黑客派

jrebel 破解方法

作者：sdandroid

原文链接：https://hacpai.com/article/1358592244930

来源网站：黑客派

其实jrebel 破解很简单。用到的工具有 jd-gui <a href="https://link.hacpai.com
forward?goto=http%3A%2F%2Fjava.decompiler.free.fr%2F%3Fq%3Djdgui" target="_blank" re
="nofollow ugc"> 地址。jd-gui是 java 反编译工具，非常好用。
<a href="https://link.hacpai.com/forward?goto=http%3A%2F%2Fdl.sdandroid.com%2Fu
2F62586490%2Fjrebel-crack.jpg" target="_blank" rel="nofollow ugc"><img src="https://static
hacpai.com/images/img-loading.svg" alt="" width="1112" height="718" data-src="http://dl.
dandroid.com/u/62586490/jrebel-crack.jpg">
用 jd-gui 打开jrebel的jar就可以看到如图。这个UserLicense 类是，用来读取jre
el.lic 的，既然可以读取，反过来我们也可以重写License。
我们重写的license 包括以下内容就可以了。
Map testmap=new HashMap();
 testmap.put("Name", "test");
 testmap.put("Pro
uct", "JavaRebel");
 testmap.put("Seats", "Unlimited");
 testmap.put("override", "true")

 testmap.put("Comment", " ####### ######");
 testmap.put("enterprise", "true");<
r> testmap.put("Organization", "test");
 testmap.put("commercial", "true");
 testmap.
ut("noBanner", "false");
不知道如何重写license 可以在jrebel 文件中查看 是如何读取文件的。
用我们重写过的license 替换原来的，启动 jrebel ，jrebel 会认为这个license是非法的。因为我
自己重写的license 是通不过jrebel的验证的。
解决办法就是取消jrebel的验证。这里要用到 javassist 去修改class文件。jrebel 的源代
是经过混淆处理的，很难看。
public byte[] getSignature()
 {
 return this.signature;
 }
这个方法就是验证lic 是否有效，jd 收索 看哪里到用来这个方法，再修改那个方法直接返回true
可以了。应该可以看到多个地方有调用，我们只需要修改，调用getSignature的方法返回
类型是boolean 的修改就可以了。
修改完后，写到本地份文件，再用反编译工具查看是否正确。
再就是把修改过后的class 替换原来的就行了，替换方法 <a href="https://link.hacpai.c
m/forward?goto=http%3A%2F%2Fwww.sdandroid.com%2Fjar-update-file.html" target="_bla
k" rel="nofollow ugc">http://www.sdandroid.com/jar-update-file.html

javassist 的具体使用自行收索。

再启动jrebel 时就没有了非法的提示了。

这里就不提供源码的，实在有不懂的可以联系我。

