X's Write up

队伍 ID：x　　队长 QQ：1583810565

参赛队员：李欣　　17180210027　　1583810565

以下题目均由本人一个人做的（太菜了根本没人和我组队）

- Welcome:

刚开始以为是这道题出了 bug，后来才知道就是这么给的，签到题，直接给出了 flag，复制粘贴即可。

- Nazo：

这里一共有十七个小题，在此不一一赘述，挑几个我觉得比较难的写一下吧。

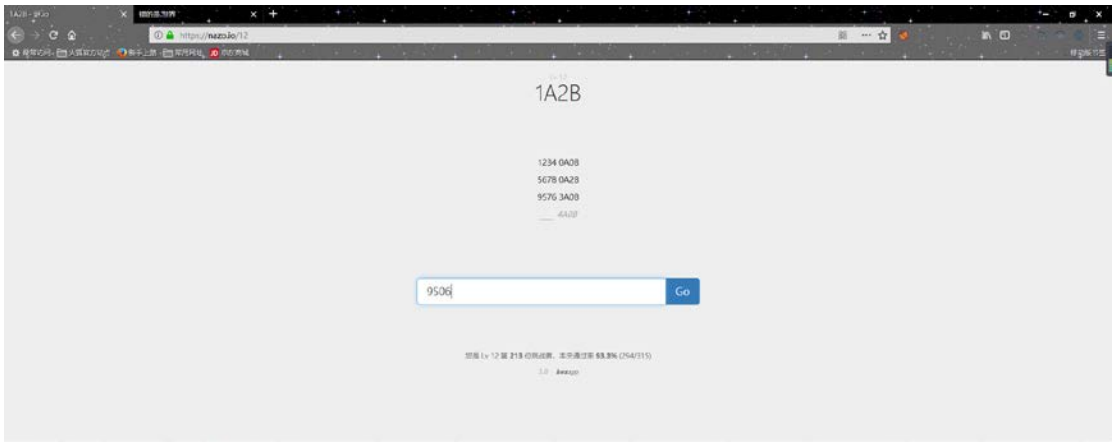
8.刚开始看到题目一脸懵，百度了一下 IDNs，发现以下内容：国际化域名（ Internationalized Domain Names ）是用本国语表示的域名前缀 + 国际顶级域名后缀（ .com/.net/.org ）组成的域名。

然后看看题目，发现，“错的是”后面有个点，这会不会是一个域名呢？然后复制粘贴到地址栏，回车，果然出现了一个网页，没想到网址也可以中文啊！又学会了一种好玩的东

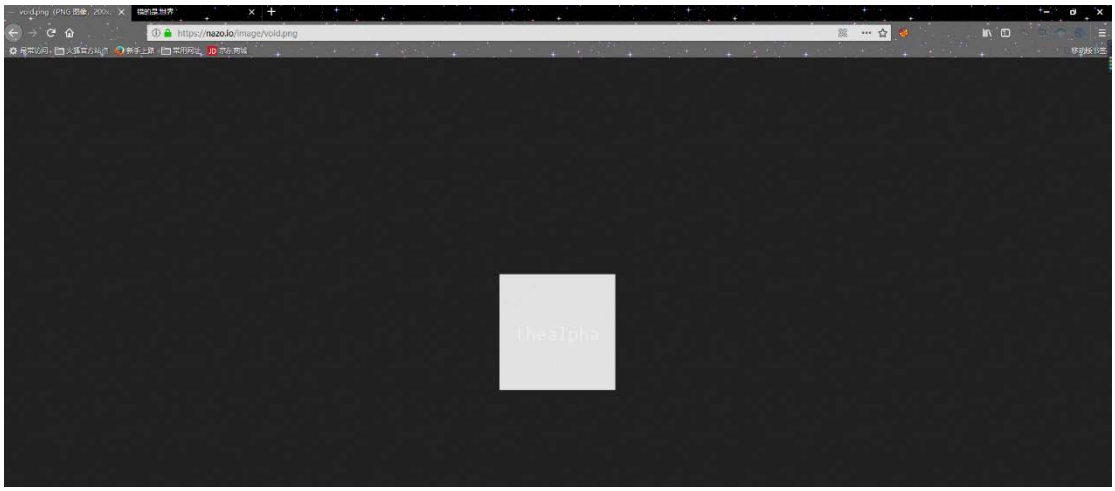
西。

11.Unicode：这题直接就看出来了 flag，一次就猜对了。

12.1A2B：百度了一下，发现这是一个游戏，以下内容出自百度：运用你的逻辑推理能力，猜出答案正确的数字，提供三种模式选择，利用“A”代表数字正确位置正确，利用“B”代表数字正确但位置不正确，答案之间的数字不会重覆。那么接下来就是推理咯~经过推理，得到答案：9506

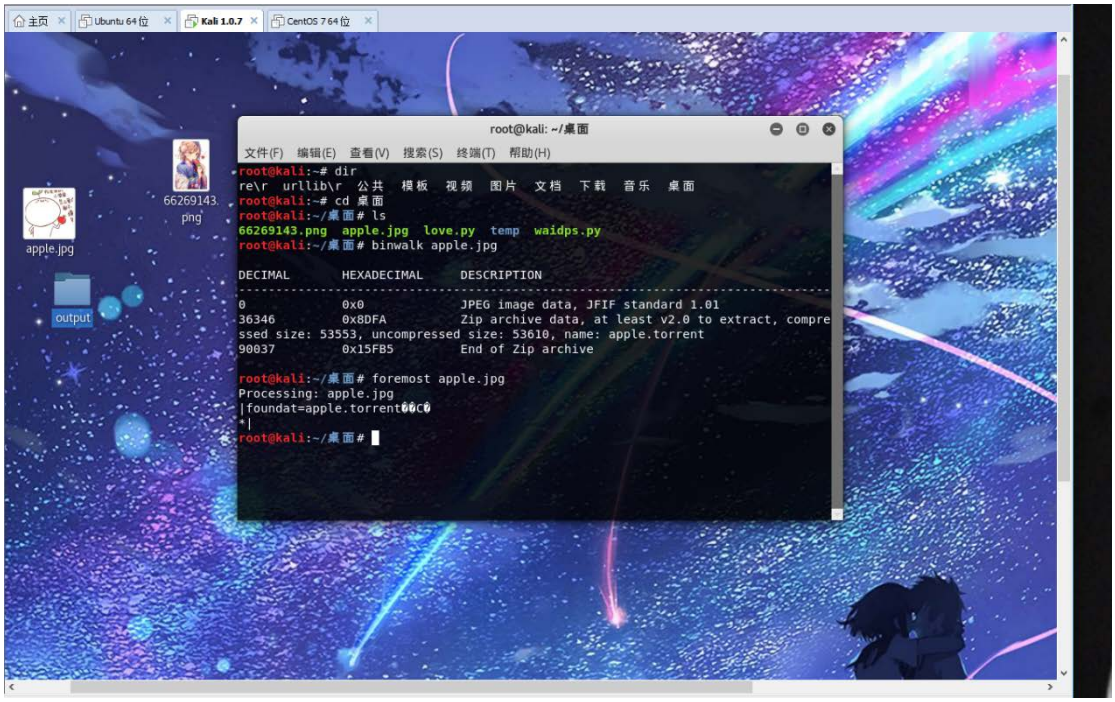


13. 虚无：看起来啥都没有，查看源码看到了图片标签，原来有一张图片，点开图片就看到了 flag。

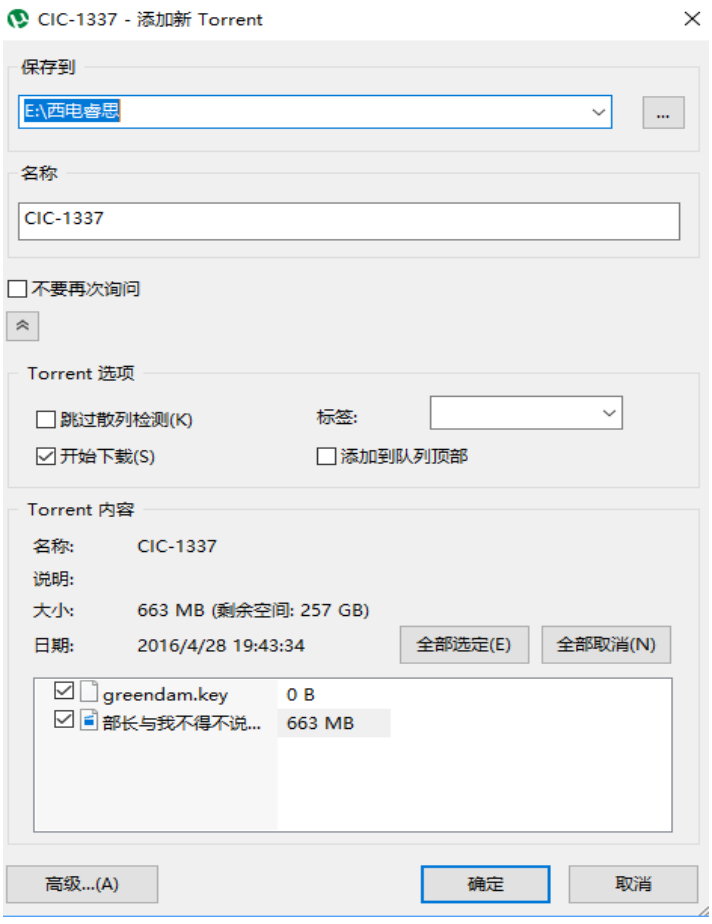


14. 我爱记歌词：看到之后第一想法就是答案是“种子”？torrent？结果都不对。然后查看源码：

然后图片描述说：我真的不是配图，那么猜想 flag 应该就在这张图里面，另存为图片，打开 kali 虚拟机，用 binwalk 跑一下，发现里面隐藏一个压缩文件。然后用 foremost 分离一下图片，得到一个压缩文件：

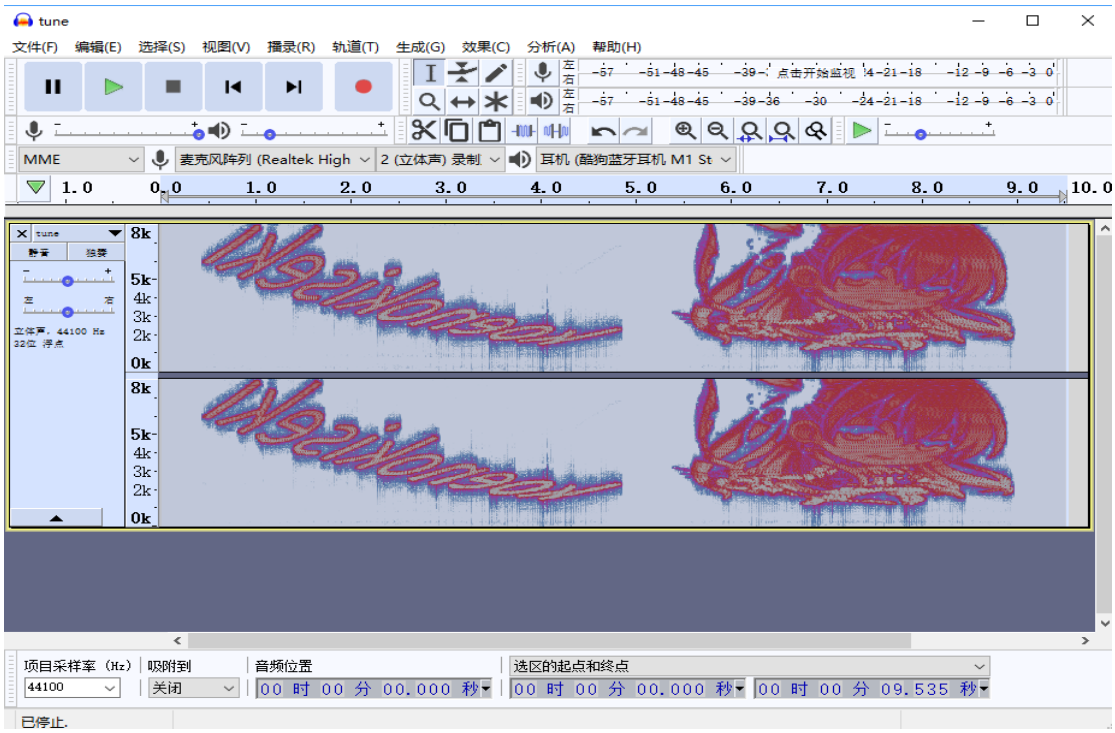


解压之后发现一个种子文件，忽然想到刚开始的“种子”，打开种子文件，看到了 flag：

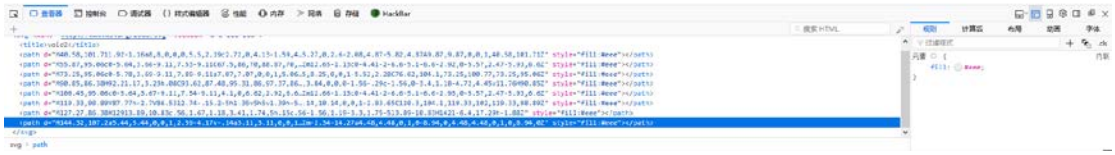


很想下载那个 mkv 文件啊，hhh，可惜是下载不了的。Flag 就是 greendam。

15. 声音的轨迹：看到这题想起来有的 CTF 题目是查看波形图之类的，于是另存为声音文件，用音频分析软件 Audacity，查看它的频谱图，发现 flag。



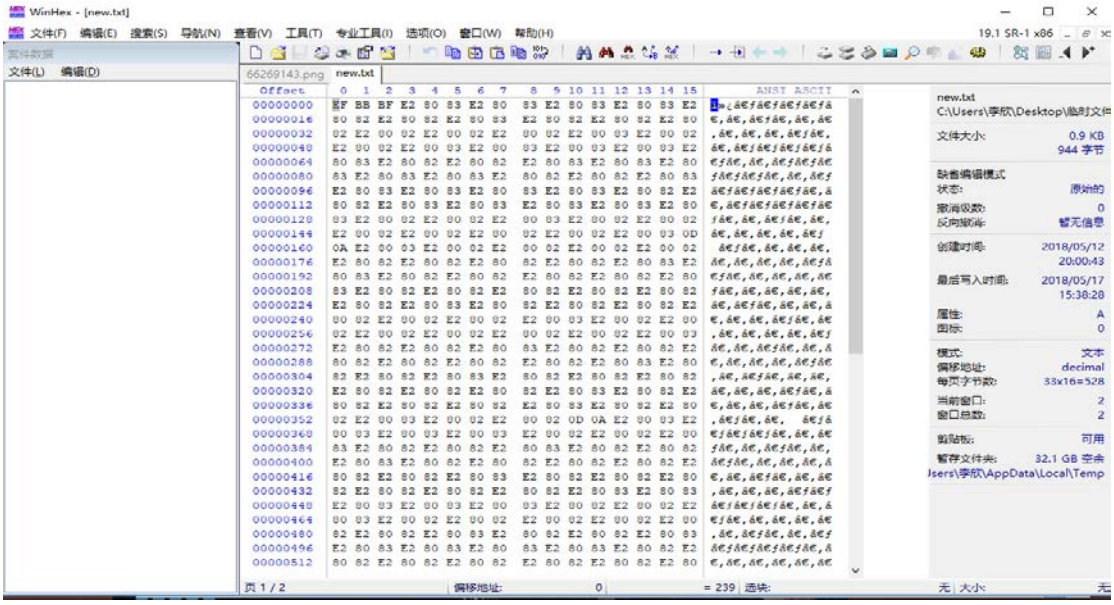
16. 虚掩：看到这题的名字就知道，网页上本来是有东西的，但是被掩盖住了。查看源码



把 SVG 图片上面覆盖的内容去掉就看到了 flag。

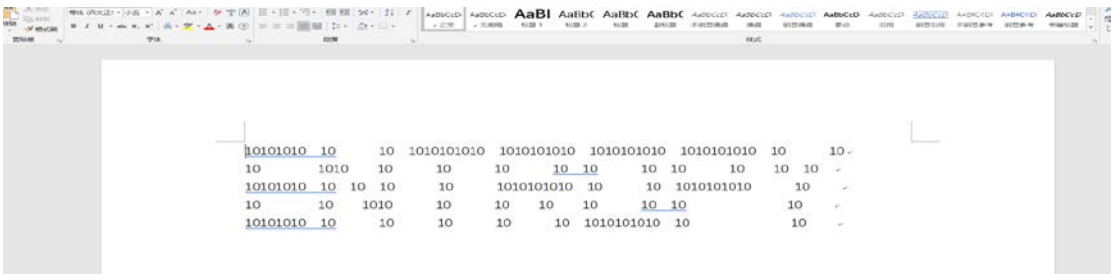
17.虚空：这题真是做到绝望，这一题比前面十六个题都强，太可怕了。最开始发现有几行空白可以选中，然后复制粘贴到文本文件中。

用 winhex 打开：



E2 80 83 ？E2 80 82 ?百度了一下，这是两种不同的空格，全角空格和半角空格。

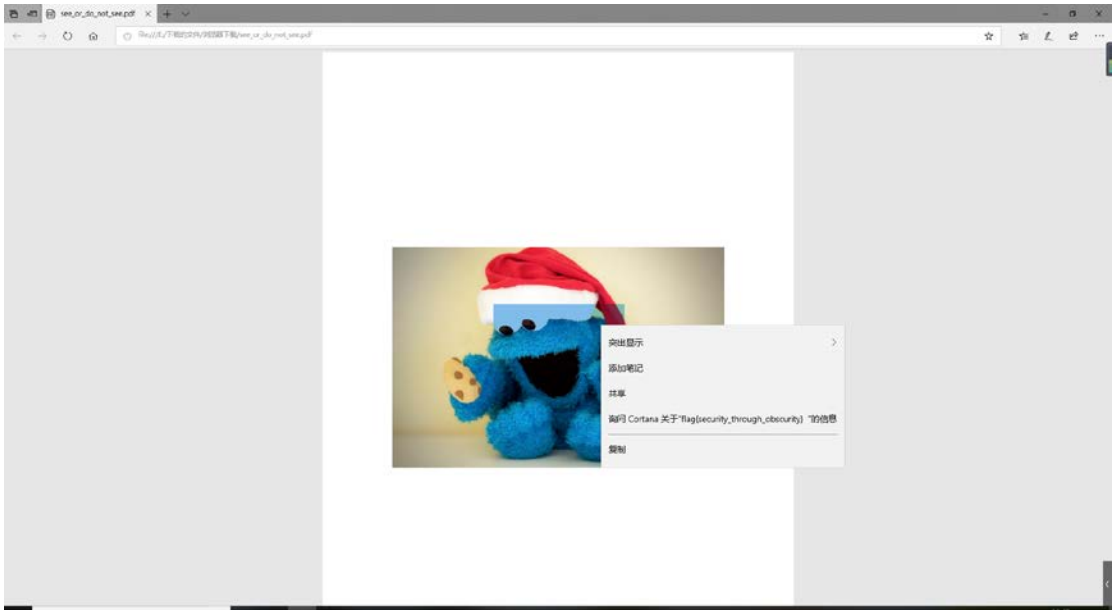
（用 burpsuite 抓包也是这个结果，走了好多弯路）然后想，这会不会是 E2 80 83 代表“1”，E2 80 82 代表“0”，然后连成二进制呢？看了一下那么长果断排除。然后想会不会是摩尔斯密码呢？然后试了半天觉得也不是。后来，偶然间发现，如果把每一行的半角空格加上全角空格的数量乘以二，结果每行的字符数就相等了。难道全角字符可以拼成 flag？于是速度把文本复制到 word，使用替换功能，把全角空格换成两个字符，结果令人吃惊！



隐约的看到了 flag 在向我招手！flag 就是：ENTROPY。出题人脑洞真的大！

- See_or_do_not_see:

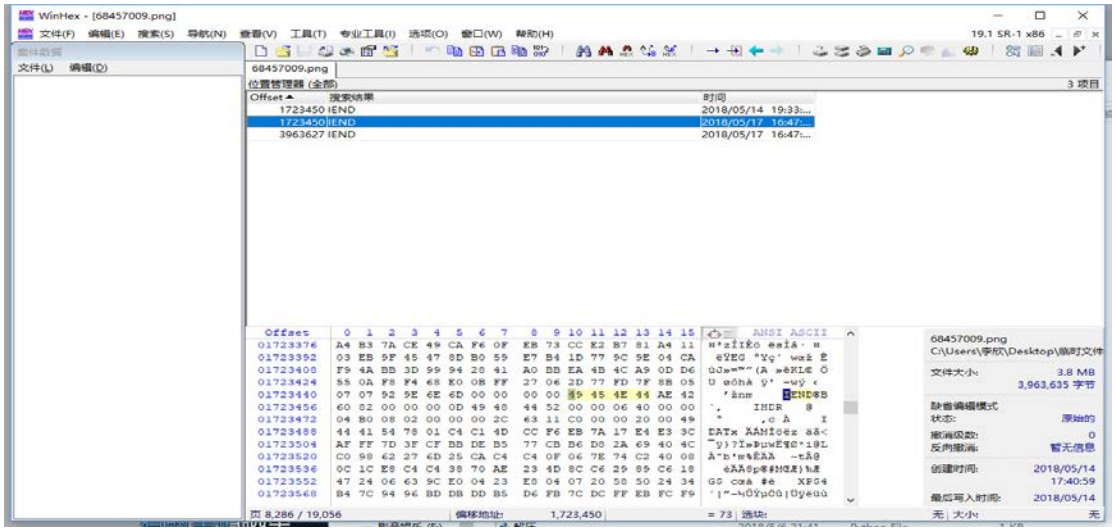
下载下来 PDF 文件之后，用 winhex 打开后，没有任何发现，然后直接用浏览器打开，在图片上忽然发现图片有一部分可以选中！选中之后，右键，发现了不可思议的事情（\笑哭）：



Flag 是隐藏在图片后面的，但是居然可以选中，然后复制粘贴就好咯~

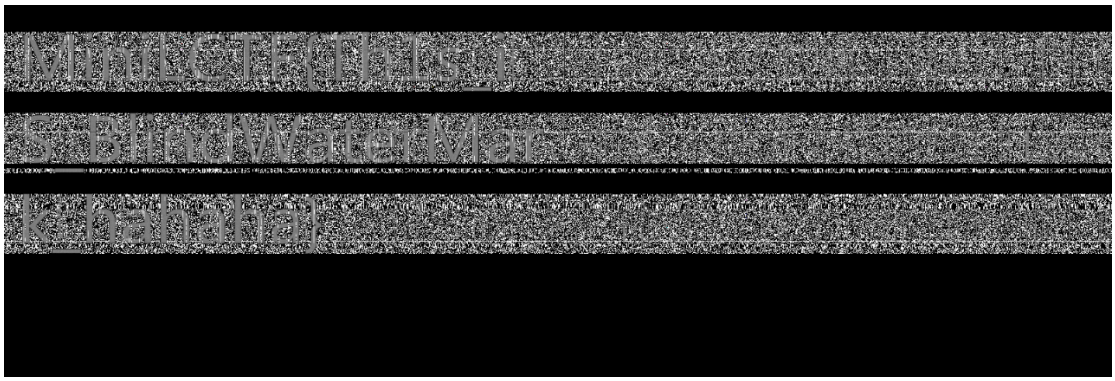
- Moe：

下载下来图片，首先老办法，用 binwalk 跑一下，没发现啥，但是用 foremost 分离出的图片只有 1.3M 左右，但是源文件可是 4M 左右的啊，这里面肯定有猫腻。于是用 winhex 打开图片文件，简单的搜索了一下 png 图片的十六进制结构，使用 winhex 里面的文本搜索功能发现文件在中间就结束了：



然后发现后面好像还是一个 png 文件，但是由于提前结束了，后面的内容就被忽略了。

于是，现在要做的就是把后半部分 png 图片提取出来，用 winhex 把前面的图片删掉，手动给后面的图片加上头，然后另存为，发现这两张图片长得一模一样，但是，图片的大小不一样，然后百度了一下，发现可能是用了水印，然后参照百度上给的方法，下载了一个提取水印的 py 文件。然后参照这个脚本的使用方法，打开 cmd，键入指令 python bwm.py decode 1.png 2.png wm_out.png 获得了一张图片！（这中间花了三个小时下了两个 python 库，网速慢的真是可以！！！）图中就是 flag：



第一次输入 flag 的时候还输错了，把“Th1s”输成了“This”，看了老半天才发现，呜呜呜呜~

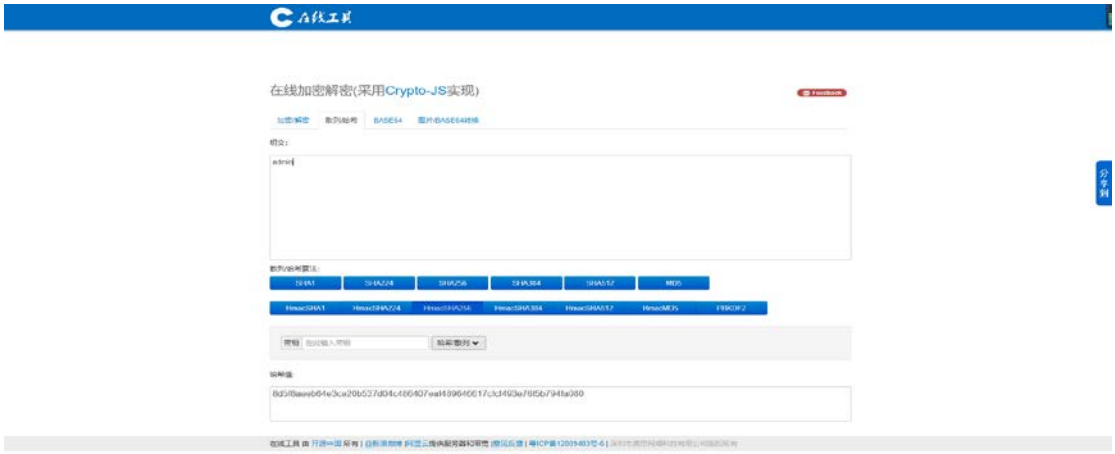
- Easy bypass：

查看源码：

```
<?php
highlight_file(__FILE__);
if(empty($_POST['hmac']) || empty($_POST['host'])){
        header('HTTP/1.0 400 Bad Request');
        exit;
}
$secret = getenv("SECRET");
if(isset($_POST['nonce']))
        $secret = hash_hmac('sha256',$_POST['nonce'],$secret);
$hmac = hash_hmac('sha256',$_POST['host'],$secret);
if($hmac !== $_POST['hmac']){
        header('HTTP/1.0 403 Forbidden');
        exit;
}
echo exec('cat ../flag.txt');
?>
```

发现如果 nonce 为空的话，那么我们随便输入一个 host 值，比如 host=admin，根据源码可以知道，这时候只需要让 hmac 的值等于“admin”经过 sha256 加密后的值即可得到 flag，由于 SECRET 我们并不知道，这就是为什么我们要让 nonce 为空，nonce 为空的话，host 经过加密后的值我们就可以不需要密钥轻易得到。然后，再看源码，nonce 又不能让它为空，于是就想到了构造一个数组 nonce[]=，这样就巧妙绕过了判断。接下来用

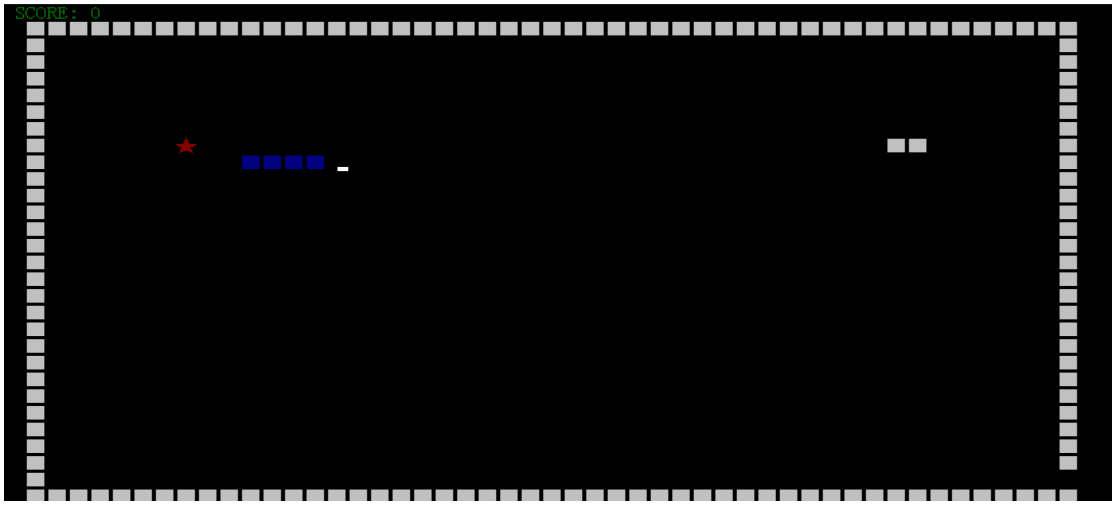
hackbar post 一下数据就 OK 了！



- 贪吃蛇：

开始玩了一下，发现手残党根本玩不下去，后来抱着试试看的态度，既然是逆向题，那就用 IDA 打开看一下：

发现了地图，于是想着是不是能把“XDSEC”去掉，这样就简单一些了。我发现“XDSEC”和边界使用“1”，所以，打开 winhex，找到地图这段代码，把“XDSEC”去掉，然后保



那两个小格可能是漏删了，不过不影响，手残党看到了一丝希望，又玩了十几分钟终于玩出来了！（这中间有 bug，食物会出现在蛇身体里，这样蛇就没办法吃下一个了，因为下一个食物不再出现了！）吃到 30 个就得到了 flag。

想加入协会跟着师傅们学技术啊，自己学真的很没方向，能不能带带我这个菜鸡~~~