PHP+MySQL实现简单的登录（SQL注入入门实验）

原创

江左盟宗主 于 2018-06-03 00:10:15 发布 15691 收藏 39
分类专栏： 渗透测试 文章标签： php简单登录 SQL注入入门 PHPSQL注入入门 SQL注入简单登录

本文链接：https://blog.csdn.net/qq_32261191/article/details/80553276


渗透测试 专栏收录该内容
25 篇文章 18 订阅
订阅专栏

本实验是入门级的SQL注入实验，手工注入吧，用sqlmap就没意思了，简单过程：用户输入用户和密码然后提交，服务端收到用户和密码并查询数据库输出到页面。

一、创建数据库

create database web1;

创建两张表，一张保存登录用户和密码，另一张保存flag：

create table test(user varchar(15),password varchar(16));

create table flag();

二、编写用户登录页面

index.htnl：

```
<!DOCTYPE HTML>
<html>
 <head>
  <meta charset="utf-8">
  <title>简单SQL注入页面</title>
 </head>

 <body style="background-color: #006400">

  <h2 align="center" style="color: white">图书管理系统后台登录</h2>
  <!--将用户输入的user,和pass提交到login.php-->
  <form align="center" action="login.php" method="post" enctype="multipart/form-data">
          <!--用户输入的账号存储在user变量，密码存储在pass变量-->
   <p style="width: 100%;height: 30px;display: block;line-height: 200px;text-align: center;color:white;font
   <p style="width: 100%;height: 30px;display: block;line-height: 200px;text-align: center;color:white;font

   <p style="width: 100%;height: 30px;display: block;line-height: 200px;text-align: center;"><input type="s

  </form>

 </body>
</html>
```

三、编写后台处理页面

login.php：

```
   <?php
//连接数据库，主机，用户名，密码，数据库
                    $con=mysqli_connect("localhost","root","666666","web1");
if(!$con)
{//连接失败会输出error+错误代码
 die("error:".mysqli_connect_error());
}
       //把用户在index.html输入的账号和密码保存在$user和$pass两个变量中
       $user=$_POST['user'];
$pass=$_POST['pass'];
       //数据库查询语句，就是这样的查询方式存在着致命的SQL注入
       $sql="select * from test where user='$user' and password='$pass'";
//echo $sql;
       //查询结果保存在$res对象中
       $res=mysqli_query($con,$sql);
//var_dump($res);
       //把$res转换成索引数组以便输出到页面
       $row=mysqli_fetch_array($res,MYSQLI_NUM);
//var_dump($row);
       //如果数组不为空就遍历数组到页面
       if(!is_null($row))
{
 for($i=0;$i<count($row);$i++)
 {
                echo $row[$i];
                echo "<br>";
 }
}
else
{
 echo "登录失败！";
}
?>
```