# *{web}*

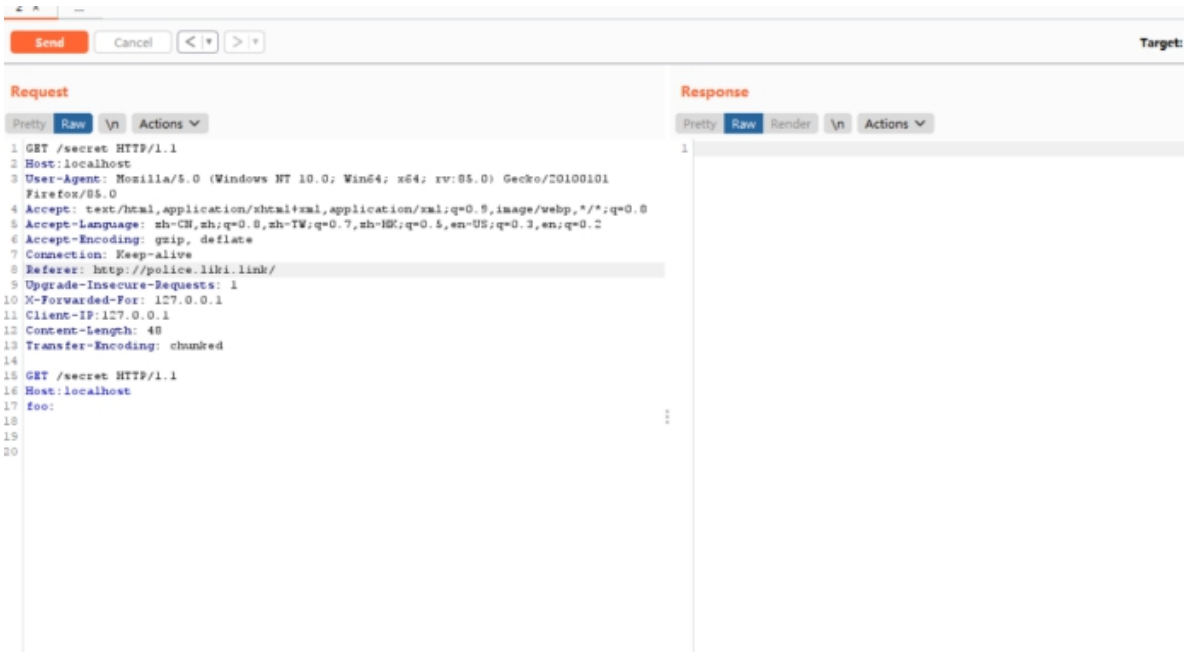
## *Hitchhiking_in_the_Galaxy*

405换请求头，然后换host，然后换来源，然后构造本地访问


## *宝藏走私者*

没太理解，参考了网上的走私攻击，但是用到题目中就不太行

一直bp构造发包，误打误撞做出了。但是用到下一题就不行了，，，，



## *智商检测鸡*

不会写脚本，一题一题算的.....

# *{MISC}*

## *Base全家福*

根据几种base加密所用字符，把所给字符串对照。

base64（A-Z、a-z、0-9、+、/）64个可见字符构成，“=”符号用作后缀填充。

base58的编码表相比base64少了数字0，大写字母I，O，小写字母 l (这个是L），以及 符号‘+’和‘/’

base32的编码表是由（A-Z、2-7）32个可见字符构成，“=”符号用作后缀填充。

base16中只有数字0-9以及大写字母ABCDEF

先base64

GY4DMNZWGE3EINRVG5BDKNZWGUZTCNRTGMYDMRBWGU2UMNZUGMYDKRRUHA2DOMZUGRCDGMZVIYZTEMZQGMZDGMJXIQ======

然后base32

6867616D657B57653163306D655F74305F4847344D335F323032317D

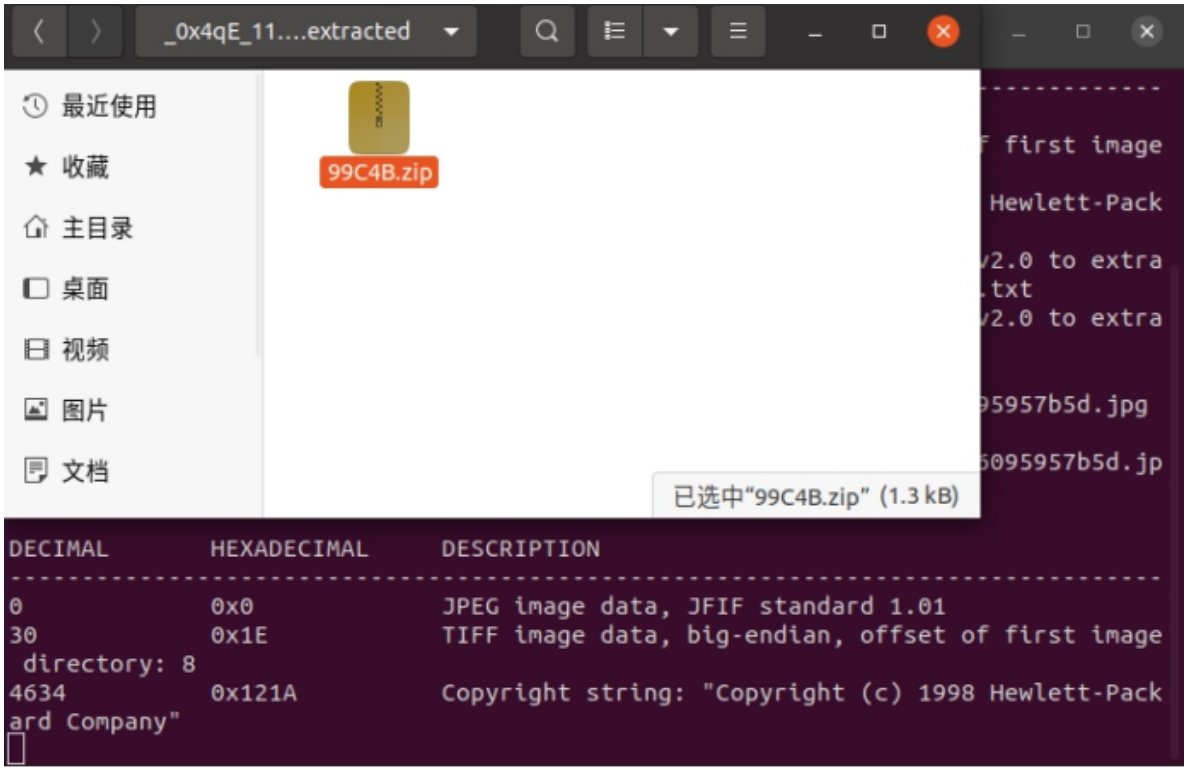
然后base16

hgame{We1c0me_t0_HG4M3_2021}

## *不起眼压缩包的养成的方法*

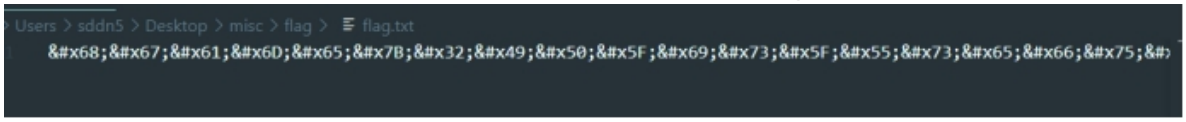
题目提示压缩包且图片备注也提示了。

Binwalk 分出压缩包




然后压缩包备注：Password is picture ID (Up to 8 digits)

八位数字就没去搜索ID，直接爆破：结果发现是套娃，里面还有一个压缩包，和一个文档，压缩包里还有文档，并且两个文档的CRC值相同,然后用明文爆破。爆破出一个flag文档，打开是：




是html的编码，然后将中间的分号去掉，保存成html的格式并打开

```
hgame{2IP_is_Usefu1_and_Me9umi_i5_W0r1d}
```

## *Galaxy*

Wireshark打开所给文件，导出http对象，发现一张png格式的图片。

放到Winhex中，png结尾后没找到特别的东西。拖到Linux中，binwalk没发现什么。


确定不是图片包含文件之类的。

然后winhex 分别调整图片的长和宽，找到flag。

hgame{Wh4t_A_W0nderful_Wallpaper}