

# 攻防世界MISC进阶之Avatar

原创

[harry\\_c](#) 于 2019-08-10 23:52:22 发布 1203 收藏 2

分类专栏: [攻防世界](#) 文章标签: [Avatar](#) [攻防世界进阶](#) [MISC](#) [安全](#) [渗透](#)

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/harry\\_c/article/details/99130169](https://blog.csdn.net/harry_c/article/details/99130169)

版权



[攻防世界](#) 专栏收录该内容

29 篇文章 2 订阅

订阅专栏

## 攻防世界MISC进阶之Avatar

第一步: [分析](#)

第二步: [实操](#)

第三步: [答案](#)

### 第一步: 分析

难度系数: 2星

题目来源: su-ctf-quals-2014

题目描述: 一个恐怖份子上传了这张照片到社交网络。里面藏了什么信息?

文件下载之后, 考虑过几种思路, 首相是否存在隐藏文件, 使用分解工具分解, 未能成功。使用图片查看器查看, 未能成功, 在博客上找到了一个大佬的工具outguess。

### 第二步: 实操

下载工具: <https://github.com/crovick/outguess>解压后复制到虚拟机

使用安装命令: `./configure && make && make install`

使用outguess -h查看是否安装成功

```
[harry@localhost ~]$ outguess -h
outguess: invalid option -- 'h'
OutGuess 0.2 Universal Stego (c) 1999-2001 Niels Provos

outguess [options] [<input file> [<output file>]]
  -[sS] <n>      iteration start, capital letter for 2nd dataset
  -[iI] <n>      iteration limit
  -[kK] <key>    key
  -[dD] <name>   filename of dataset
  -[eE]          use error correcting encoding
  -p <param>    parameter passed to destination data handler
  -r            retrieve message from data
  -x <n>        number of key derivations to be tried
  -m           mark pixels that have been modified
  -t           collect statistic information
  -F[+-]       turns statistical steganalysis foiling on/off.
               The default is on.
[harry@localhost ~]$
```

使用: `outguess -r /home/harry/Desktop/Tools/lamb.jpg -t hidden.txt`

注意-r后面是下载后的图片的存放位置, hidden是使用工具找到的最终答案。

```
[harry@localhost ~]$ outguess -r /home/harry/Desktop/Tools/lamb.jpg -t hidden.t
xt
Reading /home/harry/Desktop/Tools/lamb.jpg....
Extracting usable bits: 28734 bits
Steg retrieve: seed: 94, len: 41
```

### 第三步: 答案

打印答案:

```
[harry@localhost ~]$ cat hidden.txt
We should blow up the bridge at midnight
```

至此最终的flag为: We should blow up the bridge at midnight



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)