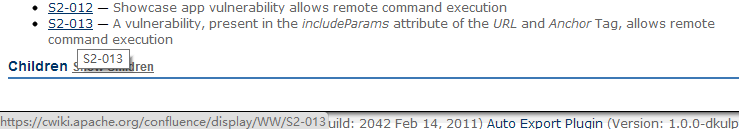
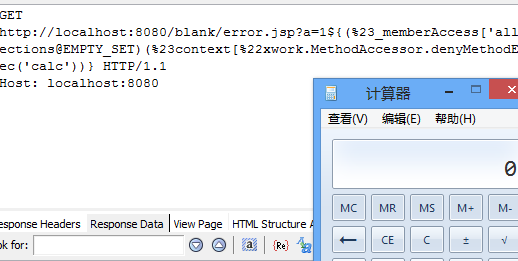
by 空虚浪子心 http://www.inbreak.net 微博：http://t.qq.com/javasecurity  
**摘要**  
Apache官方的struts2产品，最近出了一个远程代码执行漏洞，编号“S2-013”，目前是0DAY，官方没有修补方案出现。  
http://struts.apache.org/development/2.x/docs/security-bulletins.html — （公告）  
官方安全公告给出了编号和简要介绍，“A vulnerability, present in the includeParams attribute of the URL and Anchor Tag, allows remote command execution”。  
但是并没有说原理，也没有发布任何补丁。  
**分析：**  
事实上，这次struts2官方一共发了两个漏洞，还有个叫s2-012，但是这个漏洞，看题目，应该是我之前在《Xcon2012 攻击JAVA WEB》时的已经爆出来了，所以本文只说另一个。  
struts2官方的开发傻乎乎的，比如这个漏洞，要么官方就不要发出来，既然发出来了，就应该发补丁，但是官方仅仅发了这段话，对于详细内容，普通用户不开放访问。  
  
从这段话可以大致总结一下几点：  
1、未修补的远程代码执行漏洞  
2、includeParams参数在URLTAG中出现了问题。  
仅根据这两点，熟悉struts2运行机制和之前漏洞原理的人，都可以轻易分析出具体利用POC。  
**漏洞触发：**  
由于官方没有发补丁，所以最新版本的struts2还是有漏洞的，可以下载最新：Apache Struts 2.3.14 GA的示例应用。  
经过简单测试，就看到了想要的结果。  
根据官方给的信息，问题出在a标签，所以写个jsp页面，内容如下：

|  |
| --- |
| <s:a includeParams="all">Click here.</s:a> |

这个是struts2标签库的a标签，该标签会在页面上显示当前URL，当includeParams=all时，就会显示具体参数内容。  
唯一需要解的迷，就是如何让参数内容作为OGNL表示试执行，但是这个迷未免太好猜了，我随手测试就出结果。  
访问url：  
http://localhost:8080/blank/error.jsp?aaa=${struts2的常用POC，你懂得}  
就可以直接弹计算器，POC代码大家都有的，我只截个图：  
  
几乎没有什么分析过程，就拿到了POC，最终为了研究修补方案，只好被迫研究了漏洞原理。  
**漏洞原理：**  
Struts2标签库中的url标签和a标签的includeParams这个属性，代表显示请求访问参数的含义，一旦它的值被赋予ALL或者GET或者POST，就会显示具体请求参数内容。按照正常的需求，把参数urlEncode一下也就够了， 问题在于，struts竟然多做了一步，这丫把参数做了OGNL解析！  
代码：

|  |
| --- |
| **package** org.apache.struts2.views.uti.DefaultUrlHelper这个**class**的parseQueryString方法。  **public** Map<String, Object> parseQueryString(String queryString, **boolean** forceValueArray) {  Map<String, Object> queryParams = **new** LinkedHashMap<String, Object>();  **if** (queryString != **null**) {  ......  **if** (paramName != **null**) {  paramName = translateAndDecode(paramName);  String translatedParamValue = translateAndDecode(paramValue);  ......  translateAndDecode会调用  **private** String translateVariable(String input) {  ValueStack valueStack = ServletActionContext.getContext().getValueStack();  **return** TextParseUtil.translateVariables(input, valueStack);  } |

最终TextParseUtil.translateVariables会直接调用OGNL解析执行。  
**漏洞修补：**  
等官方吧，我反正不急的。或者有好人转发时，请顺便写上方案。