网站安全狗 Linux 版（Apache）使用手册 v1.0.0

1. 软件说明

网站安全狗 Linux 版（Apache）（英文：SafeDog For Linux Apache）是一款集网站内容安全防护、网站资源保护及网站流量保护功能为一体的服务器工具，为用户在 Internet 的网络服务提供完善的保护，避免 Apache 服务器出现故障以及受到黑客攻击。

2. 软件运行环境

- 软件当前版本支持的 linux 服务器的操作系统包括：centos 5.3，RHEL 5.0，Ubuntu 11.04。其它版本号的支持，未经过完整测试。
- 确保安装有 apache server 2.0 以上版本，否则软件中的功能无效。

3. 软件安装

下载软件的安装包，ApacheSafeDog_v1.0.tar.gz 到 linux 服务器上，以 root 身份进入安装包所在的目录，运行如下命令进行安装：

```
tar xzvf ApacheSafeDog_v1.0.tar.gz
cd ApacheSafeDog_v1.0
chmod +x install.sh
./install.sh
```

运行时会提示输入 apache 服务器的配置文件路径（绝对路径）,请根据您所安装的 apache 的目录，填写真实的配置文件路径。举例：/usr/local/apache2/conf/httpd.conf

注意：

（1）提示：若您在输入时，不慎输入错误，请按组合键 CTRL+Backspace 删除。

（2）网站狗的安装目录为/etc/ApacheSafeDog，请不要删除此目录及目录下的任何内容。

（3）安装完成后，请重新启动 apache 服务器，以使网站安全狗软件生效。

（4）如果重启 apache 服务器时失败，并提示 Permission denied 错误，请参看 7.SElinux 的相关设置

4. 软件卸载

以 root 身份进入网站安全狗的安装目录/etc/ApacheSafeDog。运行如下命令进行卸载：

```
chmod +x uninstall.sh
./uninstall.sh
```

当出现提示：Are you sure to remove ApacheSafeDog?[y/n]时输入 y。

卸载完成后，请重新启动 apache 服务器。

5. 网站安全狗软件功能

修改网站安全狗的配置文件所在目录/etc/ApacheSafeDog/conf 下的配置文件来启用网站安全狗的相应功能。

请注意以下事项：

（1）以下配置文件各字段的值只是举例，请根据您的实际需要自行设定。设定前请参考每个字段前的注释信息。

（2）修改完的配置，会在一分钟后自动生效。如果您需要让其立即生效，请重启 apache 服务器。

（3）白名单和黑名单的优先级高于其他防护，其中白名单又高于黑名单。如果您在设置了某个防护后，发现其未起效等异常，请检查是否是设置了白名单和黑名单导致的。

（4）修改配置中的字段时，请在英文状态下输入，提示信息字段 TipInfo 和正则表达式规则说明字段 Description 除外。

5.1. CC 攻击防护（WPCAntiCC.conf）

[功能说明]

CC 攻击(ChallengeCollapsar)是借助代理服务器生成指向受害主机的合法请求，实现 DOS 和伪装。模拟多个用户不停的进行访问那些需要大量数据操作，大量 CPU 时间的页面，使得页面打开速度缓慢。

CC 攻击防护基本原理是防止一个 IP 多次不断刷新而断开与该 IP 的连接，防止服务器瘫痪，达到了防攻击目的。

[配置说明]

#是否开启防 CC 攻击功能，1 表示开启，0 表示关闭

```
ChkCC=0
```

#CC 攻击者的 IP 冻结时间，以分钟为单位

```
FreezeMinute=1
```

#是否允许代理访问，1 表示允许，0 表示不允许

```
IsAllowProxy=0
```

#是否需要返回提示信息，1 表示允许，0 表示不允许

```
IsTipInfo=1
```

#单 IPGet 方式在规定时间内允许访问页面的次数

```
MaxGetNumber=80
```

#单 IPGet 方式的规定时间

```
MaxGetSeconds=60
```

#单 IP Post 方式在规定时间内允许访问页面的次数

```
MaxPostNumber=20
```

#单 IP Post 方式的规定时间

```
MaxPostSeconds=60
```

#发现代理访问时，发送给浏览器的信息

ProxyTipInfo=本服务器禁止代理访问！

#保护的资源类型，采用如下格式：后缀名丨后缀名丨后缀名，各字符间不要有空格或制表符。最后一个后缀名之后不要包含竖线（|）

#例如：rar|jpg|gif|exe

```
Resource=asp|aspx|cgi|jsp|php
```

#发现被 CC 攻击时，是否将该攻击写入日志，1 表示允许，0 表示不允许

```
SendAlert=1
```

#不受防 CC 攻击规则保护的本服务器上的域名数目,若该字段为 0，则 Site0 等字段就不存在

```
SpeSiteCount=3
```

#定义您的服务器上不受防 CC 攻击规则保护的域名，这里的域名必须与 APACHE 配置的 serverName,ServerAlias 字段所设的字段匹配。

#填写以下字段时请注意字段名末尾的数字：Site**0**，Site**1**，Site**2**。请严格按照此规则定义字段名字。

#举例：如果你只有一个 site 需要定义，则字段名应为：Site**0** ，如果你有四个 site 需要定义，则字段名应

#为：Site0，Site1，Site2，Site3.

#这里的站点必须是本服务器上的站点。

```
Site0=www.test1.com
Site1=www.test2.com
Site2=www.test3.com
```

#发现 CC 攻击时，发送给浏览器的信息

```
TipInfo=您的请求过于频繁，谢谢合作！
```

[验证生效方法]

如果你开启了防 CC 攻击功能，并且有客户端（浏览器）在访问您的网站时，违反了您所设定的规则，服务器会阻止访问并返回您所设定的提示信息。

5.2. 网站资源防盗链功能（WPCLinkGate.conf）

[功能说明]

盗链是指服务提供商自己不提供服务的内容，通过技术手段绕过其它有利益的最终用户界面(如广告)，直接在自己的网站上向最终用户提供其它服务提供商的服务内容，骗取最终用户的浏览和点击率。受益者不提供资源或提供很少的资源，而真正的服务提供商却得不到任何的收益。

本程序通过 Reference 技术和 Session 技术解决防盗链问题。Reference 技术通常用于图片、mp3 等资源这种容易被人用 html 嵌入到其他网站资源的资源。Session 技术一般只用于论坛和社区网站。

两种防护方式：

（1）引用（Reference）方式：是通过判断 referer 变量的值来判断图片或资源的引用是否合法，只有在设定范围内的 referer，才能访问指定的资源，从而实现了防盗链的目的。Reference 方式能够让本域名和其他指定信任域名正常链接被保护资源。该技术主要用来保护下载类资源，如 rar，jpg 等

（2）会话（Session）方式：先从客户端获取用户信息，然后根据这个信息和用户请求的文件名字一起加密成字符串(Session ID)作为身份验证。只有当认证成功以后，服务端才会把用户需要的文件传送给客户。一般我们会把加密的 Session ID 作为 URL 参数的一部分传递给服务器，由于这个 Session ID 和用户的信息挂钩，所以别人就算是盗取了链接，该 Session ID 也无法通过身份认证，从而达到反盗链的目的。这种方式对于分布式盗链非常有效。该技术主要用来保护影音资源，如 mp3，flv 等

[配置说明]

#是否开启防盗链功能，1 开启，0 关闭

```
ChkLinkGate=1
```

#引用方式

#referenc 校验设置：状态（0 不启用 1 启用）

```
Reference=1
```

#referenc 校验：本域名信任（0 关闭 1 开启）

```
RLocalSite=1
```

#referenc 校验：其他域名信任（0 关闭 1 开启）

```
ROtherSite=1
```

#其他信任域名列表个数，若为 0，则 TSite0 等字段不存在

```
TrustCount=2
```

#其他信任域名列表，这里的本机网站域名必须与 APACHE 配置的 serverName,ServerAlias 字段所设的字段匹配，格式为:本机网站域名，本机网站域名，本机网站域名…;信任域名,信任域名…,注意：多个本机网站域名之间用英文逗号隔开（这些本机网站域名指的是同一个网站的多个域名），多个信任域名之间也用英文逗号隔开。“本机网站域名”和“信任域名”之间用英文分号隔开。最后一个本机网站域名和最后一个信任域名之后不包括逗号（,）。

#填写以下字段时请注意字段名末尾的数字：TSite**0**，TSite**1**，TSite**2**。请严格按照此规则定义字段名字。

#举例：如果你只有一个 site 需要定义，则字段名应为：TSite**0** ，如果你有四个 site 需要定义，则字段名应为：TSite**0**，TSite**1**，TSite**2**，TSite**3**.

```
TSite0=www.test1.com,www.test1-1.com;www.google.com.hk,www.baidu.com
TSite1=www.test2.com;www.sina.com,www.sohu.com
```

#引用方式保护的资源类型，格式为：后缀名|后缀名|后缀名，各字符间不要有空格或制表符。最后一个

后缀名之后不要包含竖线（|）

#例如：rar|jpg|gif|exe

```
Resource=rar|jpg
```

#不受引用方式防盗链规则保护的本服务器上的域名数目，若为 0，则 Site0 等字段不存在

```
SpeSiteCount=1
```

#不受引用方式防盗链规则保护的域名，这里的站点必须是本服务器上的站点。域名必须与 APACHE 配置的 serverName,ServerAlias 字段所设的字段匹配

```
Site0= www.test3.com
```

#会话方式

#session 方式校验：状态（0 不启用 1 启用）

```
Session=1
```

#session 校验：本域名信任（0 关闭 1 开启）

```
SLocalSite=1
```

#设置校验的用户名

```
Name=name
```

#设置校验的密码

```
Password=password
```

#客户端校验行为：1 基于浏览器内存方式 2 基于文件方式

```
Browser=1
```

#session 有效时间，单位为分钟

```
TimeOut=10
```

#会话方式保护的资源类型，格式为：后缀名丨后缀名丨后缀名，各字符间不要有空格或制表符。最后一个后缀名之后不要包含竖线（|）

```
SResource=mp3|flv
```

#不受会话方式防盗链规则保护的本服务器上的网站个数

```
SSpeSiteCount=1
```

#不受会话方式防盗链规则保护的域名，这里的站点必须是本服务器上的站点。

```
SSite0=www.test4.com
```

#发现盗链时，是否将该攻击写入日志（0 否 1 是）

```
SendAlert=1
```

#发现被盗链的时，返回给客户端的信息

```
TipInfo=您请求的资源受到防盗链保护，谢谢合作！
```

[验证生效方法]

如果你开启了网站资源防盗链功能，并且有客户端（浏览器）在访问您的网站时，违反了您所设定的规则，服务器会阻止访问并返回您所设定的提示信息。

5.3. 网站特定资源防下载功能（WPCRejectDown.conf）

[功能说明]

网站特定资源保护通过对某些特定资源的设置来确保它们不被下载或盗用

注意：填写的路径（Path）和保护资源类型（Resource）中只要客户端的访问条件满足其中一种都会被拦截

[配置说明]

#是否开启防下载功能，1 表示是，0 表是否

```
ChkRejectDown=1
```

#禁止下载的路径规则数,

```
PathCount=3
```

#禁止下载的路径，格式：本服务器上的域名(或物理路径)/文件夹名称;类型,其中"类型"为：1 表示物理路径，2 表示网络路径，本机网站域名必须与 APACHE 配置的 serverName,ServerAlias 字段所设的字段匹配。

#填写以下字段时请注意字段名末尾的数字：Path**0**，Path**1**，Path**2**。请严格按照此规则定义字段名字。

#举例：如果你只有一个 site 需要定义，则字段名应为：Path**0** ，如果你有四个 site 需要定义，则字段名应为：Path**0**，Path**1**，Path**2**，Path**3**.

#为：Path**0**，Path**1**，Path**2**，Path**3**.

```
Path0=www.test1.com/database;2
Path1=www.test2.com/database;2
Path2=/etc/apache/htdocs/discuz/data;1
```

#保护的资源类型，格式为：后缀名|后缀名|后缀名，各字符间不要有空格或制表符 ，最后一个后缀名之后不要包含|号。例如：rar|jpg|gif|exe

```
Resource=mdb|dll
```

#发现文件被非法下载时，是否将该攻击写入日志，1 表示是，0 表是否

```
SendAlert=1
```

#发现文件被非法下载时，发送给浏览器的信息

```
TipInfo=您请求的资源禁止访问，谢谢合作！
```

[验证生效方法]

如果你开启了特定资源防下载功能，并且有客户端（浏览器）在访问您的网站时，违反了您所设定的规则，服务器会阻止访问并返回您所设定的提示信息。

5.4. SQL 防注入功能（WPCDefSql.conf）

[功能说明]

SQL 注入英文名叫 SQL Injection，是存在于应用程序数据库层的安全漏洞。攻击者利用这个漏洞在输入的资料字串中夹带 SQL 指令。一旦应用程序忽略了检查，这些夹带进去的指令就会被数据库服务器误认为正常的 SQL 指令而执行，从而导致数据库结构以及系统资料外泄，最终使系统遭到破坏。

网站安全狗的设计是根据攻击特征库，对用户输入进行过滤，从而达到防护 SQL 注入的目的。

此功能中用户可以根据实际需要对过滤规则进行新增、修改、删除。

[配置说明]

#是否开启防注入功能（1 开启，0 关闭）

```
ChkSqlAttackStatus=1
```

#发现被注入时，是否将该攻击写入日志（1 发送，0 不发送）

```
SendAlert=1
```

#手动在线更新 SQL 规则地址

```
UpdateUrl=http://www.safedog.cn/upload/configFile/sqlRule.dat
```

#防 sql 注入正则表达式规则数

```
Count=5
```

#检测 Cookie 内容是否用第 0 条正则表达式

```
CheckCookie0=1
```

#检测 Post 内容是否用第 0 条正则表达式

```
CheckPost0=1
```

#检测 URL 内容否用第 0 条正则表达式

```
CheckUrl0=1
```
#第 0 条正则表达式规则
```
Sql0=;{0,1}'{0,1}\){0,1}(\+| )*\b(and|or)\b(\+| )+.*(=|<|>).*
```
#对第 0 条正则表达式规则的说明。这个字段是为了向用户说明该正则表达式的用途，安全狗程序不会使用
#该字段，故该字段可有可无，但建议用户在新建一个正则表达式时都添加该字段，方便理解和记忆。
```
Description0=防止 and or 方式注入
```

#检测 Cookie 内容是否用第 1 条正则表达式
```
CheckCookie1=1
```
#检测 Post 内容是否用第 1 条正则表达式
```
CheckPost1=1
```
#检测 URL 内容否用第 1 条正则表达式
```
CheckUrl1=1
```
#第 1 条正则表达式规则
```
Sql1=\b(create|drop|backup)\b(\+| )+\bdatabase\b(\+| )+\w*
```
#第 1 条正则表达式的说明
```
Description1=防止对数据库进行创建、删除、备份操作
```

```
CheckCookie2=1
CheckPost2=1
CheckUrl2=1
Sql2=\b(drop|truncate|create)\b(\+| )+\btable\b(\+| )+\w*
Description2=防止对数据库进行删除、创建表操作
```

```
CheckCookie3=1
CheckPost3=1
CheckUrl3=1
Sql3=\bdbo\.\w+
Description3=防止数据库系统的存储过程被执行
```

```
CheckCookie4=1
CheckPost4=1
CheckUrl4=1
Sql4=\bdeclare\b(\+| )+.+
Description4=防止注入存储过程
```
#是否检测 URL 路径长度（1 是，0 否）
```
ChkUrlLenStatus=1
```
#URL 路径最长的长度
```
MaxUrlLen=16385
```
#发现被注入时，发送给浏览器的信息
```
TipInfo=您的请求带有不合法的参数，谢谢合作！
```

[验证生效方法]

如果你开启了 SQL 防注入功能，并且有客户端（浏览器）在访问您的网站时，违反了您所设定的规则，服

务器会阻止访问并会返回您所设定的提示信息。

5.5. IP 白名单（WPCWhiteIP.conf）

[功能说明]

IP 白名单设置可以通过设置一些值得信赖的 IP 地址为白名单地址，从而使它们能够顺利地访问网站

注意：IP 白名单的优先级比 IP 黑名单的高

[配置说明]

#是否开启允许白名单 IP 功能，1 表示开启，0 表示关闭

```
ChkWhiteIP=1
```

#是否允许爬虫网站功能，1 表示允许，0 表示不允许

```
AllowSpider=1
```

#搜索引擎爬虫的关键字数量，若个数为 0，则 SpiderKey0 等字段不存在

```
SpiderCount=8
```

#搜索引擎爬虫的关键字

```
SpiderKey0=baiduspider+
SpiderKey1=googlebot/
SpiderKey2=iaskspider/
SpiderKey3=msnbot/
SpiderKey4=sogou push spider/
SpiderKey5=sogou web spider/
SpiderKey6=yahoo! slurp
SpiderKey7=yodaobot/
```

#白名单 IP 段的个数，若个数为 0，则 WhiteIP0 等字段不存在

```
WhiteIPCount=3
```

#白名单 IP 段，格式为：IP,子网掩码:IP 段开始-IP 段结束

```
WhiteIP0=172.25.31.35,255.255.255.255:172.25.31.35-172.25.31.35
WhiteIP1=192.168.12.12,255.255.255.252:192.168.12.13-192.168.12.14
WhiteIP2=12.25.31.25,255.255.255.240:12.25.31.17-12.25.31.30
```

[验证生效方法]

如果你将某个 IP 添加进了白名单，即使客户端（浏览器）在访问您的网站时，违反了您所设定的防护规则，服务器也会允许此行为。

5.6. IP 黑名单（WPCBlackIP.conf）

[功能说明]

IP 黑名单设置可以通过设置一些不良 IP 地址为黑名单地址，从而限制它们访问网站。

[配置说明]

#是否开启拦截黑名单 IP 功能（1 开启，0 关闭）

```
ChkBlackIP=0
```

#发现黑名单访问时，是否将该攻击写入日志（1 开启，0 关闭）

```
SendAlert=1
```

#黑名单 IP 段的个数，若个数为 0，则 BlackIP0 等字段就不存在

```
Count=3
```

#黑名单 IP 段,格式为：IP,子网掩码:IP 段开始-IP 段结束

```
BlackIP0=192.168.3.23,255.255.255.255:192.168.3.23-192.168.3.23
BlackIP1=10.23.45.44,255.255.255.224:10.23.45.33-10.23.45.62
BlackIP2=175.62.6.32,255.255.255.248:175.62.6.33-175.62.6.38
#发现黑名单访问时，发送给浏览器的信息
TipInfo=请不要进行不合法的请求，谢谢合作！
```

[验证生效方法]

如果你将某个 IP 添加进了黑名单，该 IP 在访问您的网站时，服务器会阻止访问并返回您所设定的提示信息

5.7. 防护日志设置（WPCLog.conf）

[功能说明]

网站安全狗会将其防护攻击的日志写入其安装目录下的 Analysis/SynSvr.dat 数据库。

[配置说明]

```
#日志保存天数
SaveDays=30
```

5.8. 防护总开关设置（WPCGeneralDefInfo.conf）

[功能说明]

该文件是网站安全狗防护功能的总开关。

注意：如果关闭总开关，网站安全狗所有防护功能均失效。

[配置说明]

```
[GeneralInfo]
#这里必须要保持两个字段都为 1，总开关才能开启，若其中一个为 0，或两个都为 0 时，总开关都会关闭。
Switch=1
SynServerStatus=1
```

6. 日志查看工具——sdalog

[功能说明]

sdalog 工具可以从安装目录下的 Analysis/SynSvr.dat 数据库中读取日志并展示给用户。

支持分时间段查询，分类型查询，将查询结果输出到文件。

[使用说明]

(1)在 linux 的 shell 终端中运行 sdalog 命令，并带上相应参数。参数说明如下：

(a)`sdalog --help` 或 `sdalog -h`

该命令可以在线查看 sdalog 的帮助信息

(b)`sdalog --file` 或 `sdalog -f`

该命令将在网站安全狗的安装目录下新建一个.log 文件，文件的名称是当前时间。并将查询到的防护记录存放到该文件中。

(c) `sdalog --time=2011-10-12-07:45:42/2011-12-30-22:32:10`

该命令将会查询并显示 2011-10-12-07:45:42 到 2011-12-30-22:32:10 之间的防护记录

该参数的格式为：sdalog --time=起始时间/结束时间 （查询“起始时间”到“结束时间”之间的记录）

sdalog --time=起始时间/ （查询“起始时间”之后的所有记录）

sdalog --time=/结束时间 （查询“结束之间”之前的所有记录）

时间格式：YYYY-MM-DD-HH:MM:SS （如：2011-06-20-15:22:59）

也可以省略掉后面的时间，但至少保留年份。这个格式会将后面省略掉的时间默认为最小。如：

YYYY-MM （如：2011-07，这个等同于：2011-07-01-00:00：00）

YYYY （如：2011，等同于：2011-01-01-00:00:00）

YYYY-MM-DD-HH （如：2010-08-12-18，等同于：2010-08-12-18:00:00）

(d) sdalog –-type=all

该命令将查询所有类型的防护记录

该命令的格式为：sdalog –-type=类型

“类型”为下面其中一项：

all	(所有类型)
inject	(SQL 防注入防护记录)
link	(防盗链防护记录)
dl	(防下载防护记录，dl 即 download)
cc	(cc 防护记录)
blackip	(IP 黑名单防护记录)

(2).参数–-time 和–-type 以及-f 可以组合使用。

如果参数中不带–-time 参数，则默认为查询所有时间的记录。

如果参数中不带–-type 参数，则默认为查询所有类型的记录。

如果参数中不带-f 或–-file 参数，则默认将查询结果输出到终端。

举例：直接运行命令 sdalog，不带任何参数，表示查询所有时间所有类型的防护记录，并向结果输出到终端。

(3).输出到终端时，每一栏都有固定的宽度，如果结果很乱，请将终端设置为全屏。如果某一栏的记录超过固定宽度，则会被截断，剩余的部分用省略号代替。

输出到文件时，每一栏会保留完整结果。

7. SElinux 的相关设置

[说明]

（1）如果您的系统中开启了 SElinux，网站安全狗安装后，重启 apache 时可能会失败，并给出 Permission denied 错误。如下内容是解决此问题的方案，并不是网站安全狗的功能。若您的系统中并没有开启 SElinux，或重启 apache 并没有失败，请略过以下内容。

（2）查看是否开启 SElinux 的命令：getenforce

如果运行结果为 Enforcing，表示 SElinux 正在运行，并会限制相关程序的资源访问权限。

如果运行结果为 Permissive，表示 SElinux 正在运行，但不会限制程序的资源访问权限。

如果运行结果为 Disabled，表示 SElinux 被关闭。

只有在 Enforcing 状态下，重启 apache 时才会报 Permission denied 的错误。请参考如下解决方案。

[解决方案]

解决方案一、关闭 SElinux（推荐）。

打开文件/etc/selinux/config,将 SELINUX=enforcing 改为 SELINUX=disabled，然后重新启动系统。

解决方案二、设置 httpd 对网站安全狗文件的 SElinux 相关访问权限。

在开始之前请确保您已安装了 setroubleshoot 服务,并已经启动了这项服务。

（1）当重启 apache 失败并提示 Permission denied 的错误时，运行命令：

```
cat /var/log/messages|grep setroubleshoot
```

运行结果类似于下边这样：

```
Jan 10 15:09:46 localhost setroubleshoot:SELinux is preventing httpd from loading /usr/lib/libSPModule.so.0.0.0 which requires text relocationl.For complete SELinux messages. run sealert -1 d4365f9-7a80-4928-9dd0-6447aebb0b2b
```

（2）根据上面的输出提示中的 run sealert -1 d4365f9-7a80-4928-9dd0-6447aebb0b2b，运行命令：sealert -1 d4365f9-7a80-4928-9dd0-6447aebb0b2b

（3）上面这条命令的输出结果中会详细描述该错误产生的原因，解决方法及相应的附加信息等内容。您只需按照解决方法中的指示操作即可解决问题。例如：上面的输出结果中会有如下两栏：

```
以下命令将允许这个权限：
chcon -t textrel_shlib_t '/usr/lib/libSPModule.so.0.0.0'
```

你只需运行命令：`chcon -t textrel_shlib_t '/usr/lib/libSPModule.so.0.0.0'`即可。

注意：如果有多个错误，您需要重复步骤(2)和(3)多次。

解决方案三、用命令 `httpd -k restart` 重启 apache。此方案不一定在所有机器上都起用。