1、知识点

知识点	说明
stripslashes()	删除由addslashes()函数添加的反斜杠（也就是删除反斜杠）

2、源码

```
<?php

#GOAL: login as admin,then get the flag;
error_reporting(0);
require 'db.inc.php';

function clean($str){
    if(get_magic_quotes_gpc()){ //get_magic_quotes_gpc – 获取当前 magic_quotes_gpc 的配置选项设置
        $str=stripslashes($str); //返回一个去除转义反斜线后的字符串（\' 转换为 ' 等等）。双反斜线（\\）被转换为单个反斜线（\）。
    }
    return htmlentities($str, ENT_QUOTES);
}

$username = @clean((string)$_GET['username']);
$password = @clean((string)$_GET['password']);


$query='SELECT * FROM users WHERE name=\''.$username.'\' AND
pass=\''.$password.'\';';
$result=mysql_query($query);
if(!$result || mysql_num_rows($result) < 1){
    die('Invalid password!');
}

echo $flag;

?>
```

3、分析

1）先看一下这条SQL语句，接收变量usernam和password的值并用单引号'包围，进行拼接，如果查询有结果，就返回flag。

```
$query='SELECT * FROM users WHERE name=\''.$username.'\' AND pass=\''.$password.'\';';
$result=mysql_query($query);
if(!$result || mysql_num_rows($result) < 1){
    die('Invalid password!');
}

echo $flag;
```

2）变量username和password是从GET中接收到的，并对GET中的反斜杠进行删除，然后使用htmlentites过滤XSS关键词。

```php
require 'db.inc.php';

function clean($str){
    if(get_magic_quotes_gpc()){ //get_magic_quotes_gpc – 获取当前 magic_
        $str=stripslashes($str); //返回一个去除转义反斜线后的字符串（\' 转换为
    }
    return htmlentities($str, flags: ENT_QUOTES);
}

$username = @clean((string)$_GET['username']);
$password = @clean((string)$_GET['password']);
```

3）此时通过GET传入username添加单引号'闭合SQL语句中的username的值，然后添加or关键词，并注释SQL语句中后面的语句，即可让查询结果为真，得到flag。由于该题为CTF题，flag以及其他配置文件这里没有，只用于学习绕过思路。

4、利用

```
?username=admin\'\' AND pass=\'' or 1#password=x
```