

CTF-word隐写的一种感觉像万能思路的方法

原创

[why you learn hard?](#) 于 2021-11-27 22:15:49 发布 330 收藏 2

分类专栏: [misc](#) 文章标签: [ctf安全](#) [web安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/hacker_zrq/article/details/121584602

版权



[misc](#) 专栏收录该内容

16 篇文章 0 订阅

订阅专栏

参见百度百科的关于word的介绍:

docx格式的文件本质上是一个ZIP文件。将一个docx文件的后缀改为ZIP后是可以[用解压工具](#)打开或是解压的。事实上, Word2007的基本文件就是ZIP格式的, 他可以算是docx文件的容器。

docx 格式文件的主要内容是保存为XML格式的, 但文件并非直接保存于磁盘。它是保存在一个ZIP文件中, 然后取扩展名为docx。将.docx 格式的文件后缀改为ZIP后解压, 可以看到解压出来的文件夹中有word这样一个文件夹, 它包含了Word文档的大部分内容。而其中的 **document.xml**文件则包含了文档的主要文本内容。 [2]

下载下来之后就是一个很正常的word文件, 我试了网上有关word隐写的介绍, 发现都是什么调可显示字符, 但是这个题不行。

解决办法: 改后缀, 文字内容就保存在 [document.xml](#)文件中。



CSDN @学不会编程的菜鸟

注意那个[Content_Types].xml。出现这个东西十有八九必是word文档。

然后把document.xml文档用notepad或者txt打开, 或者十六进制编辑器也行, 然后查找flag即可。

文件夹	文件	大小	大小	类型
theme	document.xml	16,436	6,079	XML 文
	fontTable.xml	1,620	608	XML 文
	settings.xml	3,483	1,285	XML 文
	styles.xml	29,103	2,904	XML 文
	webSettings.xml	1,071	411	XML 文

CSDN @学不会编程的菜鸟

查找

查找 替换 文件查找 工程中查找 标记

查找目标(E):

选取范围内(I)

反向查找

全词匹配(W)

匹配大小写(C)

循环查找(P)

查找模式

普通(N)

扩展(X) (\n, \r, \t, \0, \x...)

正则表达式(G) 匹配新行

透明度(Y)

失去焦点后

始终

CSDN @学不会编程的菜鸟

他是分开来的，每个字符之间差的很远。但是可以辨认出来

```
idR="004A2138"
c><w:t>flag
></w:rPr><w:t>{
></w:rPr><w:t>0
background1"/><w:w
round1"/><w:w
```