第五季极客大挑战 Writeup

音符【BTC&XDSEC&威尔渗透大牛徒弟小组】

先晒张排行榜装下逼。

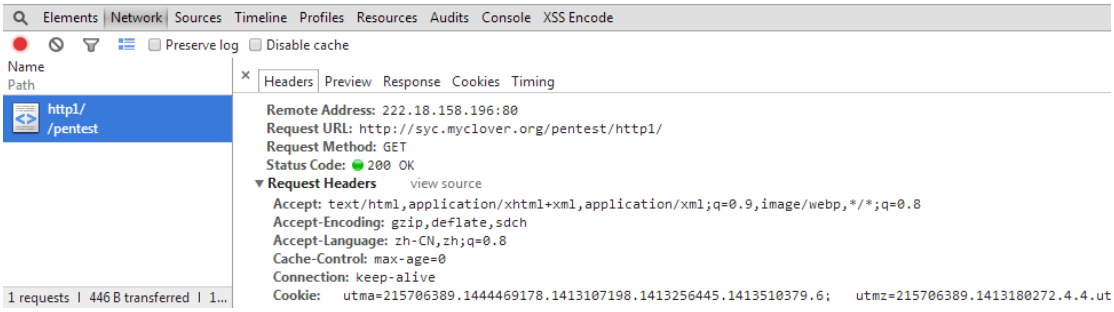
第五季极客大挑战 Challenge 排行榜 规则 威尔渗透大牛徒弟小组(4601)

队伍	学院	口号	得分	最后提交时间
威尔渗透大牛徒弟小组	信息安全工程学院	威尔渗透最后一次收徒，男生2000，女生免费（QQ[redacted]）	4601	2014-10-17 10:04:37
大一爸爸猴	统计学院	此广告位已被摩擦up主购买：www.bilibili.com/video/av1193400	4451	2014-10-17 19:21:16
jsdx	校外团队		4251	2014-10-17 18:29:17
test set	信息安全工程学院	被北京6级大风吹走了	4051	2014-10-17 17:09:39
蓝娇	信息安全工程学院	白神，我稀饭你！	4001	2014-10-16 22:41:59
F1uYu4n	校外团队	摸摸猫头	3951	2014-10-18 01:33:55
JoyChou	信息安全工程学院	洋葱，约否？	3801	2014-10-17 15:00:03
feniczy	信息安全工程学院	Hacked By Shijie	3601	2014-10-17 00:25:34
Hellokitty	校外团队		3401	2014-10-16 22:42:47
LStar	信息安全工程学院	主办方这个口号接口的名字low爆了	3401	2014-10-18 00:20:46

HTTP Base1

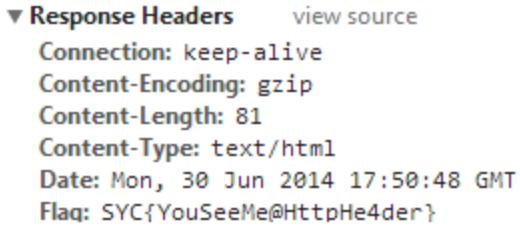
Do you know what is HTTP Header?
Go on, Hacker!

考核关于 http 头的知识
直接用 chrome 查看数据包



这是发送过去的数据包 HEADER

返回过来的数据包 HEADER



看到 flag 了。

HTTP Base2

SYC 财务系统

不允许外部访问

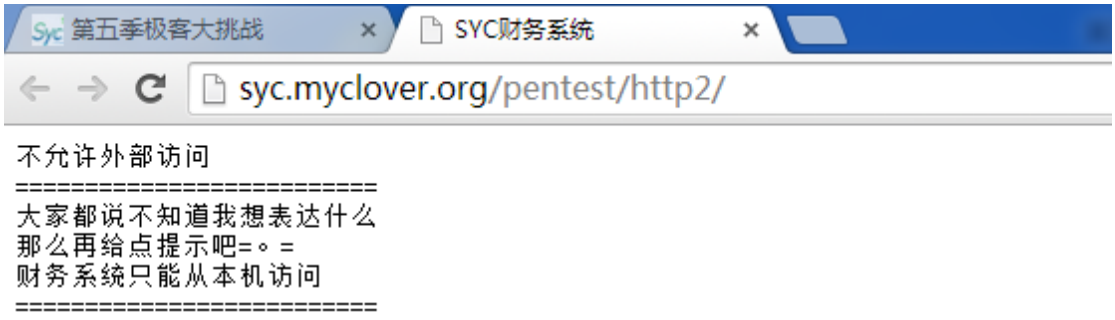
==========

大家都说不知道我想表达什么

那么再给点提示吧=。=

财务系统只能从本机访问

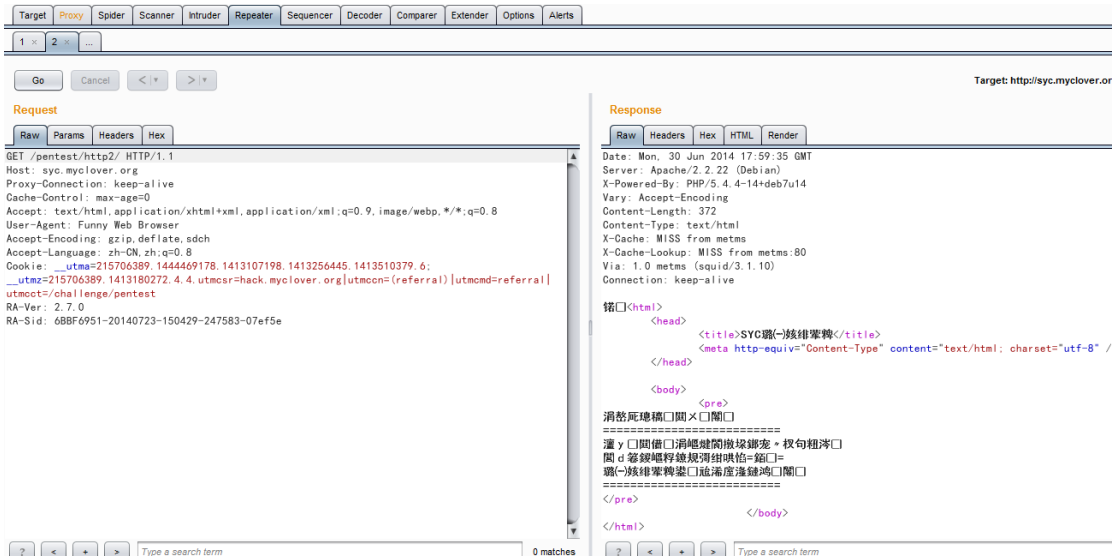
==========



一开始是没有这个提示的。
这题考核的是 IP 伪造的相关知识。
以下是一个用 php 获取客户端 ip 的脚本。

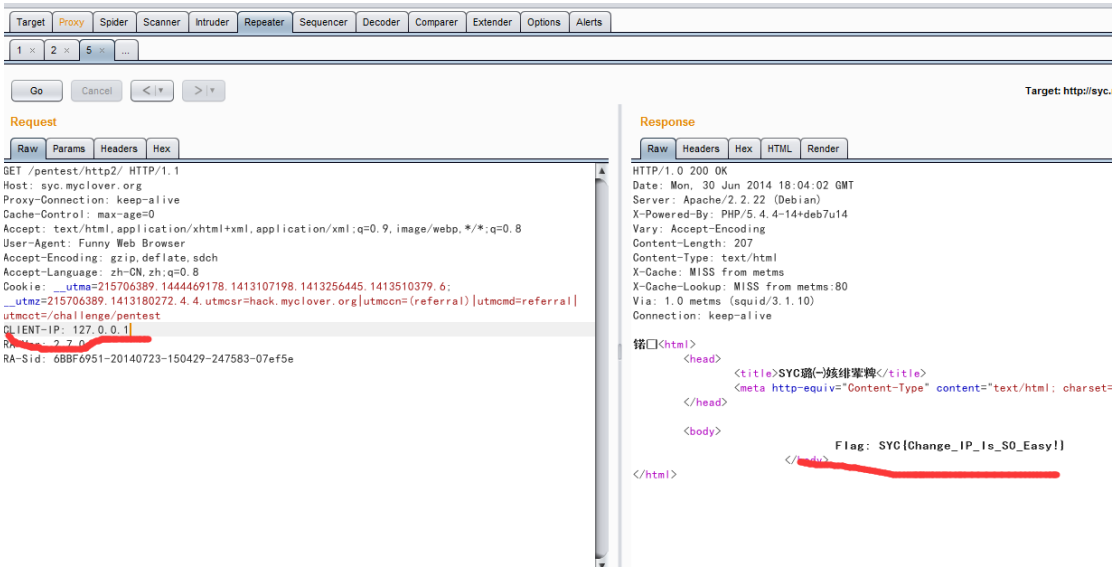
```
function getIP() {
if (@$_SERVER["HTTP_X_FORWARDED_FOR"])
$ip = $_SERVER["HTTP_X_FORWARDED_FOR"];
else if (@$_SERVER["HTTP_CLIENT_IP"])
$ip = $_SERVER["HTTP_CLIENT_IP"];
else if (@$_SERVER["REMOTE_ADDR"])
$ip = $_SERVER["REMOTE_ADDR"];
else if (@getenv("HTTP_X_FORWARDED_FOR"))
$ip = getenv("HTTP_X_FORWARDED_FOR");
else if (@getenv("HTTP_CLIENT_IP"))
$ip = getenv("HTTP_CLIENT_IP");
else if (@getenv("REMOTE_ADDR"))
$ip = getenv("REMOTE_ADDR");
else
$ip = "Unknown";
return $ip;
}

$ip = getIP() ;
echo $ip;
```

X_FORWARDED_FOR 跟 CLIENT_IP 都是在 HTTP HEADER 头中的参数，客户端在发送一个 HTTP 请求包的时候可以修改。
Burp Suite 是一款非常好的 HTTP 分析利用工具，我们用它来抓包、改包。

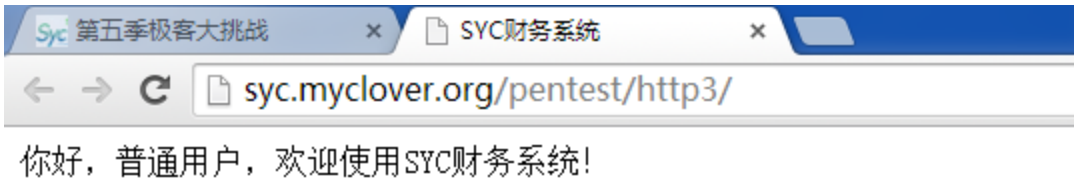


普通发包

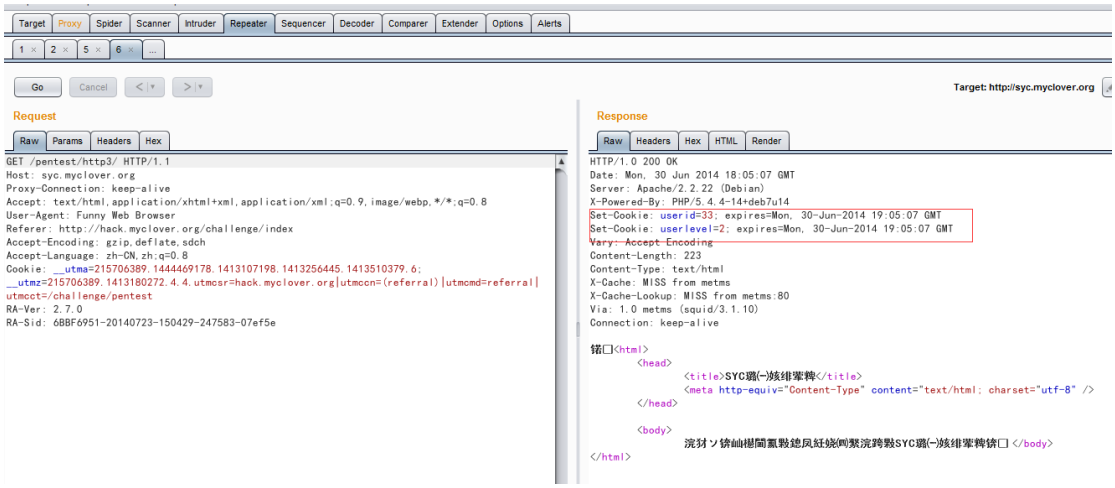
伪造 CLIENT-IP



HTTP Base3



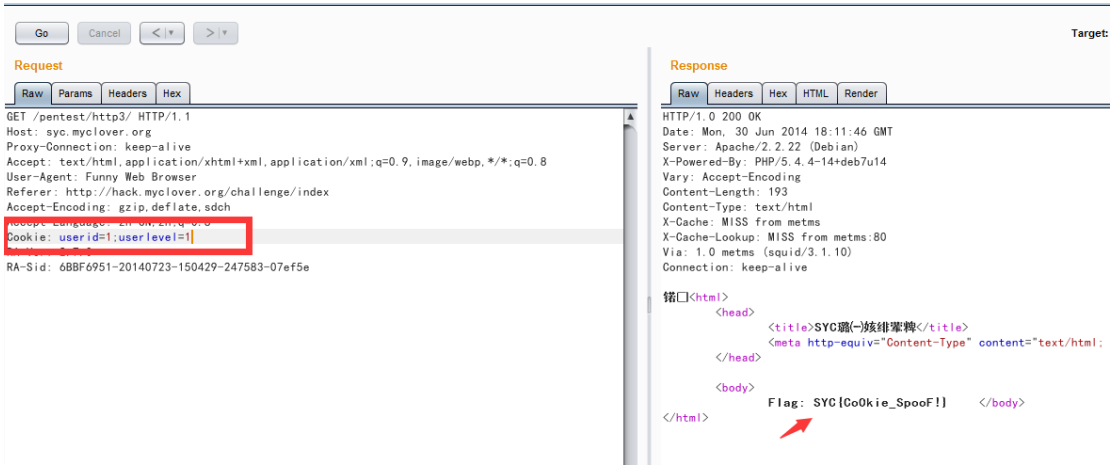
查看返回的数据包



Cookie 是什么？

Cookie 是网站用来辨别用户身份的一种信用凭证，存放在客户端。

因为存放在客户端，所以可以修改。可以修改，就可以伪造。

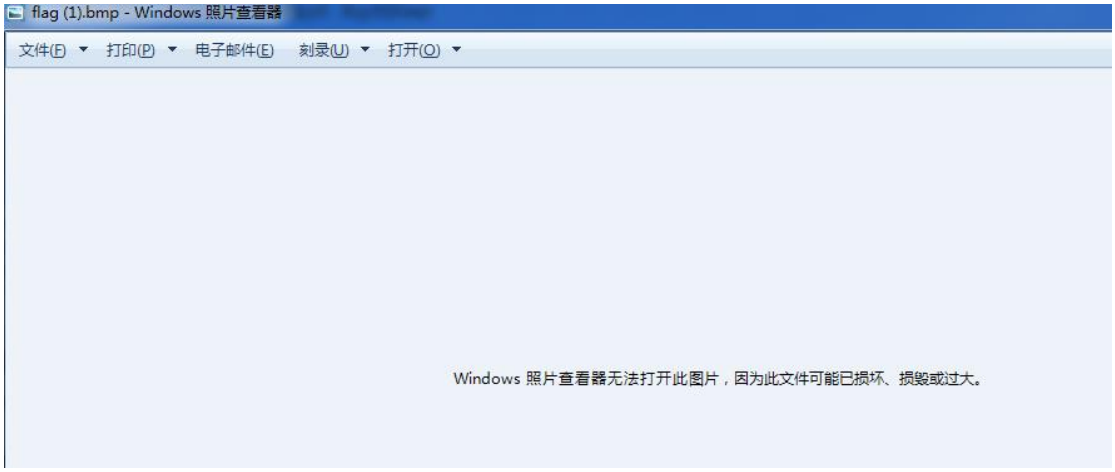


修改一下 userid 跟 userlevel，获取 flag。

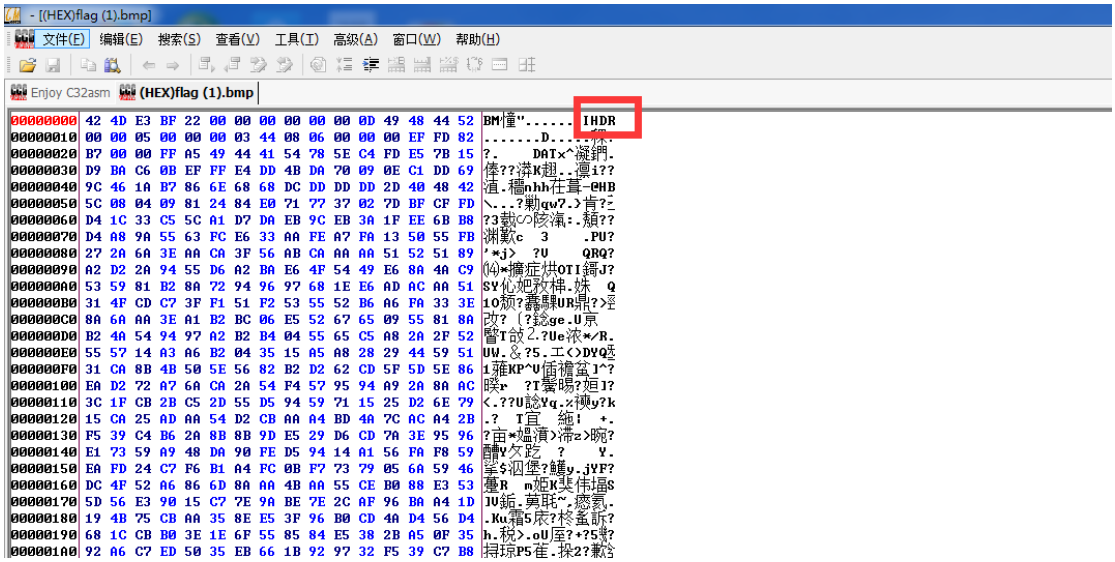
too young too simple

图片题。

下载下来一个 flag.bmp，bmp 图片后缀，却无法显示。

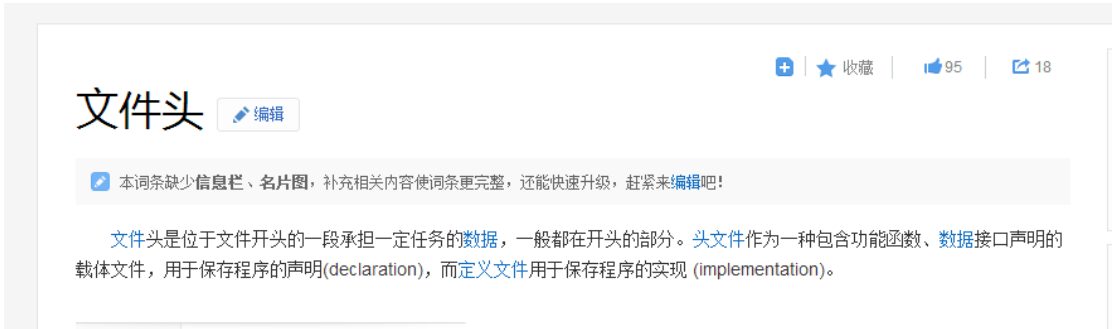


用 C32asm 查看，16 进制编辑工具。

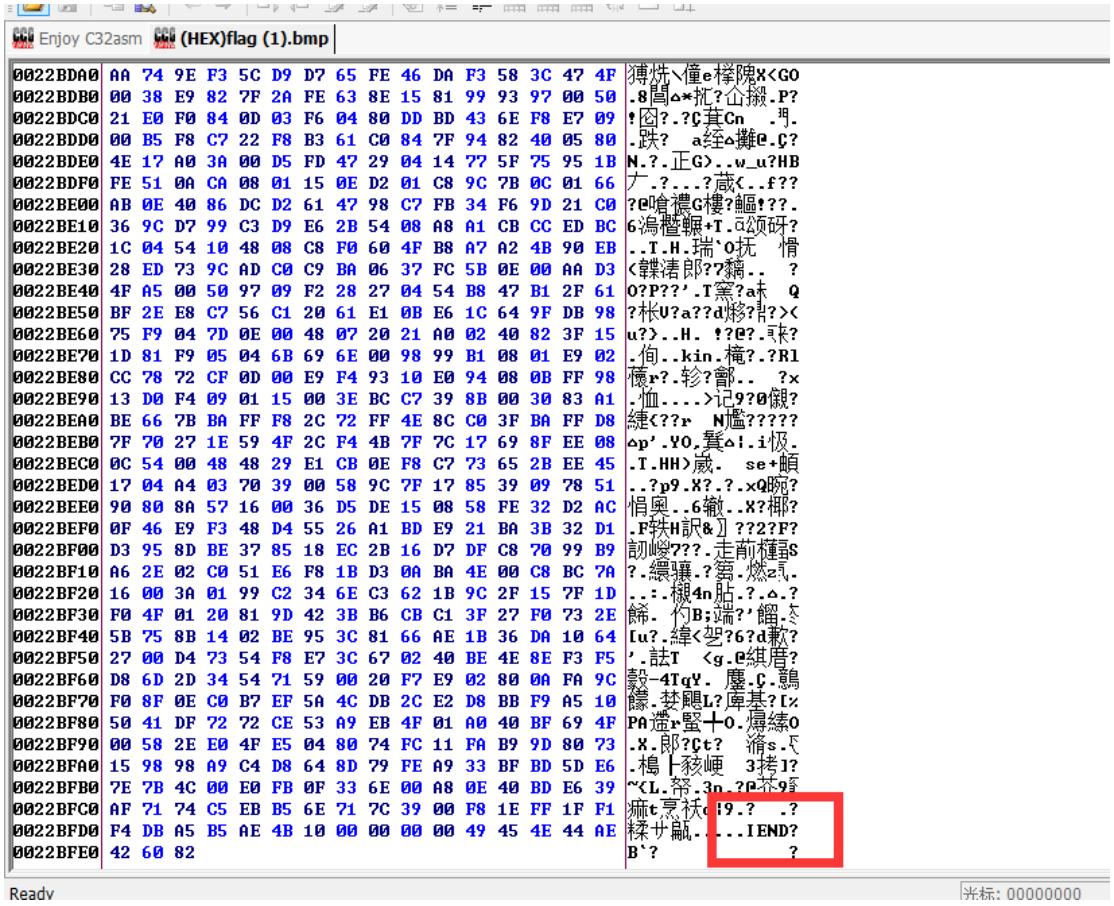


左边是文件的 16 进制格式，右边是文件的 unicode 格式。

发现文件头 确实是 42 4D 标准的 BMP 文件头



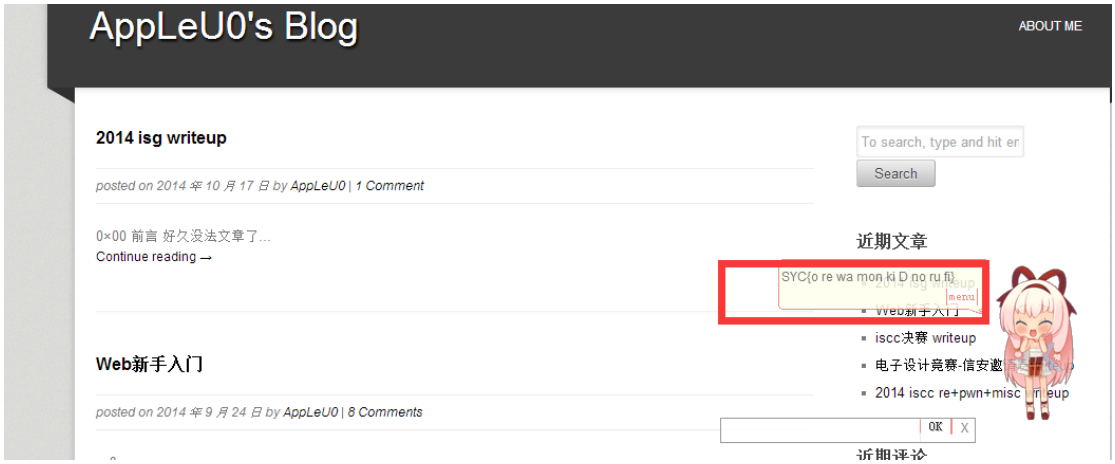
但是文件的其他部分却出现了 PNG 图片的文件格式



可以判断，这其实是一个 PNG 的图片文件。我们现在要做的很简单，就是把文件的文件头改回 png 的文件头。

PNG 的文件头是 89 50 4E 47 0D 0A 1A 0A
然后将文件名改为 png 格式。

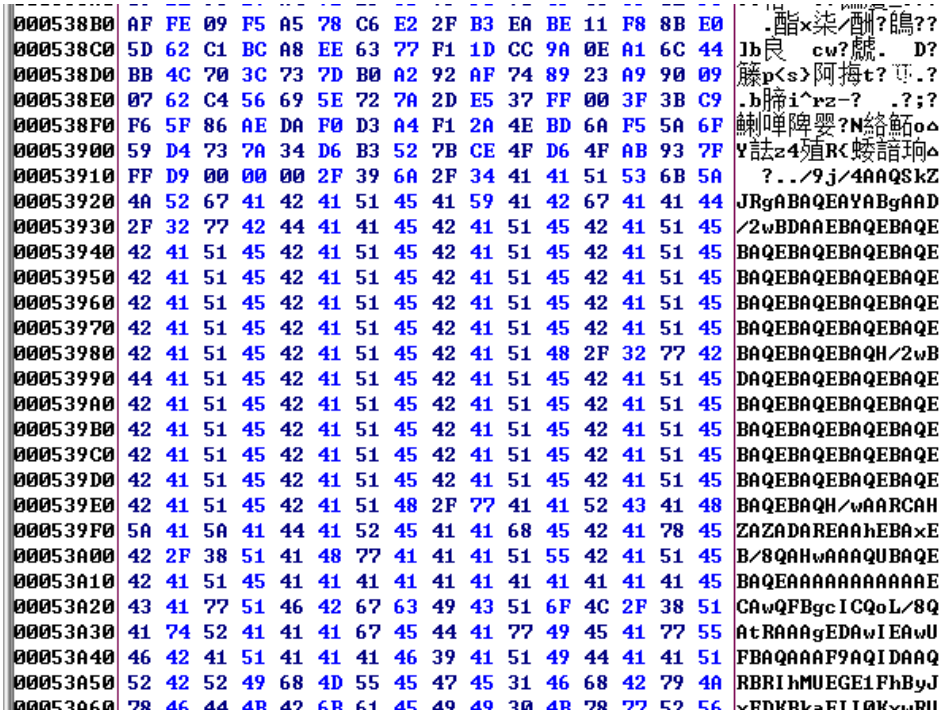
提示了一个网站，貌似是告诉谁 flag
弱弱问一句，这是在刷流量么？



拿到 flag

你喜不喜欢萌萌哒的姐姐

图片题，下载到 1.JPG
同样用 c32asm 打开。
发现文件尾有异常的地方。

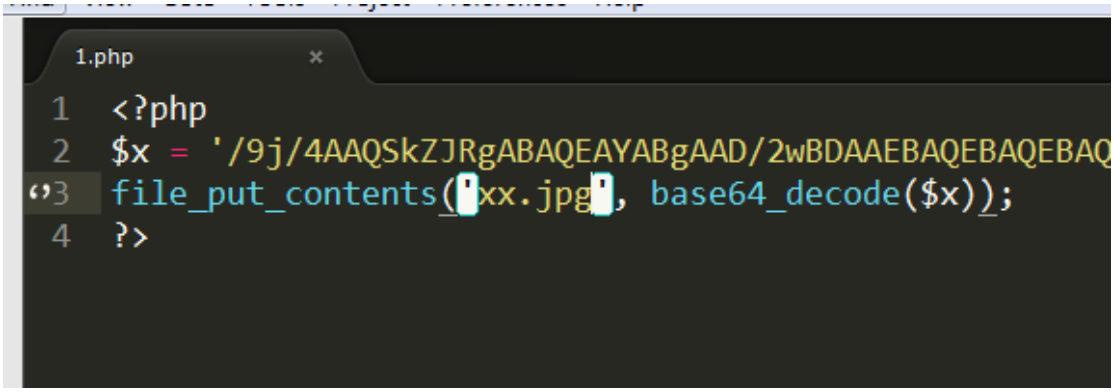


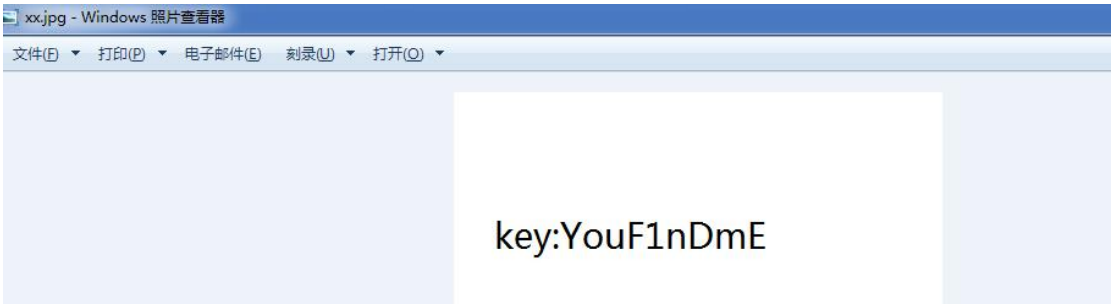
```
000538B0 AF FE 09 F5 A5 78 C6 E2 2F B3 EA BE 11 F8 8B E0   .酯x柒/酬?鴿??
000538C0 5D 62 C1 BC A8 EE 63 77 F1 1D CC 9A 0E A1 6C 44 ]b艮  cw?騽.  D?
000538D0 BB 4C 70 3C 73 7D B0 A2 92 AF 74 89 23 A9 90 09 縢p<s>阿挴t?.?
000538E0 07 62 C4 56 69 5E 72 7A 2D E5 37 FF 00 3F 3B C9 .b睇i^rz-?  .?;?
000538F0 F6 5F 86 AE DA F0 D3 A4 F1 2A 4E BD 6A F5 5A 6F 鰍嗶陴嬰?N綰鮕o
00053900 59 D4 73 7A 34 D6 B3 52 7B CE 4F D6 4F AB 93 7F Y詰z4殖R{蝮譆珣
00053910 FF D9 00 00 00 2F 39 6A 2F 34 41 41 51 53 6B 5A   ?../9j/4AAQSkZ
00053920 4A 52 67 41 42 41 51 45 41 59 41 42 67 41 41 44 JRgABAQEAYABgAAD
00053930 2F 32 77 42 44 41 41 45 42 41 51 45 42 41 51 45 /2wBDAAEBAQEBAQE
00053940 42 41 51 45 42 41 51 45 42 41 51 45 42 41 51 45 BAQEBAQEBAQEBAQE
00053950 42 41 51 45 42 41 51 45 42 41 51 45 42 41 51 45 BAQEBAQEBAQEBAQE
00053960 42 41 51 45 42 41 51 45 42 41 51 45 42 41 51 45 BAQEBAQEBAQEBAQE
00053970 42 41 51 45 42 41 51 45 42 41 51 45 42 41 51 45 BAQEBAQEBAQEBAQE
00053980 42 41 51 45 42 41 51 45 42 41 51 48 2F 32 77 42 BAQEBAQEBAQH/2wB
00053990 44 41 51 45 42 41 51 45 42 41 51 45 42 41 51 45 DAQEBAQEBAQEBAQE
000539A0 42 41 51 45 42 41 51 45 42 41 51 45 42 41 51 45 BAQEBAQEBAQEBAQE
000539B0 42 41 51 45 42 41 51 45 42 41 51 45 42 41 51 45 BAQEBAQEBAQEBAQE
000539C0 42 41 51 45 42 41 51 45 42 41 51 45 42 41 51 45 BAQEBAQEBAQEBAQE
000539D0 42 41 51 45 42 41 51 45 42 41 51 45 42 41 51 45 BAQEBAQEBAQEBAQE
000539E0 42 41 51 45 42 41 51 48 2F 77 41 41 52 43 41 48 BAQEBAQH/wAARCAH
000539F0 5A 41 5A 41 44 41 52 45 41 41 68 45 42 41 78 45 ZAZADAREAAhEBAxE
00053A00 42 2F 38 51 41 48 77 41 41 41 51 55 42 41 51 45 B/8QAHwAAAQUBAQE
00053A10 42 41 51 45 41 41 41 41 41 41 41 41 41 41 41 45 BAQEAAAAAAAAAAE
00053A20 43 41 77 51 46 42 67 63 49 43 51 6F 4C 2F 38 51 CAwQFBgcICQoL/8Q
00053A30 41 74 52 41 41 41 67 45 44 41 77 49 45 41 77 55 AtRAAAgEDAwIEAwU
00053A40 46 42 41 51 41 41 41 41 46 39 41 51 49 44 41 41 FBAQAAAAF9AQIDAAQ
00053A50 52 42 52 49 68 4D 55 45 47 45 31 46 68 42 79 4A RBRIhMUEGE1FhByJ
```

照例说图片文件中不可能存在这么一大串连续的英文字符串的，看格式应该是 base64 编码，试试解码。

虽然解出来出乱码（因为浏览器的字符集不支持输出一些不可见字符以及一些不常见 unicode 编码），但是从文件开头，我们就可以辨明，这是一个 jpg 的文件。

下面写了一个 php 小脚本来解决问题。





[美男子]

一开始还以为又是图片题，用 C32 看了有一会儿。

看来又是 cookie 伪造了。

设置下 cookie

Cookie: user=meinanzi; isboy=1;

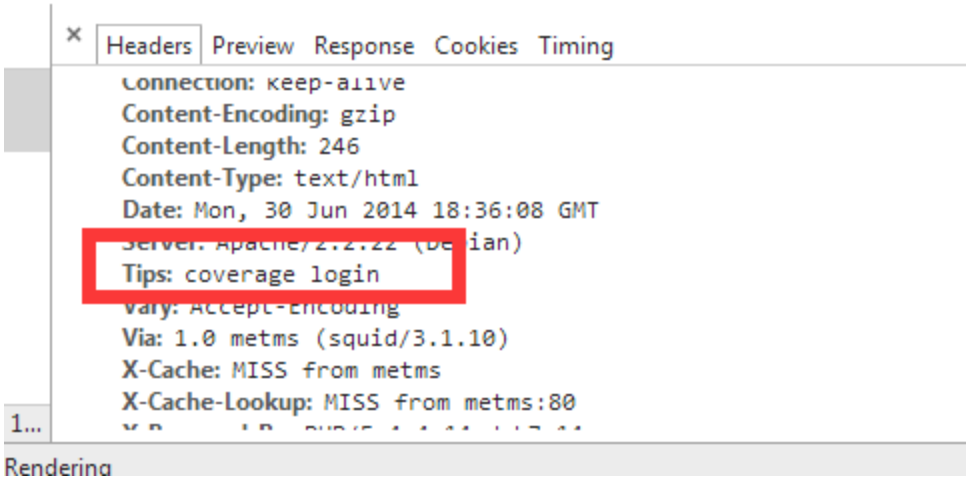
拿到 flag

Login

直接送账号密码呀，快试试。用户名 appleU0，密码 syclover

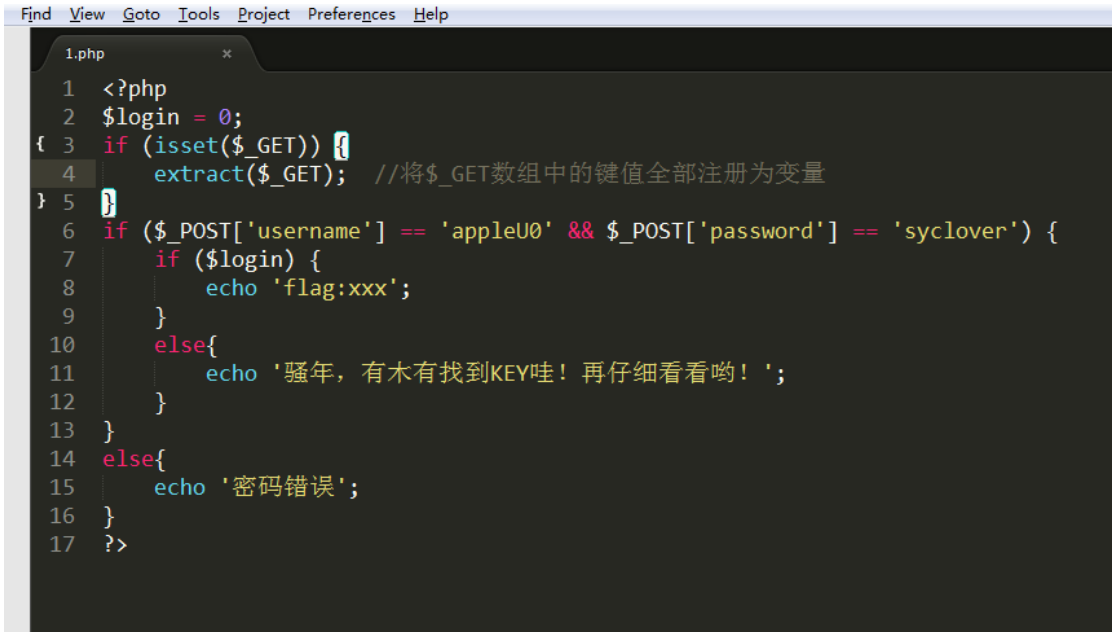
又是无聊的 http 返回包？

发现返回包中有个 TIP：



貌似是覆盖变量 login

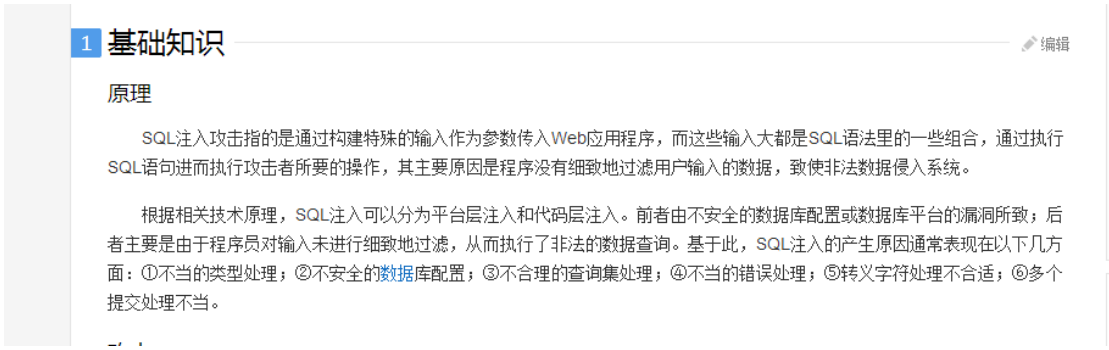
关于 php 覆盖变量的知识，我猜测他的脚本应该是这样写的。



访问：http://syc.myclover.org/pentest/memeda.php?login=1

Web Base1

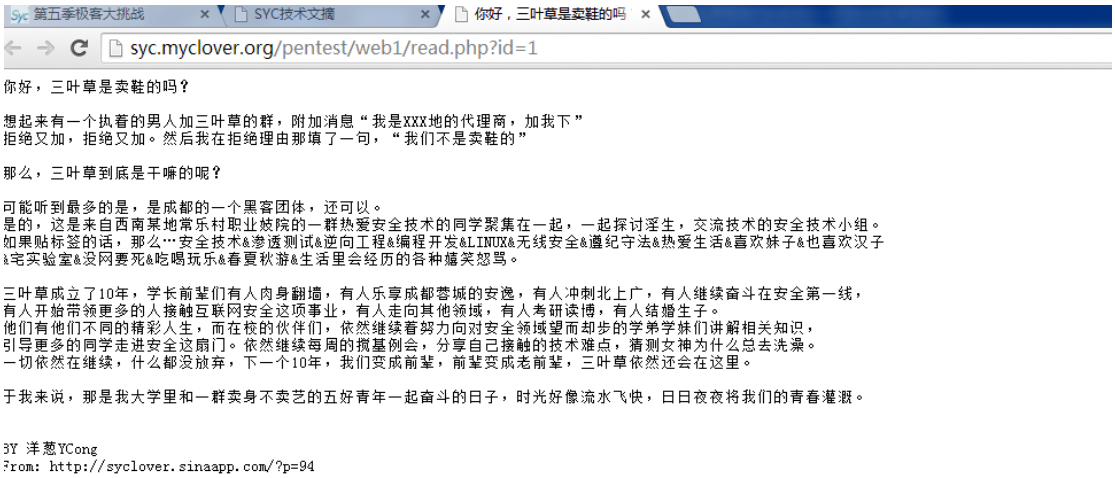
看来是 sql 注入的知识。



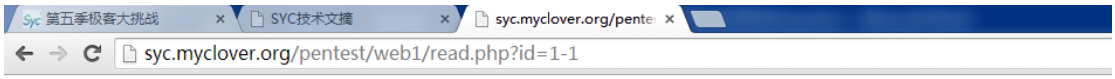
Sql 的根本原因是没有将数据与代码区分开。

Select * from table where id = +input+

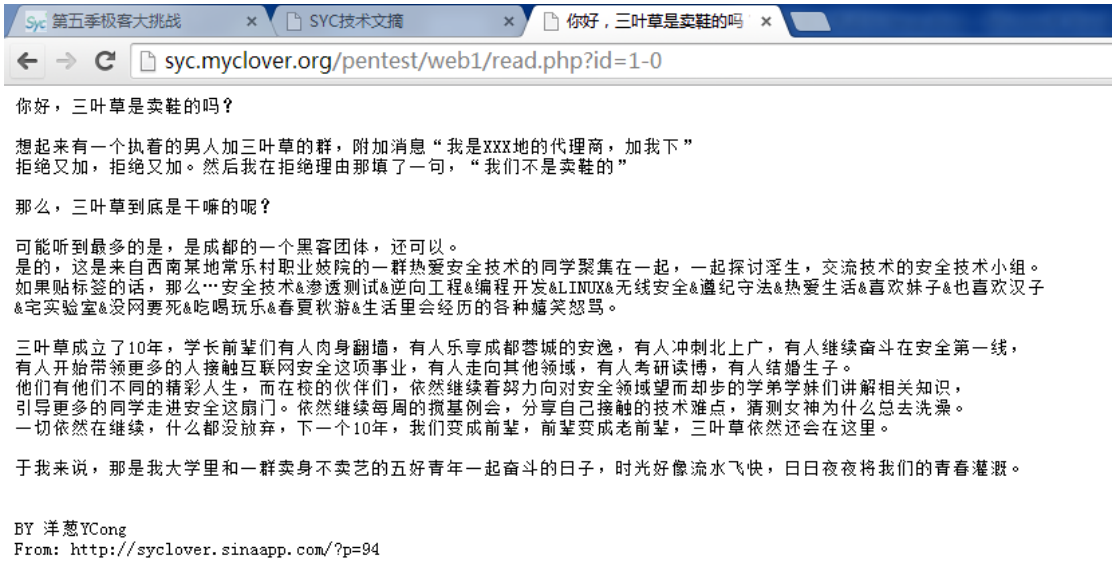
Select * from table where id = 1



Select * from table where id = 1-1



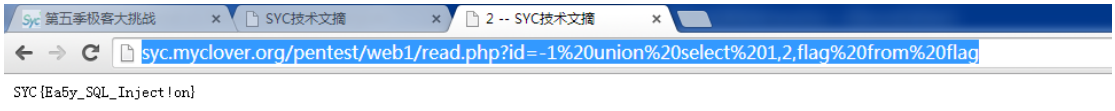
Select * from table where id = 1-0



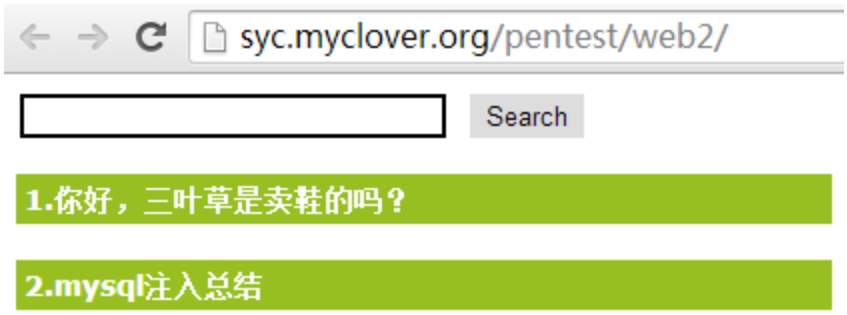
关于更多的 sql 注入的知识，自行去网上查阅。

这里直接用一个 payload：

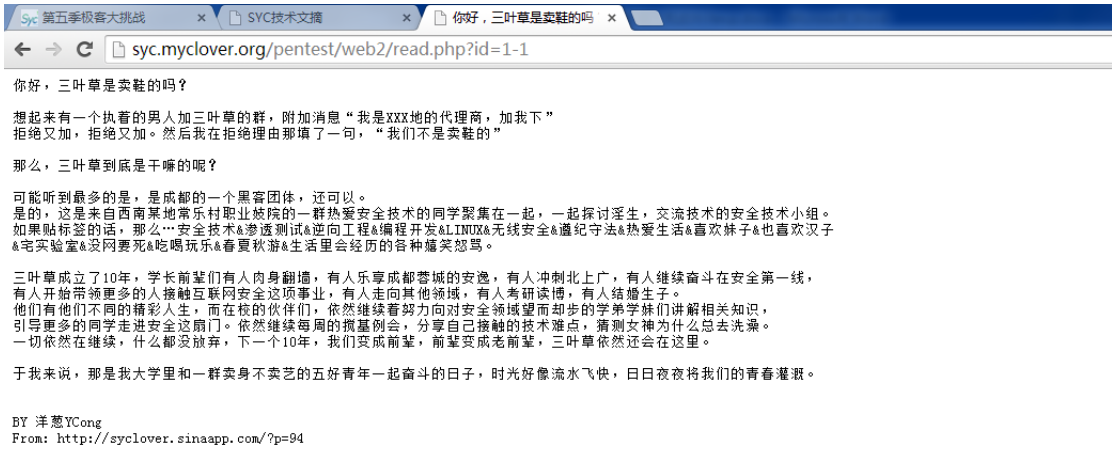
http://syc.myclover.org/pentest/web1/read.php?id=-1 union select 1,2,flag from flag



Web Base2



添加了一个搜索功能



原来的注入已经过滤了。

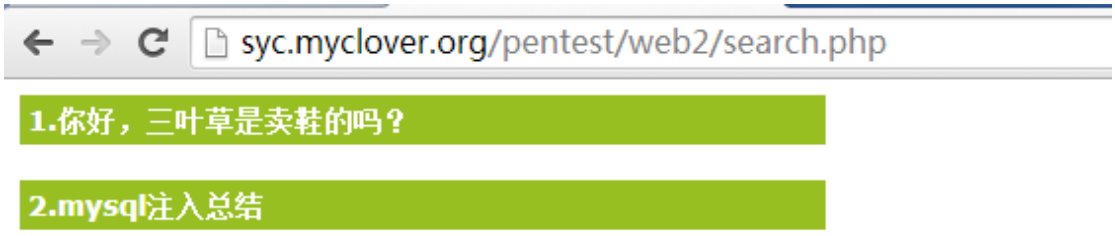
$id = $_GET[‘id’] ➔$id=intval($_GET[‘id’])

目测在搜索处出现注入

Select * from table where content like ‘%+input+%’

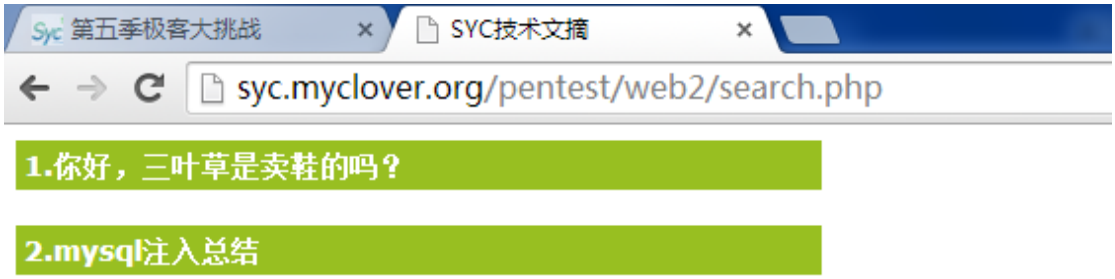
1

Select * from table where content like ‘%1%’



1%' and 1=1 and '%'='

Select * from table where content like ‘% 1%' and 1=1 and '%'='%’



1%' and 1=1 and '%'='

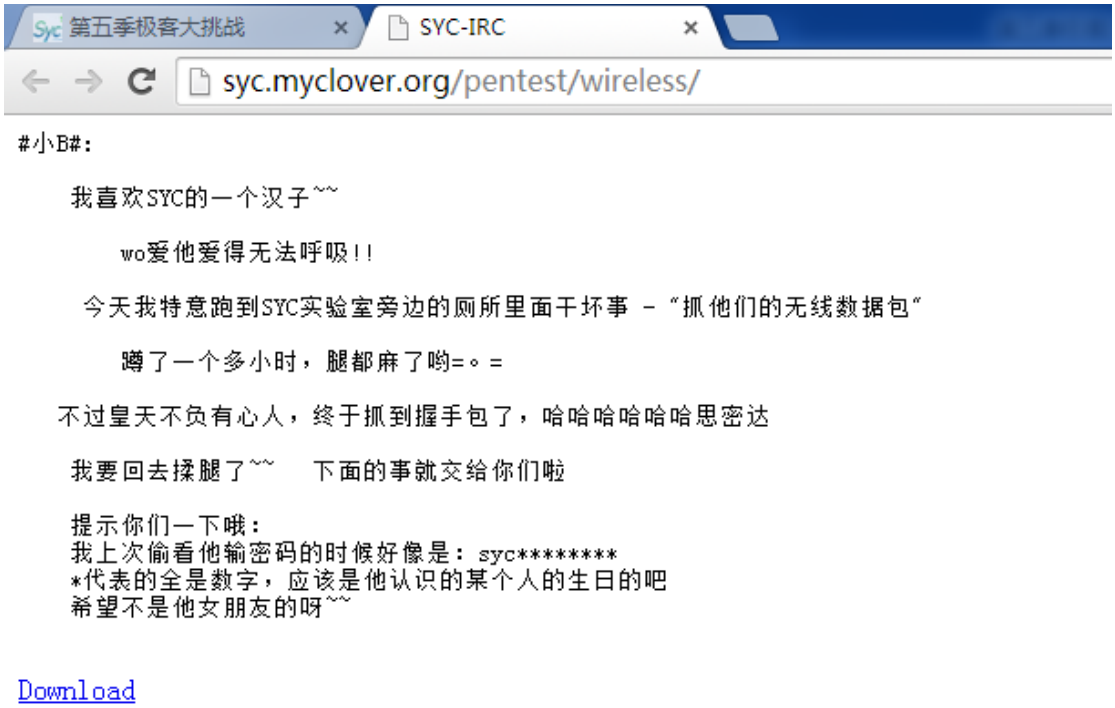
Select * from table where content like ‘% 1%' and 1=2 and '%'='%’

Payload：

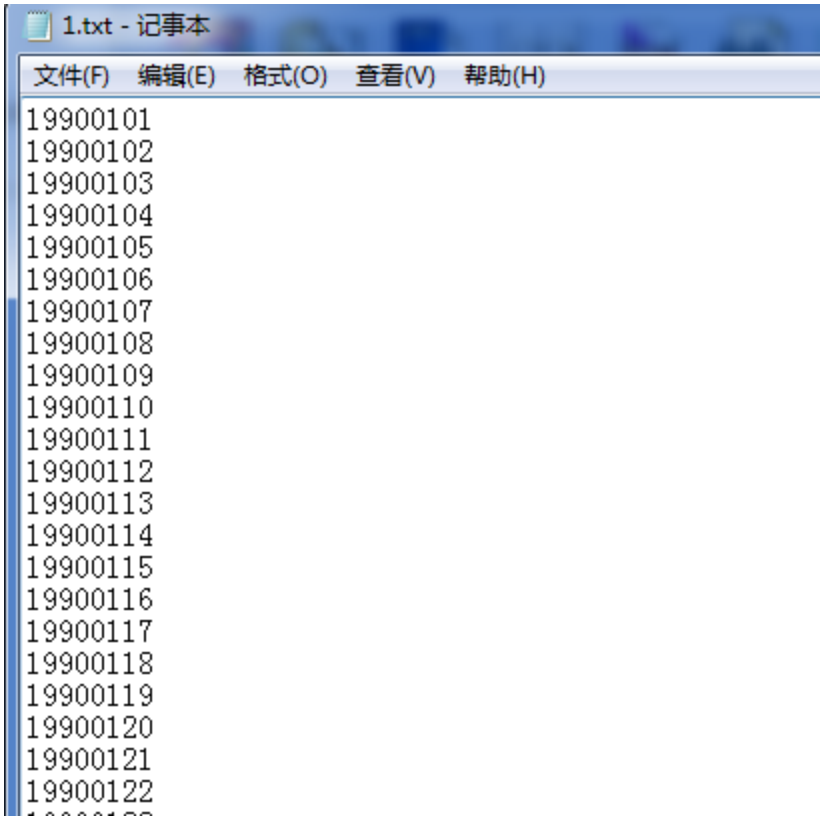
1%' union select 1,flag from `#flag`--

Wireless

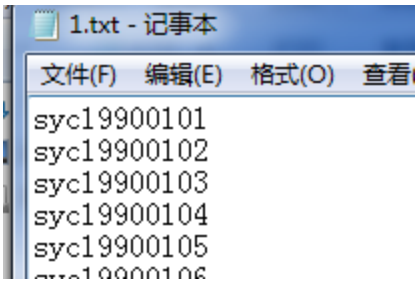
看名字就知道是无线相关的



下载下来一个 wificap-01.cap，目测是一个 wpa2 握手包，暴力破解下就好了。8 位生日嘛，生成个字典跑一下。

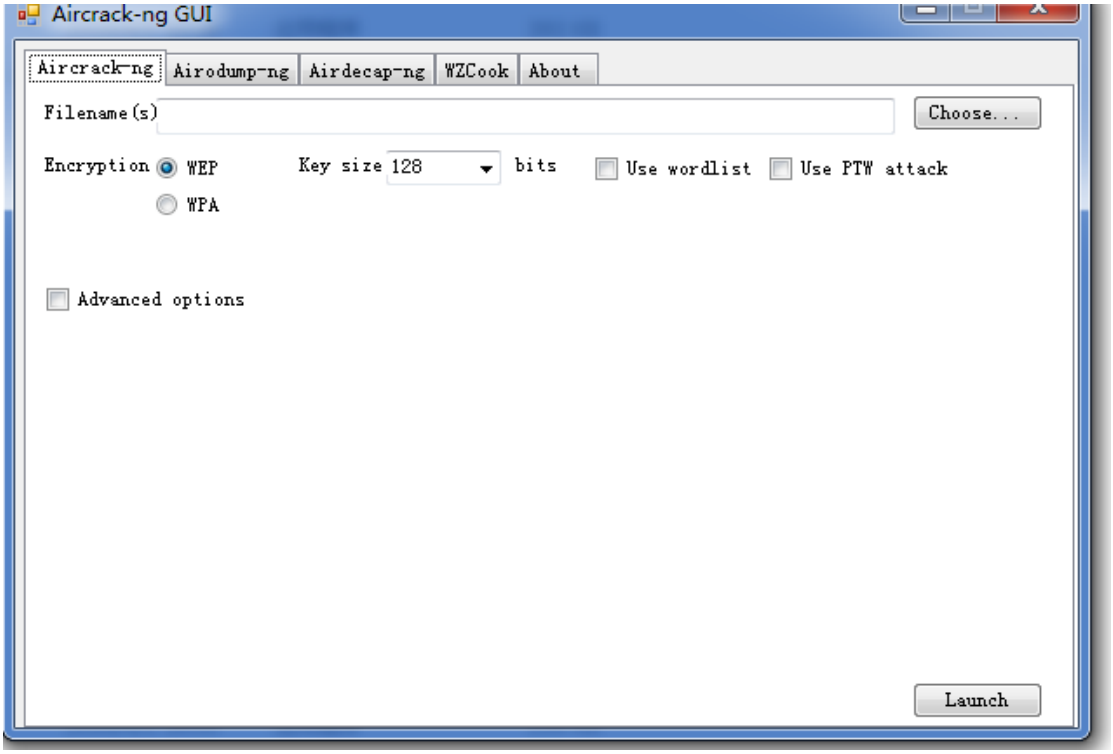


然后前面还要加上 syc

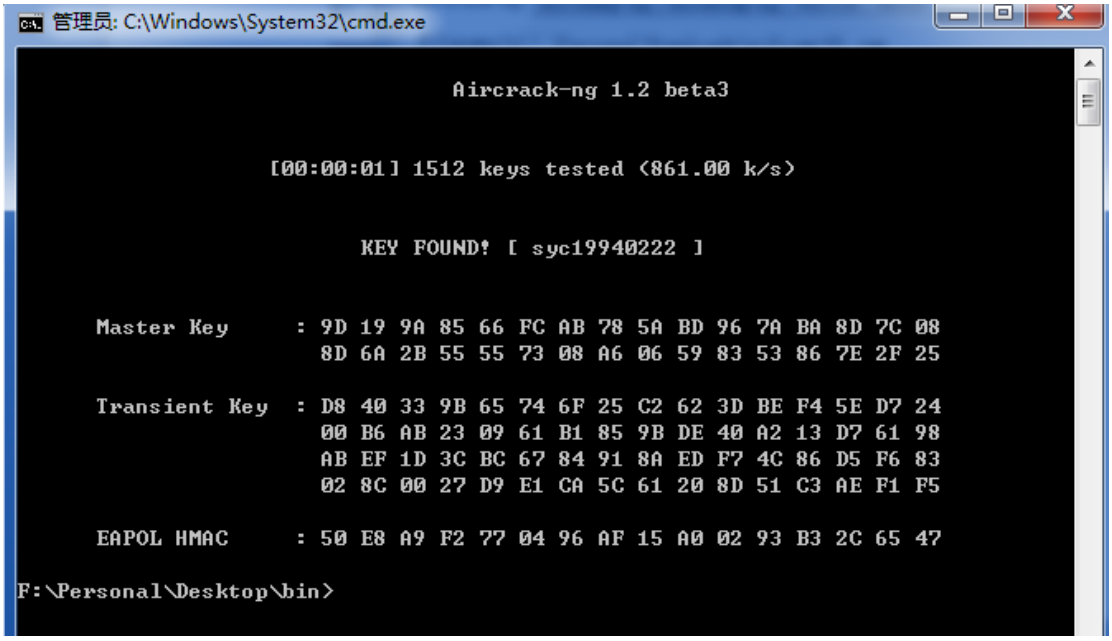


3000+条

一个简单的跑包工具 aircrack-NG



有 gui 就是好



3 秒就跑出来了