

Weaver Software

上海浦东耀华支路39弄9号泛微软件大厦

邮政编码：200127

电话：+86 21 50942228

传真：+86 21 50942278

**Ecology系统安全配置说明**

**Submitted By Weaver**

**设计说明书**

文档版本控制

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **文档简要信息：** | | | | | | | |
| 文档主题(Title) | | | | Ecology系统安全配置说明 | | | |
| 作者(Author) | | | | 柳炉 | | | |
| 审批者 (To Be Approved By) | | | |  | | | |
| 说明 (Comments) | | | | Ecology系统安全配置说明 | | | |
| 文件名称(File Name) | | | |  | | | |
| **文档版本历史：** | | | | | | | |
| 序号 | 日期 | 版本 | 变更说明 | | 修改人 | 审批人 | 注释 |
|  | 2015/03/20 | 1 | 新建 | | 柳炉 |  |  |
|  | 2015/03/22 | 2 | 针对使用非UTF-8编码开发的页面配置 | | 柳炉 |  |  |
|  | 2015/03/30 | 3 | 增加webservice安全验证 | | 柳炉 |  |  |
|  | 2015/04/02 | 4 | 修正本文件说明格式，方便理解阅读 | | 柳炉 |  |  |
|  | 2015/04/07 | 5 | 增加xss过滤字符的说明 | | 柳炉 |  |  |
|  | 2015/04/13 | 6 | 增加log日志访问权限控制 | | 柳炉 |  |  |
|  | 2015/04/22 | 7 | 增加参数值检查最小长度限制 | | 柳炉 |  |  |
|  | 2015/5/26 | 8 | 增加httponly配置 | | 柳炉 |  |  |
|  | 2015/6/15 | 10 | 增加一些必须配置的项 | | 柳炉 |  |  |
|  | 2015/10/19 | 11 | 增加cookie检查 | | 柳炉 |  |  |
|  | 2015/10/27 | 12 | 增加对攻击源IP进行告警和封杀的功能 | | 柳炉 |  |  |
|  | 2015/11/24 | 13 | 增加了cookie+ip绑定、登录前页面参数格式严格限制、登录检查功能 | | 柳炉 |  |  |
|  | 2016/3/31 | 14 | 增强了文件上传格式检查，增强了规则库，默认开启登录校验 | | 柳炉 |  |  |
|  | 2016/5/27 | 15 | 默认开启了cookie重置、修复了安全包被绕过的bug，增强了安全规则库。 | | 柳炉 |  |  |
|  | 2016/7/14 | 16 | 新增自动更新规则库，安全包更新自动提醒，系统安全检测，攻击检查等功能，并且完善了规则库。 | | 柳炉 |  |  |
|  | 2018-5-23 | 17 | 完善文档，完善安全补丁包，修复新发现的问题 | | 柳炉 |  |  |
|  | 2020-09-16 | 18 | 完善文档，增加新增的安全防护配置说明 | | 柳炉 |  |  |

**目录**

[1 引言 4](#_Toc514849184)

[1.1 编写目的 4](#_Toc514849185)

[1.2 定义 4](#_Toc514849186)

[1.3 安全包使用说明 4](#_Toc514849187)

[1.3.1 检测安全包是否生效 4](#_Toc514849188)

[1.3.2 开启安全包自动更新功能 5](#_Toc514849189)

[1.3.3 查看当前系统环境信息及安全包版本信息 5](#_Toc514849190)

[1.3.4 系统安全体检 6](#_Toc514849191)

[1.3.5 安全监控 6](#_Toc514849192)

[1.3.6 备份与恢复 6](#_Toc514849193)

[1.3.7 安全包功能开启情况 7](#_Toc514849194)

[1.4 修复的漏洞情况说明 7](#_Toc514849195)

[1.4.1 xss过滤字符说明 8](#_Toc514849196)

[1.4.2 SQL注入过滤规则说明 8](#_Toc514849197)

[1.5 配置详细说明 8](#_Toc514849198)

[1.5.1 系统安全规则库文件配置说明 8](#_Toc514849199)

[1.5.2 Ecology安全补丁常见拦截问题说明 23](#_Toc514849200)

[1.5.3 其他事项 23](#_Toc514849201)

# 引言

## 编写目的

本文档主要描述了Ecology系统安全补丁包配置说明。方便升级同事进行升级包部署

## 定义

下文中提及到的WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml与WEB-INF/ weaver\_security\_rules.xml文件的格式完全一样。

## 安全包使用说明

部署安全包后，用sysadmin登录系统，访问如下地址：

**http://贵司OA访问地址/security/monitor/Monitor.jsp**

### 检测安全包是否生效



点击【安全包概要】页签，如果三项都显示为【开启】，则表示安全包正常生效。

### 开启安全包自动更新功能



点击【加入安全规则库自动更新服务】即可生效，每天凌晨1点-5点之间的某个时间点会检查安全包是否有更新，如果有更新会自动更新规则库。

### 查看当前系统环境信息及安全包版本信息



包含系统版本信息、ecology信息、中间件信息、JDK版本信息、安全包版本信息。

### 系统安全体检



【检测】：点击此按钮，会对系统的配置进行检查，针对各项给出结果，如果不符合，则可以按照修复方式加以操作；

【修复】：点击【检测】后，会出现该按钮，点击此按钮，会对系统的配置进行修复，导出resin.conf和web.xml，并在界面上给出修复的详细步骤。

### 安全监控



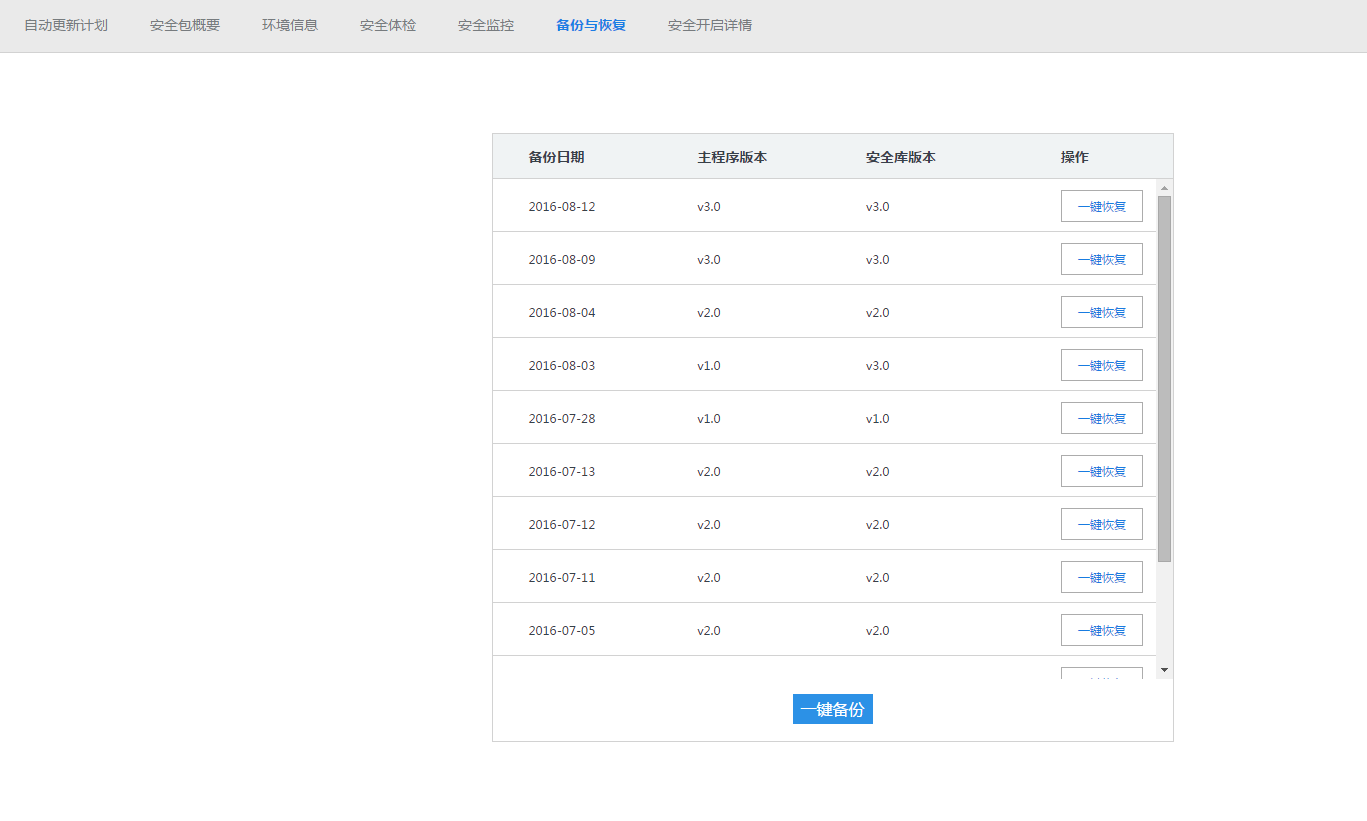
该页会对系统存在的攻击行为进行监控，如果确实发现为恶意攻击，可以手动封杀该IP地址访问系统。

【更新安全规则库缓存】：如果自定义了安全规则库，可以通过点击该按钮使安全规则库生效；

【查看攻击源IP详情】：点击此按钮，可以看到当前系统遭受攻击的情况。

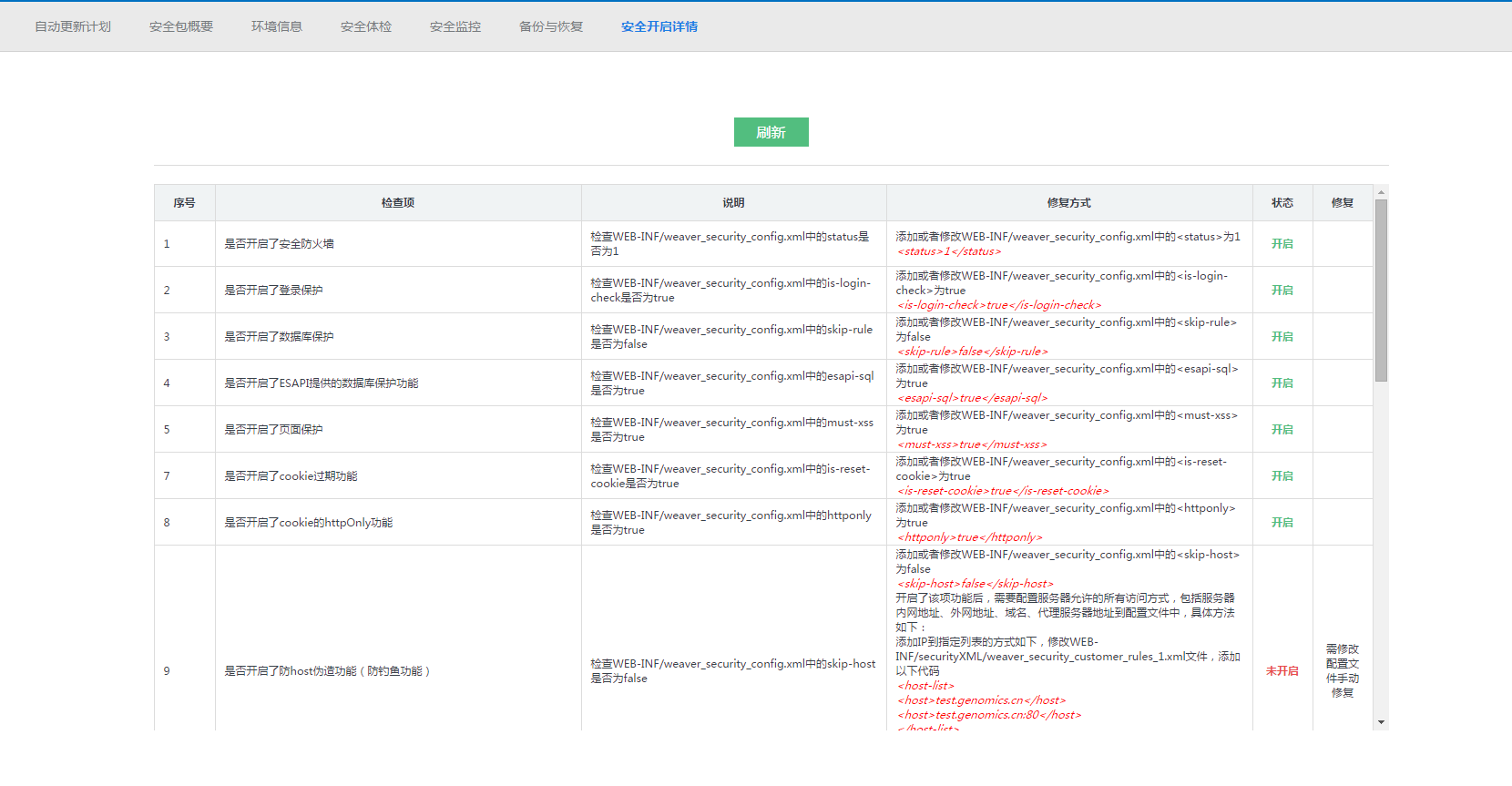
### 备份与恢复

如果系统出现安全包更新失败导致系统出现问题，可以在此页面快速恢复，以尽快让系统恢复到正常状态。



【一键备份】：会将当前的规则库进行备份；

### 安全包功能开启情况



此页会检查当前系统中所有可用的安全防护功能，并且会检查是否开启，如果没有开启，会给出开启该功能的方式。

## 修复的漏洞情况说明

1、解决XSS跨域攻击；

2、解决高危险级SQL注入攻击；

3、防范钓鱼风险；

4、Host伪造攻击；

5、referer检查；

6、webservice白名单机制；

7、cookie的httponly机制；

8、http响应拆分漏洞；

9、log文件、数据库连接访问权限控制；

10、文件上传安全检查；

11、ip白名单机制；

12、cookie+ip绑定机制；

13、攻击源IP封杀机制；

14、cookie重置功能；

15、系统超时设置功能

### xss过滤字符说明

目前，xss过滤采用关键字过滤，过滤方式采用直接删除的方式。

### SQL注入过滤规则说明

如果检查到存在SQL注入风险，则直接拦截，并给出提示信息。

## 配置详细说明

### 系统安全规则库文件配置说明

#### 规则库文件位置

**说明：**

**以下涉及到的xml文件都不能使用记事本、笔记本编辑，需要使用Editplus、Ultra等文本工具编辑保存。**

1、开关配置文件

/ecology/WEB-INF/weaver\_security\_config.xml

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?>  <root>  <status>1</status>  <second-prefix-path>/htoa</second-prefix-path>  < auto-decode-param>false</auto-decode-param>  < antisamy-protect>false</antisamy-protect>  < securitylog-keep-time>30</securitylog-keep-time>  < auto-remind>true</auto-remind>  <auto-update-rule>true</auto-update-rule>  <is-check-session-timeout>true</is-check-session-timeout>  <session-timeout>30</session-timeout>  < x-forwarded-for-pos>1</x-forwarded-for-pos>  < creator>1</creator>  < system-admin>sysadmin</system-admin>  < system-id>1</system-id>  < disable-sql-common-rule>false</disable-sql-common-rule>  <is-reset-cookie>true</is-reset-cookie>  <debug-xss-tool>false</debug-xss-tool>  <ecology-version>E8</ecology-version>  < access-freq-enable>false</access-freq-enable>  < access\_freq\_way>session</access\_freq\_way>  < access-freq-time>1</access-freq-time>  < access-freq-count>600</access-freq-count>  <proxy-ip></proxy-ip>  < remote-addr></remote-addr>  < sensitive-replace-char>\*\*</sensitive-replace-char>  <sys-debug>false</sys-debug>  <skip-ref>false</skip-ref>  < skip-mobile-ref>true</skip-mobile-ref>  <skip-host>false</skip-host>  <must-xss>true</must-xss>  < intercept-code>404</ intercept-code>  <xss-debug>false</xss-debug>  <skip-rule>false</skip-rule>  <esapi-sql>true</esapi-sql>  <esapi-xss>true</esapi-xss>  <intercept-level>1</intercept-level>  <enable-service-check>true</enable-service-check>  <secure>false</secure>  <http-sep>true</http-sep>  <param-key>true</param-key>  <is-login-check>true</is-login-check>  < login-check-type>1</login-check-type>  <auto-decode-param>true</auto-decode-param>  <join-system-security>true</join-system-security>  <auto-update-rules>true</auto-update-rules>  <cookie-ip-check>false</cookie-ip-check>  <enable-x-frame-options>true</enable-x-frame-options>  <x-frame-options>SAMEORIGIN</x-frame-options>  <enable-x-content-type-options>false</enable-x-content-type-options>  <enable-x-xss-protection>true</enable-x-xss-protection>  <x-xss-protection>1</x-xss-protection>  <skip-mobile-ref>false</skip-mobile-ref>  <sys-max-length>5000</sys-max-length>  <session-id>ecology\_JSessionid</session-id>  <oa-server> Tegine</oa-server>  < strictest-mode>false</ strictest-mode>  < html-filter-level>0</ html-filter-level>  </root> |

status：是否开启安全防火墙；

second-prefix-path:部分客户支持二级路径配置，需要在此参数添加二级路径，防止白名单规则失效；

auto-decode-param:是否自动解码参数；

antisamy-protect:是否启用antisamy框架防御xss漏洞；

securitylog-keep-time：设置安全日志保存时间，默认为30天；

join-system-security：是否加入安全保障计划。默认为true。如果设置为false，下面2个配置均无效；

auto-remind：是否启用安全更新提醒，当auto-update-rules为true时，该参数失效；

auto-update-rules：是否自动更新安全规则库，默认为false，需要客户同意才开启；

esapi-sql：是否开启ESAPI提供的防SQL注入方式，默认开启；

esapi-xss：是否开启ESAPI提供的防XSS跨站攻击的方式，默认不开启；

is-check-session-timeout：是否启用系统超时控制，默认不开启；

session-timeout：如果启用了超时控制，设置超时时间，默认为30分钟；

x-forwarded-for-pos: 当存在代理的时候，真实IP会放在x-forwarded-for头部，但位置可能是开头，也可能是结尾。默认值为1，取结尾的IP.

creator：设置安全更新提醒人的ID，默认为1，系统管理员；

system-admin：设置安全包监控页面的访问者账号，默认为sysadmin

system-id：设置安全包监控页面的访问者ID，默认为1

disable-sql-common-rule：是否禁用sql注入黑名单规则，默认为false，不禁用；

ecology-version：配置系统版本，取值有：E9、E8、E7、E6

is-reset-cookie：是否启用cookie重置功能，默认开启；

debug-xss-tool：是否开启安全补丁包本身的调试日志打印功能，默认不开启；

access-freq-enable：是否启用接口访问频率限制，默认为false，不开启；

access\_freq\_way：频率校验方式，取值为session或者ip，默认值为session；

access-freq-time：频率统计周期，单位为分钟，默认为1分钟开始统计；

access-freq-count：频率设定，默认值为600(次/分钟)

proxy-ip：如果前端有使用nigx、F5等负载均衡软件代理，如果设置为singleIp，那么直接取request的默认IP，不从x-forwarded-for等头部获取IP。当确认没有使用转发或者代理软件时，可将此值设置为singleIp。默认值为空；

remote-addr：指定从哪个头部获取IP。有些云环境，会自定义将客户端真实IP放入某个头部，导致应用获取IP不准。对于此种情况，可直接配置此字段，指定客户端IP的字段。

sensitive-replace-char：用于指定敏感词替换值，默认替换为\*\*；

skip-ref：是否跳过referer检查，CSRF防御开关，设置为true时跳过；设置为false时需配置ref-list节点以保证其他正常跳转请求；

skip-mobile-ref：是否启用emobile、云桥请求的CSRF，默认为true。启用后（设置为false）需要将mobile的域名和IP以及云桥的域名和IP加入到referer白名单；

skip-host：是否跳过host头部检查，设置为true时跳过；设置为false时需配置host-list节点以保证系统正常运行；

must-xss：是否执行xss过滤，设置为true时执行xss过滤

xss-debug：是否启用xss过滤的日志输出。默认为false，不输出。该属性用于调试，会打印出过滤前的值和过滤后的值；

sys-debug：系统出现500错误时，是否将错误堆栈输出到客户端。默认为false。

intercept-code：设置请求被拦截时返回的错误码，默认为404；（注：出现404时，如果响应头中出现errorMsg: securityIntercept头部，表示该请求被安全补丁包拦截，可查看安全拦截日志）

skip-rule：是否跳过SQL注入检查，设置为true时跳过

min-length：配置执行SQL检查和xss检查，参数值需满足的最小长度

max-length：配置执行SQL检查和xss检查，参数值需满足的最大长度,默认值为100000，超过则不进行过滤

sys-max-length：配置系统中参数允许的最大字符数，默认为1000000。该项有利于防御恶意构造的超大参数导致拒绝服务攻击的问题。

enable-service-check：是否开启webservice安全检查，设置为true时开启。设置为true时需配置webservice-ip-list和webservice-list节点，默认不开启。

webservice-ip-check-override：配置是否强制覆盖标准配置的ip白名单。默认为false，改为true时需要单独配置IP白名单；

httponly：配置是否启用httponly安全cookie机制。

secure：如果启用的是完全的https访问，可以开启该项，对cookie增加secure属性。默认不增加。**启用此项后，http访问将无法正常登陆系统。**

http-sep：配置是否启用http拆分响应漏洞检查。

param-key：配置是否启用参数名合法性检查。

is-login-check：是否开启登录检查功能，默认不开启。

login-check-type：确定登陆拦截的范围，默认值为1，白名单中的url才进行拦截。设置为2时，只要url不在免登录白名单，就需要登录后才能访问；

cookie-ip-check：是否启用cookie和IP的绑定，启用后，登陆后，cookie和ip就绑定了，这个cookie在其他IP上无法访问系统。外网环境下，由于IP可能随时变化，所以启用后可能导致异常。

session-id：会话标志，当在resin中修改了会话标志时，需要配置此处，默认为ecology\_JSessionid。

auto-decode-param：检测前是否对待检测字符串自动解码，默认不开启

enable-x-frame-options：是否启用防点击劫持（防盗链）漏洞，默认开启。

x-frame-options：启用防点击劫持漏洞后，此项配置允许嵌套OA系统的域名，默认为SAMEORIGIN，使用同源策略。

enable-x-content-type-options：是否禁用浏览器猜测功能，默认不开启。启用可能导致功能异常

enable-content-security-policy：是否启用CSP策略，默认不开启。启用可能导致功能问题

enable-x-xss-protection：是否启用浏览器自带的xss防御机制，默认开启。

x-xss-protection：是否启用浏览器的防跨站脚本攻击功能。默认值为1，表示启用。0表示不启用。

strict-transport-security：是否启用严格的传输模式（HSTS，仅允许https加载资源），默认不开启。

skip-mobile-ref：是否启用EMobile防跨站点请求伪造功能。默认为不开启，默认值为true。如果该项配置开启，需要将EMobile的访问方式、云桥的访问方式等加入到ref-list白名单中。

is-stand-mode：强制设置是否采用标准模式重写request，即继承HttpServletRequestWrapper实现，不依赖于中间件。

is-use-error-forward：拦截信息显示是否跳转独立页面处理，默认为false，采用弹出框形式。

oa-server：设置中间件响应头部，隐藏中间件版本。默认值为Tegine

strictest-mode：是否启用严格过滤模式，默认为false。启用可能对少数功能造成影响。

html-filter-level：是否启用html字段白名单机制，默认不启用。取值为0：不启用，1：不允许任何html标签；2：仅允许jsoup定义的标签；3：自定义的html标签

2、标准规则库文件（该文件通过通用补丁包给到客户，或单独给到客户，勿单独修改）

/ecology/WEB-INF/weaver\_security\_rules.xml

/ecology/WEB-INF/securityRule/\*

3、用户自定义配置文件（可以是多个文件）

/ecology/WEB-INF/securityXML/\*.xml

示例：weaver\_security\_custom\_rules\_1.xml，如果客户需要单独添加一些规则，可以将weaver\_security\_rules.xml文件复制一份到securityXML目录下，重命名为weaver\_security\_custom\_rules\_1.xml，将里面root节点内的所有内容清空，然后添加自己的规则，格式和weaver\_security\_rules.xml一样，但无须完整节点，需要哪些就配置哪些。

4、拦截日志文件（按天存放）

/ecology/WEB-INF/secritylog/\*.log

#### 开启防火墙功能（status)

配置文件：WEB-INF/weaver\_security\_config.xml



status设置为1即为开启，设置为0即为禁用，默认开启。

#### 开启系统超时功能

配置文件：WEB-INF/weaver\_security\_config.xml



is-check-session-timeout：是否开启系统超时功能，默认为false，不开启

session-timeout:如果开启了系统超时功能，此处设置多长时间超时，单位为分钟，默认30分钟

#### 是否禁止系统被其他系统嵌套（enable-x-frame-options）

配置文件：WEB-INF/weaver\_security\_config.xml



enable-x-frame-options：是否启用防盗链机制，默认为开启（true），开启后，系统不能被其他第三方系统嵌入iframe。



x-frame-options：如果上面开关设置为true，此处设置防盗链策略，默认策略为同源策略（即相同的域名可以嵌套本系统）

配置白名单（即配置了白名单之后，该页面不受此设置影响，允许被其他第三方系统嵌套）

配置文件：WEB-INF/ securityXML/weaver\_security\_custom\_rules\_1.xml



可以配置多个url，也可以配置url中的一部分，放行某个目录中的所有文件和子目录中的文件。

#### 启用XSS浏览器自带的防跨站功能(X-XSS-Protection)

配置文件：WEB-INF/weaver\_security\_config.xml



x-xss-protection：启用浏览器自带的防跨站功能，默认开启（true）

配置白名单（即配置了白名单之后，该页面不受浏览器防跨站功能的影响）

配置文件：WEB-INF/ securityXML/weaver\_security\_custom\_rules\_1.xml



可以配置多个url，也可以配置url中的一部分，放行某个目录中的所有文件和子目录中的文件。

#### 参数缓存相关配置（intervalTime、scanTime）

配置文件：WEB-INF/weaver\_security\_config.xml



经过加密的sql参数在服务器上保留的时间，默认是480分钟。



sql参数缓存清除线程扫描间隔时间，默认为30分钟扫描一次。

#### 攻击源IP封杀配置(forbidden-info子节点)

配置文件：WEB-INF/weaver\_security\_config.xml



设定IP封杀的模式。默认为1，邮件告警模式。

0：不开启IP封杀功能；

1：开启攻击邮件告警，但不自动拦截；

2：开启自动拦截模式，但不发送告警邮件；

3：开启自动拦截模式，同时发送告警邮件。



当开启自动拦截模式时，设定封杀时长。默认为2小时。

当开启告警或者自动拦截模式时，设定拦截的级别，取值为1和2。默认为拦截最危险的攻击。



设置为1：仅拦截违反一般规则的攻击，主要是SQL注入攻击拦截；

设置为2：违反了特殊规则的攻击也进行拦截，比如违反参数格式行为等。



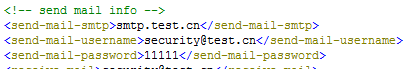
当开启告警或者自动拦截模式时，设定当同一IP持续攻击达到设定次数时，执行告警或者自动拦截。默认为3次。



当开启告警时，多封告警邮件发送的时间间隔，默认为3分钟。



当开启告警时，对同一IP持续攻击最多发送的告警邮件次数。默认为10封。



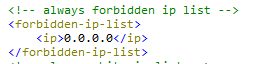
当开启告警时，设置告警邮件的发送邮件服务器地址、发送账号及密码。



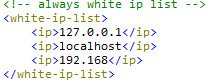
当开启告警时，设置告警邮件的接收账号密码。

#### 设置永久黑名单和永久白名单

配置文件：WEB-INF/ securityXML/weaver\_security\_custom\_rules\_1.xml



设置永久黑名单列表。当开启攻击源IP自动拦截功能时，此处设置的IP地址将永远不能访问系统。适用于网络上经常用于攻击的一些IP地址。

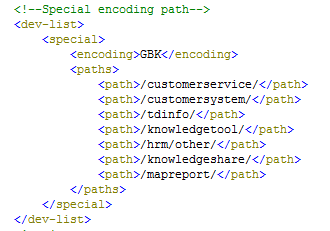


设置永久白名单列表。当开启攻击源IP自动拦截功能时，此处设置的IP地址将不会被自动封杀（但违反输入规则依旧会取消此次请求），优先级高于永久黑名单设置。适用于局域网访问外部网络时，本地映射的外网地址。避免由于有人测试时被拦截，导致全局域网内都无法访问系统。**（注意：当开启了自动封杀IP功能时，请务必将Emobile、Emssage、E-brige等和Ecology通信的地址加入到白名单中）**

#### 关于二次开发页面的配置问题（dev-list、encoding、path）

配置文件：WEB-INF/ securityXML/weaver\_security\_custom\_rules\_1.xml

对于E8，该节点配置需要以GBK编码接收数据的页面地址；



E8配置示例

对于E7和E6，该节点配置需要以UTF-8编码接收数据的页面地址。



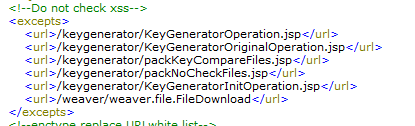
E7配置示例

encoding：页面接收参数采用的编码格式

path：采用encoding指定编码开发的页面URL。可以配置多个url，也可以使用正则表达式来描述一个目录下的所有文件

#### 无需安全过滤器检查的链接配置

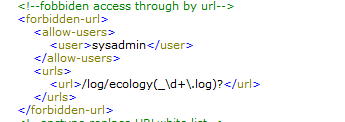
配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



请将要排除的URL添加到excepts节点中。可以配置多个url，也可以使用正则表达式来描述一个目录下的所有文件

#### URL（log日志）访问权限控制

配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



该配置主要用于配置某些特定的URL仅允许部分用户允许访问，防止信息泄露。如log日志文件访问权限控制。

allow-users：配置允许访问的用户loginId，需要配置多个用户则配置多个<user>节点即可。

urls：配置只能是allow-users中配置的用户才能访问的URL，若需配置多个URL则配置多个<url>节点即可。（可以配置多个url，也可以使用正则表达式来描述一个目录下的所有文件）

#### 无需登录访问开关配置（is-login-check）

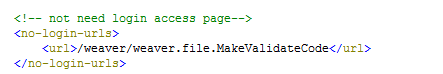
配置文件：WEB-INF/weaver\_security\_config.xml



该值设置是否对页面进行登录访问检查，默认为false，不进行登录访问检查。设置为true时，所有页面都必须登录后才能访问。（访问例外配置可以参考1.3.1.10配置）

#### 无需登录访问页面例外配置（no-login-urls）

配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



当<is-login-check>设置为true时，此处配置的url不进行登录验证。（可以配置多个url，也可以使用正则表达式来描述一个目录下的所有文件）

#### ref跨站攻击检查（skip-ref、skip-mobile-ref）

配置文件：WEB-INF/weaver\_security\_config.xml

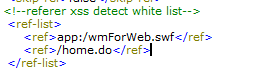


<skip-mobile-ref>false</skip-mobile-ref>

该值设置是否跳过ref攻击检查，默认为true，不需要检查referer来源。设置为false则检查referer来源。

#### ref白名单（ref-list）

配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



当开启skip-ref设置为false时，允许的referer取值。可以配置多个url，也可以使用正则表达式来描述一个目录下的所有文件

#### httponly配置

配置文件：WEB-INF/weaver\_security\_config.xml



该值设置是否将cookie设置为httponly模式，默认为true。启用httponly

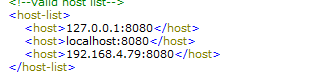
#### host攻击检查相关（skip-host、url-params、host-list）

配置文件：WEB-INF/weaver\_security\_config.xml



该值设置是否跳过host头部检查，取值为true的false。默认为true，即不检查host header的合法性。

配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



合法的host header列表。这里需要配置Ecology服务器内外网IP、域名（如果是80端口，那么需要配置带端口的不带端口两种模式）。

配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



配置需要进行URL检查的参数，防范钓鱼网址攻击。该项需要skip-host设置为false才生效。其访问的地址域名必须是host-list中允许的地址。

配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



针对<url-params>中配置的检查参数，如果有些页面允许接收传递URL格式的参数，那么将该页面地址配置在<url-except-params>节点下。

#### webservice安全相关配置

1、开启webservice安全验证

配置文件：WEB-INF/ weaver\_security\_config.xml



该值改为true即开启了webservice安全验证。如开启了该验证，必须配置webservice和webservice-ip-list节点数据，否则webservice将不可用。

2、配置需要验证的webservice白名单

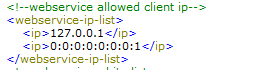
配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



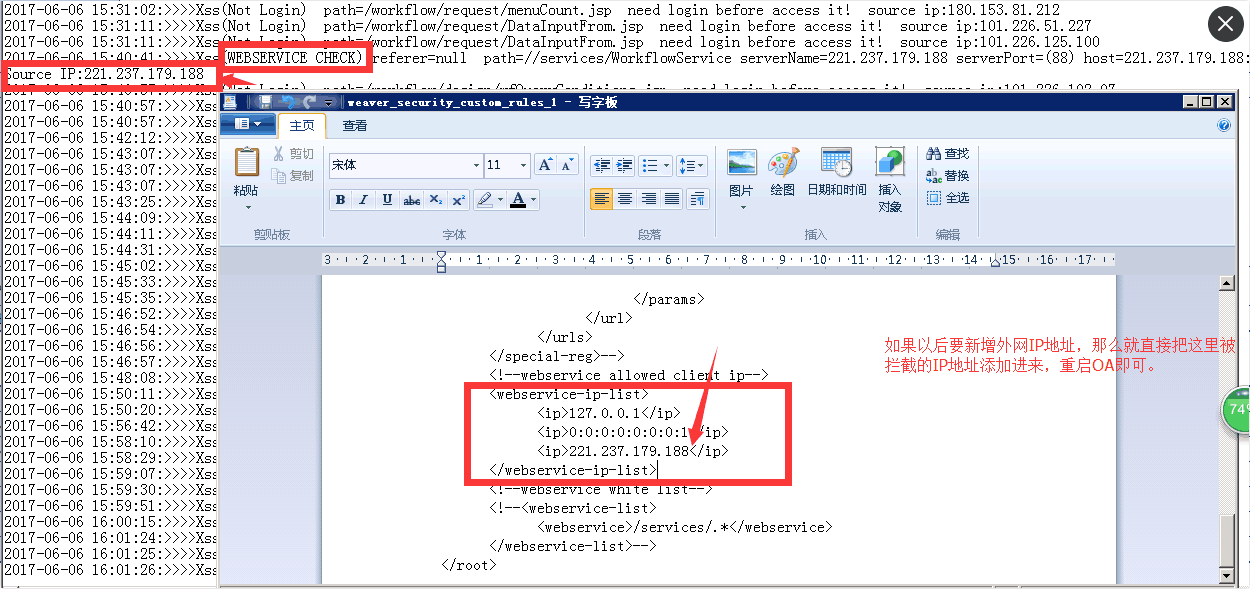
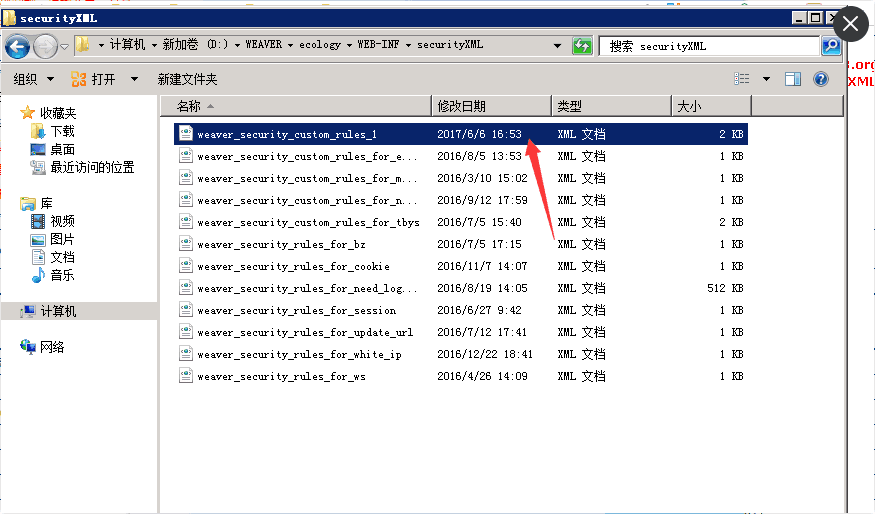
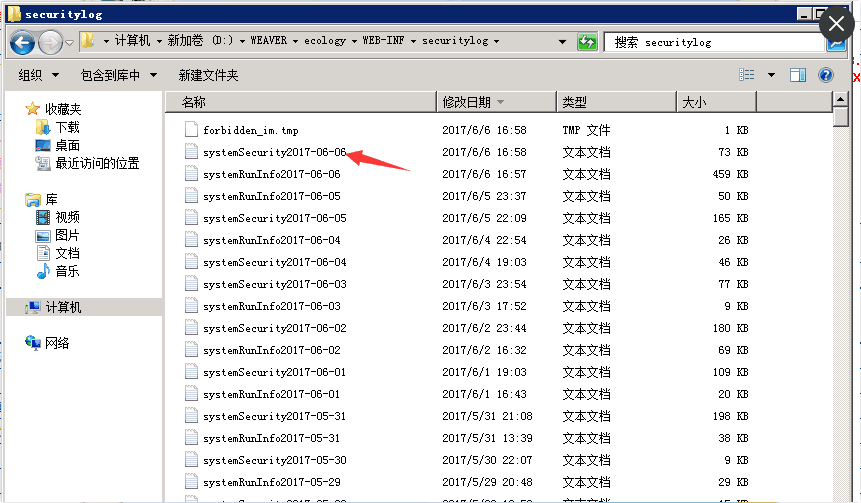
webservice代表一个或多个webservice请求地址，使用正则表达式配置，可以有多个<webservice>节点

3、配置允许的webservice客户端地址

配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



<ip>节点配置允许访问系统的webservice ip地址，可以配置多个节点。



#### xss注入攻击检查与过滤相关

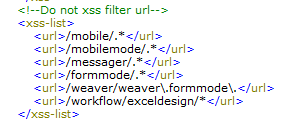
相关参数：xss-must、xss-type、xss、xss-list、xss-keyword-list、xss-filter-list

配置文件：WEB-INF/ weaver\_security\_config.xml



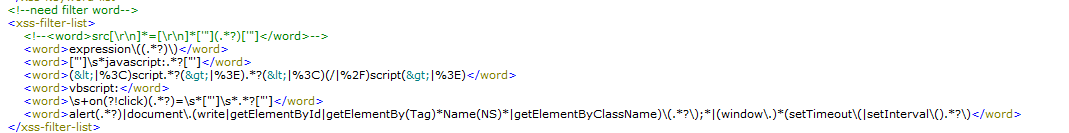
该值设置是否启用xss注入攻击检查，取值true|false，默认为true，即进行xss检查与过滤。该值设置false时，xss相关参数不生效。

配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



这里配置不需要进行xss过滤的地址。

配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



xss-filter-list配置需要被过滤的关键字，列表中的关键字都会被替换为空字符串。

#### SQL注入攻击相关

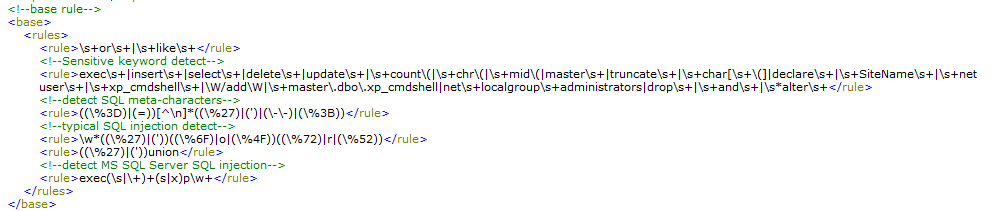
相关参数：skip-rule、base、special-non、special-reg

配置文件：WEB-INF/ weaver\_security\_config.xml



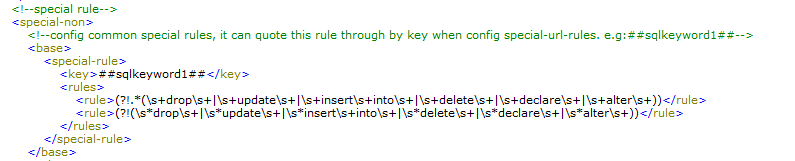
该值确定是否跳过SQL注入攻击检查，取值false|true，默认为false，开启SQL注入检查。设置为true，则不进行SQL注入检查。只有当该值设置为false时，其他参数才有效。

配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml



通用规则列表。多个rule间or关系，只要有一条符合，则该参数存在SQL注入攻击风险，系统会停止业务逻辑的进行，返回错误信息。

配置文件：WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml

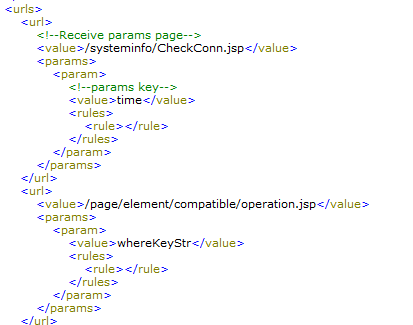


special-non和special-reg用于配置特殊规则，使得某些由于业务需要而无法通过通用规则检查的参数能够正常运转。

special-rule节点配置了特殊规则定义，后面设置具体参数的特殊规则时，可以直接饮用这里定义的规则即可。

rule节点间是And关系，即参数值必须满足这里所有的rule，才能通过SQL注入检查。

special-non中配置固定参数规则，special-reg中配置动态参数规则。



图一



图二

图一即配置的是固定参数规则，参数名是确定的。图二配置的是动态参数规则，即参数名不确定，但具有一定的规则。

#### 特殊规则配置说明

|  |
| --- |
| <url>  <value>/formmode/browser/CommonMultiBrowser.jsp</value>  <params>  <param>  <value>sqlwhere</value>  <rules>  <rule>##sqlkeyword1##</rule>  </rules>  </param>  </params>  </url> |

<value>：配置参数接收的URL地址。

<params>：同一个URL中的多个参数都配置到该节点下。

<param>：每个param节点对应一个参数的信息。

<param>-》<value>：该节点配置的是参数名。

<rule>：配置或者引用该参数应该满足的规则，多个rule间是and关系。

### Ecology安全补丁常见拦截问题说明



### 其他事项

随着不断发现漏洞，会不断地完善规则库及防火墙功能。