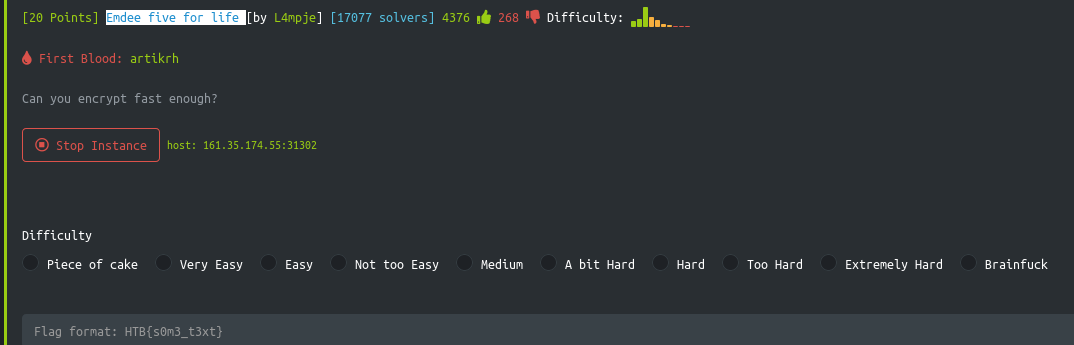
***Hack the Box Reports:***

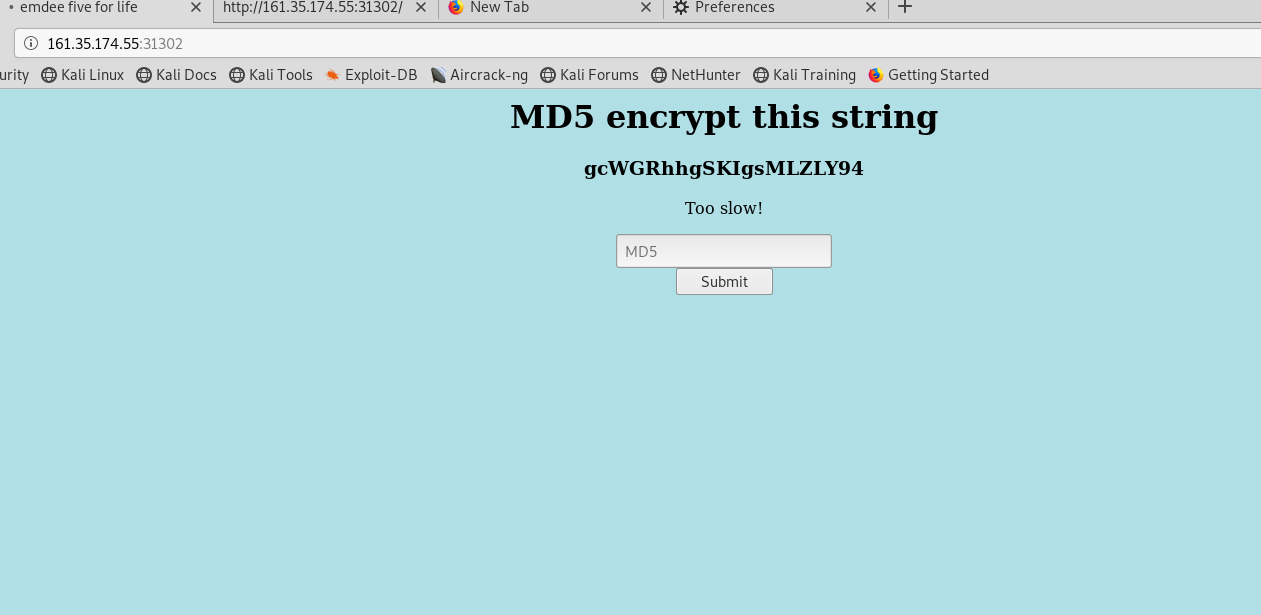
Emdee Five for Life:

Challenge: “Can you encrypt fast enough?”



After copying the host Url

I entered it in Firefox and got the website:



I first google MD5 encrypted and copied the hash and tried to encrypt it and kept getting the error message “Too slow!”

So, I then had to open the leafpad and create a python script to get a GET request from the target box.

#!/bin/usr/python

import requests

import hashlib

import re

req = requests.session()

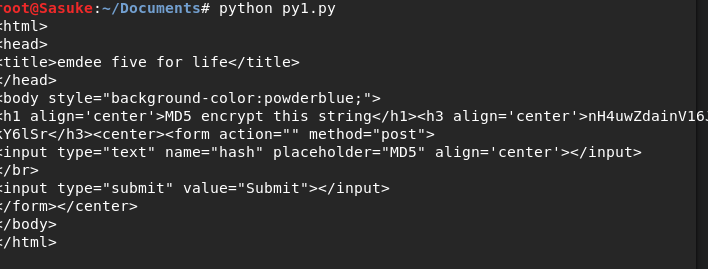
url = "http://161.35.174.55:31302/"

## GET REQUEST

rget = req.get(url)

html = rget.content

print(html)



Now that I got a get request from the Target, I had to now strip any unnecessary HTML contents and split a random string from it.

Here is python script #2

#!/bin/usr/python

import requests

import hashlib

import re

req = requests.session()

url = "http://161.35.174.55:31302/"

##GET Requet

rget = req.get(url)

html = rget.content

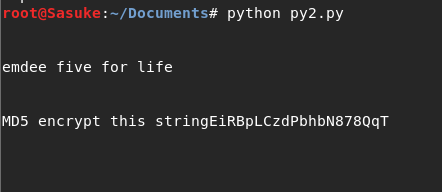
###Strip HTML

def html\_tags(html):

clean = re.compile('<.\*?>')

return re.sub(clean, '', html)

print(html\_tags(html))



Now that the unnecessary HTML content is gone, I just need to split a random string from the output

Python Script 3

#!/bin/usr/python

import requests

import hashlib

import re

req = requests.session()

url = "http://161.35.174.55:31302/"

### GET Request

rget = req.get(url)

html = rget.content

### Strip HTML

def html\_tags(html):

clean = re.compile('<.\*?>')

return re.sub(clean, '', html)

### Split Random String

out1 = html\_tags(html)

out2 = out1.split('string')[1]

out3 = out2.rstrip()

print(out3)



Now we can only output a random string. Now I have to use MD5 and encrypt the string a POST request to submit it

Python Script 4:

#!/bin/usr/python

import requests

import hashlib

import re

req = requests.session()

url = "http://161.35.174.55:31302/"

### GET Request

rget = req.get(url)

html = rget.content

### Strip HTML

def html\_tags(html):

clean = re.compile('<.\*?>')

return re.sub(clean, '', html)

### Split Random String

out1 = html\_tags(html)

out2 = out1.split('string')[1]

out3 = out2.rstrip()

### MD5 Encrypt

mdHash = hashlib.md5(out3).hexdigest()

print(mdHash)

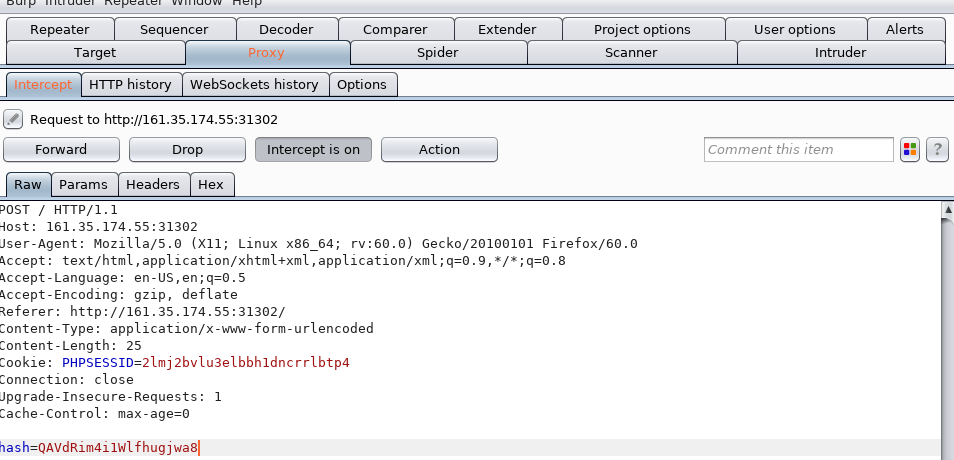


Now the MD5 is encrypted . Now I need to POST Request to submit to the target server

I opened Burp Suite and opened Firefox and went to settings>General>Network>Proxy>Manual Proxy through burp suite

I then refreshed the page on firefox url <http://161.35.174.55:31302/>

And got RAW text



I can see that it is posted with hash= parameter. Now I need to modify our exploit to submit the encrypted string with hash= parameter as a POST request.

Python Script 5:

#!/bin/usr/python

import requests

import hashlib

import re

req = requests.session()

url = "http://161.35.174.55:31302/"

### GET Request

rget = req.get(url)

html = rget.content

### Strip HTML

def html\_tags(html):

clean = re.compile('<.\*?>')

return re.sub(clean, '', html)

### Split Random String

out1 = html\_tags(html)

out2 = out1.split('string')[1]

out3 = out2.rstrip()

### MD5 encrypt

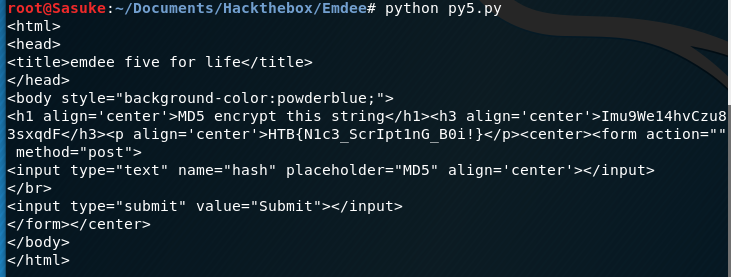
mdHash = hashlib.md5(out3).hexdigest()

### POST Encrypt

data = dict(hash=mdHash)

rpost = req.post(url=url, data=data)

print(rpost.text)



Success! I found the flag!

