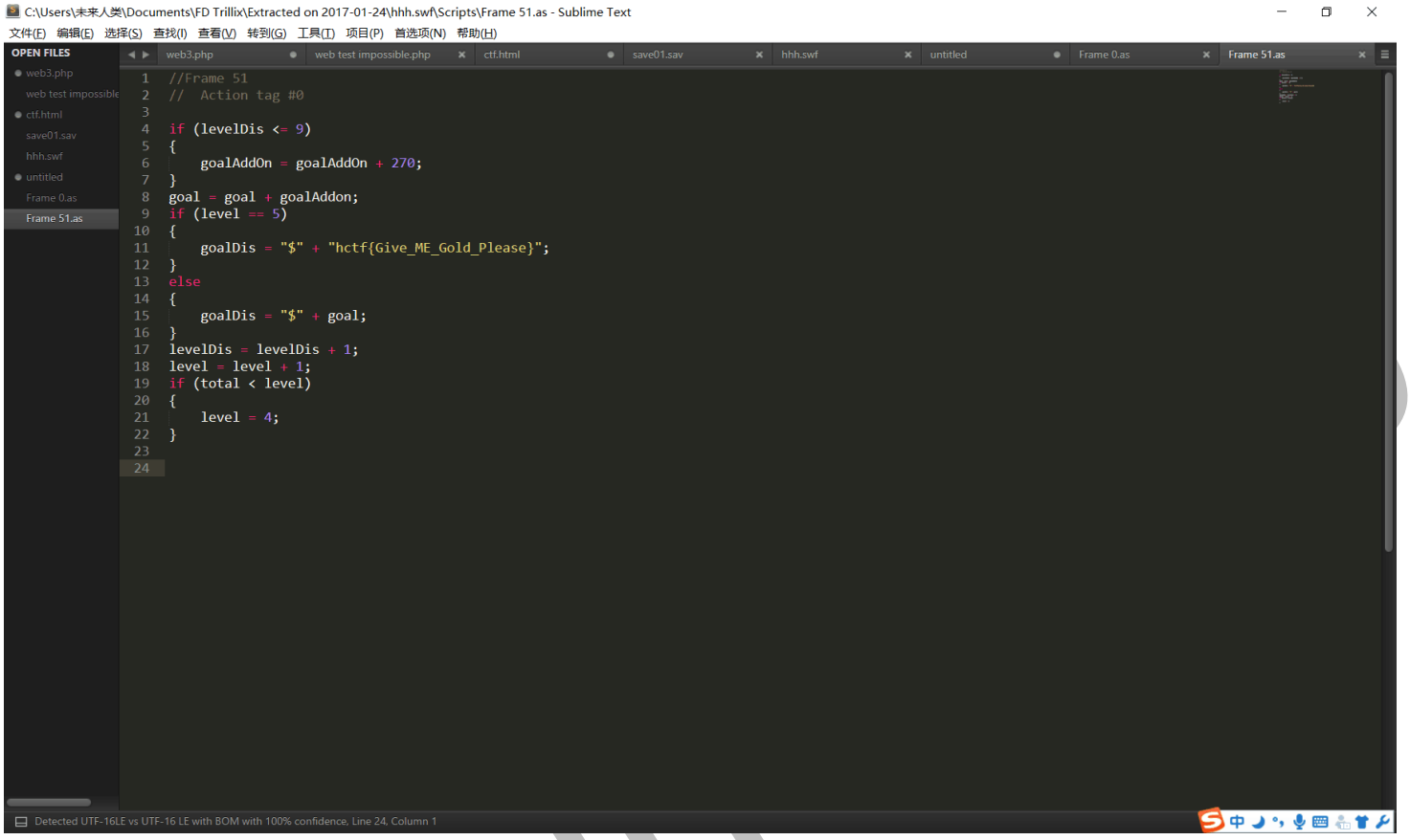
RE 黄金矿工

先尝试了下通关，发现FLAG被挡住了= =只能正常做了

因为通关过程中发现FLAG是改变的文本形式出现的，所以使用SWF分析工具提取其中的文本然后寻找，在一个文件中找到了FLAG

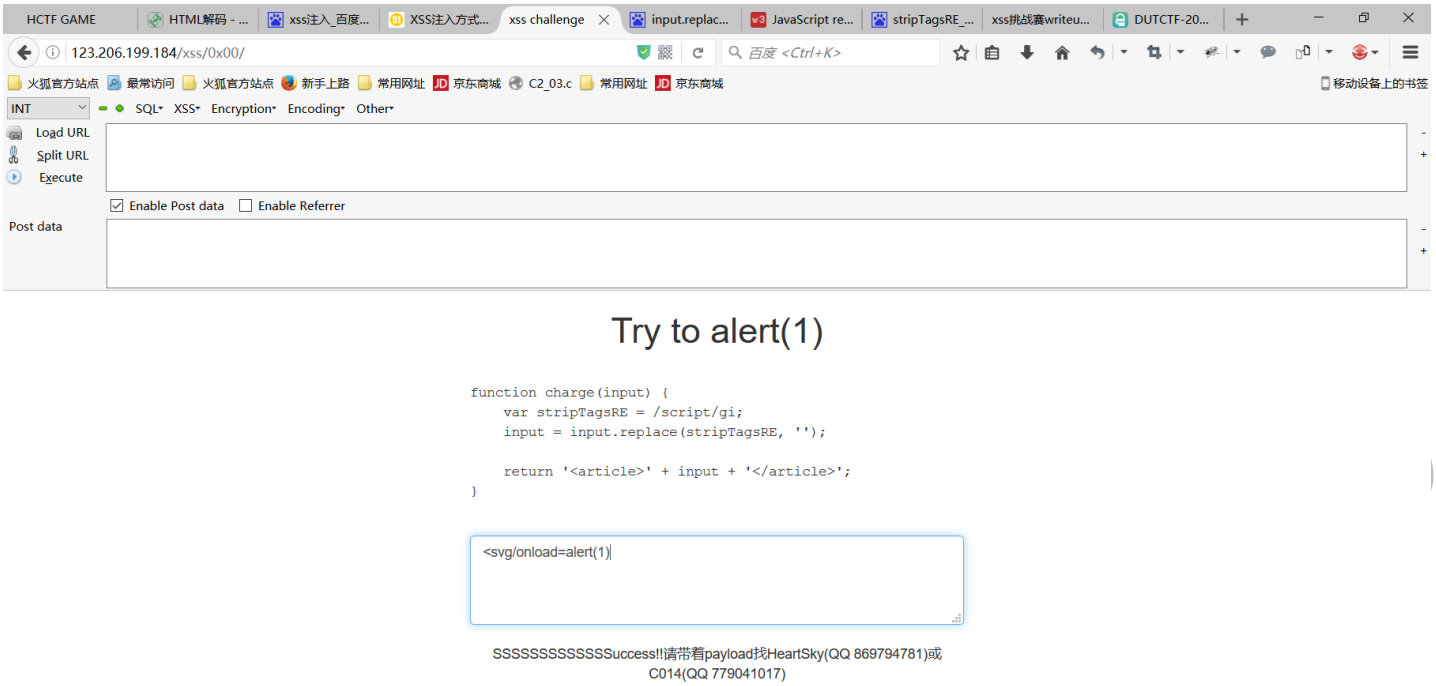


WEB LFI0

百度LFI漏洞，发现可以利用show.php?file=来遍历目录，根据提示在../flag.php发现flag

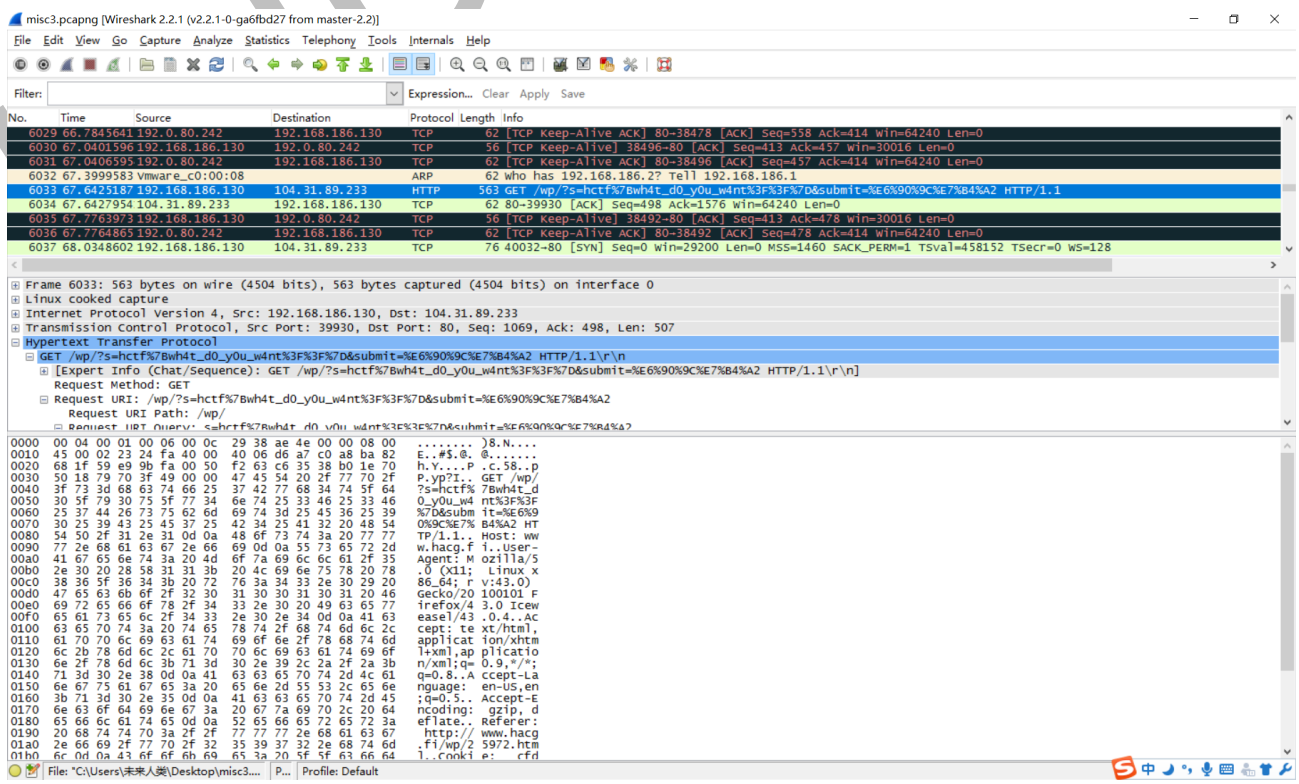
XSS 0

过滤script 用经典xss语句 <svg/onload=alert(1) 弹窗成成功



MISC 我是一个有格调的MISC题目

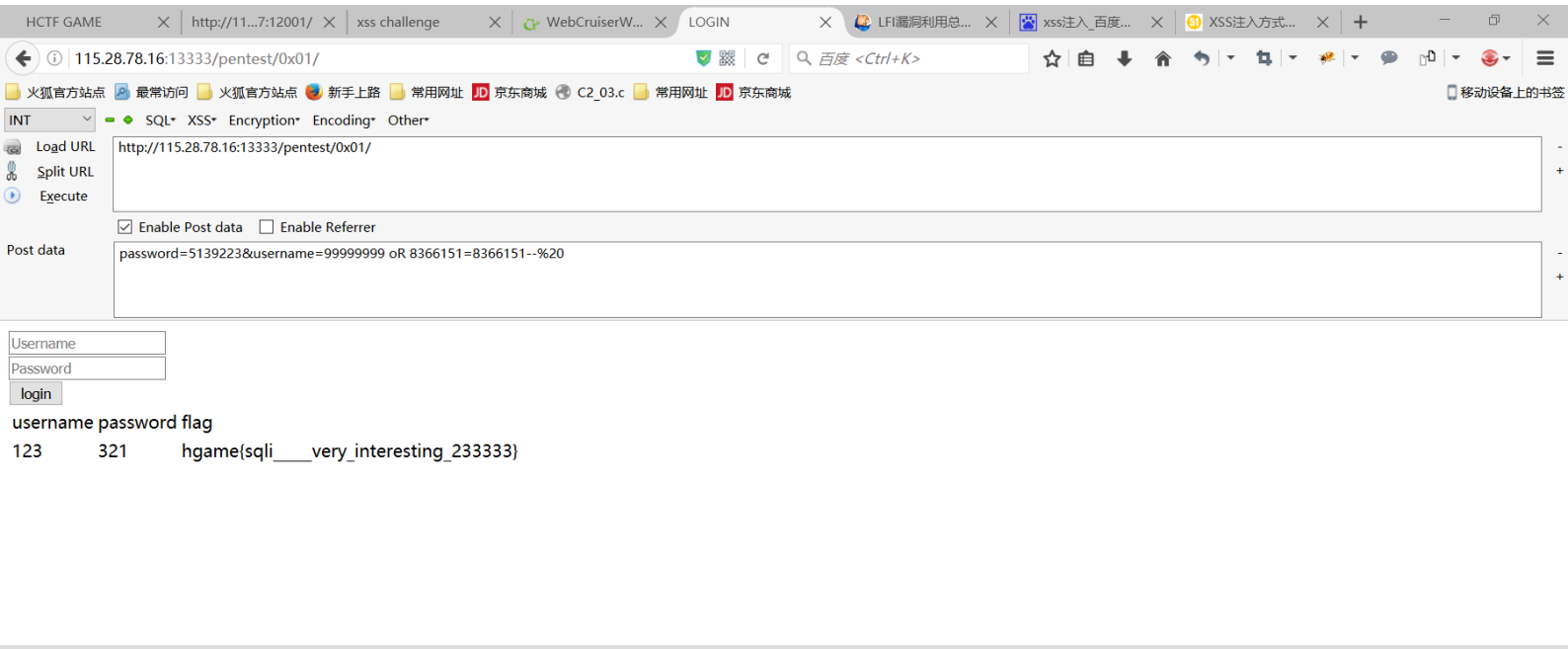
wireshark打开流量包，发现了带有hctf的可疑链接，访问得到FLAG
还有里面的本子链接什么鬼= =！！

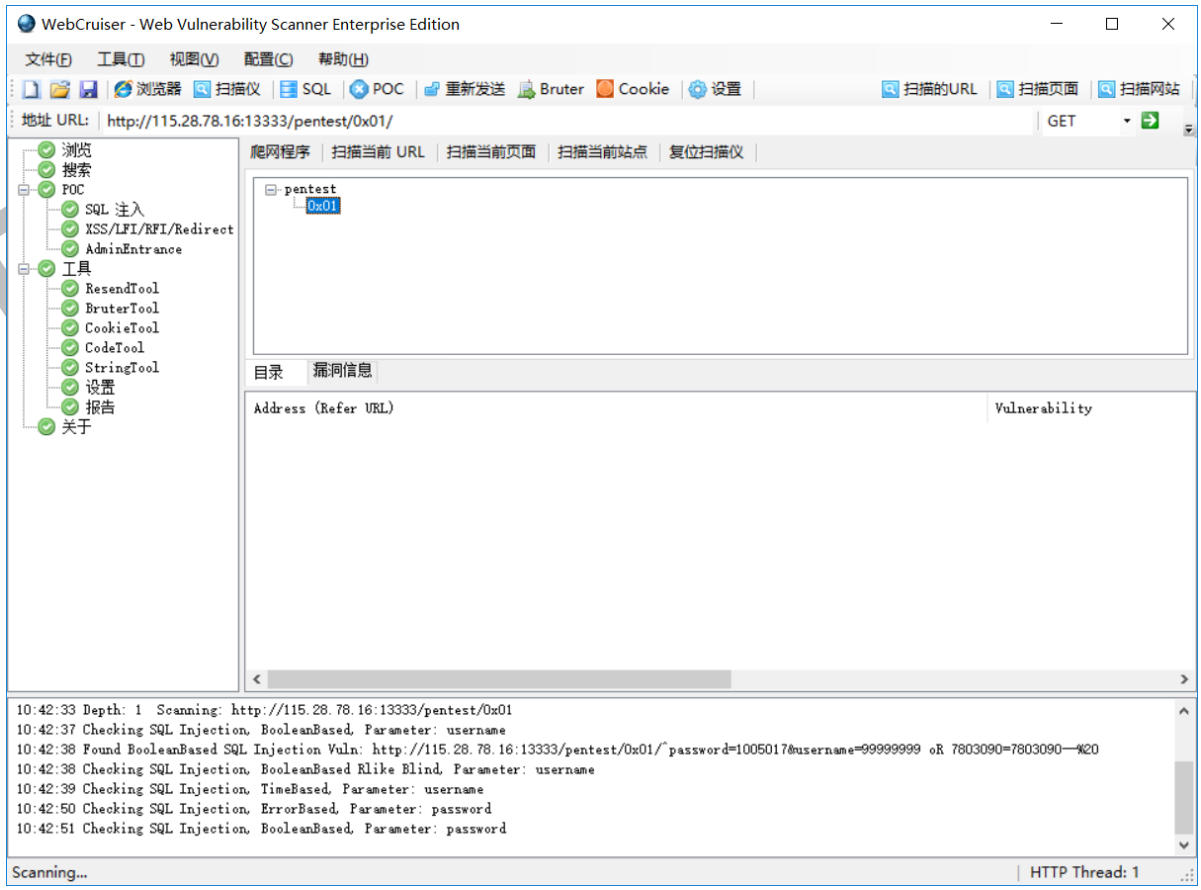


104.31.89.233//wp/?s=hctf{wh4t_d0_y0u_w4nt%3F%3F}&submit=搜索

渗透 最简单的渗透题

工具扫描发现万能账号密码
直接登录得到FLAG





ez game

根据提示vim备份泄露和条件竞争，还有阅读表单中的GOGOGO=苟
联想到HCTF2016 香港记者那道题
竞争条件发生在当多个进程或者线程在读写数据时，其最终的的结果依赖于多个进程的指令执行顺序。
借用并改编了WP的条件竞争脚本代码，放在压缩包里了
跑了好久最终得到FLAG

```
login: 056570d9-6307-48de-af95-5578cd34a27d-372hshuedq2tutv2smhe16f6n7
success
login: 056570d9-6307-48de-af95-5578cd34a27d-372hshuedq2tutv2smhe16f6n7
login: 056570d9-6307-48de-af95-5578cd34a27d-372hshuedq2tutv2smhe16f6n7
Hello, 473342ba-7745-42cd-8c77-4bb8657bb309This is your flag: hctf{mmp_you_yi_xie_wenti}
Hello, 473342ba-7745-42cd-8c77-4bb8657bb309This is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 473342ba-7745-42cd-8c77-4bb8657bb309This is your flag:
hctf{mmp_you_yi_xie_wenti}Hello, 473342ba-7745-42cd-8c77-4bb8657bb309This is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 473342ba-7745-42cd-
8c77-4bb8657bb309This is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 473342ba-7745-42cd-8c77-4bb8657bb309This is your flag: hctf{mmp_you_yi_xie_wenti}Hello,
473342ba-7745-42cd-8c77-4bb8657bb309This is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 473342ba-7745-42cd-8c77-4bb8657bb309This is your flag:
hctf{mmp_you_yi_xie_wenti}Hello, 473342ba-7745-42cd-8c77-4bb8657bb309This is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 473342ba-7745-42cd-
8c77-4bb8657bb309This is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 473342ba-7745-42cd-8c77-4bb8657bb309This is your flag: hctf{mmp_you_yi_xie_wenti}
username is exist
login: 056570d9-6307-48de-af95-5578cd34a27d-372hshuedq2tutv2smhe16f6n7
 login: 056570d9-6307-48de-af95-5578cd34a27d-372hshuedq2tutv2smhe16f6n7
Hello, 473342ba-7745-42cd-8c77-4bb8657bb309This is your flag: hctf{mmp_you_yi_xie_wenti}
```