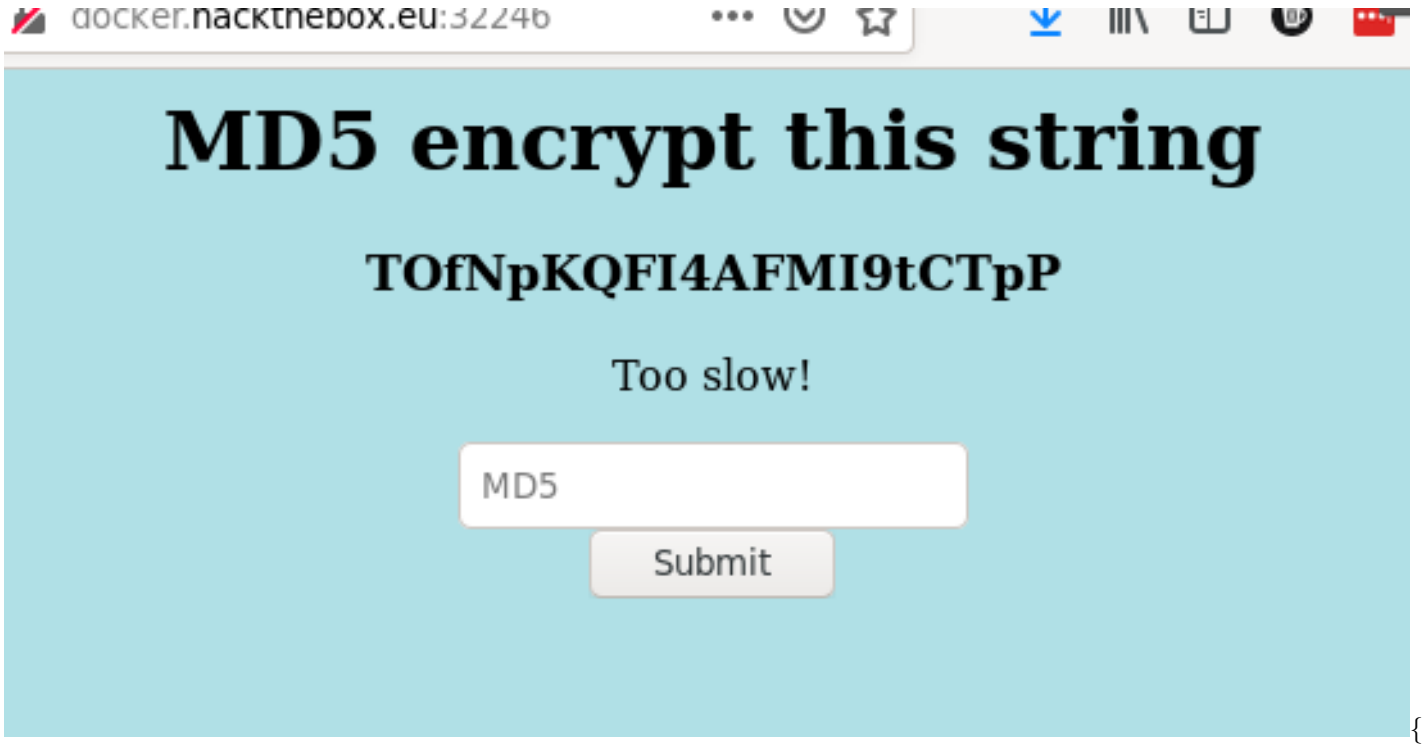
Al acceder a la web vemos que nos da un string y nos pide que lo cifremos en MD5 y lo enviemos.



{:height= width="100%"}

Si lo enviamos con el navegador vemos que nos dice *Too slow!*, por lo que se puede suponer que es necesario realizar un script que haga esta acción para realizarlo de forma mas rápida.

Si analizamos el trafico vemos que unicamente se envía un POST en el que el form contiene el hash del string proporcionado, por lo que en principio solo sera necesario realizar un GET a la web para obtener el string, calcular el hash y realizar un POST para capturar la respuesta y obtener el flag, pero esta primera prueba no ha funcionado, por lo que se ha realizado un análisis mas detallado del tráfico.



{:height= width="100%"}

Si analizamos la cabecera vemos que hay un campo para cookies, tanto en el GET como en el POST, por lo que este puede ser el motivo por el que falle el POST.

```
Cookie pair: PHPSESSID=fnroeunk08h8hl7v0ubhn4bcr6
```

Finalmente se actualiza el código para tener en cuenta los cookies en el POST y se realiza la petición. El código que realiza esta acción se puede ver a continuación:

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

import requests
import hashlib
import re

regex = "<h3 align='center'>(.*)</h3>"


def encrypt_md5(string: str) -> str:
    result = hashlib.md5(string.encode())
    return result.hexdigest()


# Get a la web para obtener el valor a cifrar
response = requests.get('http://docker.hackthebox.eu:32246/')


# Creacon de la peticion post
response_regex = re.search(regex, response.text)
form = {'hash': encrypt_md5(response_regex.group(1))}
response_post = requests.post('http://docker.hackthebox.eu:32246/', data=form, cookies=response.cookies)


print(response_post)
print(response_post.text)
```

Al ejecutarlo se obtiene la siguiente salida, en la que se puede ver el flag. Cabe destacar que este código se ha ejecutado varias veces y en alguna ocasión ha indicado que has sido muy lento, por lo que el timeout es muy bajo.

```
<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'>d3FXG8iZJs19dw6HkUXi</h3><p align='center'>
<input type="text" name="hash" placeholder="MD5" align='center'></input>
</br>
<input type="submit" value="Submit"></input>
</form></center>
</body>
</html>
```