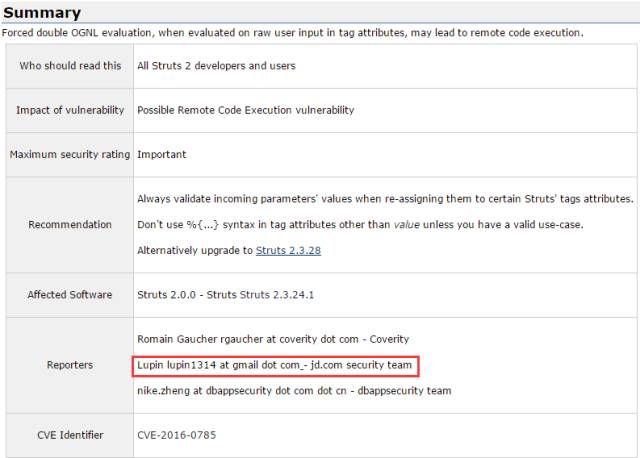
**京东安全团队获Struts2官方致谢**

[京东](http://www.wtoutiao.com/tag/938.html)

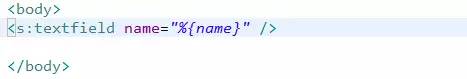
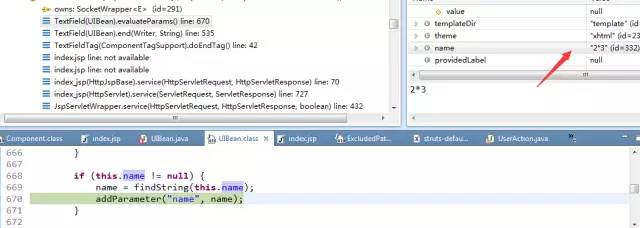
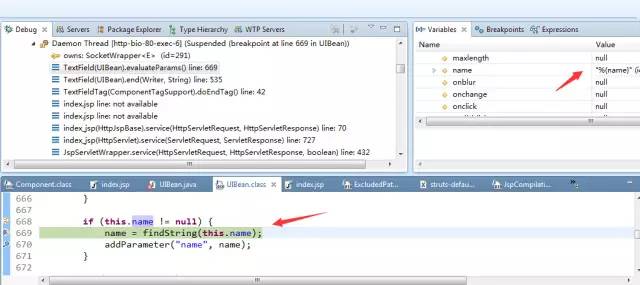
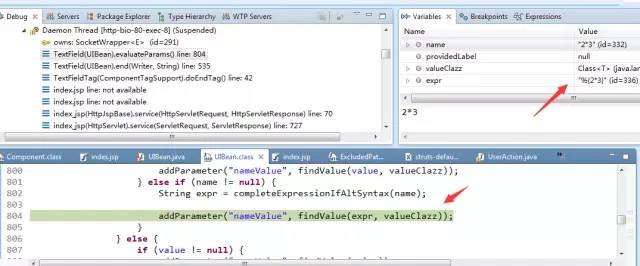
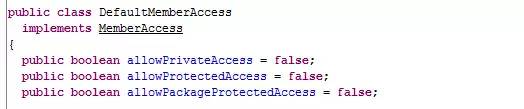
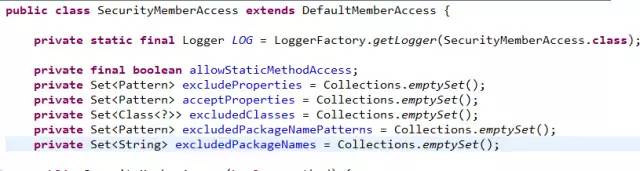
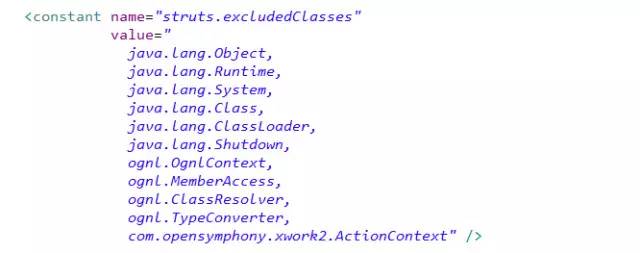
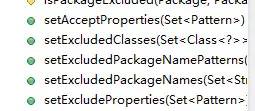
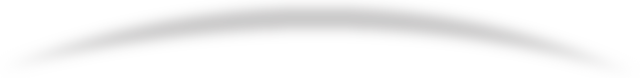
[京东安全应急响应中心](http://www.wtoutiao.com/author/jsrc_team.html) · 2016-03-23 17:21



 京东信息安全研究员Lupin提交对S2-029漏洞的另一场景分析，近日收到Struts2官方的确认和感谢。各种咨询信息扑面而来，为满足大家需求，本次特邀Lupin为大家详细介绍Struts2的UI标签通过name属性计算value的过程，各位看官就请跟随

Lupin来揭开这层神秘的面纱吧！

Lupin京东信息安全研究员  
这篇文章在S2-029漏洞发布第二天本就已撰写完毕，但当时这个漏洞在圈子里众说纷纭，我自己也不确定此漏洞是否为S2-029，便将这个问题反馈给Struts2官方。Struts2很快有了回复：这个问题如果在老版本中确实可确定为一个漏洞，但新版本中已不能通过OGNL执行系统命令。  
这个我是知道的，在去年测试时，便就已经发现Struts2框架加入了OGNL“沙盒”，限制OGNL的功能，各种危险操作会被拦截，但这个“沙盒”在设计时又犯了错误，导致里面的黑名单可以被重置，从而执行任意代码。  
后来，由于国内对于S2-029漏洞的关注，已经有一些文章中提到了“沙盒”可以被重置，这个也就不再是秘密，我再次把这个问题反馈给了官方，官方此次给予了肯定，把这个问题一并加入了S2-029。  
关于第一个老外提交漏洞的各种分析，此处不再赘述，各位看官请跟随我来看Struts2的UI标签通过name属性计算value的过程。org.apache.strtus2.components.UIBean.javaevaluateParams方法（省略部分代码）

UIBean类是struts2中各种UI标签的父类，里面封装了UI标签的一些通用动作，分析一下evaluateParams方法的关键代码，首先可以看到如果name值不为null，会去调用findString方法取值，findString方法会去调用。  
TextParseUtil.translateVariables把name的值当做OGNL表达式执行，然后赋值给局部变量name，这是第一次OGNL代码执行；再往后看，如果标签中没有指定value的值，会去根据局部变量name的值执行findVlaue方法，findValue方法最终会调用TextParseUtil.translateVariables方法，完成第二次OGNL代码执行。  
这样分析不太容易明白，我们调试一下，首先引入一个标签，代码如下：name是我们action类中的一个属性，然后在evaluateParams方法下断点，调试。浏览器访问：http://localhost/Test.action?name=2\*3，第一次OGNL表达式执行 ，也就是%{name}执行，结果是2\*3。第二次2\*3被当做OGNL代码执行，结果放入value中。 到这里就非常清楚了，总结一下：1、标签的name属性通过%{name}去action中取值；2、%{name}执行，执行结果为2\*3（OGNL第一次执行）；3、%{2\*3}执行，执行结果为6，放在value属性中（OGNL第二次执行）。  
关于OGNL沙盒Struts2官方为了加强安全性，对ognl代码进行了更强的安全校验，包括类和包名的黑名单，以及对一些访问属性的限制。Strtus-default.xml中的配置：http://img6.wtoutiao.com/mmbiz/Z9MuUwaeeGLkRP07gG9jqicBEIdY6aUANcn1laeZNmibHy89A9GAssuiclff4gKb3eDjlYISCFI13icqOmJDibKqnrA/0?wx_fmt=jpeg在isAccessible方法中会根据这些限制对OGNL语法树做检测，但是我们仔细观察不难发现这些属性都有public的set方法，并且构建空set集合方法也很多，比如：@java.util.Collections@EMPTY\_SET、#{}.entrySet()等等。完全可以把相应的各种限制都解除，解除了限制之后执行任意代码完全没有问题。参考：http://struts.apache.org/docs/s2-029.html  
Lupin，京东信息安全研究员。  
主要负责京东网络安全的应急响应与日常安全检测。擅长web安全以及java代码层面安全与漏洞挖掘。