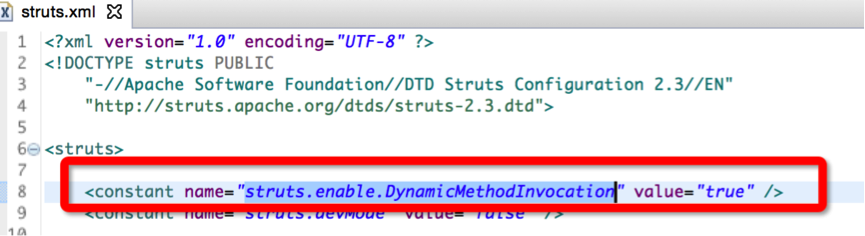
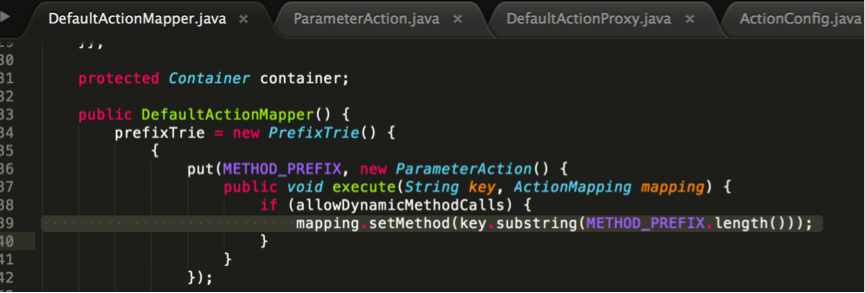
Struts2 s2-032远程代码执行分析

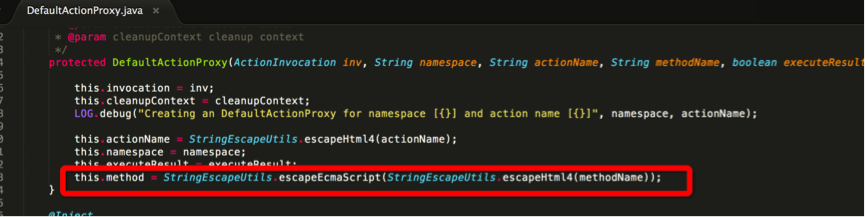
1. 介绍：  
Struts 2是Struts的下一代产品，是在 struts 1和WebWork的技术基础上进行了合并的全新的Struts 2框架。其全新的Struts 2的体系结构与Struts 1的体系结构差别巨大。Struts 2以WebWork为核心，采用拦截器的机制来处理用户的请求，这样的设计也使得业务逻辑控制器能够与 ServletAPI完全脱离开，所以Struts 2可以理解为WebWork的更新产品。虽然从Struts 1到Struts 2有着太大的变化，但是相对于WebWork，Struts 2的变化很小。

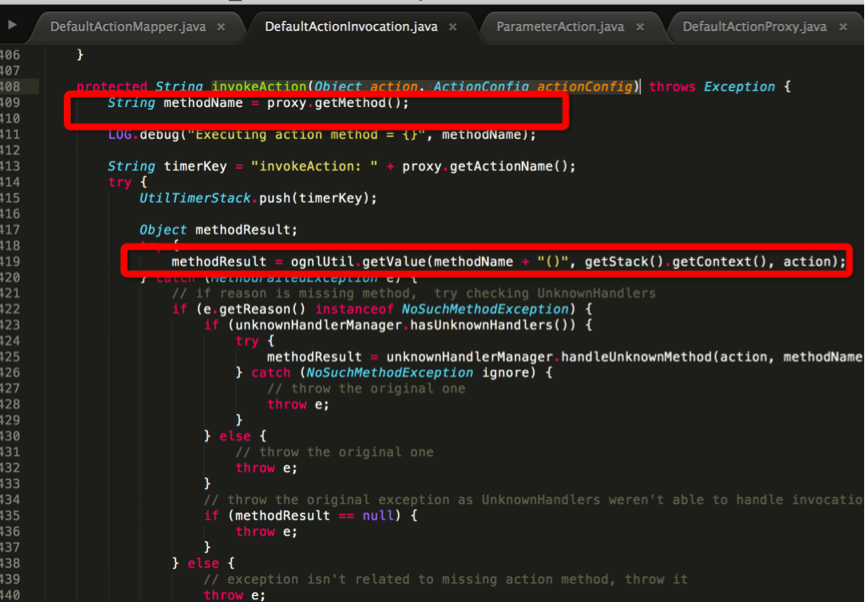
4月15号安恒安全研究院在Struts 2上发现了一个严重的远程代码执行漏洞（CVE-2016-3081)

[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/04/3E531F28-2E05-48AE-8293-88AD63993547.jpg)

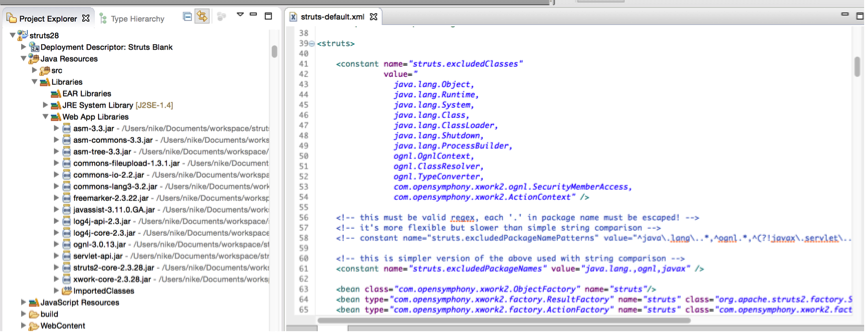
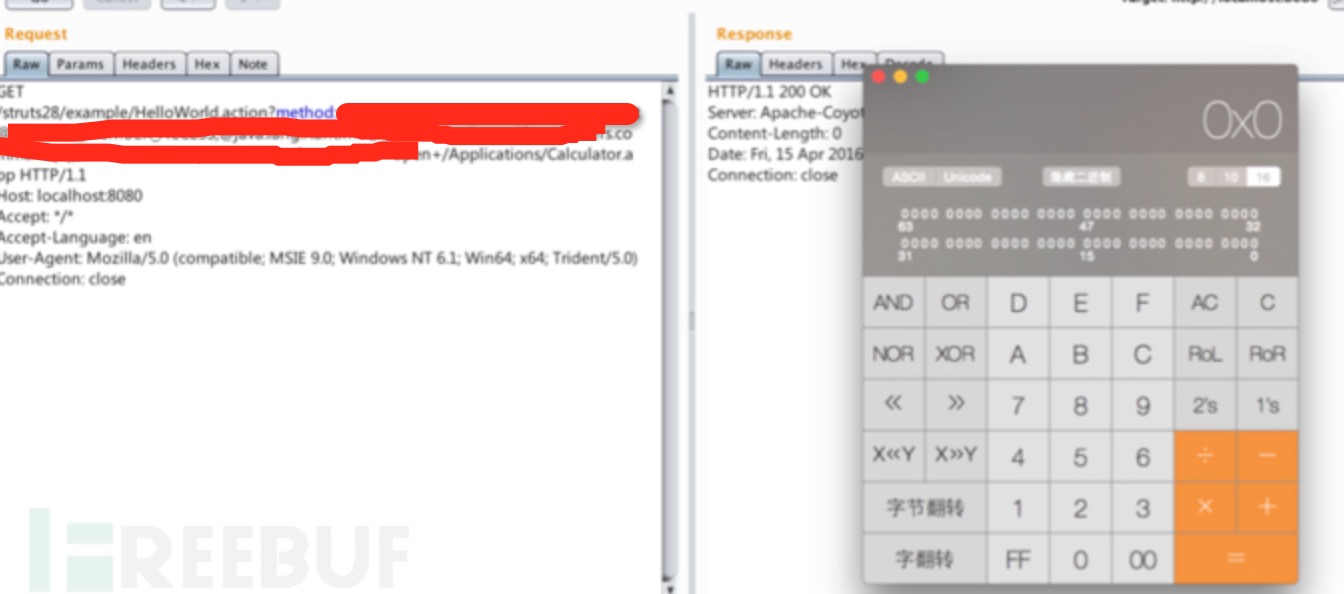
2. 漏洞分析  
前提：开启动态方法调用。  
[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/04/%E6%97%A0%E6%A0%87%E9%A2%98.png)

假如动态方法调用已经开启,然后我们要调用对应的login方法的话 我们可以通过<http://localhost:8080/struts241/index!login.action>来执行动态的方法调用。这种动态方法调用的时候method中的特殊字符都会被替换成空，但是可以通过[http://localhost:8080/struts241/index.action?method:login来绕过无法传入特殊字符的限制](http://localhost:8080/struts241/index.action?method:login%C0%B4%C8%C6%B9%FD%CE%DE%B7%A8%B4%AB%C8%EB%CC%D8%CA%E2%D7%D6%B7%FB%B5%C4%CF%DE%D6%C6)。  
[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/04/%E6%97%A0%E6%A0%87%E9%A2%981.png)

接收到的参数会经过处理存入到ActionMapping的method属性中。DefaultActionProxyFactory将ActionMappping的method属性设置到ActionProxy中的method属性（虽然做了escapeEcmaScript，escapeHtml4过滤，但是我们可以通过变量传递方式绕过，具体可以参考poc）。如下图  
[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/04/%E6%97%A0%E6%A0%87%E9%A2%982.png)

而DefaultActionInvocation.java中会把ActionProxy中的method属性取出来放入到ognlUtil.getValue(methodName + “()”, getStack().getContext(), action);方法中执行ognl表达式，如下图  
[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/04/%E6%97%A0%E6%A0%87%E9%A2%983.png)

3. 沙盒绕过:  
通过ognl表达式静态调用获取ognl.OgnlContext的DEFAULT\_MEMBER\_ACCESS属性，并将获取的结果覆盖\_memberAccess属性，这样就可以绕过SecurityMemberAccess的限制。

a. 测试环境：  
[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/04/%E6%97%A0%E6%A0%87%E9%A2%984.png)  
b. 结果：  
[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/04/7C698310-4B58-447D-BAF5-996A277E1126.jpg)

修复方案：

升级至struts 2.3.20.2,struts 2.3.24.2, struts 2.3.28.1