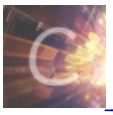
C Sharp shellcode图片隐写

原创

None安全团队 于 2022-04-07 18:04:07 发布 115 收藏

分类专栏： 免杀 文章标签： 系统安全

本文链接：https://blog.csdn.net/qq_39997096/article/details/124022840



之前做的shellcode图片隐写的一个小玩意（大佬们有手就行 主要是思路交流嘛）

现在还有没有用我没测了 改改应该都不是啥问题

基本原理就是通过像素(rgb)存储shellcode的值 计算机基础比较好的同学就想到了 那岂不是万物皆可shellcode 只要你能再转回来。

shellcode图片隐写主要作用就是 shellcode分离加密 上传到可信任域名上

（例如为微软网站上传头像）

具体的操作也比较简单

就是读取shellcode 转成char数组 把每个的值按顺序排列到每个像素上使用rgb来存储这个值。

加载器这块就是从像素中读回来 还原shellcode 然后在进行内存加载执行

然后加了一点反沙箱 其他没什么东西

1.选择 payload.bin文件 生成 shellcode图片

2.shellcode图片上传到服务器上

3.图片url放入 shellcode url里

4.生成代码

在这里插入图片描述

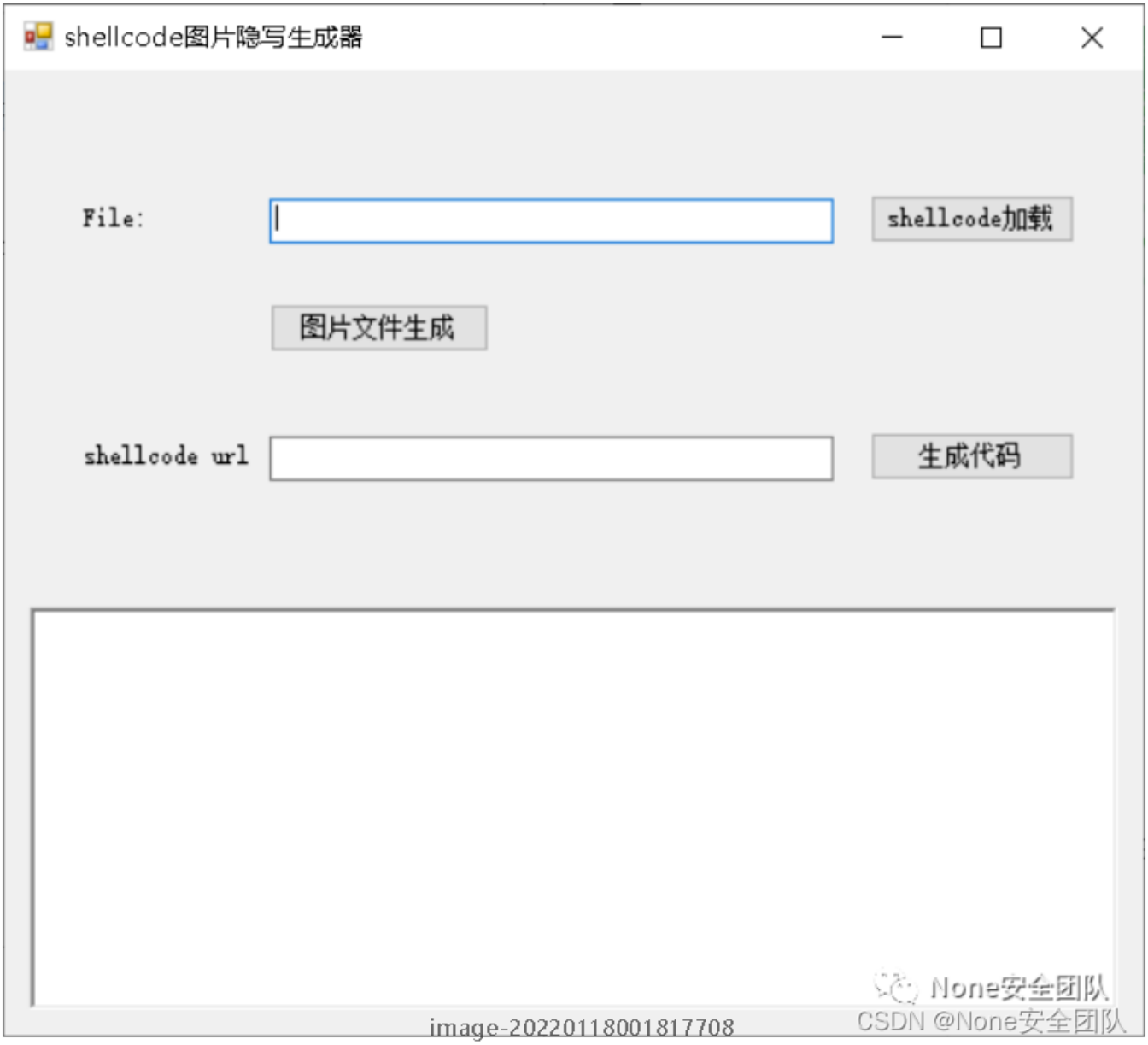


image-20220118001817708

shellcode图片隐写源代码：https://github.com/sshenlian/shellcode_hide

"把握好自己的节奏 别被外界干扰 别被恐惧和欲望支配"