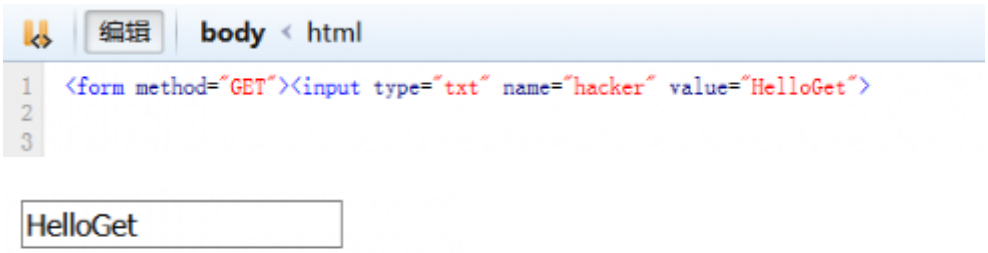
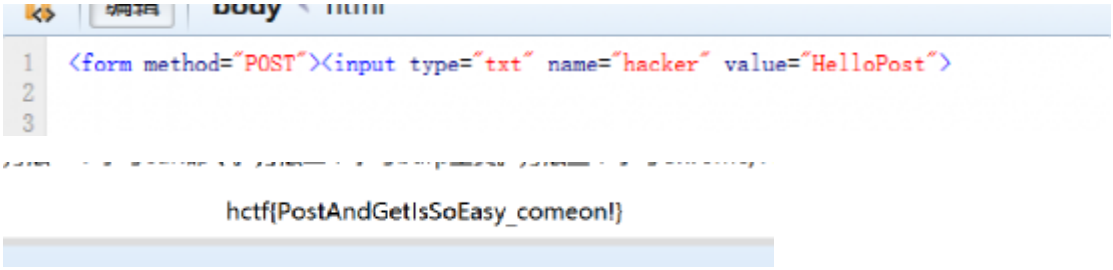
14 lightless 的渗透教室入门篇（一）

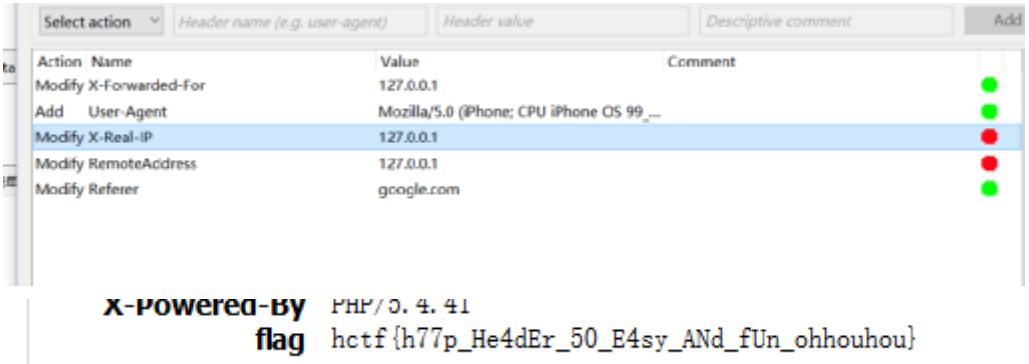
<form method="POST"><input type="txt" name="hacker" value="HelloPost">





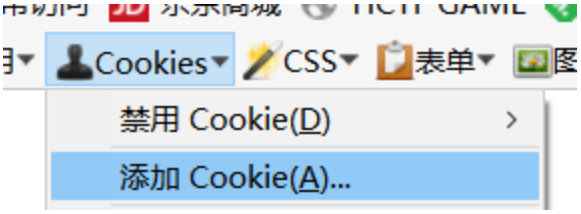
15 lightless 的渗透教室入门篇（二）

用火狐插件 Modify headers 改 UA 成上次 HCTFWEB 签到的那个 ios99 的 XFF 改成 127.0.0.1(本机回环 IP) referer 为 google.com flag 在响应头里面



16 lightless 的渗透教室入门篇（三）

cookie 用火狐 web developer 伪造两组 admin=1 isLogin=true



flag: hctf{hao_hao_kan_zi_liao!!!}, 通过伪造cookie，你可以绕过一些限制，或是伪造身份。

19 密码学教室入门（二）

hgame 前五个一一对应　推出字母-5 再根据英文得 1

21 这 TM 是啥

上网找哪些字符的解法找到 www.jsfuck.com　发现它与其它正常字符编码后天区别　多了一个括号　输入 js 的字符去掉最后的括号

得 flag

```
script>
  1
  2
  3
/script>
```

```
+[]+!+[]]+(!!
+[+[]]]) ()
```

Run This

```
)[!+[]+!+[]]+(!!
+[]+[+[]]])
```

Run This

```
"function anonymous() {
var f = "hctf{j5fuck_1z_m1233}"; alert("Hack by LoRexxar, 你的flag被我拿走了")
}"
```

22 我是谁我在哪？？？

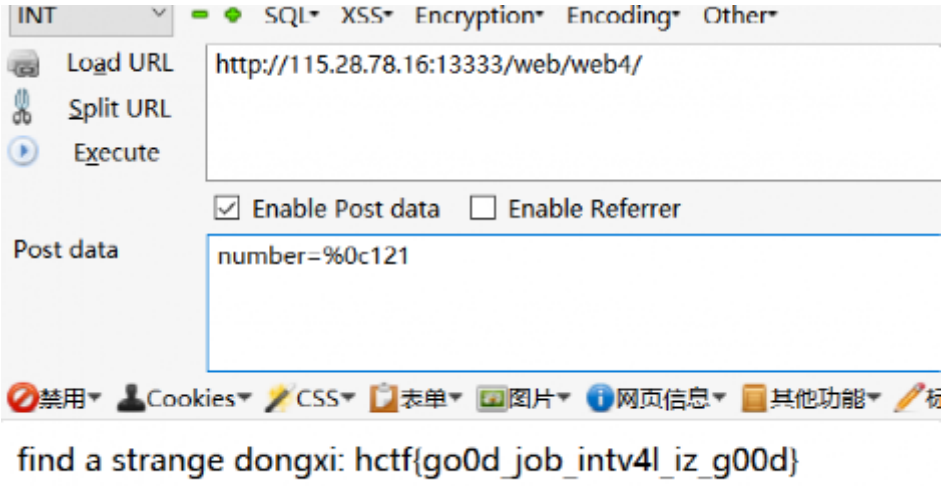
在网络里面有个包中有 flag

GET index.php

flag　hctf{1t_iz_4_4mall_tr1ck}

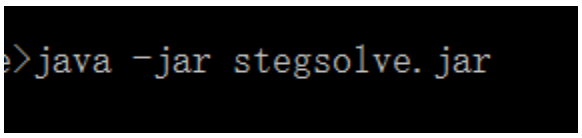
25 神奇的数字

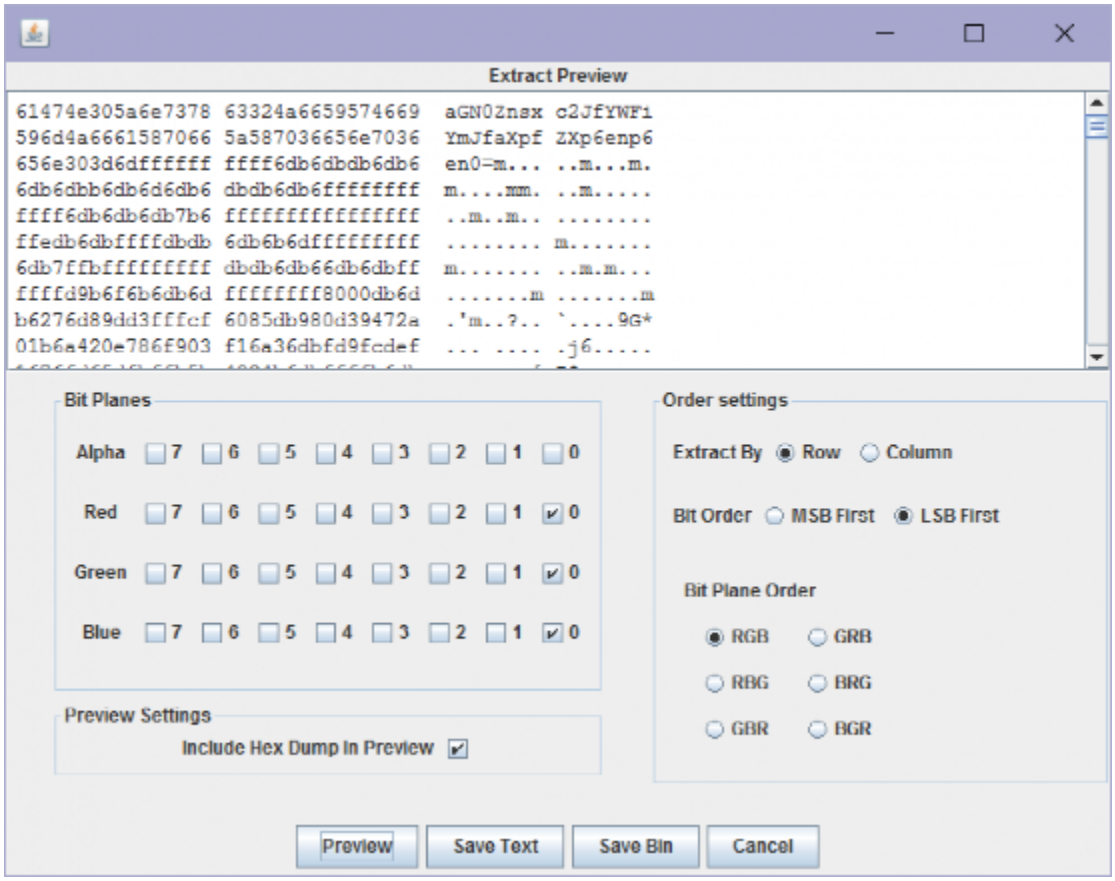
百度内容发现 http://www.chnpanda.com/961.html



30 Explorer 的图库之三

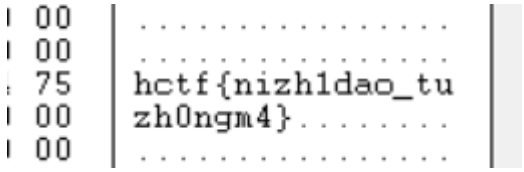
在 linux 下用 foremost xxxx.jpg 分离出一个小女孩 png 的图片　百度 png 隐写　发现 LSB 隐写改法　然后用 stegsolve 打开再用 analyse-dataextract red green bule　第 0 位　　勾中 LSBfirst 勾中 RGB　在开头得到加密的 payload　然后测试发现用 base64 可以解密　得 flag





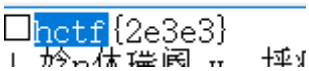
31 Explorer 的图库之二

在 linux 下用 binwalk 分离文件。binwalk xxx 观察偏移量 发现藏有东西 然后 dd if=xxx of=xxx.gzip skip=偏移量 bs=1 在把 gzip 解压得到 flag 然后 flag 文件用 CFF 打开得到 flag



32 Explorer 的图库之一

直接文件转成 TXT 搜索 hctf 字符



37 密码学教室番外篇

hgamr 前五个一一对应 得字母+9 符号不变 数字一个一个+1+2+3 试下去。。得 flag