# 深入浅出 Spring Security

## 一场系统安全之旅

江南一点雨

华为云MVP、华为云云享专家

# 目录

# HttpFirewall 简介



## 什么是 HttpFirewall

HttpFirewall是Spring Security提供的Http防火墙，它可以用于拒绝潜在的危险请求或者包装这些请求进而控制其行为。通过HttpFirewall可以对各种非法请求提前进行拦截并处理，降低损失。

# HttpFirewall 简介



## 什么是 HttpFirewall

在Servlet容器规范中，为HttpServletRequest定义了一些属性，如contextPath、servletPath、pathInfo、queryString等，这些属性都可以通过get方法获取。

在Servlet容器规范中并没有定义这些属性可以包含哪些值，例如在servletPath和pathInfo中都可以包含RFC2396规范（https://www.ietf.org/rfc/rfc2396.txt）中定义的参数，不同容器对此处理方案也不同，有的容器会对此进行预处理，有的容器则不会。这种比较混乱的处理方式有可能会造成安全隐患，因此Spring Security中通过HttpFirewall来检查请求路径以及参数是否合法，如果合法，才会进入到过滤器链中进行处理。

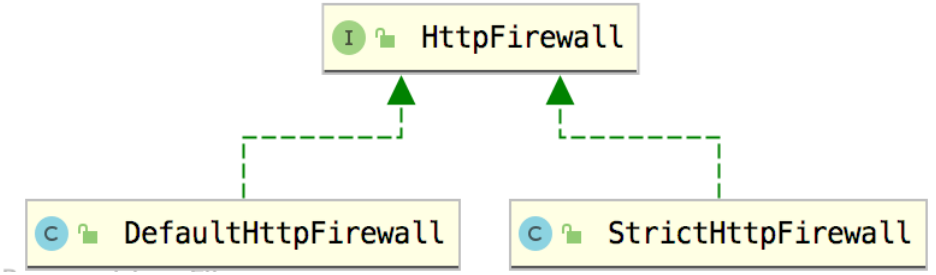
# HttpFirewall 简介



## 什么是 HttpFirewall

Spring Security 中的 HttpFirewall 有两个实现类：

- DefaultHttpFirewall：虽然名字中包含Default，但这并不是框架默认使用的Http防火墙，它只是一个检查相对宽松的防火墙。
- StrictHttpFirewall：这是一个检查严格的Http防火墙，也是框架默认使用的Http防火墙。



# HttpFirewall 严格模式

## StrictHttpFirewall

HttpFirewall严格模式就是使用StrictHttpFirewall，默认即此。严格模式下对请求做出了诸多限制。

# HttpFirewall 严格模式

## StrictHttpFirewall

（1）rejectForbiddenHttpMethod：校验请求方法是否合法。
（2）rejectedBlacklistedUrls：校验请求中的非法字符。
（3）rejectedUntrustedHosts：检验主机信息。
（4）isNormalized：判断参数格式是否合法。
（5）containsOnlyPrintableAsciiCharacters：判断请求字符是否合法。

# HttpFirewall 普通模式

## DefaultHttpFirewall

HttpFirewall普通模式就是使用DefaultHttpFirewall，该类的校验规则就要简单很多。

一般来说，并不建议开发者在项目中使用DefaultHttpFirewall，因为相比于StrictHttp Firewall，DefaultHttpFirewall的安全性要差很多。

# 谢 谢