在输入验证，类型转换，字符串过滤后，应该不需要了；

参考：

<http://breezylee.iteye.com/blog/2063615>

公司官网，

/////////////////////////////////////////////////////////////////////

实现：

1，在web.xml加一个filter，

//init可以没有；

<filter>

<filter-name>xssFilter</filter-name>

<filter-class>com.common.filter.XssFilter</filter-class>

<init-param>

<param-name>exclusions</param-name>

<param-value>/css/\*,/images/\*,/js/\*,/attached/\*,/page/common/\*,/druid/\*</param-value>

</init-param>

</filter>

<filter-mapping>

<filter-name>xssFilter</filter-name>

<url-pattern>/\*</url-pattern>

<dispatcher>REQUEST</dispatcher>

</filter-mapping>

2，XssFilter 的实现方式是实现servlet的Filter接口

**public** **class** XssFilter **implements** Filter {

@Override

**public** **void** doFilter(ServletRequest request, ServletResponse response, FilterChain chain) **throws** IOException, ServletException {

chain.doFilter(**new** XssHttpServletRequestWrapper((HttpServletRequest) request), response);

}

关键是XssHttpServletRequestWrapper的实现方式，继承servlet的HttpServletRequestWrapper，并重写相应的几个有可能带xss攻击的方法，

**public** **class** XssHttpServletRequestWrapper **extends** HttpServletRequestWrapper {

**public** XssHttpServletRequestWrapper(HttpServletRequest request) {

**super**(request);

}

@Override

**public** String getHeader(String name) {

**return** StringEscapeUtils.*escapeHtml4*(**super**.getHeader(name));

}

@Override

**public** String getQueryString() {

**return** StringEscapeUtils.*escapeHtml4*(**super**.getQueryString());

}

@Override

**public** String getParameter(String name) {

**return** StringEscapeUtils.*escapeHtml4*(**super**.getParameter(name));

}

@Override

**public** String[] getParameterValues(String name) {

String[] values = **super**.getParameterValues(name);

**if** (values != **null**) {

**int** length = values.length;

String[] escapseValues = **new** String[values.length];

**for** (**int** i = 0; i < length; i++) {

escapseValues[i] = StringEscapeUtils.*escapeHtml4*(values[i]);

}

**return** escapseValues;

}

**return** **super**.getParameterValues(name);

}

}