HGAME Week2 Write Up

--Ash

WEB：

ID40--从 0 开始 LFI 之 0

打开 http://119.29.138.57:12000/，F12 看源码，根据题目提示 LFI、flag 路径在../flag 以及页面显示图片为 show.php?file=1.jpg，于是更改 URL 为
http://119.29.138.57:12000/show.php ,之后构造
http://119.29.138.57:12000/show.php?file=../flag.php 得 flag

```
hctf{lnc1ude_i5_s0_d4ngerous}
```

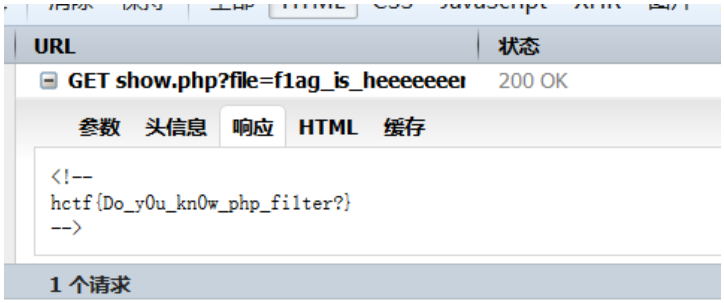
ID41--从 0 开始 LFI 之 1

打开 http://119.29.138.57:12001/，和上题类似，先试试
http://119.29.138.57:12001/show.php?file=../flag.php，得到一个假 flag，firebug 抓包可看到有一行注释提示思路

于是按照百度出来的 wp 的思路，构造
http://119.29.138.57:12001/show.php?file=php://filter/read=convert.base64-encode/resource=../flag.php 用 base64 编码的方式获取网页内容，

可得之后解密可得网页内容为GFnX2k1X24wdF9oZXJlfQo8IS0tIGhoaC
根据提示，重新构造
http://119.29.138.57:12001/show.php?file=f1ag_is_heeeeeeere/flag.html，发现打开是空白页

面，firebug 看响应，发现一行注释，得到 flag



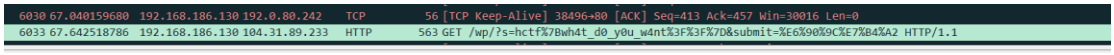
RE：

ID48--re 从零开始的逆向之旅：Gold Miner
玩黄金矿工得 flag 系列，flag 在第 7 关。。。。

MISC：

ID61--我是一个有格调的 misc 题目

下载文件，后缀是 pcapng，于是去百度，发现是 wireshark 的抓包数据，于是用 wireshark 打开，这么多数据看的就晕。。于是尝试搜索 flag 格式 hctf 得到一串 URL 编码后的 flag



解码后得 flag:hctf{wh4t_d0_y0u_w4nt??}
（嗯。。。出题人抓了这么多数据。。。很好奇出题人浏览的网站。。。恩。。。于是尝试打开 flag 对应的网站。诶诶诶(⊙o⊙)…麻麻你听我解释啊~我真的是在打比赛啊(° 。° 〃)。。。）