CVE-2017-12615漏洞分析：

目录

[复现 1](#_Toc35010752)

[分析 2](#_Toc35010753)

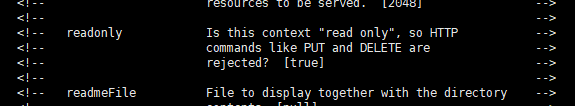
[Bypass 分析 4](#_Toc35010754)

[影响 5](#_Toc35010755)

## 复现

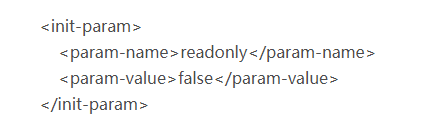
根据描述，在 Windows 服务器下，将 readonly 参数设置为 false 时，即可通过 PUT 方式创建一个 JSP 文件，并可以执行任意代码。

通过阅读 conf/web.xml 文件，可以发现：

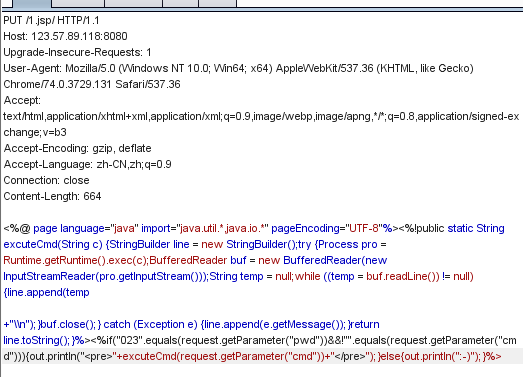


默认 readonly 为 true，当 readonly 设置为 false 时，可以通过 PUT / DELETE 进行文件操控。

配置 readonly 为 false。



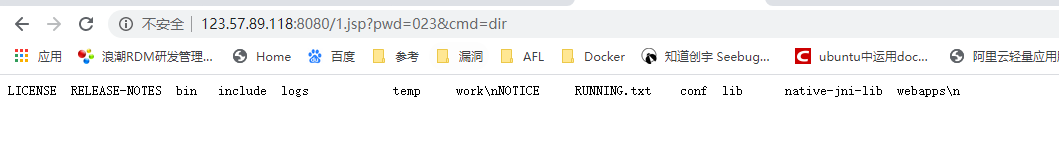
用burpsuit发送攻击代码：



检查服务器端发现上传成功：



输入命令dir进行测试：



## 分析

Tomcat 的 Servlet 是在 conf/web.xml 配置的，通过配置文件可知，当后缀名为 .jsp 和 .jspx 的时候，是通过JspServlet处理请求的：



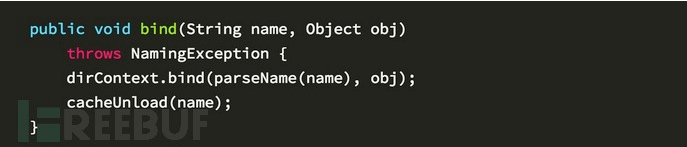
而其他的静态文件是通过DefaultServlet处理的：



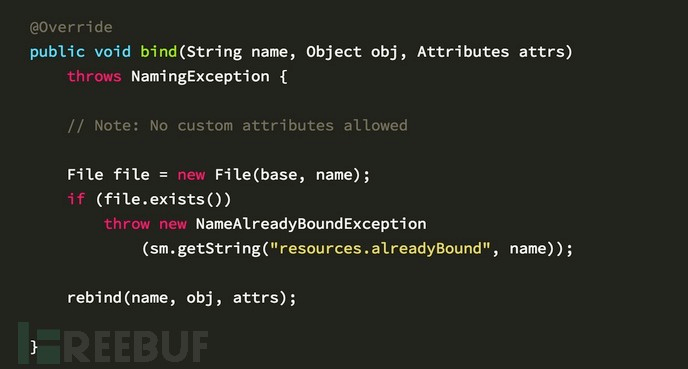
可以得知，“1.jsp ”（末尾有一个和空格）并不能匹配到 JspServlet，而是会交由DefaultServlet去处理。当处理 PUT 请求时：



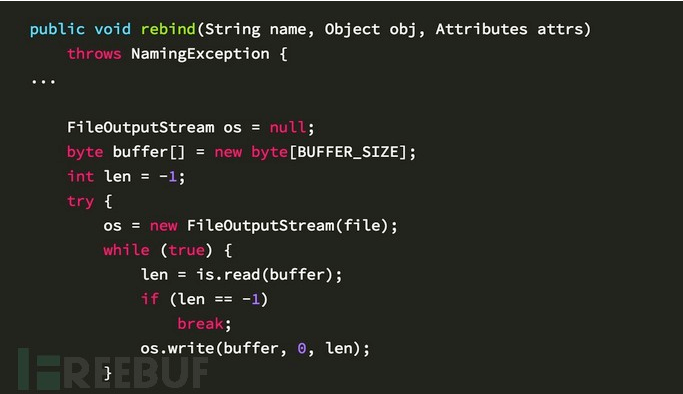
会调用resources.bind：



dirContext 为FileDirContext：



调用 rebind创建文件

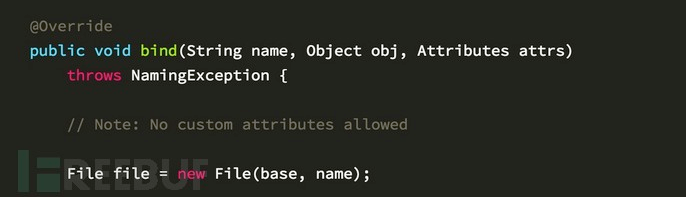


又由于 Windows 不允许“ ”作为文件名结尾，所以会创建一个 .jsp 文件，导致代码执行。

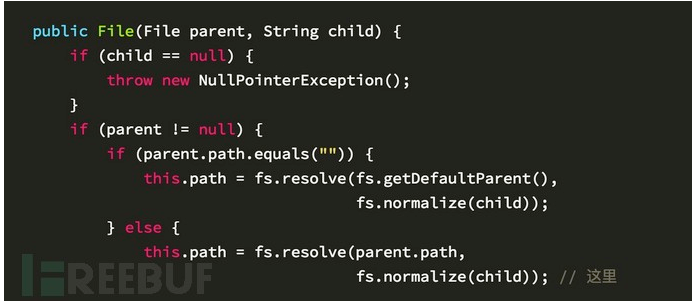
## ****Bypass 分析****

然而，经过黑盒测试，当 PUT 地址为/1.jsp/时，仍然会创建 JSP，会影响 Linux 和 Windows 服务器，并且 Bypass 了之前的补丁，分析如下。

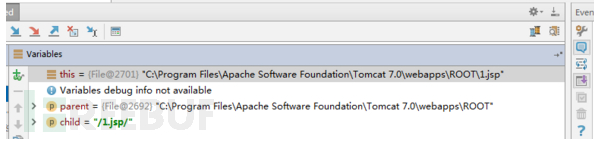
在进入 bind 函数时，会声明一个 File 变量：



进入 File 后，会对 name 进行 normalize



最后得到的 path 就是没有最后 / 的 path 了:



## 影响

由于存在去掉最后的 / 的特性，那么这个漏洞自然影响 Linux 以及 Windows 版本。而且经过测试，这个漏洞影响全部的 Tomcat 版本，从 5.x 到 9.x 无不中枪。目前来说，最好的解决方式是将 conf/web.xml 中对于 DefaultServlet 的 readonly 设置为 true，才能防止漏洞。