Wirte Up:

Web：

Web1 ： Are you from Europe？

url: http://123.206.203.108:10001/European.html

我查看了一下网页的源码，发现了

```
            }
        }

        function getCard(num) {
            var SSR = 0.0000001;
            var SR = 0.15;
            var cards = [];
            var card;
            if (times > 100) {
                SSR *= 100;
            }
```

然后自建了一个 TXT 文件，把源码放在里面，修改了一下 SSR 的概率[话说 0.000001 真狠]，然后十连抽就抽到了 flag。

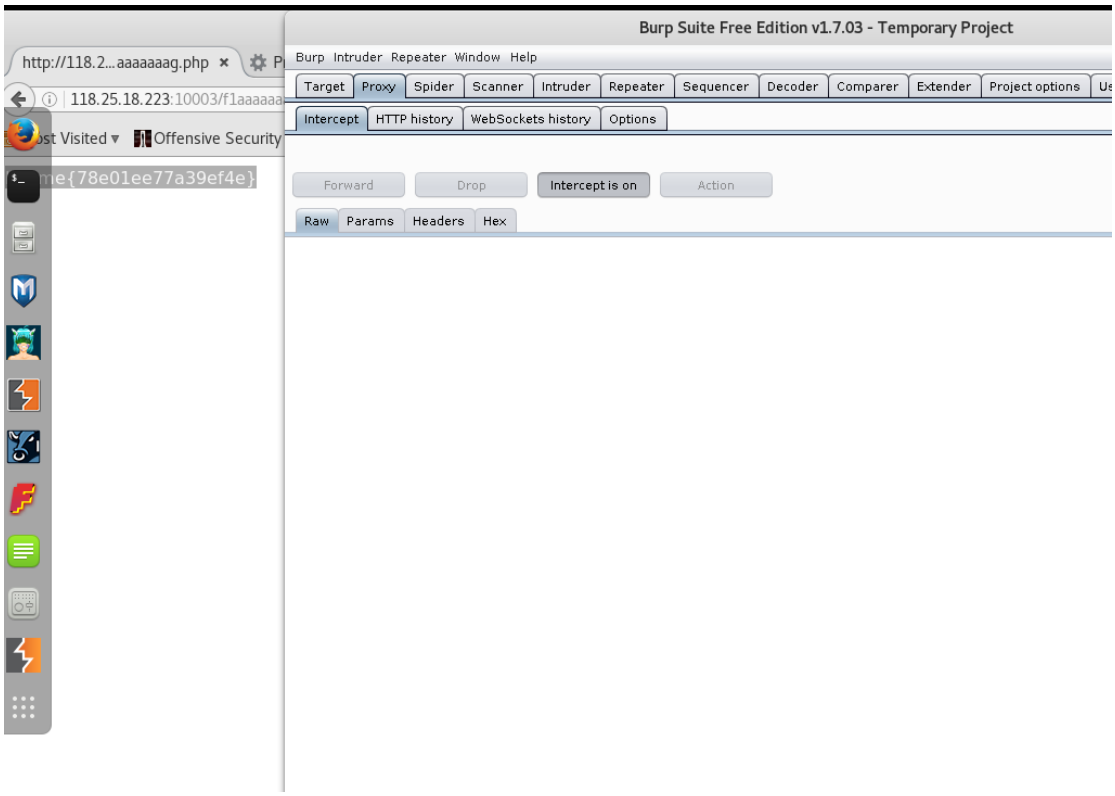
Web-3 ： can u find me

url: http://118.25.18.223:10003/

看到题目，现在网页输入 robot.txt，查询到一个 f1aaaaaaaag.php，继续打开，提示发现要 admin 才能才开。于是打开 Burp Suite

通过抓包

把 User=guest 改成 User=admin，就得到了 flag。

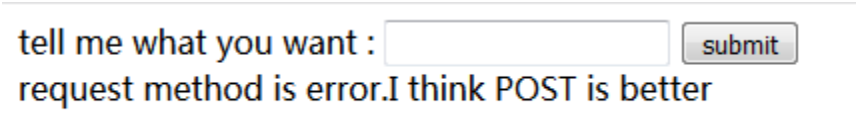


Web-4：tell me what you want

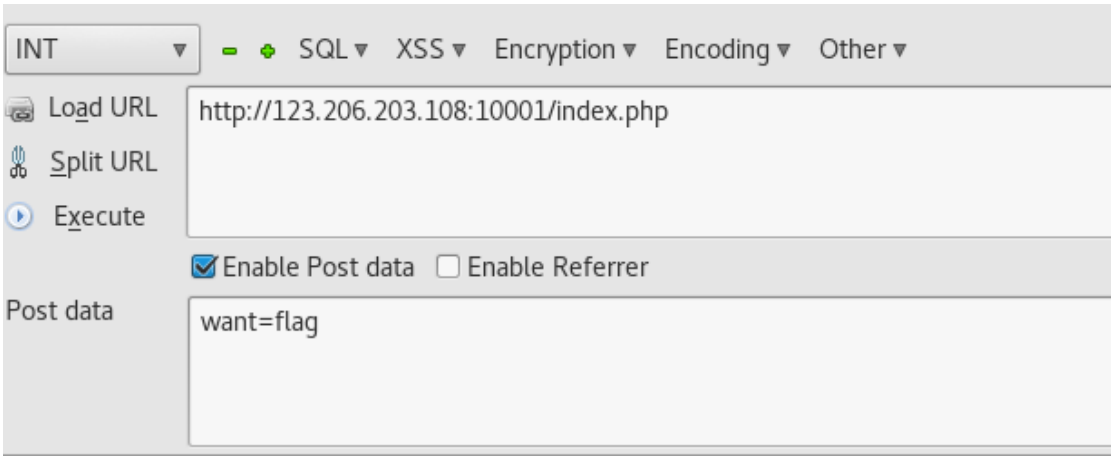
url：http://123.206.203.108:10001/

首先我试了一下 flag

提示要

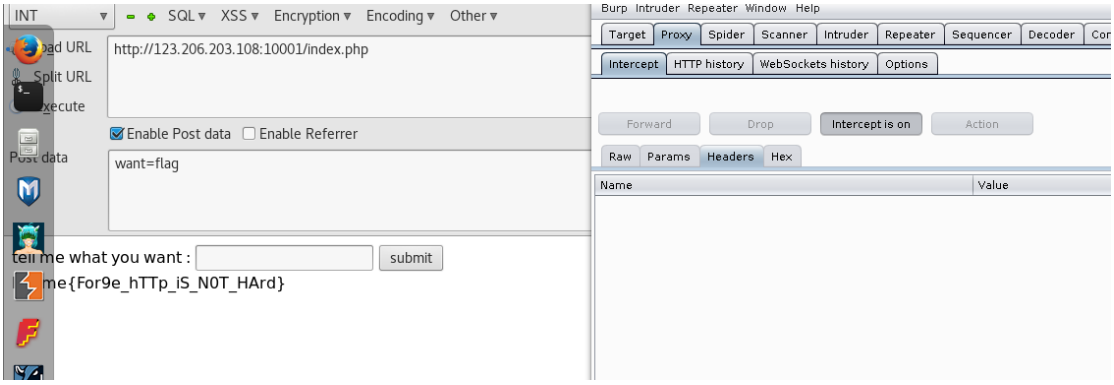


打开 hackbar，POST 了参数



然后他就罗列了各种条件。。。。。

通过 BurpSuite 抓包改包，满足他的各种条件，包括 referer=www.google.com，X-Forwarded-For=127.0.0.1，改浏览器=Icefox/57.0 终于



Web-5：我们不一样

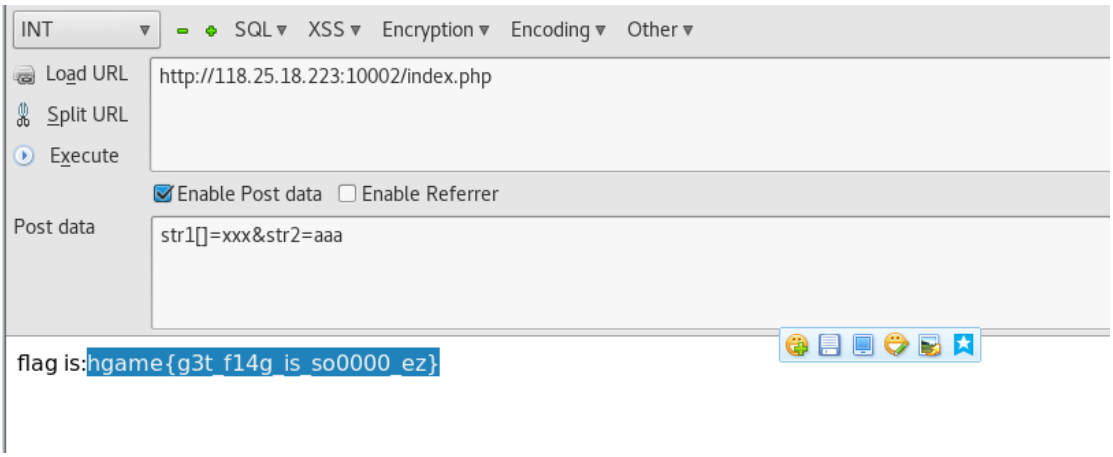
url：118.25.18.223:10002

看到这串代码，我知道了题目要求提交俩个参数并且让他们值不一样但是长度一样，并且以 POST 方式传输

```php
include_once("flag.php");
if(isset($_POST['str1'])&&isset($_POST['str2'])){

    if ($_POST['str1']!=$_POST['str2']&&strcmp($_POST['str1'],$_POST['str2'])==0) {
        echo "flag is:".$flag;
        exit();
    } else{
        echo "Something wrong..";
    }
}
```

于是打开 hackbar，构造了一下参数

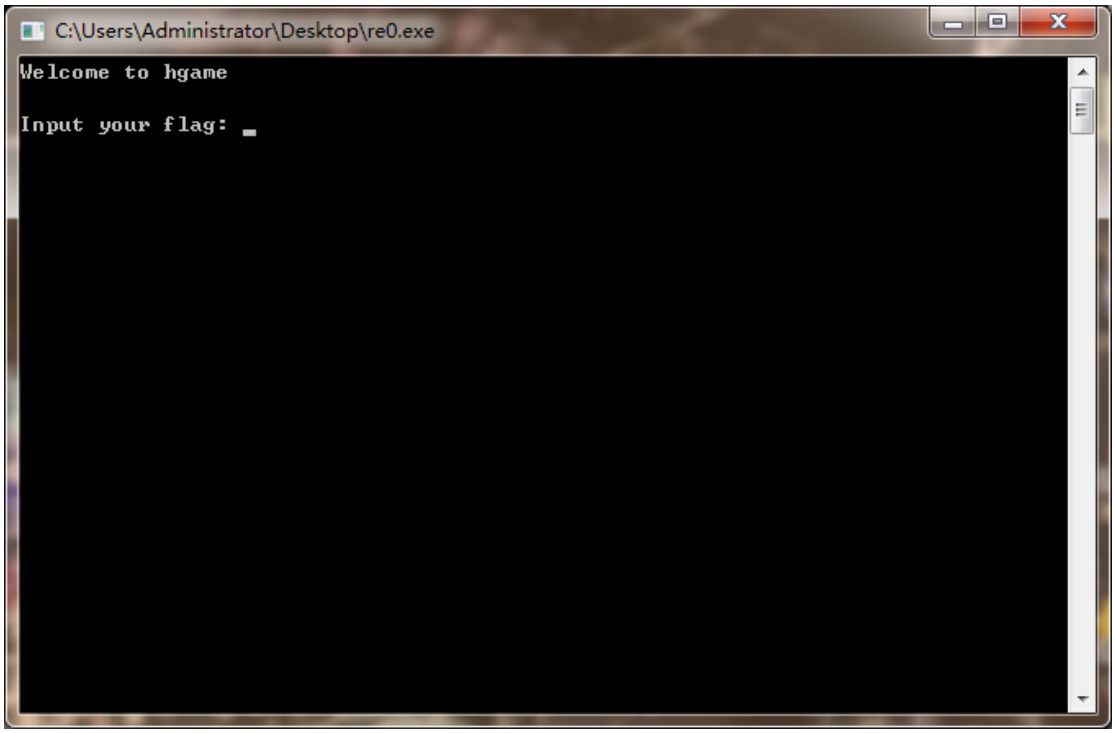


就 OK 了

Re：

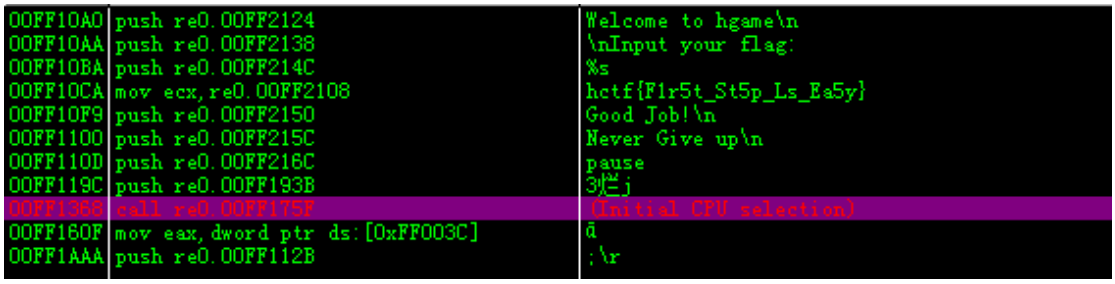
re0：

下载下来的 exe 文件打开



于是丢进 OD 里面

通过智能搜索想找到入口位置



于是就发现了 flag

MISC：

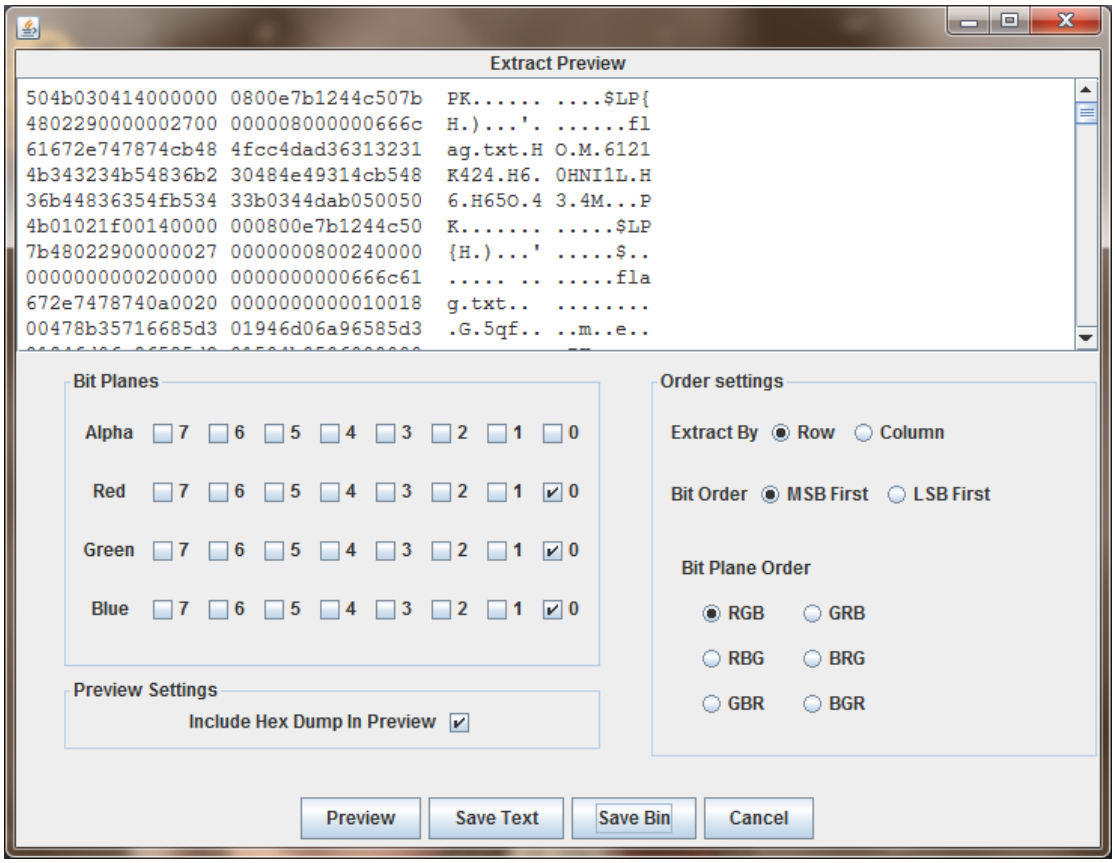
白菜 1

url：http://p1kaloi2x.bkt.clouddn.com/flag.png

因为提示了是 lsb 隐写

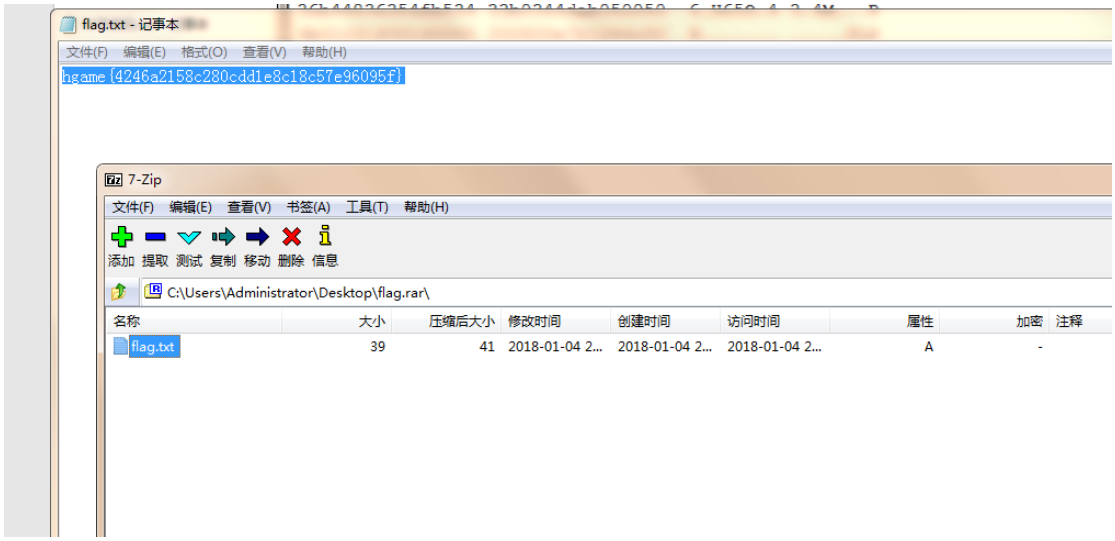
于是我把在 StegSolve 中打开图片

通过 Stegsolve-->Analyse-->Data Extract



找到了这个 flag.txt

于是 Save Bin 保存为 flag.rar 在解压文件里发现了 flag.txt，打开就是我要的 flag



白菜 2

url：http://p1kaloi2x.bkt.clouddn.com/misc2.jpg

我猜想可能隐藏了什么文件

把图片放入 Kali 的桌面上，运行

```
root@kali:~/Desktop# binwalk misc2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
1037199       0xFD38F         Zip archive data, at least v2.0 to extract,
ssed size: 41, uncompressed size: 39, name: flag.txt
1037368       0xFD438         End of Zip archive

root@kali:~/Desktop#
```

发现了隐藏在里面的文件

运行

```
root@kali:~/Desktop# foremost misc2.jpg -o w
```

可以得到 zip 的解压文件，就可以再里面找到 flag。