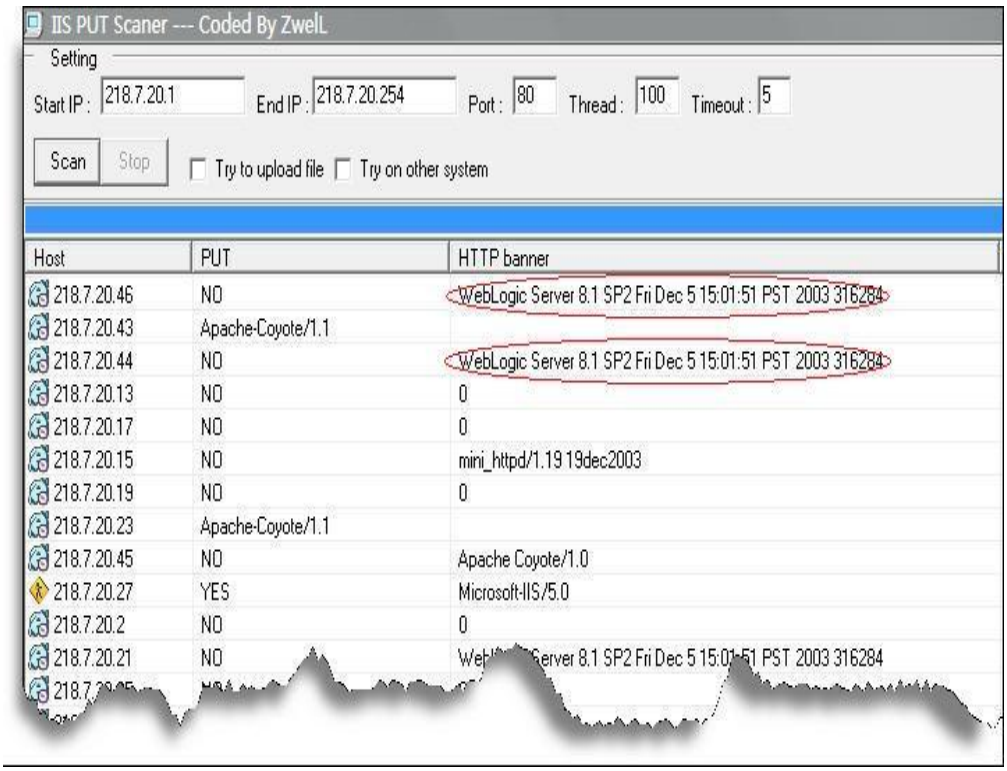
WebLogic 简单抓鸡大法

一、寻找目标

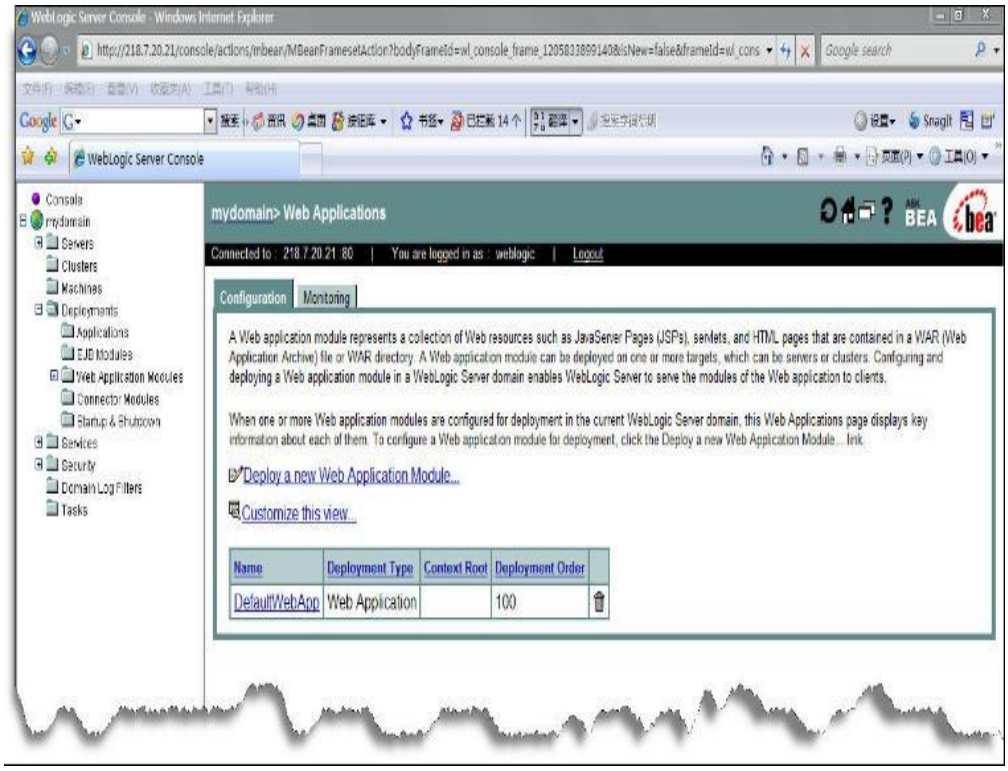
1、批量扫描 WebLogic 缺省的 WEB 管理端口（http 为 7001，https 为 7002），开放这两个端口的一般都是安装有 WebLogic 的主机。
2、Google 搜索关键字“WebLogic Server Administration Console inurl:console”，URL 后面是 console 结尾的，一般为目标。
3、IISput 批量扫描，当发现 HTTP banner 下显示“WebLogic Server”字样的一般为使用 WebLogic 的网站，如图 1。



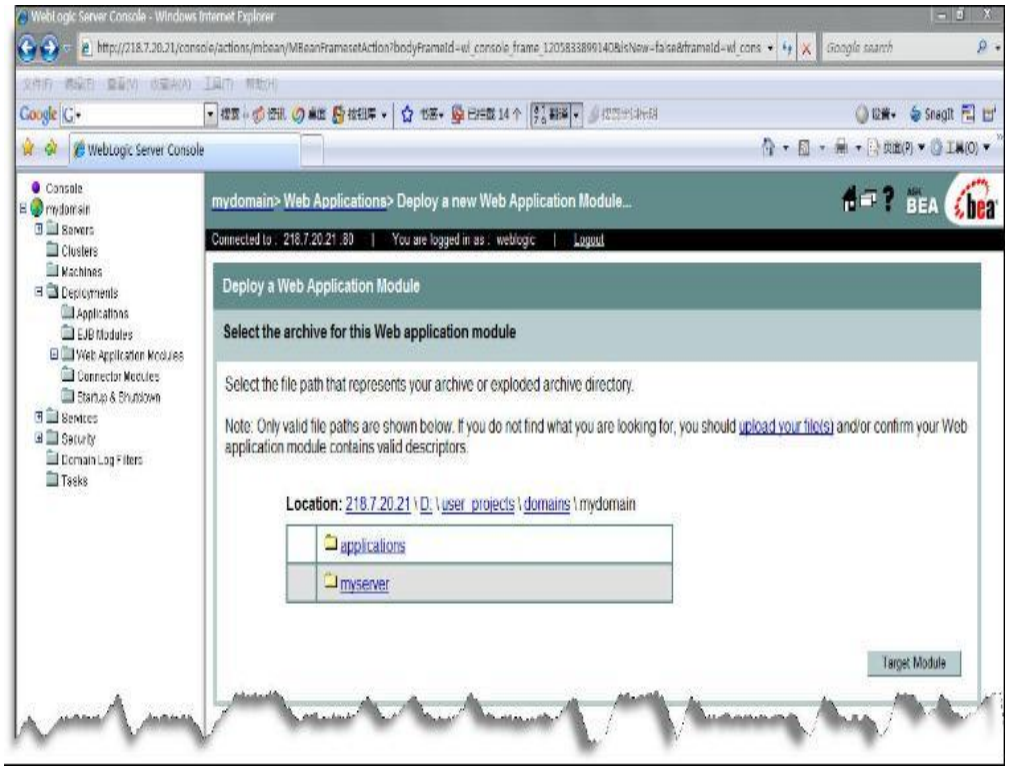
二、默认口令攻击

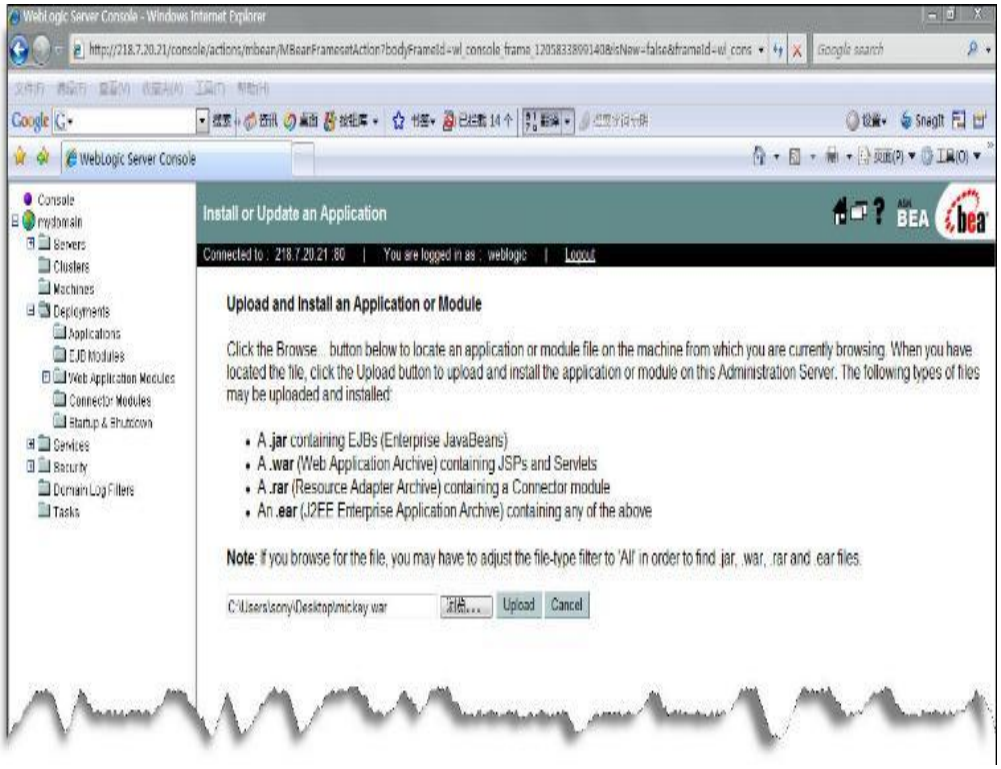
在找到的目标 URL 后面加上 console，回车就会自动跳转到管理登录页面。默认的缺省密码有以下几组：
1、用户名密码均为：weblogic
2、用户名密码均为：system
3、用户名密码均为：portaladmin
4、用户名密码均为：guest
如果尝试完了都不能登录，可以交叉换用用户名和密码，比如用户名为 weblogic，密码为 system，这个可以自己灵活变通，当然也可以做个字典文件暴破。示例目标的用户名密码均为 weblogic，分别在 Username 和 Password 填入 weblogic，即可进入管理后台（需要安装 jre，否则看不到正面介绍的内容），如图 2。

然后找到“mydomain”->“Deployments”->“Web Application Modules”->“Deploy new Web Application Moudule...”，如图 3。



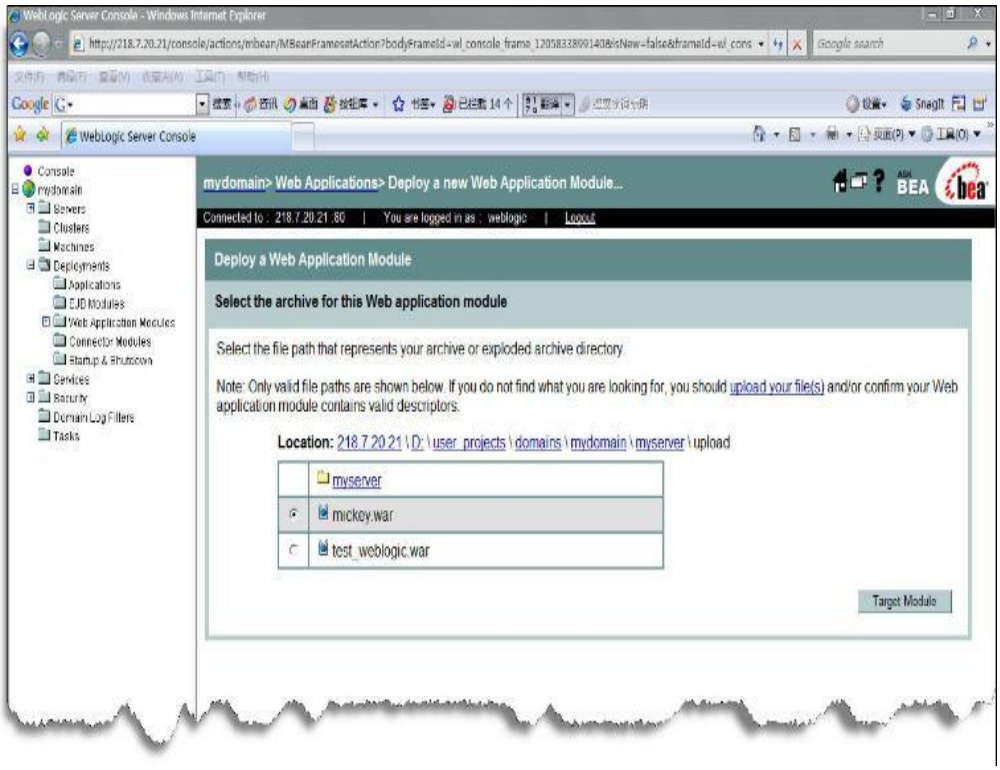
再点选图 4 里的“upload your file(s)”，在跳转后的页面上传 war 包（war 包和 Tomcat 弱口令利用的包一样，注意马的免杀即可），如图 4、图 5。

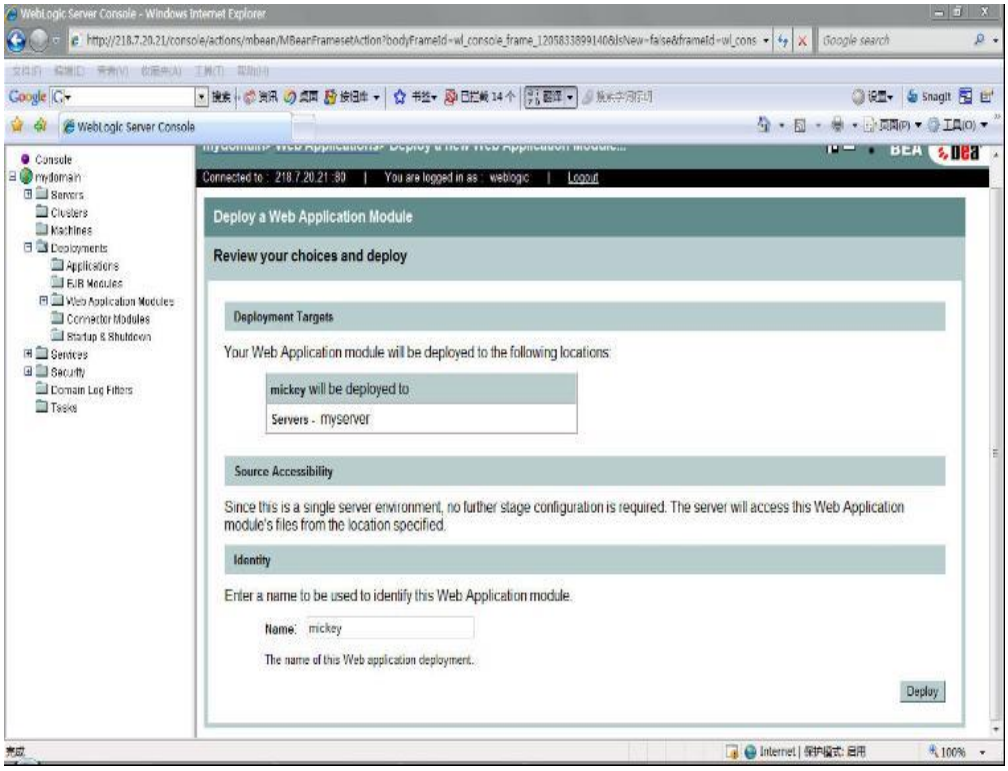




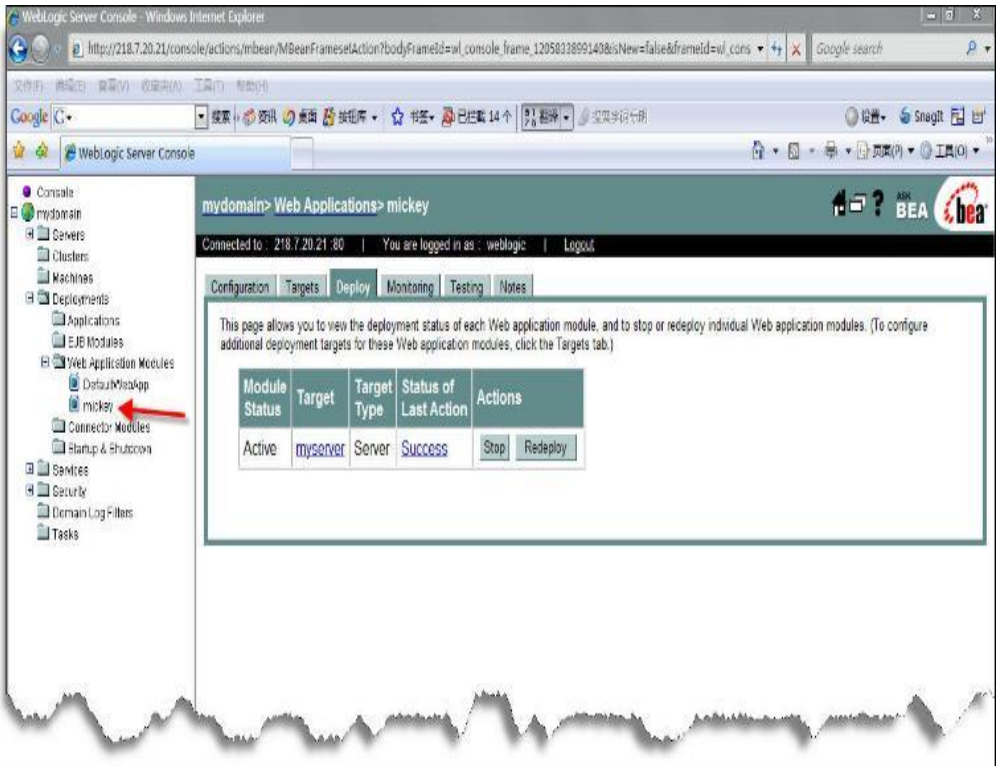
然后在 upload 目录下找到刚才上传的 mickey.war 并选中，再点击“Target Module”

，然后“Deploy”，如图 6、图 7。

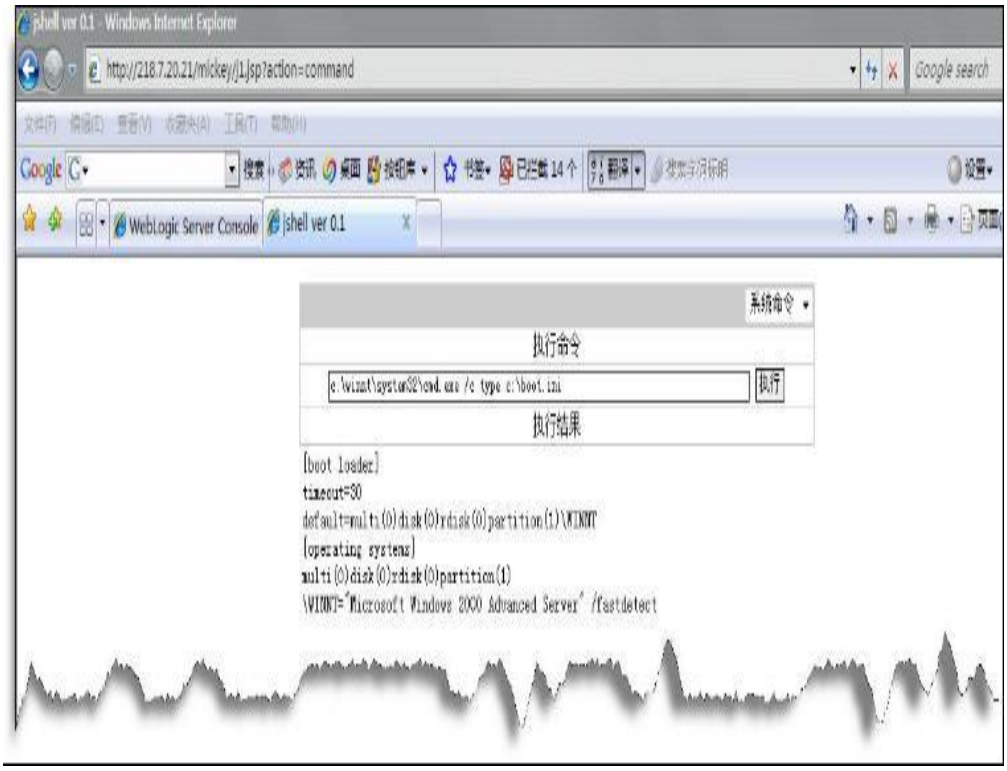


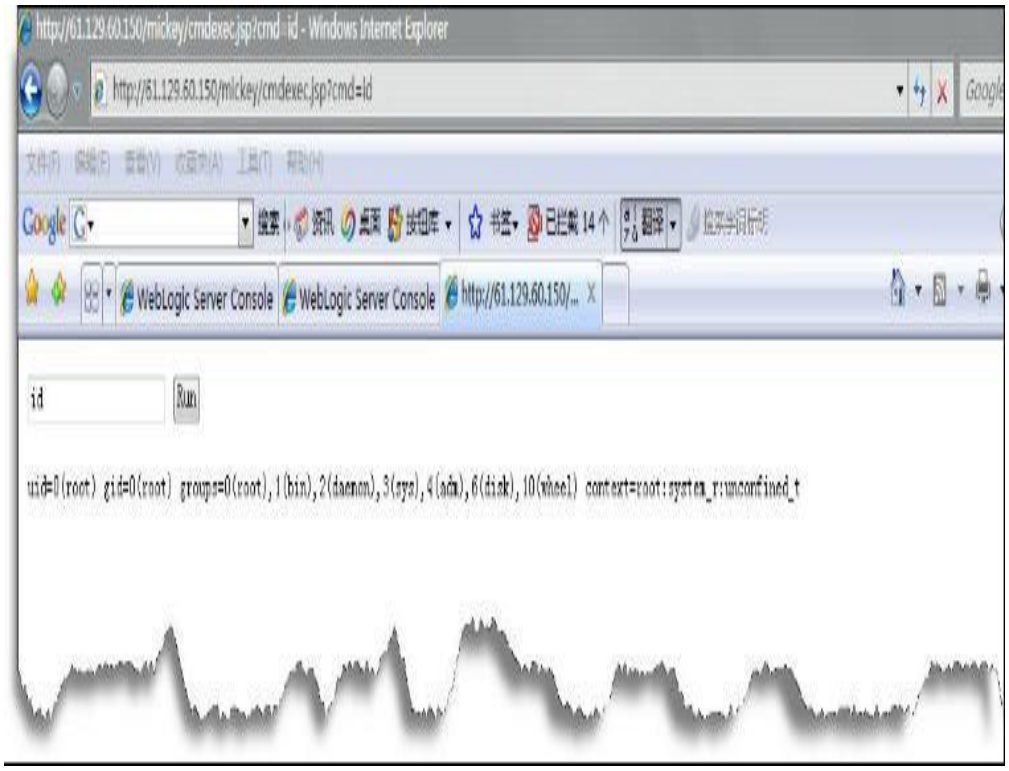


部署完毕后就会在“Web Application Modules”下面看到 mickey 项，如图 8。



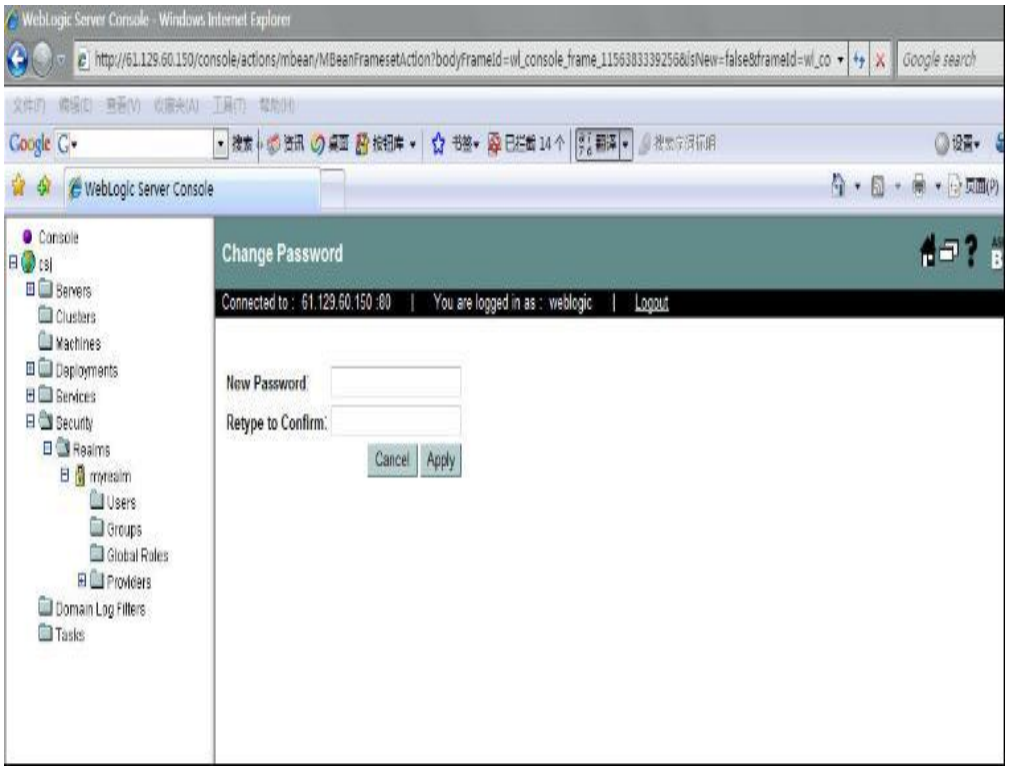
最后就可以访问 Webshell 了，URL 格式为：http://www.xxx.com/mickey/j1.jsp（j1.jsp 为 JSP 后门文件名，这个是在 war 包里面设置的），Windows 系统下为 system 权限，Unix/Linux 下为 root 权限，如图 9、图 10。





三、攻击防范

可以防火墙设置过滤 7001、7002 端口，也可以设置只允许访问后台的 IP 列表，如果非要远程管理 WebLogic，就要设置一个比较强壮的密码口令。点击“Security”->“myrealm”->“Users”->“要更改密码的用户名”，然后在“New Password”填入新密码，在“Retype to Confirm”再次填入新密码，然后“Apply”即可更改密码，如图 11。



四、补充知识

在 Unix/Linux 系统环境下，按上述方法得到的 JSP Webshell 的文件列表功能不可用。除非文件位于 war 包之外，也就是说可以把 war 包内的 JSP 木马复制到 Web 服务器的另一个单独的目录里即可正常使用。