

ctf base全家桶递归解密

原创

小光头发多 于 2021-09-11 21:28:43 发布 1059 收藏 4

分类专栏: [ctf](#) 文章标签: [python](#) [base64](#)

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/weixin_38031584/article/details/120243471

版权



[ctf](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

base家族人丁兴旺, 常见的有base16、base32、base64、base58、base62、base85、base91、base92、base100, 在ctf中还有一些加密的组合, 如zlib+base64, 这是常用的网络通信的手段, zlib 压缩可以将字符串体积明显缩小(只有较长才能体现出来), 而base64可以将刚刚压缩的二进制码变成可见字符, 便于在语言中进行传递及网络通信。在ctf中, 如果字符串可以使用base64解密, 而解密后又有很多不可见字符, 那就可能是zlib+base64的编码方式, 对已经来临的intel 电脑, script boy也想让它替我思考, 直接写递归爆破吧, 如果是常见base加密, 使用递归, 不管加了多少次都能爆出来。

实现思路很简单, 写一个basex的函数, 通过递归调用这个函数, 在递归中最重要的就是停止条件, 如果没有停止条件就会出现栈溢出, 如果python没有栈溢出检查, 可以直接把电脑跑炸。

```
-----
not zlib
*****base16*****
Fatal Python error: Cannot recover from stack overflow.
Python runtime state: initialized
```

那么在basex函数中什么才是递归调用的终止条件呢?

函数报错

如果解密完后字符串为空

有不可见字符 (base128除外, base128含有控制字符)

程序结构如下



递归调用



程序使用pyinstaller打包好了，可以直接使用



贴入测试数据

```
QZZ|KQbjRRS8QZRQdCYwR4_DoQ7~jy0)*kPR90|UQ&li}Qb1A=S8PT|Rc1T~R8=)gR%>ip0)*kRR90|OQZZUZQb1x6QEX&MQdV$PQ&1xoQf
```



下载地址: [csdn站下载](#)

或者

```
“鸡术有限”公众号回复“base”获取
```