JavaScript、CSS、HTML、SQL 防止注入

JavaScript、CSS、HTML、SQL 防止注入
- 1、简介
- 2、使用方法
  - 2.1、web.xml 配置
  - 2.2、xss.properties 配置
  - 2.3、filter-exclude.xml 白名单配置
    - 1、配置示例：白名单放行url
    - 2、配置示例：只做部分filter规则拦截
    - 3、配置示例：只过滤某些特定参数
    - 4、配置示例：对某些特定参数放行
    - 5、配置示例：上传文件过滤

1、简介

`xss-filter` 是一个 `JavaWeb` 工程下的过滤器，可以拦截request参数列表中的特殊字符串，如：`js`、`css`、`html`、`sql`等特殊字符，防止恶意提交代码给系统造成影响故障。

2、使用方法

2.1、web.xml 配置

> 找到系统web工程下的`web.xml`，在`web.xml`中加入如下配置

```
    <filter>
        <filter-name>xss-filter</filter-name>
        <filter-class>com.masget.xss.XssFilter</filter-class>
    </filter>
    <filter-mapping>
        <filter-name>xss-filter</filter-name>
        <url-pattern>/*</url-pattern>
    </filter-mapping>
```

> 其中`<url-pattern>/*</url-pattern>`是拦截所有的`url`,这里可以灵活配置，根据业务的需要拦截需要拦截的`URL`。如：拦截`*.do`,`*.mvc`,`/mvc/web/*`具体的配置需要根据业务本身来做。

2.2、xss.properties 配置

> `xss.properties`一般放在classpath路径下，位于目录：`src/java/resources` 该文件是一些全局配置数据

```
# 默认拦截过滤动作filter
default.filter=css,js,html,sql

# 默认检查文件大小
file.check.size=true
# 默认检查文件类型
file.check.type=true

# 文件过滤拦截参数编码格式
file.charset=UTF-8
# 最大上传文件大小
file.max.size=10240000
# 过滤的文件mini/type类型
file.limit.type=application/octet-stream;text/html
# 允许上传的文件类型
file.allowed.type=.zip,.rar,.doc,.docx,.xls,.xlsx,.ppt,.pptx,.gif,.jpeg,.jpg,.pdf,.png,.bmp,.mp3
,.txt,.xml
```

以上配置在`filter-exclude.xml`配置的时候会用到

2.3、filter-exclude.xml 白名单配置

> **白名单**配置主要是放行一些不需要过来的`url`,由于这些`url`根据业务需要填入一些**敏感特殊**的字符或部分特殊的字符。
>
> `filter-exclude.xml`一般放在classpath路径下，和`xss.properties`同级目录，位于目录：`src/java/resources`

完整示例

```xml
<?xml version="1.0" encoding="UTF-8"?>
<root>
    <filter-excludes>
        <!-- 排除过滤URL或param参数 -->
        <!-- url 代表排除拦截过滤URL -->
        <!-- url 支持通配符
            The mapping matches URLs using the following rules:
                ? matches one character
                * matches zero or more characters
                ** matches zero or more 'directories' in a path
        -->
        <!-- filter 代表拦截过滤的方式：js,sql,html,css -->
        <!-- check-size 检查上传文件大小  check-type 检查上传文件类型 -->
        <!-- exclude-param 过滤白名单：代表拦截过滤接口不过滤的字符串参数 -->
        <!-- include-param 过滤黑名单：代表拦截过滤接口过滤的字符串参数 -->


        <!-- 对当前url的参数userName、password过滤js,sql,html,css 操作 -->
        <exclude url="masget/pay/weixin.do" filter="html">
            <exclude-param>userName</exclude-param>
            <exclude-param>password</exclude-param>
            <include-param>remark</include-param>
        </exclude>

        <!-- 对当前url过滤js,sql,html 操作 -->
        <exclude url="masget/pay/alipay.do" filter="js,sql,html"/>

        <!-- 直接放行指定url -->
        <exclude url="masget/pay/unionpay.do" />

        <exclude url="masget/pay/alipay_upload.do" filter="js,sql,html" check-size="true"
check-type=""/>

        <!-- 所有/chehuotongweb/xss/example/开头的都执行此过滤配置 -->
        <exclude url="/chehuotongweb/xss/example/**" filter="js,file" check-size="false" check-
type="false"/>
    </filter-excludes>
</root>
```

- `filter-excludes` 白名单模块元素节点，可以有一个或多个，所有配置在该节点下进行配置。
- `exclude` 白名单节点
  - `url` 过滤的url，支持**通配符**原则（?,*,**） `AntPathMatcher.java` 具体可以查看使用方法
  - `filter` 需要执行的过滤规则，目前支持：`js/css/html/sql` 四种规则，可以配置0个或多个。

    当不配置filter且没有配置 `exclude-param` 和 `include-param` 的时候，表示直接放行该url。

    当不配置filter且有配置 `exclude-param` 或 `include-param` 的时候，表示filter的配置为缺省的默认值。即是 `xss.properties` 配置文件中的 `default.filter`
  - `check-size` 是否否检文件大小，仅当是文件上传接口情况下
  - `check-type` 是否检查文件类型，仅当是文件上传接口情况下
- `exclude-param` 参数白名单，该配置是指定前端的参数名称，表示该参数**不执行任何过滤规则**

- `include-param` 参数黑名单，该配置是指定前端的参数名称，表示只对该参数进行过滤。

  注意：配置`include-param`不能和`exclude-param`同时使用，同时使用情况下`include-param`将被忽略

1、配置示例：白名单放行url

> 直接放行，不做任何处理

示例

```
<!-- 直接放行指定url -->
<exclude url="masget/pay/unionpay.do" />
```

2、配置示例：只做部分filter规则拦截

> 只做部分规则拦截，如某些接口只拦截`js、html`，有些接口只拦截`sql`等

示例

```
<!-- 对当前url过滤js,sql,html 操作 -->
<exclude url="masget/pay/alipay.do" filter="js,sql,html"/>

<!-- 对当前url过滤html 操作 -->
<exclude url="masget/pay/alipay.do" filter="html"/>

<!-- 对当前url过滤sql 操作 -->
<exclude url="masget/pay/alipay.do" filter="sql"/>
```

3、配置示例：只过滤某些特定参数

> 只对某个特定参数过滤，如一个`save()`操作接口保存两个字段数据，分别是：`age`、`name`，由于`age`是年龄为int类型，不可能出现特殊字符。而`name`可以填入一些比较特殊的字符串或注入。

示例

```
<!-- 对当前url的参数name过滤js,sql,html 操作 -->
<exclude url="masget/pay/weixin.do" filter="js,sql,html">
  <include-param>name</include-param>
</exclude>

<!-- 对当前url的参数name、remark 过滤所有filter 操作 -->
<exclude url="masget/pay/weixin.do">
  <include-param>name</include-param>
  <include-param>remark</include-param>
</exclude>
```

4、配置示例：对某些特定参数放行

> 只对某些特定的参数进行过滤，如一个接口参数很多，但有那么几个参数需要特定过滤下。而其他参数不需要。

示例

```
<!-- 对当前url的参数name 不做任何过滤，其他参数执行配置的filter操作 -->
<exclude url="masget/pay/weixin.do" filter="js,sql,html">
  <exclude-param>name</exclude-param>
</exclude>

<!-- 对当前url的参数name、remark 不做过滤操作，其他参数执行所有filter操作 -->
<exclude url="masget/pay/weixin.do">
  <exclude-param>name</exclude-param>
  <exclude-param>remark</exclude-param>
</exclude>
```

5、配置示例：上传文件过滤

> 对上传的文件名称和附加其他参数进行过滤

示例

```
<!-- 检查上传文件大小（对文件名和其他参数进行 js,sql,html filter的过滤处理 ），不检查上传文件类型 -->
<exclude url="masget/pay/alipay_upload.do" filter="js,sql,html" check-size="true" check-
type="false"/>

<!-- 所有/chehuotongweb/xss/example/开头的都执行此过滤配置 -->
<exclude url="/chehuotongweb/xss/example/**" filter="js,file" check-size="false" check-
type="false"/>
```