Ta+3CloudV4.1-web安全使用文档

--技术支持：康鼎武

## 配置文件介绍-config.properties

### isHostFilter

配置host白名单的的开关如：isHostFilter=true

### isXSSFilter

配置XSS过滤的开关如：isXSSFilter=true

### urlFilter

配置host黑名单开关如：urlFilter=true

## 配置文件介绍-security.properties

### xssWhiteList

配置xss过滤的白名单url，可配置多个，每一个url之间以'|'号隔开,URL从上下文后边的第一个'/'开始,通配符使用'.\*',例如 /indexAction.\*.do|/indexAction1.\*.do

### skipChars

Xss特殊字符编译时直接对下列的字符进行跳过处理，直接在下面的字符串后边添加要跳过的字符，不需要分隔符、空格等

### hostWhiteList

配置host地址的白名单,只有配置了的ip:port或者www.cloud.com:8080允许才允许访问,以'|'号隔开，通配符使用'.\*',例如: 192.168.28.145:8081

### urlBlackList

配置url请求黑名单,在黑名单中的请求不允许访问,以'|'号隔开,以'/'开头，通配符使用'.\*', 例如: /indexAction.\*.do

### img-src

指定图像和网站图标的有效来源。

具体可参考：<https://cloud.tencent.com/developer/section/1189862>

<scheme-source>一种模式，如'http:' 或 'https:'。**冒号是必需的，不应使用单引号**。您也可以指定数据模式（不推荐）。

data:允许将data:URI用作内容源。*这是不安全的; 攻击者也可以注入任意数据：URI。谨慎使用这一点，绝对不适用于脚本。*

mediastream:允许将[mediastream:URI](https://developer.mozilla.org/en-US/docs/Web/API/MediaStream_API" \t "_blank)用作内容源。

blob:允许将[blob:URI](https://developer.mozilla.org/en-US/docs/Web/API/Blob" \t "_blank)用作内容源。

filesystem:允许将[filesystem:URI](https://developer.mozilla.org/en-US/docs/Web/API/FileSystem" \t "_blank)用作内容源。

'self'指受保护文档的来源，包括相同的URL方案和端口号。你必须包括单引号。一些浏览器特别排除blob和filesystem从源指令。需要允许这些内容类型的网站可以使用Data属性来指定它们。

'unsafe-inline'允许使用内联资源，如内联[<script>](https://developer.mozilla.org/en-US/docs/Web/HTML/Element/script" \t "_blank)元素，javascript:URL，内联事件处理程序和内联[<style>](https://developer.mozilla.org/en-US/docs/Web/HTML/Element/style" \t "_blank)元素。你必须包括单引号。

'unsafe-eval'允许使用eval()和类似的方法从字符串创建代码。你必须包括单引号。

'none'指空集；也就是说，没有URL匹配。单引号是必需的。'nonce- <base64-value>'使用加密随机数（使用一次的数字）的特定内联脚本的白名单。每次发送策略时，服务器都必须生成唯一的随机数值。提供一个无法猜测的随机数是非常重要的，因为绕过资源的策略是微不足道的。例如，查看不安全的内联脚本。

### defaultUnsafe

提供对default-src的配置，参数通image-src

### frameOption

配置是否允许页面在iframe中展现,DENY不允许,SAMEORIGIN只允许在相同域名展现,ALLOW-FROM uri只在指定的uri中展现,不配置时为不限制