/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\* 程序作者：爱的伊苏 \*/

/\* 程序完成时间：2019/2/6 \*/

/\* 有任何问题请联系：740531307@qq.com \*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//@永远得意的笑下去

首先明确这是一道代码审计题目

$user = $\_POST[user];

$pass = md5($\_POST[pass]);

$sql = "select pw from php where user='$user'"

$query = mysql\_query($sql);

$row = mysql\_fetch\_array($query, MYSQL\_ASSOC);

if (($row[pw]) && (!strcasecmp($pass, $row[pw])))

为最终判断条件，可以发现row[pw]取决于sql的语句

只要我们能够修改$sql的值，此题解决。在这里我们可以利用sql语句，直接给$sql返回一个值。

测试用户名为username

1. 最前面的单引号：闭合原文的where user='

2. AND 0=1:为了使前面的表达式返回值为空.

3. 接着我们使用UNION SELECT MD5(2)，直接把MD5值作为返回值retuen给$sql，这样在查询的时候$query就会有值.

4. 最后的#用来注释掉后面没用的东西

username:username' union select md5(1)#   
password:1

即可得到flag