

菩提树下的杨过

博客园

首页

新随笔

订阅

管理

公告



注：技术发展日新月异，随着时间推移，无法保证本博客所有内容的正确性，如有误导，请大家见谅！

英文名：Jimmy.Yang

中文名：杨俊明

一妹儿：yjmyzz#126.com

扣扣：二妻八舅么舅五零妻

昵称：菩提树下的杨过

园龄：11年5个月

荣誉：推荐博客

粉丝：3755

关注：6

+加关注

搜索

找找看

随笔分类(1454)

01.WebForm/MVC(105)

02.FrameWork/C#(142)

03.WinForm(22)

04.JavaScript(85)

05.CSS(25)

06.Design Pattern(14)

07.WPF/Silverlight(118)

08.Database(86)

09.Open Source(171)

10.Delphi(17)

11.Ruby(16)

12.Flex/Flash/AS3.0(124)

13.C/Objective-C(15)

15.Java/Scala(288)

16.linux/mac(41)

17.Hadoop(17)

随笔-1201 文章-1 评论-2788

Spring Security笔记：解决CsrfFilter与Rest服务Post方式的矛盾

基于Spring Security+Spring MVC的web应用，为了防止跨站提交攻击，通常会配置csrf，即：

```
1      <http ...>
2          ...
3          <csrf />
4      </http>
```


如果应用中有Post方式访问的Rest服务(参考下面的代码)，会很不幸的发现，所有POST方式请求的服务会调用失败。

```
1      @RequestMapping(value = "/user/create", method =
RequestMethod.POST)
2      @ResponseBody
3      public UserInfo createUser(@RequestBody(required =
true) UserInfo user,
4          HttpServletRequest request,
5          HttpServletResponse response)
6          throws Exception {
7          ...
8      }
```

原因在于：启用csrf后，所有http请求都会被CsrfFilter拦截，而CsrfFilter中有一个私有类DefaultRequiresCsrfMatcher


```
1      private static final class
DefaultRequiresCsrfMatcher implements RequestMatcher {
2          private Pattern allowedMethods =
Pattern.compile("(GET|HEAD|TRACE|OPTIONS)$");
3
4          /* (non-Javadoc)
5           * @see
6           org.springframework.security.web.util.matcher.RequestMatc
7           her#matches(javax.servlet.http.HttpServletRequest)
```

[18.Python/ML/AI\(52\)](#)[19.Others\(116\)](#)**随笔档案(1201)**[2019年4月 \(5\)](#)[2019年3月 \(4\)](#)[2019年2月 \(6\)](#)[2019年1月 \(10\)](#)[2018年12月 \(11\)](#)[2018年9月 \(3\)](#)[2018年8月 \(5\)](#)[2018年7月 \(3\)](#)[2018年6月 \(1\)](#)[2018年5月 \(4\)](#)[2018年4月 \(6\)](#)[2018年3月 \(6\)](#)[2018年2月 \(1\)](#)[2018年1月 \(1\)](#)[2017年12月 \(6\)](#)[2017年11月 \(5\)](#)[2017年10月 \(5\)](#)[2017年9月 \(4\)](#)[2017年8月 \(9\)](#)[2017年7月 \(4\)](#)[2017年6月 \(5\)](#)[2017年5月 \(3\)](#)[2017年4月 \(7\)](#)[2017年3月 \(1\)](#)[2017年2月 \(2\)](#)[2017年1月 \(2\)](#)[2016年12月 \(1\)](#)[2016年9月 \(1\)](#)[2016年6月 \(3\)](#)[2016年5月 \(2\)](#)[2016年4月 \(1\)](#)[2016年3月 \(13\)](#)[2016年2月 \(10\)](#)[2016年1月 \(15\)](#)[2015年12月 \(14\)](#)[2015年11月 \(4\)](#)[2015年10月 \(5\)](#)[2015年9月 \(18\)](#)[2015年8月 \(17\)](#)[2015年7月 \(6\)](#)

```
request) {  
    8             return  
    !allowedMethods.matcher(request.getMethod()).matches();  
    9         }  
    10     }  
    
```

从这段源码可以发现，POST方法被排除在外了，也就是说只有GET|HEAD|TRACE|OPTIONS这4类方法会被放行，其它Method的http请求，都要验证_csrf的token是否正确，而通常post方式调用rest服务时，又没有_csrf的token，所以校验失败。

解决方法：自己弄一个Matcher

```
  
1 package com.cnblogs.yjmyzz.utils;  
2  
3 import java.util.List;  
4 import java.util.regex.Pattern;  
5  
6 import javax.servlet.http.HttpServletRequest;  
7  
8 import  
org.springframework.security.web.util.matcher.RequestMatc  
her;  
9  
10 public class CsrfSecurityRequestMatcher implements  
RequestMatcher {  
11     private Pattern allowedMethods = Pattern  
12         .compile("(GET|HEAD|TRACE|OPTIONS)$");  
13  
14     public boolean matches(HttpServletRequest request)  
    {  
15  
16         if (excludeUrls != null &&  
excludeUrls.size() > 0) {  
17             String servletPath =  
request.getServletPath();  
18             for (String url : excludeUrls) {  
19                 if (servletPath.contains(url)) {  
20                     return false;  
21                 }  
22             }  
23         }  
24         return  
!allowedMethods.matcher(request.getMethod()).matches();  
25     }  
26  
27     /**
```

2015年6月 (9)
2015年5月 (11)
2015年4月 (6)
2015年3月 (1)
2015年2月 (5)
2015年1月 (9)
2014年12月 (5)
2014年11月 (17)
2014年10月 (15)
2014年9月 (10)
2014年8月 (9)
2014年7月 (14)
2014年5月 (2)
2014年4月 (12)
2014年3月 (7)
2014年2月 (8)
2014年1月 (18)
2013年12月 (1)
2013年11月 (8)
2013年10月 (7)
2013年9月 (3)
2013年8月 (5)
2013年7月 (3)
2013年5月 (4)
2013年4月 (1)
2013年2月 (3)
2013年1月 (2)
2012年12月 (8)
2012年11月 (16)
2012年9月 (1)
2012年7月 (1)
2012年6月 (1)
2012年5月 (1)
2012年4月 (1)
2012年3月 (2)
2012年2月 (2)
2012年1月 (4)
2011年12月 (4)
2011年11月 (2)
2011年10月 (4)
2011年9月 (5)
2011年8月 (2)
2011年7月 (1)
2011年6月 (12)

```
28      * 需要排除的url列表
29      */
30      private List<String> execludeUrls;
31
32      public List<String> getExecludeUrls() {
33          return execludeUrls;
34      }
35
36      public void setExecludeUrls(List<String>
execludeUrls) {
37          this.execludeUrls = execludeUrls;
38      }
39  }
```



这里添加了一个属性execludeUrls，允许人为排除哪些url。

然后在配置文件里，这样修改：



```
1      <http entry-point-ref="loginEntryPoint" use-
expressions="true">
2          ...
3          <intercept-url pattern="/rest/**"
access="permitAll" />
4          ...
5          <csrf request-matcher-
ref="csrfSecurityRequestMatcher"/>
6      </http>
7
8      <beans:bean id="csrfSecurityRequestMatcher"
class="com.cnblogs.yjmyzz.utils.CsrfSecurityRequestMatche
r">
9          <beans:property name="execludeUrls">
10              <beans:list>
11                  <beans:value>/rest/</beans:value>
12              </beans:list>
13          </beans:property>
14      </beans:bean>
```



这里约定所有/rest/开头的都是Rest服务地址，上面的配置就把/rest/排除在csrf验证的范围之外了。

作者：[菩提树下的杨过](#)

出处：<http://yjmyzz.cnblogs.com>

本文版权归作者和博客园共有，欢迎转载，但未经作者同意必须保

- 2011年5月 (15)
- 2011年4月 (16)
- 2011年3月 (11)
- 2011年2月 (9)
- 2011年1月 (8)
- 2010年12月 (10)
- 2010年11月 (13)
- 2010年10月 (10)
- 2010年9月 (5)
- 2010年8月 (12)
- 2010年7月 (32)
- 2010年6月 (19)
- 2010年5月 (21)
- 2010年4月 (30)
- 2010年3月 (49)
- 2010年2月 (23)
- 2010年1月 (22)
- 2009年12月 (47)
- 2009年11月 (26)
- 2009年10月 (12)
- 2009年9月 (7)
- 2009年8月 (14)
- 2009年7月 (2)
- 2009年6月 (27)
- 2009年5月 (14)
- 2009年4月 (4)
- 2009年3月 (14)
- 2009年2月 (9)
- 2009年1月 (3)
- 2008年11月 (5)
- 2008年10月 (8)
- 2008年9月 (34)
- 2008年8月 (40)
- 2008年6月 (2)
- 2008年5月 (8)
- 2008年4月 (10)
- 2008年3月 (20)
- 2008年2月 (12)
- 2008年1月 (24)
- 2007年12月 (36)
- 2007年11月 (27)

友情链接

cloudgamer

留此段声明，且在文章页面明显位置给出原文连接，否则保留追究法律责任的权利。

分类: [15.Java/Scala](#)

标签: [rest](#), [spring-mvc](#), [spring-security](#), [csrf](#)

好文要顶

关注我

收藏该文

[菩提树下的杨过](#)
[关注 - 6](#)
[粉丝 - 3755](#)

荣誉: [推荐博客](#)
[+加关注](#)

11

« 上一篇: [oracle: job使用](#)
» 下一篇: [java:POI导出excel](#)

posted @ 2015-01-06 12:33 菩提树下的杨过 阅读(21365) 评论(7) 编辑 收藏

评论列表

#1楼 2015-08-03 14:34 bingyulei

如果把post都排除了，你还加csrf过滤器干嘛
支持(2) 反对(0)

#2楼[楼主] 2015-08-03 15:07 菩提树下的杨过

@ bingyulei
同一个web application中，即有常规的页面（供普通用户使用），也有少量的rest服务，提供给内部其它应用调用。

常规页面，按正常csrf过滤。

rest服务是以post方式，让调用方post一个request xml过来的，如果不排除，服务调用方就没法用了。
支持(0) 反对(0)

#3楼 2015-12-30 10:17 我只是一个菜鸟

我把csrf 关闭了，我现在遇到就是这样的问题，post请求没有失效，但是post请求所带的参数对象后端获取不了，我把post请求改成GET请求就可以获取到参数了，我现在想在不开启csrf情况进行一些rest 服务，我该怎么呢？
支持(0) 反对(0)

#4楼[楼主] 2015-12-30 10:28 菩提树下的杨过

@ 我只是一个菜鸟
按文中的思路处理，不好使么？

JeffreyZhao

包建强

计算机的潜意识

司徒正美

万一

张逸:晴窗笔记

积分与排名

积分 - 1555140

排名 - 43

最新评论

1. Re:基于Spring的简易SSO设计
学习。。。

--民工也Coding

2. Re:spring cloud: 使用consul来替
换eureka
consul坑这么多,

--eip

3. Re:C#: Func的同步、异步调用
支持

--~雨落忧伤~

4. Re:利用mybatis-generator自动生
成代码
idea可以使用吗

--599466636

5. Re:Oracle: ODP.NET Managed
小试牛刀
@qgshaha我有 遇到, 请问你解决没?
如何解决的啊! ...

--sqlserver爱好者

#5楼 2015-12-30 10:56 我只是一个菜鸟

嗯, 按照你文中的配置了, 常规的页面我也排除了, 但是很奇怪, 常规的
页面POst请求没有问题, 只有rest 服务的post请求会出现参数后台接收
不了的情况, 这是我的spring-security.xml中配置

+ View Code

支持(0) 反对(0)

#6楼 2015-12-30 12:08 我只是一个菜鸟

@ 菩提树下的杨过
问题解决了, 不是spring-security.xml配置文件的问题, 是请求的
Content-Type问题, Content-Type: multipart/form-data;
boundary=----这样就接不到参数, 改成Content-Type:
application/x-www-form-urlencoded 这样就可以接到了, 最终解决
的方法是在spring-mvc.xml的配置文件中加了下配置

```
1 <bean id="multipartResolver"
2     class="org.springframework.web.multipart.
3     <property name="maxUploadSize" value="104
4     </bean>
```

具体中间的原因还待自己去探求。
谢谢你帮助, 看你的博客解决了我很多问题

支持(0) 反对(0)

#7楼 2018-06-11 18:44 啊哈哈哈哈-

@ 我只是一个菜鸟
怎么关闭。我怎么关不了。http.csrf().disable();

支持(0) 反对(0)

刷新评论 刷新页面 返回顶部

注册用户登录后才能发表评论, 请 [登录](#) 或 [注册](#), [访问网站首页](#)。

【推荐】超50万C++/C#源码: 大型实时仿真组态图形源码

【推荐】Java工作两年, 一天竟收到33份面试通知

【活动】“魔程”社区训练营--用实例教你快速学会Scratch和Python

【推荐】程序员问答平台, 解决您开发中遇到的技术难题

相关博文：

- [Spring Security笔记：自定义登录页](#)
- [利用Spring MVC搭建REST Service](#)
- [Springboot+SpringSecurity\(一\)](#)
- [Spring Security学习（二）Spring Security Guides](#)
- [SpringSecurity笔记：解决CsrfFilter与Rest服务Post方式的矛盾](#)

最新新闻：

- 一线 | 任正非：5G技术别人两三年肯定追不上华为
 - 中国智能音箱出货量同比增长近500% 已超过美国
 - 任正非：家人现在仍在用苹果手机 苹果生态很好
 - 朱诺号团队发现木星和地球存在相似之处：磁场会经历长期变化
 - 任正非回应美国禁令延期90天：没意义 我们准备好了
- » [更多新闻...](#)