nginx安装ngx_lua_waf防护

ngx_lua_waf基于ngx_lua的web应用防火墙，使用起来简单，高性能和轻量级。

♦防止sql注入，本地包含，部分溢出，fuzzing测试，xss,SSRF等web攻击

♦防止svn/备份之类文件泄漏

♦防止ApacheBench之类压力测试工具的攻击

♦屏蔽常见的扫描黑客工具，扫描器

♦屏蔽异常的网络请求

♦屏蔽图片附件类目录php执行权限

♦防止webshell上传

配置方法如下，nginx编译安装可参考https://blog.whsir.com/post-2134.html

1、下载ngx_devel_kit

```
cd /usr/local/src
wget https://github.com/simpl/ngx_devel_kit/archive/v0.3.0.tar.gz
tar zxf v0.3.0.tar.gz
```

2、下载lua-nginx-module

```
wget https://github.com/openresty/lua-nginx-module/archive/v0.10.11.tar.gz
tar zxf v0.10.11.tar.gz
```

3、安装luajit

```
wget http://luajit.org/download/LuaJIT-2.0.5.tar.gz
tar zxf LuaJIT-2.0.5.tar.gz
cd LuaJIT-2.0.5
make
make install
```

4、导入环境变量

```
export LUAJIT_LIB=/usr/local/lib
export LUAJIT_INC=/usr/local/include/luajit-2.0
```

5、编译nginx模块（注意增加模块不需要make install）

```
cd /usr/local/src/nginx-1.12.2
./configure --add-module=/usr/local/src/ngx_devel_kit-0.3.0 --add-
module=/usr/local/src/lua-nginx-module-0.10.11 --with-ld-opt=-Wl,-
rpath,$LUAJIT_LIB
make
mv /usr/local/nginx/sbin/nginx /usr/local/nginx/sbin/nginx.bak
cp objs/nginx /usr/local/nginx/sbin/
systemctl reload nginx
```

```
PS：如果报错
nginx: error while loading shared libraries: libluajit-5.1.so.2: cannot open
shared object file: No such file or directory
```

```
解决方法:
ln -s /usr/local/lib/libluajit-5.1.so.2 /lib64/libluajit-5.1.so.2
```

6、下载ngx_lua_waf

```
cd /usr/local/nginx/conf
wget https://github.com/loveshell/ngx_lua_waf/archive/v0.7.2.tar.gz
tar zxf v0.7.2.tar.gz
mv ngx_lua_waf-0.7.2 waf
```

7、在nginx.conf的http字段内添加以下内容

```
lua_package_path "/usr/local/nginx/conf/waf/?.lua";
lua_shared_dict limit 10m;
init_by_lua_file /usr/local/nginx/conf/waf/init.lua;
access_by_lua_file /usr/local/nginx/conf/waf/waf.lua;
```

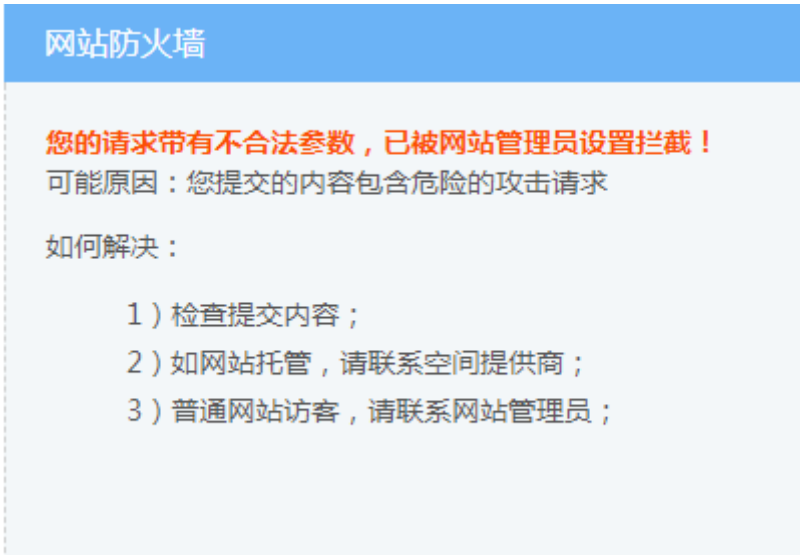
8、最后重启nginx（reload也可以的）

```
systemctl restart nginx
```

9、验证（看到如下图即表示配置成功）

http://域名或IP地址/index.php?id=../etc/passwd

例如：http://192.168.157.132/index.php?id=../etc/passwd




```
config.lua配置文件说明

RulePath = "/usr/local/nginx/conf/waf/wafconf/"
--规则存放目录
attacklog = "off"
--是否开启攻击信息记录，需要配置logdir
logdir = "/usr/local/nginx/logs/hack/"
--log存储目录，该目录需要用户自己新建，切需要nginx用户的可写权限
UrlDeny="on"
--是否拦截url访问（如果你用了phpmyadmin，开启此项会有问题）
Redirect="on"
--是否拦截后重定向
CookieMatch = "on"
--是否拦截cookie攻击
```

```
postMatch = "on"
--是否拦截post攻击（如果开启，可能会导致网站后台无法正常上传文件）
whiteModule = "on"
--是否开启URL白名单
black_fileExt={"php","jsp"}
--填写不允许上传文件后缀类型
ipWhitelist={"127.0.0.1"}
--ip白名单，多个ip用逗号分隔
ipBlocklist={"1.0.0.1"}
--ip黑名单，多个ip用逗号分隔
CCDeny="on"
--是否开启拦截cc攻击(需要nginx.conf的http段增加lua_shared_dict limit 10m;)
CCrate = "100/60"
--设置cc攻击频率，单位为秒.
--默认1分钟同一个IP只能请求同一个地址100次
html=[[Please go away~~]]
--警告内容,可在中括号内自定义
备注:不要乱动双引号，区分大小写
```