NCTF-南邮网络攻防平台WriteUp：SQL注入1

原创

1cePeak 于 2018-03-30 10:19:43 发布 1184 收藏
分类专栏： 网络安全 文章标签： 网络安全 CTF 南邮

**********蒟蒻萌新拿一血**********

SQL注入1

传送门：http://chinalover.sinaapp.com/index.php

Source

先看源码

```
<html>
<head>
Secure Web Login
</head>
<body>
<?php
if($_POST[user] && $_POST[pass]) {
    mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQL_USER,SAE_MYSQL_PASS);
  mysql_select_db(SAE_MYSQL_DB);
  $user = trim($_POST[user]);
  $pass = md5(trim($_POST[pass]));
  $sql="select user from ctf where (user='".$user."') and (pw='".$pass."')";
    echo '</br>'.$sql;
  $query = mysql_fetch_array(mysql_query($sql));
  if($query[user]=="admin") {
      echo "<p>Logged in! flag:********************* </p>";
  }
  if($query[user] != "admin") {
    echo("<p>You are not admin!</p>");
  }
}
echo $query[user];
?>
<form method=post action=index.php>
<input type=text name=user value="Username">
<input type=password name=pass value="Password">
<input type=submit>
</form>
</body>
<a href="index.phps">Source</a>
</html>
```


划重点（敲黑板

```
$sql="select user from ctf where (user='".$user."') and (pw='".$pass."')";
  echo '</br>'.$sql;
$query = mysql_fetch_array(mysql_query($sql));
if($query[user]=="admin") {
    echo "<p>Logged in! flag:********************</p>";
}
```

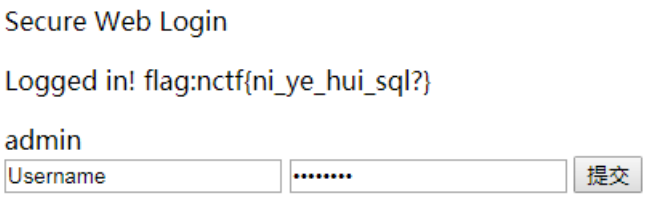

题目要求输入user，password，我们要避开密码的验证，可以构造语句，在输入user的时候把后面的password用#注释掉。

Source

输入 admin‘）#

因为后面的语句被#注释了，要把源码原来的）补上。

这里flag就拿到了



Source