S2-045漏洞分析

exploitcat / 2017-03-08 07:30:00 / 浏览数 2568 安全技术 漏洞分析 顶(0) 踩(0)

这个分析写的我有点汗颜，强烈建议抵制struts2，改为更加可靠的SpringMVC。

背景是，Struts2默认处理multipart报文的解析器是jakarta，是这个组件出现了问题。

该组件定义在了struts-default.xml中，因此，只要不修改parser，并且版本在受影响范围内，肯定是有问题的。

令我非常疑惑的是，一个content-type怎么就能用ognl解析并执行的呢？所以下面来单步调试一下。

问题出现在org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest类中的buildErrorMessage方法里：

传入了非法的Content-type之后会引发JakartaMultiPartRequest类报错，因此会来到这个方法去处理错误信息，进入findText函数：

又调用了getDefaultMessage方法，继续：

关键在这个translateVariable方法里，进入方法定义你就会发现猫腻了。。。。。

居然将错误信息当做ognl表达式执行了，当然，是提取出有效的部分，注意到$以及 %，exp上是%{.....}，实际上${....}也可以，不知道会不会绕过某些waf呢。

最终在OgnlTextParser的evaluate方法执行了命令，非常奇怪的逻辑。。。。。为什么非要解析错误信息里的ognl呢

最后，不管是出于什么目的泄露poc都是无耻的行径！！！

上一篇：一条命令引发的思考 下一篇：NTFS 3g本地提权漏洞—【CV...

1. 0 条回复
   - 动动手指，沙发就是你的了！