nginx+naxsi 配置 WAF

实验环境：CentOS-7.6

下载 nginx 源码：

```
wget http://nginx.org/download/nginx-1.7.9.tar.gz
```

下载 naxsi 源码：

```
git clone https://github.com/nbs-system/naxsi.git
```

安装相关依赖软件包：

```
yum install install -y libpcre3-dev libpcre3 gcc make zlib1g-dev
```

（或者 `apt-get install libpcre3-dev libpcre3 gcc make zlib1g-dev`）

```
yum -y install pcre-devel
```

```
yum install -y zlib-devel
```

解压缩：

```
tar -zxvf nginx-1.7.9.tar.gz -C /usr/local/
```

```
mv naxsi /usr/local/
```

编译：

```
cd /usr/local/nginx-1.7.9/
```

```
./configure --prefix=/usr/local/nginx --add-module=/usr/local/naxsi/naxsi_src
```

（这里注意两个路径：前面的是 naxsi 的位置，后面的是 nginx 预安装位置）

```
make && make install
```

然后在/usr/local/下生成 nginx 文件夹，
生成的可执行文件/usr/local/nginx/sbin/nginx

启动 nginx：

```
/usr/local/nginx/sbin/nginx
```

默认是 80 端口，浏览器访问一下：

nginx 启动相关命令：
nginx 启动
nginx -s reload 重启
nginx -s stop 停止

配置 naxsi 核心文件
拷贝 naxsi 的核心配置文件到 nginx 的配置文件夹下

```
cp /usr/local/naxsi/naxsi_config/naxsi_core.rules /usr/local/nginx/conf/
```

然后 Nginx 反向代理配置：

```
vi /usr/local/nginx/conf/nginx.conf
```

添加这样一行：

```
events {
    worker_connections  1024;
}


http {
    include       mime.types;
    include     /usr/local/nginx/conf/naxsi_core.rules;
    default_type  application/octet-stream;

    #log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
    #                  '$status $body_bytes_sent "$http_referer" '
    #                  '"$http_user_agent" "$http_x_forwarded_for"';

    #access_log  logs/access.log  main;

    sendfile        on;
    #tcp_nopush     on;
-- INSERT --
```

然后创建一个虚拟主机的安全规则文件，这里我命名为 test.rules，创建文件：/usr/local/nginx/conf/test.rules，文件的参考内容如下：

```
#LearningMode; #Enables learning mode
SecRulesEnabled;
#SecRulesDisabled;
DeniedUrl "/RequestDenied";
#include "/tmp/naxsi_rules.tmp";
```

```
## check rules
CheckRule "$SQL >= 8" BLOCK;
CheckRule "$RFI >= 8" BLOCK;
CheckRule "$TRAVERSAL >= 4" BLOCK;
CheckRule "$EVADE >= 4" BLOCK;
CheckRule "$XSS >= 8" BLOCK;
```

然后配置 nginx.conf

```
vi /usr/local/nginx/conf/nginx.conf
```

添加内容如下：

```
server {
    listen       80;
    server_name  localhost;

    #charset koi8-r;

    #access_log  logs/host.access.log  main;

    location / {
        include       /usr/local/nginx/conf/test.conf;
        root   html;
        index  index.html index.htm;
    }

    #error_page  404              /404.html;

    # redirect server error pages to the static page /50x.html
    #
    error_page   500 502 503 504  /50x.html;
```

Location / {}中配置反向代理 web 应用格式如下，我这里就不配置了

```
proxy_pass http://192.168.254.111:80;
```

配置处置结果结果，当阻断攻击时返回 403 状态码（需自己写一个 403.html 放在/usr/local/nginx/html/目录下）

```
    }

    #当检测到攻击时返回响应码
    location /RequestDenied{
        return 403;
    }

    error_page 403 /403.html;
    location = /403.html{
         root /usr/local/nginx/html;
         internal;
    }

    #error_page  404              /404.html;
```

403.html 参考页面：

```
<html>
<head>
<title>Error 403 Request Denied</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>
<body>
<h2>Error 403 Request Denied</h2>
禁止发起攻击！
For some reasons, your request has been denied.
</body>
</html>
```

重启 nginx

```
/usr/local/nginx/sbin/nginx -s reload
```

尝试发起攻击：