ctf 绕过php,第三届NSCTF测试题Code php 之MD5碰撞和php strcmp函数绕过

转载

王知遇 于 2021-03-19 03:12:29 发布 120 收藏
文章标签： ctf绕过php

第三届NSCTF测试题Code php 之MD5碰撞和php strcmp函数绕过

1、打开网页如图，F12发现code.txt：

2、需要php代码审计，提示需要get方式提交3个参数(v1、v2、v3)且v1和v2的值不同，但md5后的值相同(中间是&&与符号)，为真时再利用strcmp函数判断v3和$flag是否相同，为真输出flag;

3、在问了几个朋友后，得到一些提示，首先MD5碰撞有工具，可以生成，另外strcmp函数有绕过漏洞，这就简单了

4、下载fastcoll工具创建一个文本文件init.txt，随便写入1，使用命令fastcoll -p init.txt -o 1.txt 2.txt就可以在当前目录生成不同内容但MD5相同的文件：

5、用下面代码计算MD5并URLENCODE，这里就是v1和v2参数用的;

```
}echo 'MD5:'. md5( (readmyfile("1.txt")));echo "
";echo 'URLENCODE '. urlencode(readmyfile("1.txt"));echo "
";echo 'URLENCODE hash '.md5(urlencode (readmyfile("1.txt")));echo "
";echo 'MD5::'.md5( (readmyfile("2.txt")));echo "
";echo 'URLENCODE '. urlencode(readmyfile("2.txt"));echo "
";echo 'URLENCODE hash '.md5( urlencode(readmyfile("2.txt")));echo "
";?>
```

6、strcmp函数的绕过是这样的(参考：https://blog.csdn.net/dyw_666666/article/details/82349432)，重点截图如下：

7、开始burp的操作，参数值不要用双引号，连接多个参数用&，拿到flag：

PS1：后来还找到MD5碰撞绕过的其他思路，利用PHP处理0e开头md5哈希字符串的缺陷，有空可以试下：

PS2：最后又发现一个帖子写到居然全部用数组参数绕过，也就是strcmp函数和MD5碰撞都可以用数组绕过。。。真是惊喜一波接着一波呀。。。

参考：

如何用不同的数值构建一样的MD5 – 第二届强网杯 MD5碰撞 writeup – 先知社区

MD5碰撞和MD5值(哈希值)相等_Sea_Sand息禅-CSDN博客_md5后的值相同

PHP处理0e开头md5哈希字符串缺陷/bug & PHP expresses two different strings to be the same [duplicate]_ncafei的博客-CSDN博客_0e830400451993494058024219903391