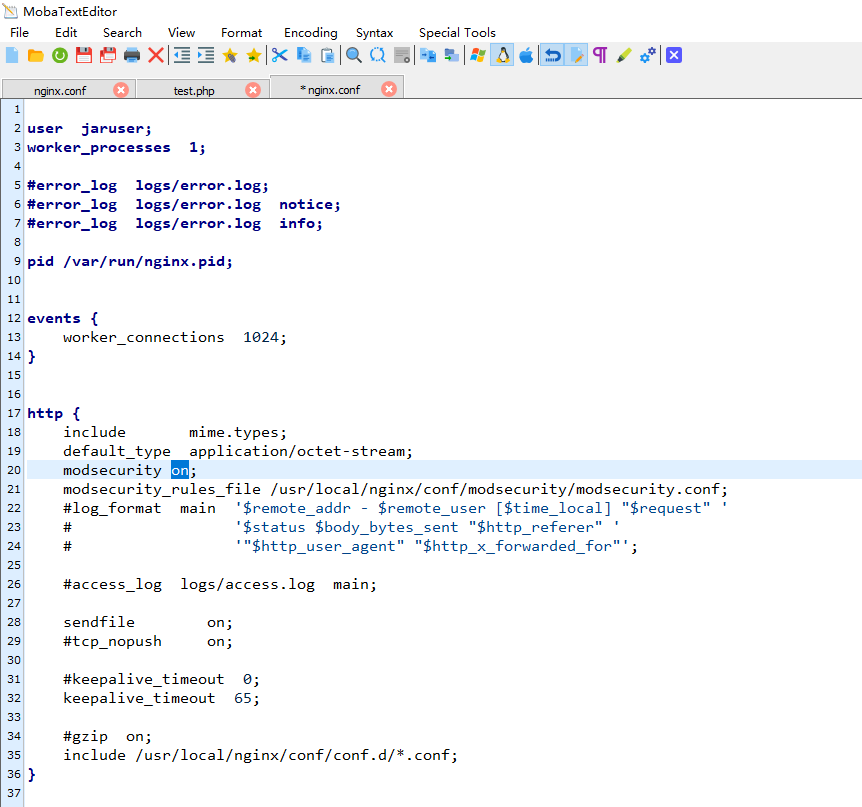
**Nginx+modsecurity**

1. **启用modsecurity**

靶机上的waf(nginx的modsecurity模块)默认没有启用，需要修改nginx的配置文件以后重启nginx

1）配置文件路径：/usr/local/nginx/conf/nginx.conf



上图中的off修改为on

2）/usr/local/nginx/conf/modsecurity/modsecurity.conf中

SecRuleEngine DetectionOnly 改为 SecRuleEngine On

同时，添加

include /usr/local/nginx/conf/modsecurity/crs-setup.conf

include /usr/local/nginx/conf/modsecurity/rules/\*.conf

修改以后需要重新加载，具体命令如下：

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

或者杀掉nginx，然后重新启动进程

1. **Modsecurity的规则路径：**

/usr/local/nginx/conf/modsecurity/modsecurity.conf ，里面包含了下面目录下的规则

/usr/local/nginx/conf/modsecurity/rules

modsecurity.conf中还指定了审计日志的路径：

SecAuditLog /var/log/modsec\_audit.log

1. **modsecurity规则的语法**

SecRule是ModSecurity主要的指令，用于创建安全规则。其基本语法如下：

SecRule VARIABLES OPERATOR [ACTIONS]

* VARIABLES

代表HTTP包中的标识项，规定了安全规则针对的对象。常见的变量包括：ARGS（所有请求参数）、FILES（所有文件名称）等。

* OPERATOR

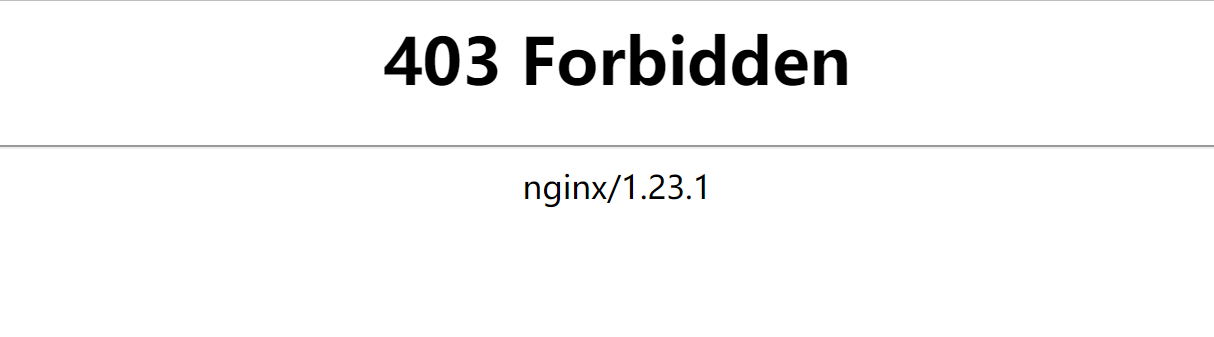
代表操作符，一般用来定义安全规则的匹配条件。常见的操作符包括：@rx(正则表达式）、@streq(字符串相同）、@ipmatch(IP相同）等。

* ACTIONS

代表响应动作，一般用来定义数据包被规则命中后的响应动作。常见的动作包括：deny（数据包被拒绝）、pass(允许数据包通过）、id（定义规则的编号）、severity(定义事件严重程度）等。

修改规则以后，可以运行nginx -t测试规则的语法是否正确。

值得注意的是，如需获取更加深入的语法，请**参考官方手册**。被拦截的实验结果如下图所示：



由上图可知，消息中包含的恶意代码被拦截。

1. **查看WAF拦截日志**

Vim /var/log/ modsec\_audit.log，查看WAF拦截日志.

参考文献：

http://cloud.tencent.com/developer/article/1791249