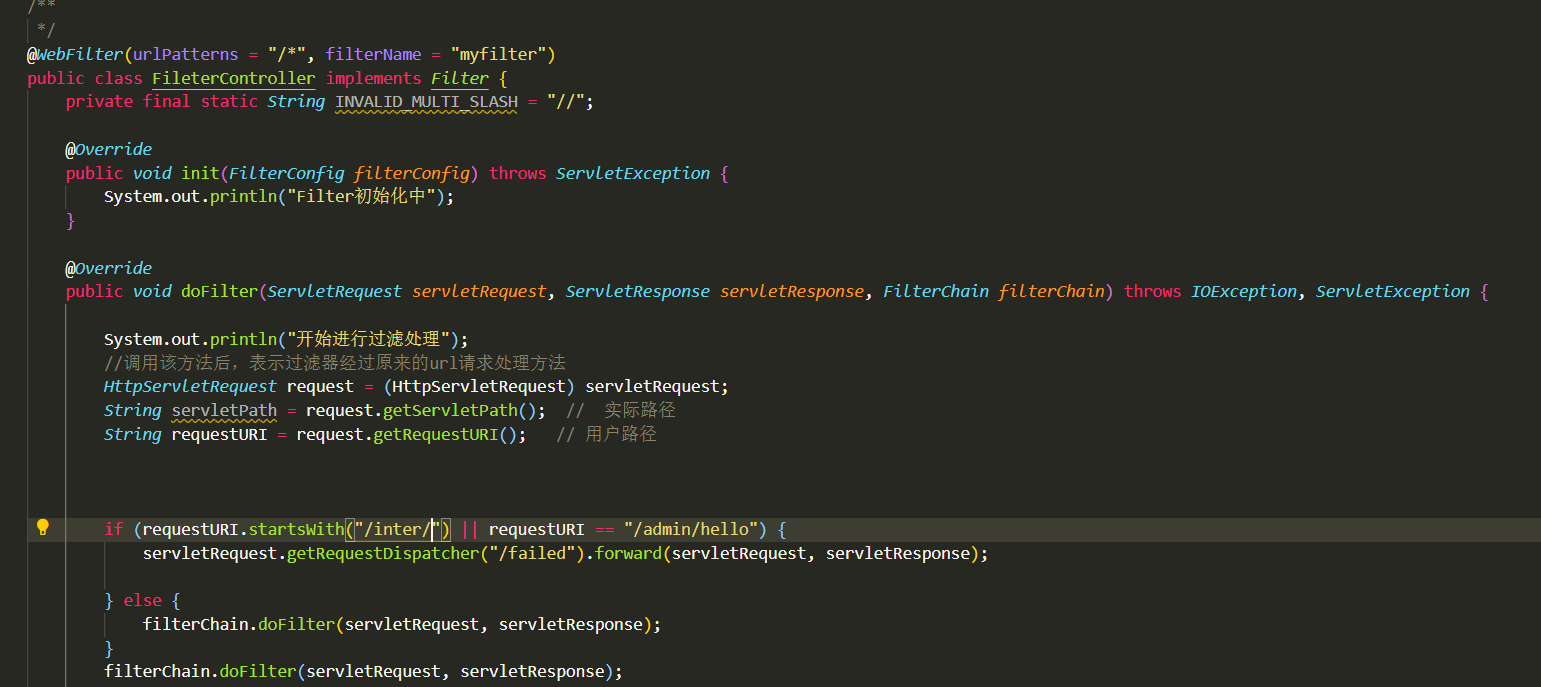
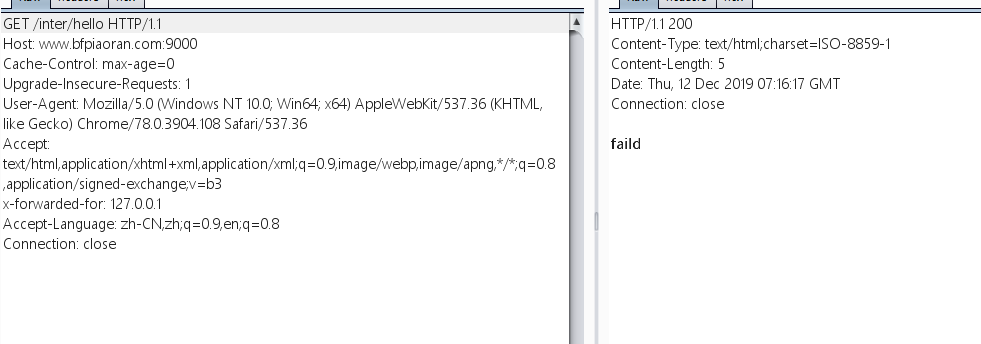
由于业务发展需要一些验证签名的内部接口于是开发信心满满的开发了一个验签的类，

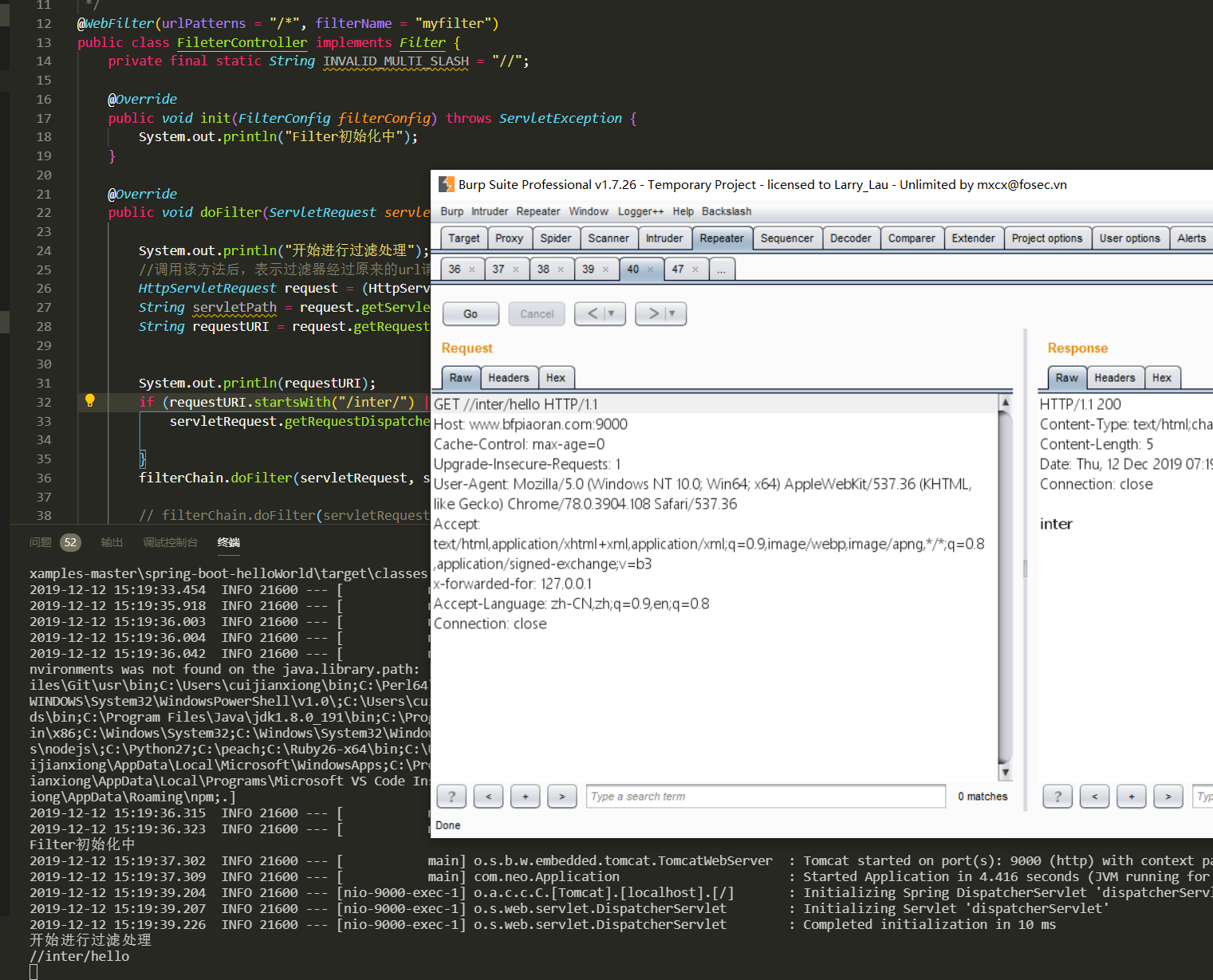
验签类本身是没问题的。由于需要对url进行判断是否验签于是加了个filter



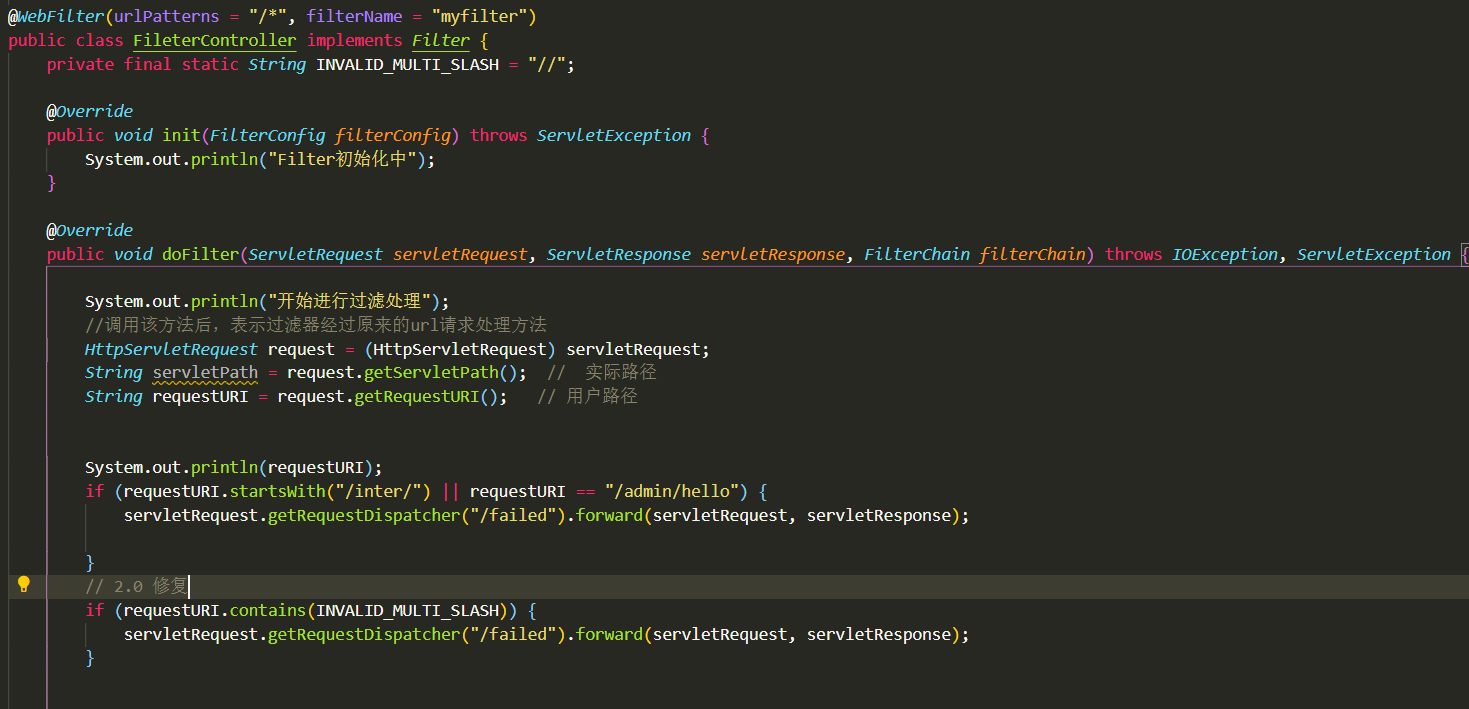
就像上面这样



咋一看一点问题都没有 但是谁想到加个 “/”就饶过了



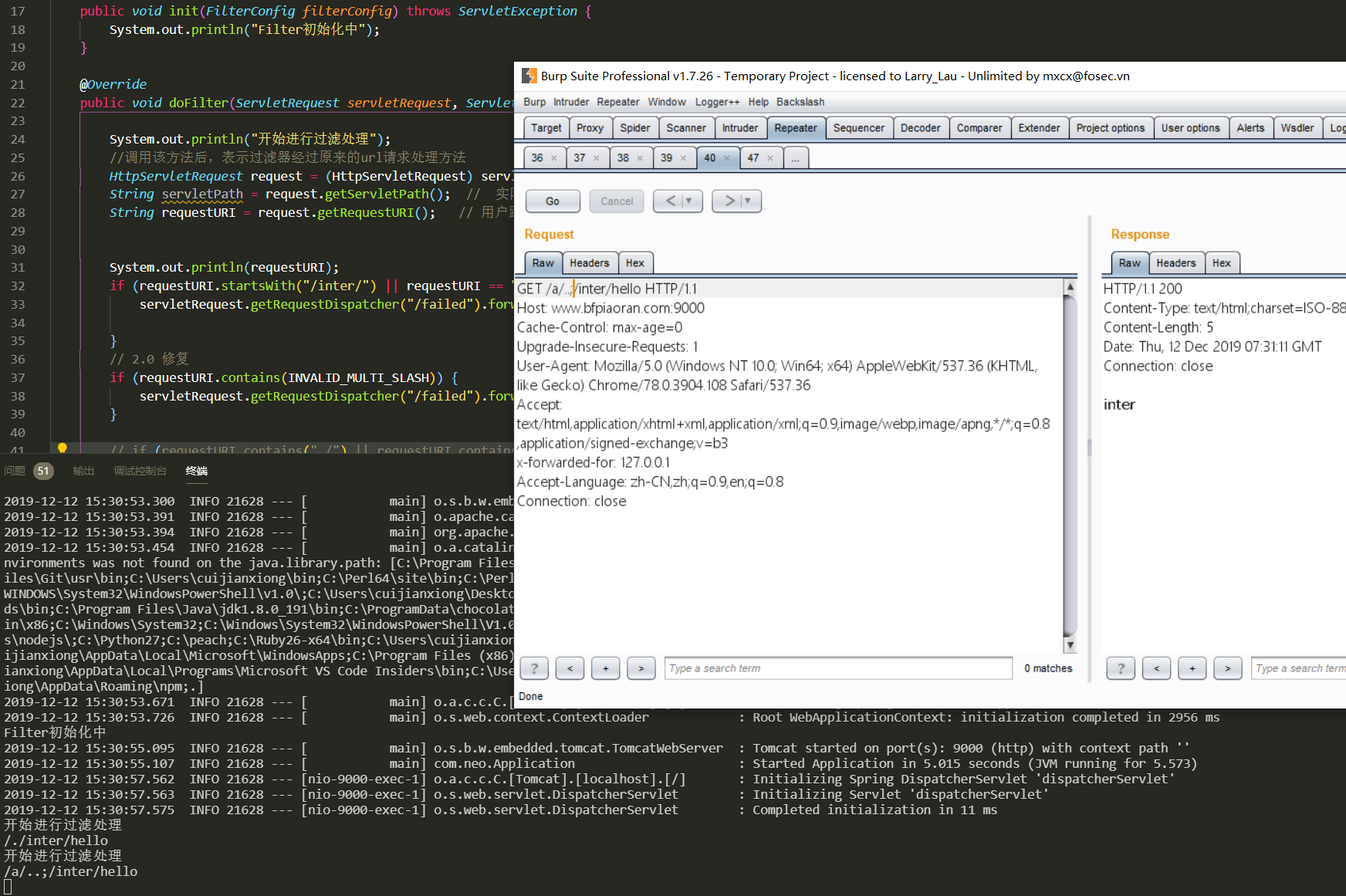
于是开发以 哦 行 我再改一下



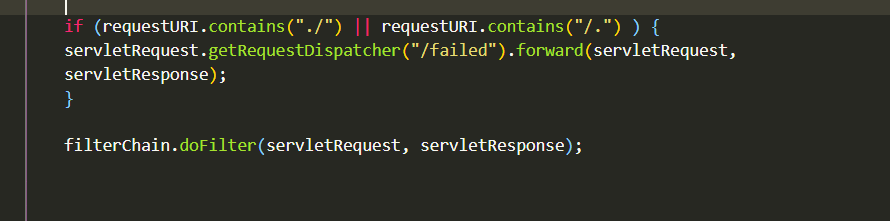
这样绕不过了吧

没一会安全看了下代码有找开发 /a/..;/inter/hello

一样绕过



开发看了眼叹了口气行 我再改

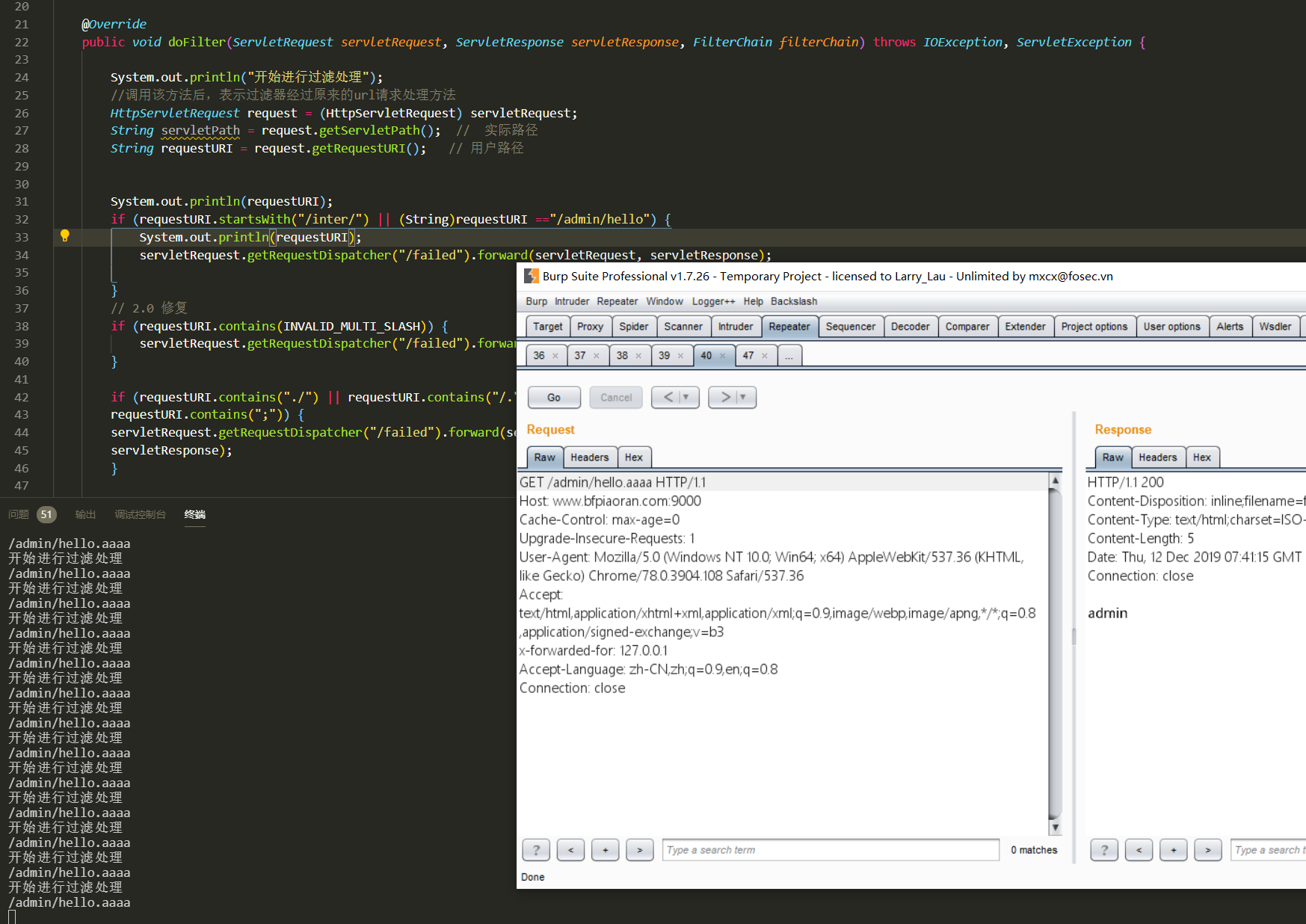


于是又加了行代码



这回绕不过了吧

谁成想过了一阵子安全又来找了



问这个是怎么回事

原来开发为了防止他人误操作加了后缀的容错

于是打算关上 安全忍不住了 你不要用getRequestURI()了

换成getServletPath()吧



安全长舒了一口气

但殊不知更深的坑还在继续。。。。。。