## C:\资料夹\Computer\网站\logo\login.png

Silic Webshell V5.1 使用手册

Silic Group Hacker Army后门管理程序

欢迎使用Silic Group Hacker Army开发的Web安全测试程序

本程序基于php开发和运行，代码行数2210 lines, 程序大小134KB(占用空间136KB)，本程序未加密，无后门。请将本脚本置于支持php的目录并访问运行，默认密码为Silic，首字母大写。

目录

**1) 主界面 - 登陆**

**2) 文件管理**

**2) 命令执行**

**3) 扫描端口**

**4) 系统信息**

**5) MySQL执行模块**

**5) MySQL管理**

**6) PostgreSQL**

**7)其他数据库**

**8) 扫描木马**

**9) 搜索文件**

**10) 批量替换**

**11) Serv-U提权**

**12) Win组件**

**13) 反弹连接**

**14) 执行php代码**

**15) ZIP解压**

**16) 一句话服务端小马集成**

**17) 密码修改**

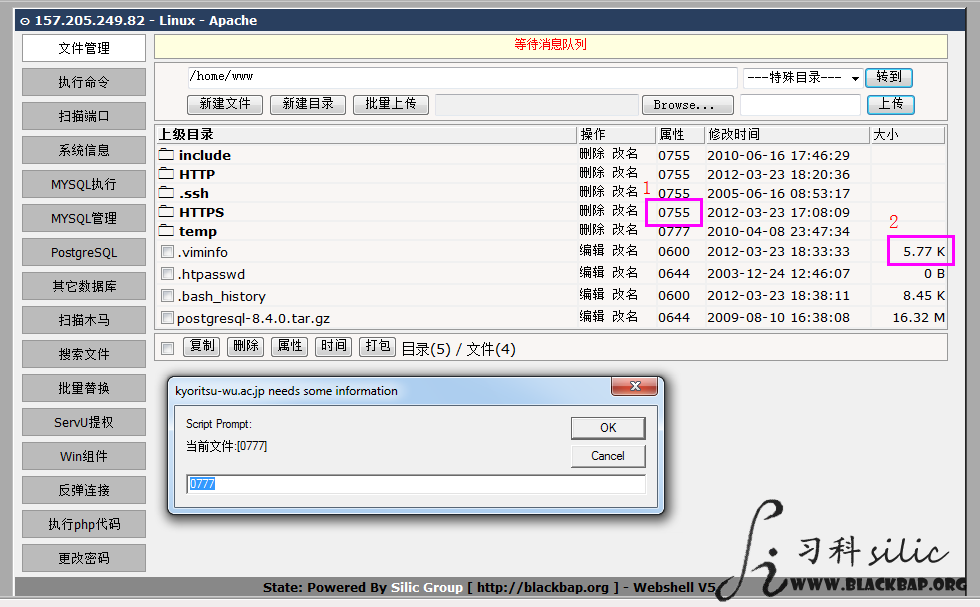
1) 主界面 - 登陆

这个没什么好说的，输入对了密码就OK了，默认密码Silic

程序采用三层MD5+Salt加密，Session验证二次MD5加密，大可不必担心被人社工

2) 文件管理

这个功能也不必多说，会用鼠标的人都会用



不过这里讲一下两个比较隐蔽的功能，第一个是图中1示中，点击文件夹的“属性”，如果有权限的话可以更改目录属性，例如0777，例如0555。

当然，有权限的情况是极少数。

第二点就是单一文件下载功能，很多人找不到Spider的单一文件下载，而“打包”又常常出现文件损坏的情况。

点击文件的“大小”就可以下载单一文件啦！

2) 命令执行

这个功能使用了php的几个命令执行函数，除非管理员比较操蛋的把exec(),shell\_exec(),system(),passthru()都禁用了，不然本功能不会失效。

这里功能在默认选项里面配备了了几个常用命令 :-)

3) 扫描端口

设置好端口和ip扫描就好了 —\_—！

ip可以是本机也可以是局域网，广域网没有测试过。

端口列表:ftp-21,ssh-22,tcp-23,25-smtp,http-80,pop3-110,PortMapper-111,

不解释135,139和445,

https-443,mssql-1433,mysql-3306,远程桌面-3389,RAdmin-4899,

PcAnyWhere-5631,PostgreSQL-5432,WebLogic-7001,Tomcat-8000,Tomcat-8080,FileZilla-14147,Serv-U-43958

4) 系统信息

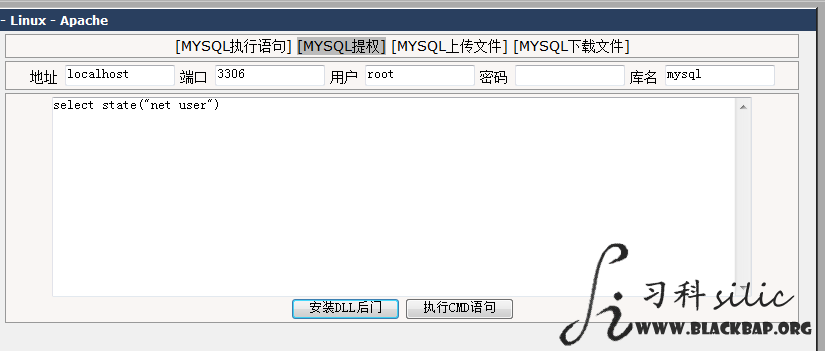
phpinfo看起来太头疼，这个更直观一些。

入侵中主要查看php是否为安全模式，被禁用的函数，是否支持oracle,sqlite,ftp和perl语法等等，以及一些其他探针

5) MySQL执行模块

此模块共分五个功能，分别是常用的MySQL语句执行（这个功能不需要解释）

第二个功能是MySQL提权，这是将以前的模块整合进来的。当然要求是有root权限的MySQL账户



第三个是MySQL脱库功能，一键导出数据库数据。当然，数据库过大很容易导致服务器宕机 :-(



第四个和第五个分别是MySQL上传和下载，可以突破一些IIS+PHP对文件读写的限制。

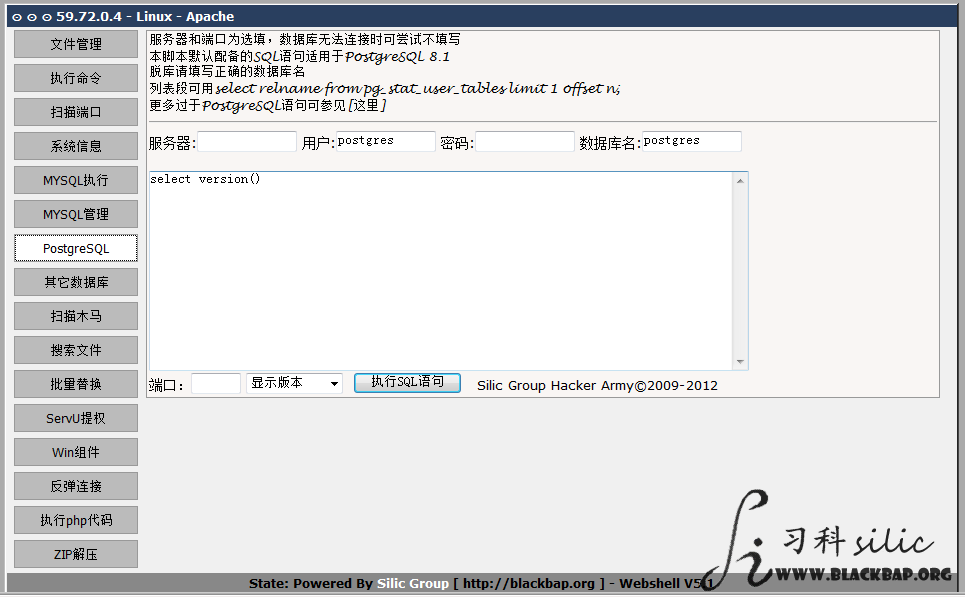
6) MySQL管理

这是一个类似phpMyAdmin的模块，有了这个模块则可以更加方便快捷的修改和操作数据库。

下一版可能会在这里增加数据库导入和备份功能

7) PostgreSQL

因为PostgreSQL在外国网站应用比国内应用的多，考虑到原版的鸡肋和应用的需要，将本功能单独列为一个模块



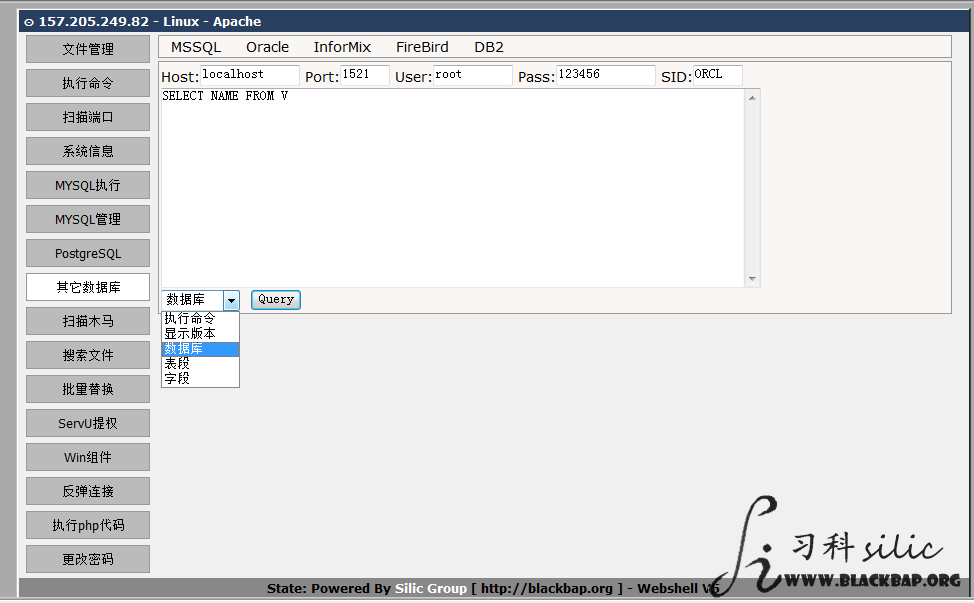
如图中所示，当PostgreSQL无法连接时，并且5432端口确实开放时，可以考虑不填写数据库和端口

默认配备的SQL语句适用于PostgreSQL 8.1，列表段还可以用select relname from pg\_stat\_user\_tables limit 1 offset n;

更多过于PostgreSQL语句可参见<http://nana.blackbap.org/?page=55>

8)其他数据库

这里面的可以操作一些主流的像MSSQL,Oracle数据库，也可以操作InforMix，FireBird，DB2这些非主流的数据库



这些操作里面同样配备了一些常用的SQL语句

9) 扫描木马

这里的扫描木马仅限于扫描脚本后门哈

特征码还不是很完善，但是只有错杀不会漏掉

10) 搜索文件

同扫描木马，是文件读写匹配功能。

这里可以选择匹配正文或者匹配文件名。

11) 批量替换

将批量挂马和批量清马功能删掉了，只保留这一个功能。

上一版本的程序挂马默认地址为blackbap.org/ad.js，鉴于各位童鞋们一不小心就给BlackBap.Org加暗链了

服务器日志显示404的错误记录多数是ad.js，所以这里我们就不在加入习科的连接了。

12) Serv-U提权

这个就不说了，因为真的没什么可说的 :-(

13) Win组件

考虑到实用性，这里我们选取了Wscript和User两个shell组件

两个组件的使用代码都可以在论坛中找到



如程序所诉，Webshell所在服务器必须为Windows系统.

因为PHP提权很灵活，只有你在非常无奈的时候才值得尝试本功能

另外，5.1版更新了一个注册表内容读取功能，有一些Wscript没被禁用的机器可以尝试一下读取注册表



14) 反弹连接

反弹连接模块由linux反弹和windows反弹两部分组成



linux反弹则有perl和C两种选择，windows则为socket一种

linux的反弹脚本可以在本论坛的linux版块中找到，而socket的反弹源码也可以在本论坛中找到

15) 执行php代码

这个功能则类似于一句话，但是可以自由扩展

16) ZIP解压

本模块使用PHP的zip\_open扩展来操作ZIP压缩文件，使用前请在【系统信息】中确认系统支持php\_zip

压缩文件路径可写下级目录和物理路径，相对目录是否可操作未测试 :-(

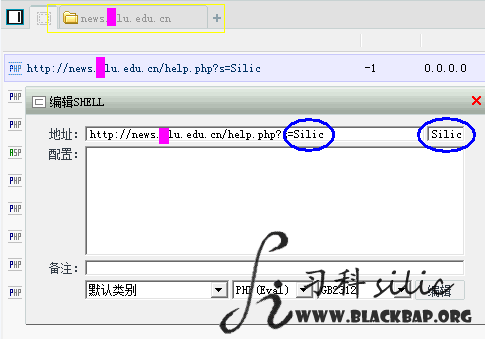


确认目标路径可写以后就可解压服务器上的ZIP文件

17) 一句话服务端小马集成

这个功能将大马小马集于一身，方便用菜刀管理

菜刀设置如下：



配置地址：“http://webshell.url/.php?s=你的密码”

配置密码：你在程序中设置的密码

例如xx.com/xx.php?s=Silic，连接密码也为Silic

一句话服务端功能使用assert函数，需要验证登陆密码(既?s=密码)没有后门，请放心

18) 密码修改

这个功能不错吧 :-D

只不过按钮隐蔽了一点，按钮在顶部导航，看图右上角的小圆X



不用去各种地方多层加密MD5，还得加salt各种改 -\_-!~

方便很多啊。改完了需要重新登录 :-)

以前的退出登陆功能也已经换到左上角了，也是一个小圆X，第一个小圆X是退出登陆，第二个是防误点的，第三个是修改密码

这个界面的灵感其实是来自Mac的

下一版可能改进：

完善扫描木马中后门的特征码

将linux的反弹中加入py脚本

\* Silic Group - 技术自由 技术创新 技术共享 技术原创 技术进步

\* [BlackBap.Org](http://blackbap.org)