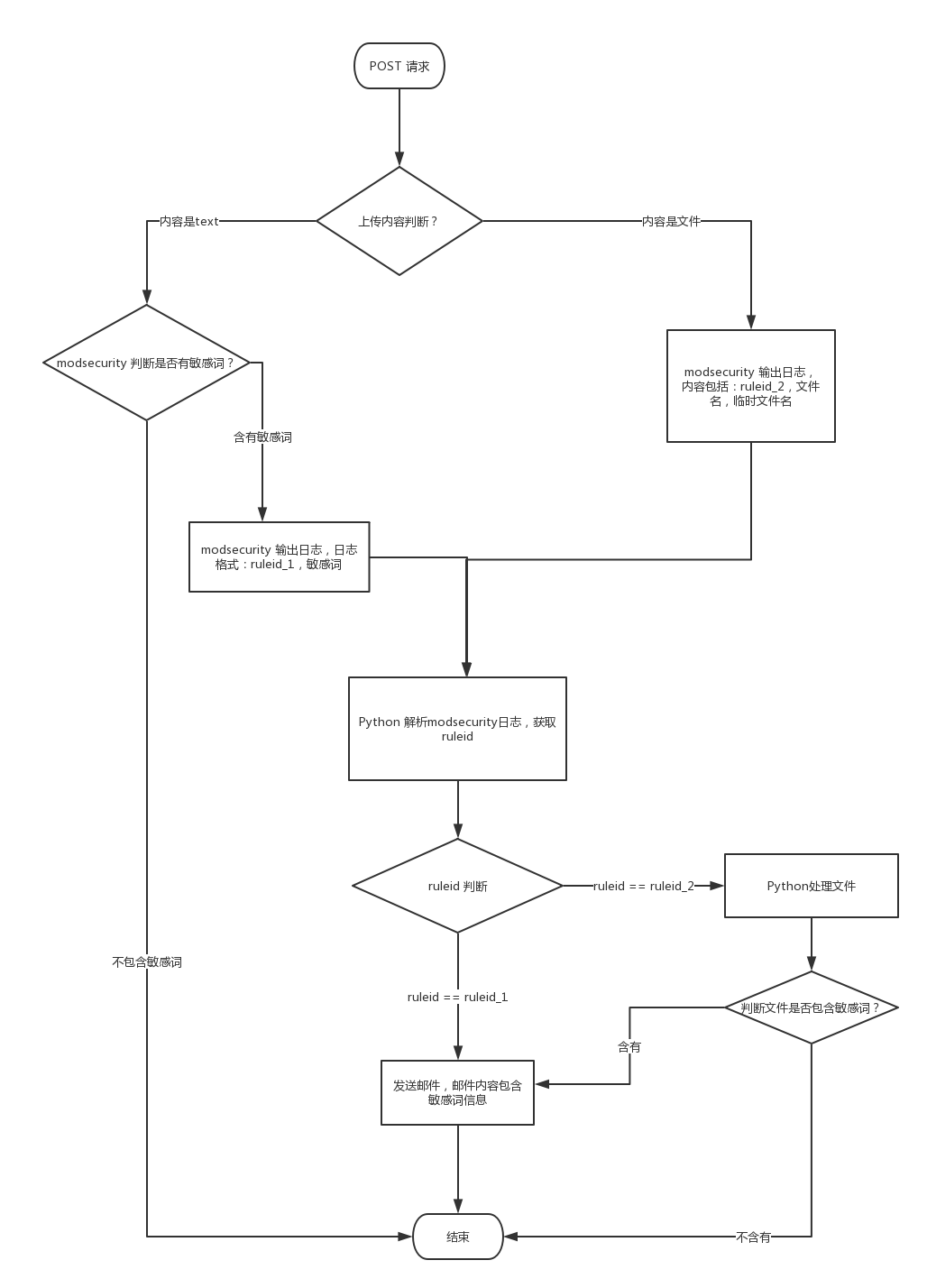
|  |  |  |
| --- | --- | --- |
| 文档说明 | | |
| 时间 | 作者 | 内容 |
| 2017/12/07 | 何梦思 | 添加敏感词警告开发方案 |
|  |  |  |

1. ***关键字告警需求***

|  |
| --- |
| 1.词库管理，敏感词库可检索敏感词 |
| 2.策略管理，检测策略及告警策略 |
| 3.支持文字、图片、压缩包内容的检测 |
| 4.告警方式配置（屏幕信息提示、声音、邮件、短信） |

1. **流程图**



1. **PHP 界面配置**
   1. **PHP 需要提供的字段**

|  |  |  |
| --- | --- | --- |
| 变量 | 类型 | 说明 |
| status | tinyint | 是否开启，0-关闭，1-开启 |
| urls | varchar | 需要防护的url，留空则所有URL，多个则用‘|’分开,如 “/test|/test2” |
| exts | varchar | 需要防护的文件扩展名，留空则为所有文件，多种类型则用‘|’隔开，如 “jgp|tar” |
| words | text | 敏感词，多个敏感词用‘|’隔开，如”法轮功|赌博” |
| content\_size | int | 需要处理的最大文件大小，超过这个阀值，则跳过处理 |
| is\_block | tinyint | 是否阻断，1-阻断，0-不阻断，默认0 |
| alert\_setting | varchar | 告警设置，json格式，interval 邮件发送间隔（单位秒）  {"type":"email","interval":3600,"email":{"receiver":"test@126.com"}} |

* 1. **界面**

3.2.1 添加配置界面，菜单名为“高级设置 => 敏感词告警”，界面参考OCR界面，需要添加邮件发送设置（发送间隔和接受者），如下



3.2.2 添加日志界面，菜单名为“日志报表 => 敏感词告警”，日志显示字段见表logs.t\_words\_monitor

* 1. **数据处理**
     1. **配置文件建表**

DROP TABLE IF EXISTS `waf`.`t\_words\_monitor` ;

CREATE TABLE IF NOT EXISTS `waf`.`t\_words\_monitor` (

`id` int(11) NOT NULL AUTO\_INCREMENT,

`status` TINYINT(1) NOT NULL DEFAULT '1' COMMENT '1-on,0-off',

`urls` varchar(2048) DEFAULT '' COMMENT 'split by | ',

`exts` varchar(500) DEFAULT 'gif|jpg|png|bmp' COMMENT 'split by | , 扩展名',

`words` longtext NOT NULL DEFAULT 'split by |',

`website\_id` int(11) NOT NULL DEFAULT '0' COMMENT 'waf2.6.1 t\_websit',

`content\_size` int(11) NOT NULL DEFAULT '0' COMMENT '',

`is\_block` TINYINT(1) NOT NULL DEFAULT '0' COMMENT '是否阻断，1-阻断，0-不阻断',

`alert\_setting` varchar(255) NOT NULL DEFAULT '' COMMENT '是否阻断，1-阻断，0-不阻断',

`update\_time` datetime NOT NULL DEFAULT CURRENT\_TIMESTAMP ON UPDATE CURRENT\_TIMESTAMP,

PRIMARY KEY (`id`),

UNIQUE KEY `website\_id` (`website\_id`)

) ENGINE=InnoDB AUTO\_INCREMENT=1 DEFAULT CHARSET=utf8;

* + 1. **日志文件建表**

DROP TABLE IF EXISTS `logs`.`t\_words\_monitor` ;

CREATE TABLE IF NOT EXISTS `logs`.`t\_words\_monitor` (

`id` int(11) NOT NULL AUTO\_INCREMENT,

`ruleid` int(11) NOT NULL COMMENT '',

`url` varchar(255) DEFAULT '' COMMENT '触发的url',

`word` varchar(500) DEFAULT '' COMMENT '匹配到的敏感词',

`client\_ip` char(16) NOT NULL DEFAULT '127.0.0.1' COMMENT '',

`client\_port` int(11) NOT NULL DEFAULT '80' COMMENT '',

`server\_ip` char(16) NOT NULL DEFAULT '127.0.0.1' COMMENT '',

`server\_port` int(11) NOT NULL DEFAULT '80' COMMENT '',

`filename` varchar(255) DEFAULT '' COMMENT '文件名',

`tmp\_filename` varchar(255) DEFAULT '' COMMENT '临时文件名',

`file\_size` int(11) NOT NULL DEFAULT '0' COMMENT '文件大小',

`update\_time` datetime NOT NULL DEFAULT CURRENT\_TIMESTAMP ON UPDATE CURRENT\_TIMESTAMP,

PRIMARY KEY (`id`),

) ENGINE=InnoDB AUTO\_INCREMENT=1 DEFAULT CHARSET=utf8;

* + 1. **发送管道**

PHP 将数据写入mysql后，通知Python 重新生成nginx 配置文件，并且重新 reload nginx

1. **Python 处理  
   4.1 添加配置**

Python收到管道消息，从表 `waf`.`t\_words\_monitor` 读取数据生成

conf/activated\_rules/content\_monitor.conf 配置，并将表中words 字段保存到

conf/activated\_rules/modsecurity\_monitor\_scanners.data 中，一行一个敏感词。

在conf/modsecurity.conf 中添加 Include activated\_rules/content\_monitor.conf（在木马扫描配置后添加） ，如下



|  |  |
| --- | --- |
| 修改文件 | 添加内容 |
| conf/modsecurity.conf | SecRequestBodyAccess On  SecResponseBodyAccess On  SecTmpDir /usr/local/bdwaf/logs\_proxy/tmp/  SecDataDir /usr/local/bdwaf/logs\_proxy/tmp/  SecUploadDir /usr/local/bdwaf/logs\_proxy/tmp/  SecUploadKeepFiles On  SecUploadFileMode 0600  Include activated\_rules/content\_monitor.conf |
| conf/activated\_rules/content\_monitor.conf | 通过表`waf`.`t\_words\_monitor`生成模板 |
| conf/activated\_rules/modsecurity\_monitor\_scanners.data | 读取表`waf`.`t\_words\_monitor`的words字段写入 |

**4.2 modsecurity日志处理**

**4.2.1 规则**

|  |  |  |
| --- | --- | --- |
| Ruleid 变量 | 取值 | 处理 |
| ruleid\_1 | 800015 或 **800025** | 发送邮件，看流程图 |
| ruleid\_2 | 800016 | 文件处理，看流程图 |

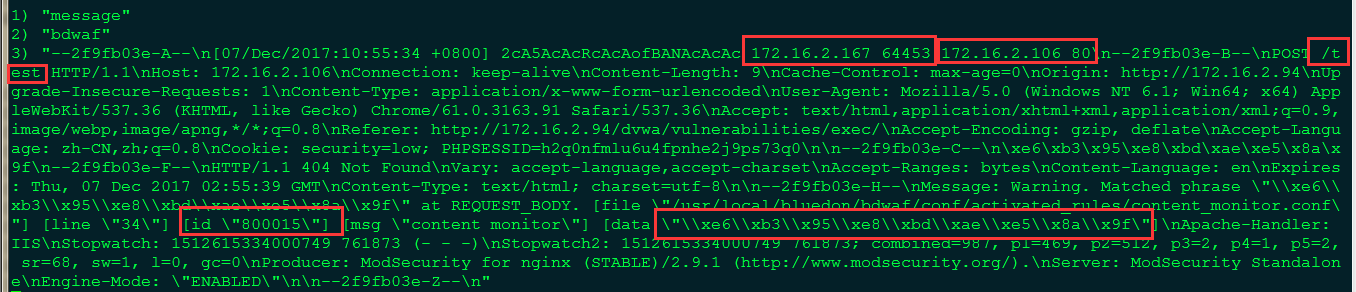
**4.2.2 文件处理**

|  |  |
| --- | --- |
| 压缩文件（tar.gz，tar，zip） | 解压一次，分析加压后的文件内容 |
| 图片文件（png，jpg等） | 通过OCR识别图片内容分析 |
| 文本文件（txt|doc等） | 读取文件分析 |
| 其他(pdf等)暂不处理 |  |

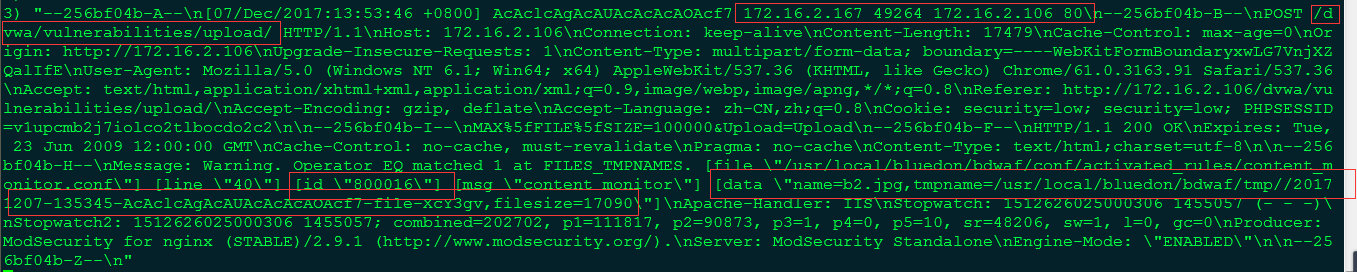
**4.2.3 modsecurity日志入库**

数据存入 `logs`.`t\_words\_monitor` 表中

**4.2.3.1 Ruleid == 800015 或者 Ruleid == 800025 的日志格式**



**4.2.3.2 Ruleid == 800016 的日志格式**



附录：

conf/activated\_rules/content\_monitor.conf

## 敏感词警告

SecAction \

"id:'800010', \

phase:1, \

t:none, \

setvar:'tx.content\_monitor\_urls=', \

setvar:'tx.content\_monitor\_file\_exts=', \

nolog, \

pass"

SecRule REQUEST\_METHOD "!^POST$" "phase:2,id:'800011',t:none,nolog,pass,skipAfter:END\_POST\_CONTENT\_MONITOR\_CHECK"

# 大于 5M 不拦截

SecRule REQUEST\_BODY "@gt 5242880" "phase:2,id:'800012',t:none,nolog,pass,skipAfter:END\_POST\_CONTENT\_MONITOR\_CHECK"

#SecRule &TX:CONTENT\_MONITOR\_URLS "@eq 0" "phase:2,id:'900101',t:none,nolog,pass,skipAfter:END\_POST\_CONTENT\_MONITOR\_CHECK"

#SecRule REQUEST\_FILENAME ".\*" "chain,phase:2,id:'900102',t:none,nolog,pass,setvar:'tx.filename=#%{request\_filename}#',skipAfter:END\_POST\_CONTENT\_MONITOR\_CHECK"

#SecRule TX:FILENAME "!@within %{tx.content\_monitor\_urls}" "t:none"

SecRule TX:CONTENT\_MONITOR\_URLS "!^$" "chain,phase:2,id:'800013',t:none,nolog,pass,skipAfter:END\_POST\_CONTENT\_MONITOR\_CHECK"

SecRule REQUEST\_FILENAME ".\*" "chain,t:none,setvar:'tx.filename=#%{request\_filename}#'"

SecRule TX:FILENAME "!@within %{tx.content\_monitor\_urls}" "t:none"

SecRule TX:CONTENT\_MONITOR\_FILE\_EXTS "!^$" "chain,phase:2,id:'800014',t:none,nolog,pass,skipAfter:END\_POST\_CONTENT\_MONITOR\_CHECK"

SecRule FILES "!\.(jpg|png)$" "t:none"

# SecRule FILES "\.(%{tx.content\_monitor\_file\_exts})$" "t:none"

# SecRule FILES\_TMPNAMES "^$" "phase:2,id:'800017',msg:'good boy',t:trim,pass"

#

SecRule &FILES\_TMPNAMES "@eq 0" "chain,phase:2,id:800015,log,pass,msg:'content monitor',logdata:'%{matched\_var}'"

SecRule REQUEST\_BODY "@lt 1024" "chain,t:none,t:length"

SecRule REQUEST\_BODY "@pmFromFile modsecurity\_monitor\_scanners.data" "t:none,t:urlDecodeUni"

# SecRule &TX:FILES "@eq 1" "phase:2,id:800016,log,pass,msg:'Content monitor, name:%{tx.files},tmpname:%{tx.files\_tmpnames}'"

SecRule &FILES\_TMPNAMES "@eq 1" "phase:2,id:'800016',pass,msg:'content monitor',logdata:'name=%{files},tmpname=%{files\_tmpnames},filesize=%{files\_sizes}'"

SecMarker END\_POST\_CONTENT\_MONITOR\_CHECK

SecRule REQUEST\_METHOD "^GET$" "chain,phase:4,id:'800021',t:none,nolog,pass,skipAfter:END\_GET\_CONTENT\_MONITOR\_CHECK"

SecRule RESPONSE\_BODY "@gt 5242880" "t:none,t:length"

SecRule TX:CONTENT\_MONITOR\_URLS "!^$" "chain,phase:4,id:'800022',t:none,nolog,pass,skipAfter:END\_GET\_CONTENT\_MONITOR\_CHECK"

SecRule REQUEST\_FILENAME ".\*" "chain,t:none,setvar:'tx.filename=#%{request\_filename}#'"

SecRule TX:FILENAME "!@within %{tx.content\_monitor\_urls}" "t:none"

SecRule TX:CONTENT\_MONITOR\_FILE\_EXTS "!^$" "chain,phase:4,id:'800023',t:none,nolog,pass,skipAfter:END\_GET\_CONTENT\_MONITOR\_CHECK"

SecRule FILES "!\.(jpg|png)$" "t:none"

SecRule RESPONSE\_BODY "@pmFromFile modsecurity\_monitor\_scanners.data" "phase:4,id:800025,log,pass,t:none,t:urlDecodeUni,msg:'content monitor',logdata:'%{matched\_var}'"

SecMarker END\_GET\_CONTENT\_MONITOR\_CHECK