# S11-1SpringActuarot-JolokiaRealm-RCE

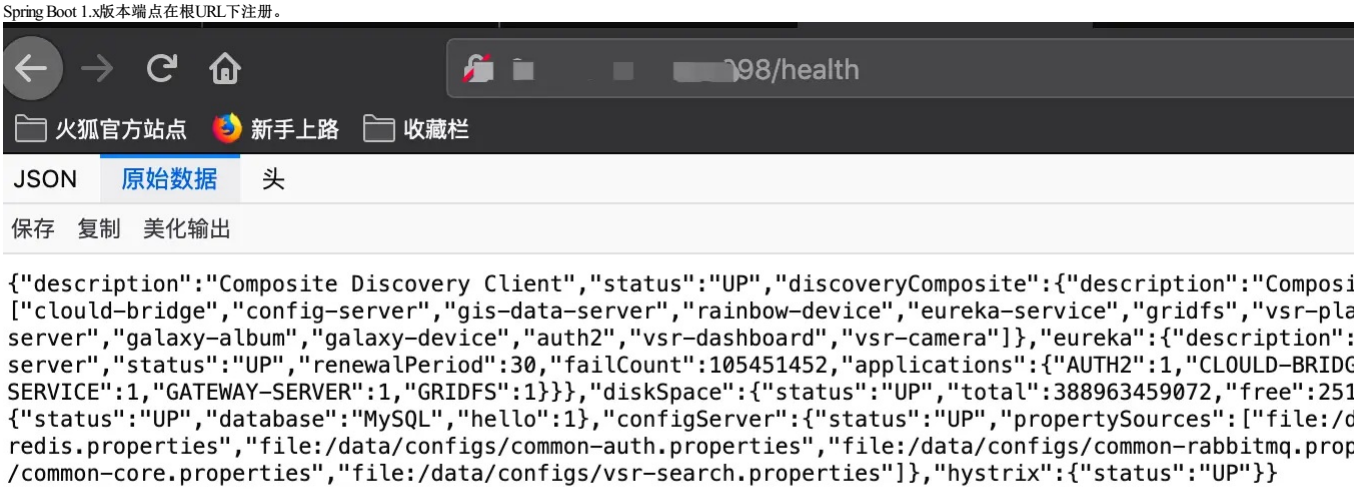
## 漏洞描述：

Actuator 是 Spring Boot 提供的服务监控和管理中间件。当 Spring Boot 应用程序运行时，它会自动将多个端点注册到路由进程中。当配置jolokia/list接口，且访问jolokia/list接口存在type=MBeanFactory和createJNDIRealm关键字时，存在Spring jolokia Realm JNDI远程代码执行漏洞。

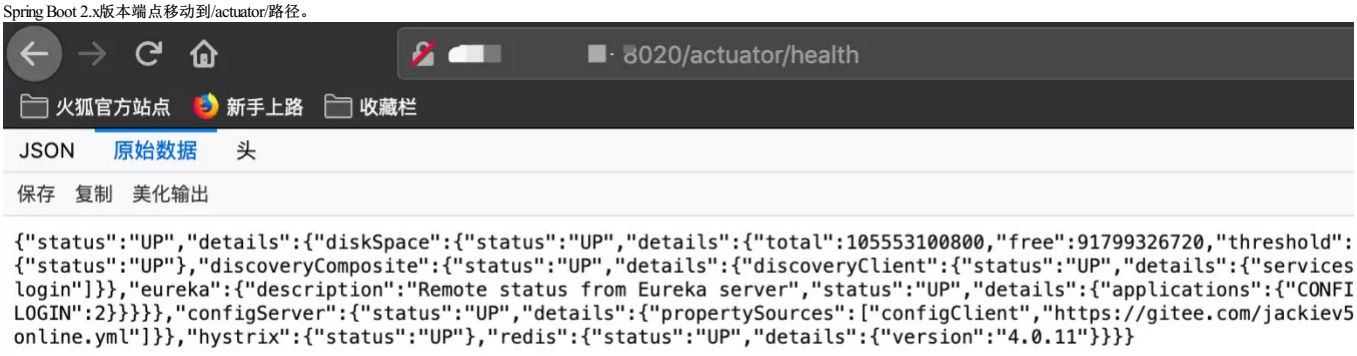
## 影响版本：

- Spring Boot < 1.5 默认未授权访问所有端点
- Spring Boot >= 1.5 默认只允许访问/health和/info端点，但是此安全性通常被应用程序开发人员禁用

Spring Boot 1.x版本端点在根URL下注册。




Spring Boot 2.x版本端点移动到/actuator/路径。

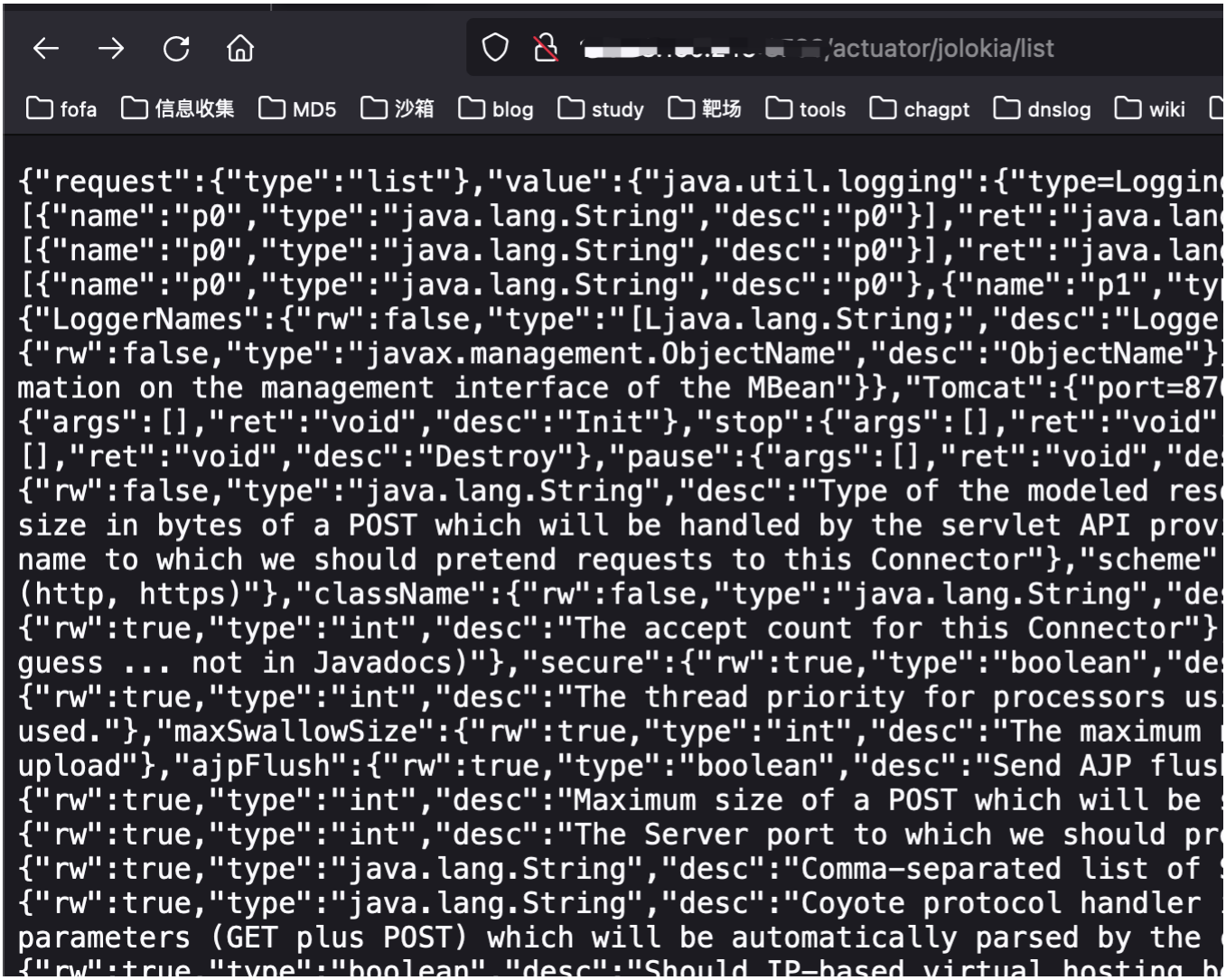



**网站图片：**

网站图片文件是一个绿色的树叶

特有的报错信息。


存在/jolokia/list接口


[redacted],'actuator/jolokia/list
fofa
信息收集
MD5
沙箱
blog
study
靶场
tools
chagpt
dnslog
wiki
{"request":{"type":"list"},"value":{"java.util.logging":{"type=Loggin
[{"name":"p0","type":"java.lang.String","desc":"p0"}],"ret":"java.lan
[{"name":"p0","type":"java.lang.String","desc":"p0"}],"ret":"java.lan
[{"name":"p0","type":"java.lang.String","desc":"p0"},{"name":"p1","ty
{"LoggerNames":{"rw":false,"type":"[Ljava.lang.String;","desc":"Logge
{"rw":false,"type":"javax.management.ObjectName","desc":"ObjectName"}
mation on the management interface of the MBean"}},"Tomcat":{"port=87
{"args":[],"ret":"void","desc":"Init"},"stop":{"args":[],"ret":"void"
[],"ret":"void","desc":"Destroy"},"pause":{"args":[],"ret":"void","de
{"rw":false,"type":"java.lang.String","desc":"Type of the modeled res
size in bytes of a POST which will be handled by the servlet API prov
name to which we should pretend requests to this Connector"},"scheme"
(http, https)"},"className":{"rw":false,"type":"java.lang.String","de
{"rw":true,"type":"int","desc":"The accept count for this Connector"}
guess ... not in Javadocs)"},"secure":{"rw":true,"type":"boolean","de
{"rw":true,"type":"int","desc":"The thread priority for processors us
used."},"maxSwallowSize":{"rw":true,"type":"int","desc":"The maximum
upload"},"ajpFlush":{"rw":true,"type":"boolean","desc":"Send AJP flus
{"rw":true,"type":"int","desc":"Maximum size of a POST which will be
{"rw":true,"type":"int","desc":"The Server port to which we should pr
{"rw":true,"type":"java.lang.String","desc":"Comma-separated list of
{"rw":true,"type":"java.lang.String","desc":"Coyote protocol handler
parameters (GET plus POST) which will be automatically parsed by the
{"rw":true,"type":"boolean","desc":"Should IP-based virtual hosting b