

Week1

web

Hitchhiking_in_the_Galaxy

题目意思是要搭上顺风车，点击超链接无法跳转，f12控制台里看到访问的地址是HitchhikerGuide.php，猜测是http请求头出了问题，工具上使用postman给<http://hitchhiker42.0727.site:42420/HitchhikerGuide.php>发送包并且使用burpsuite拦截包。

第一次使用postman发送包后提示需要使用非限制无概率引擎才能访问到这里，结合http请求头的知识先用postman发送请求再使用burpsuite拦截包，把user-agent改为Infinite Improbability Drive。

得到第二个提示茄子要求从cardinal过来，结合http请求头的知识把referer改为<https://cardinal.ink/>

第三个提示需要本地访问，加一个X-Forwarded-For: 127.0.0.1

得到flag

watermelon

游戏建模好像不是很好，f12控制台里面拉伸页面就会穿模然后合成，就混到2k然后拿到flag

智商检测鸡

硬做100个定积分题目以巩固高数知识

misc

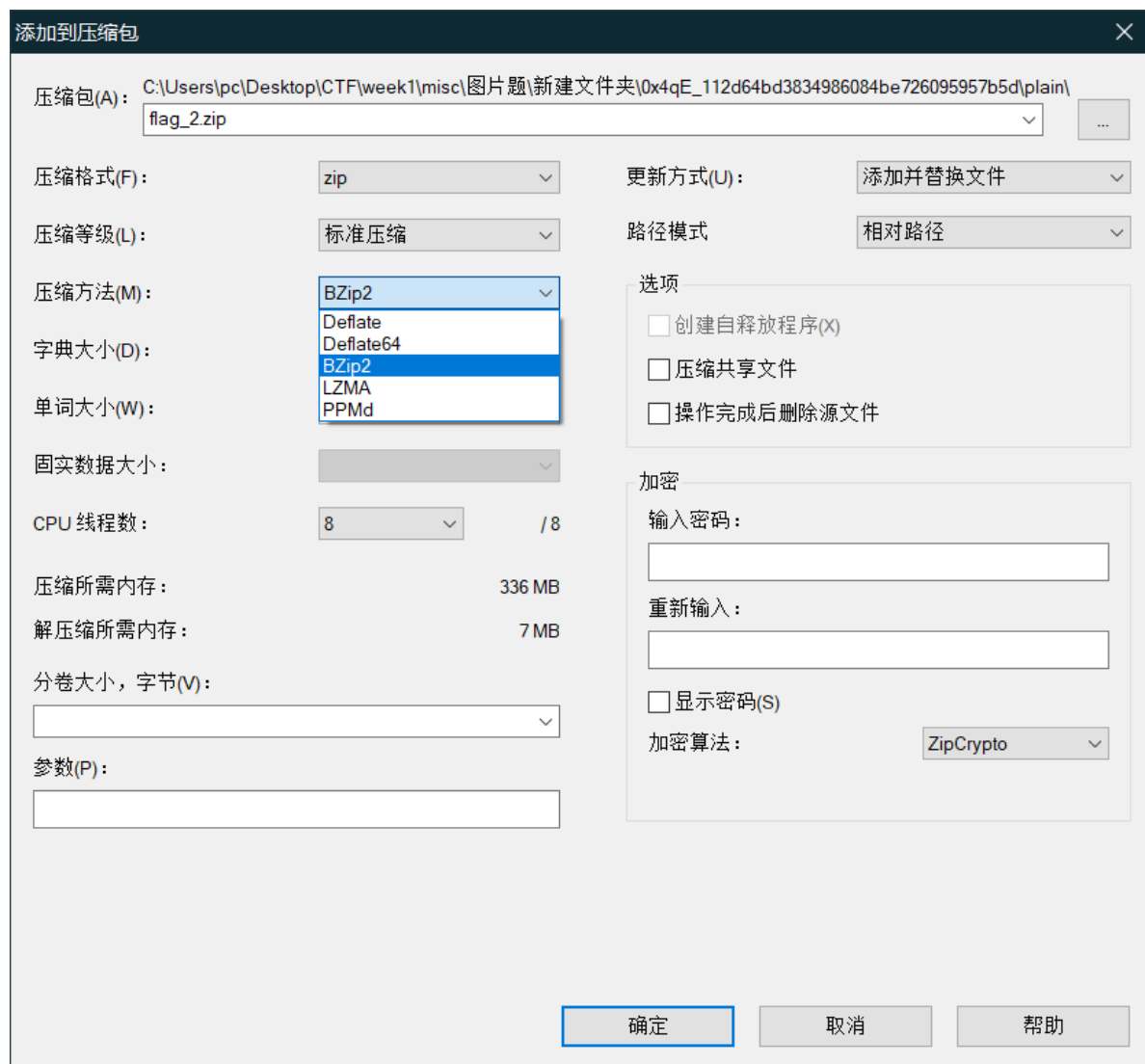
Base全家福

一看题目就知道base解码用一用就行，Google一搜常见的base编码然后先base64再base32再base16就解出来了。

不起眼压缩包的养成的方法

看题目就知道解压缩包和图片隐写相关知识，用二进制查看器发现隐藏了压缩包密码是8位数字且除了图片的内容还有压缩包的内容，结合题目把后缀改成zip，使用archive或ziperello爆破。

解压后得到的plain.zip和NO PASSWORD.txt，plain.zip里面又刚好有一个NO PASSWORD.txt，使用明文破解，把NO PASSWORD.txt压缩成zip然后使用工具对照相同部分获得明文来破解密码。不过明文破解还需要知道压缩方法，使用7-zip一个一个尝试发现是bzip2然后就破解出来了。



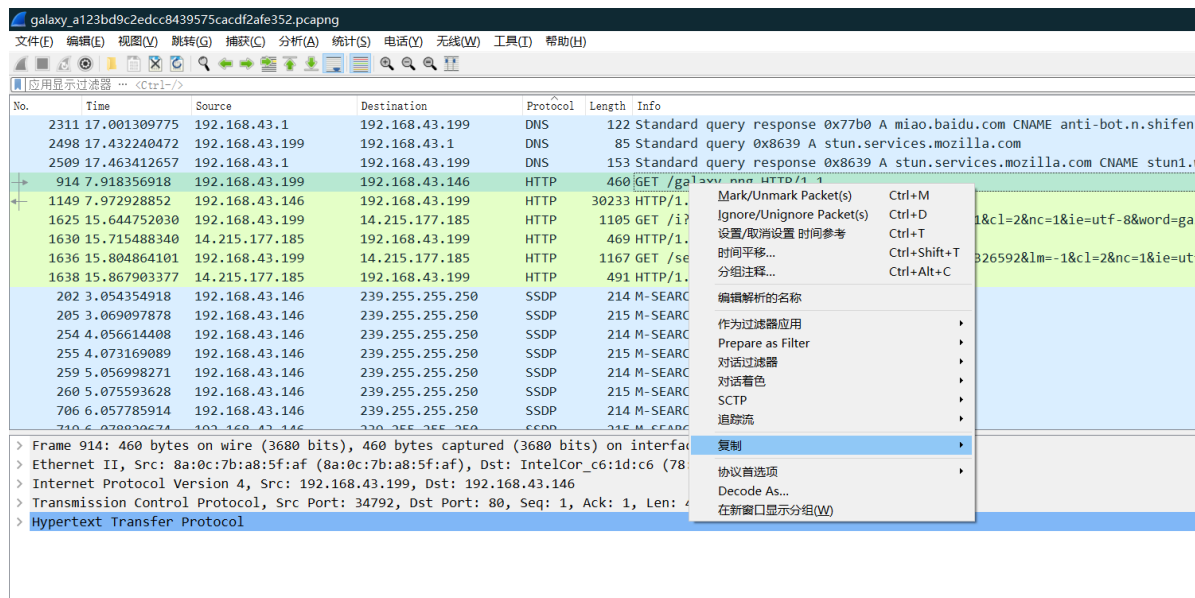
剩下的提示就是storage了，但是用一个奇怪办法解出来了没有用到这个，网上一搜ctf解压缩包然后发现可能是伪加密，使用工具解密后拿到了里面的flag.txt然后发现编码方式不对，txt应该是以ascii形式查看的，使用utf-8编码查看就得到了flag。

storage一直没用到非常奇怪。

Galaxy

用wireshark和winhex两个工具。

先用wireshark打开题目给的这个流，然后按照协议排序找到galaxy.png这个流然后以as a hex stream的形式复制到winhex，保存成png打开就找到了图片。



google搜索ctf png 图片隐写看一下常见操作，然后winhex里改png的高找到flag。