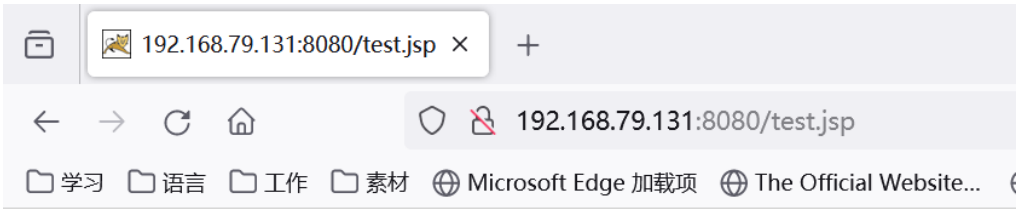
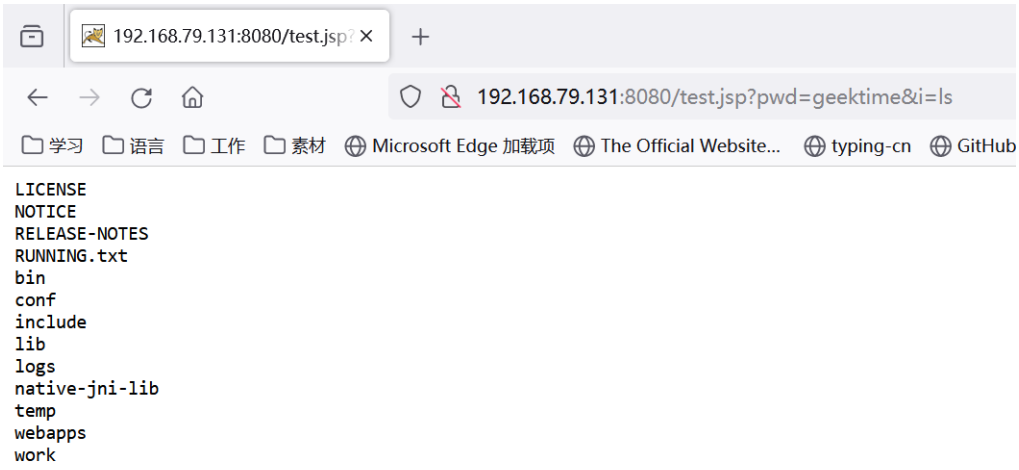
1. 安装 Java 环境并激活 Burp。

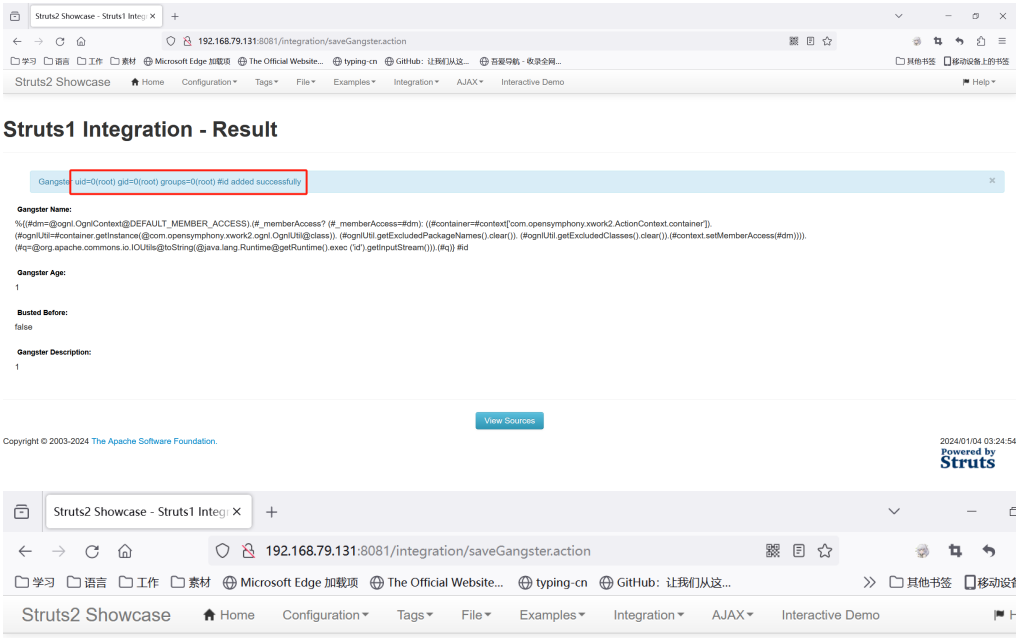
```
C:\Users\m1521>javac
用法: javac <options> <source files>
其中, 可能的选项包括:
  @<filename>                  从文件读取选项和文件名
  -Akey[=value]                传递给批注处理程序的选项
  --add-modules <模块>(,<模块>)*
        除了初始模块之外要解析的根模块; 如果 <module>
                为 ALL-MODULE-PATH,
        则为模块路径中的所有模块。
```

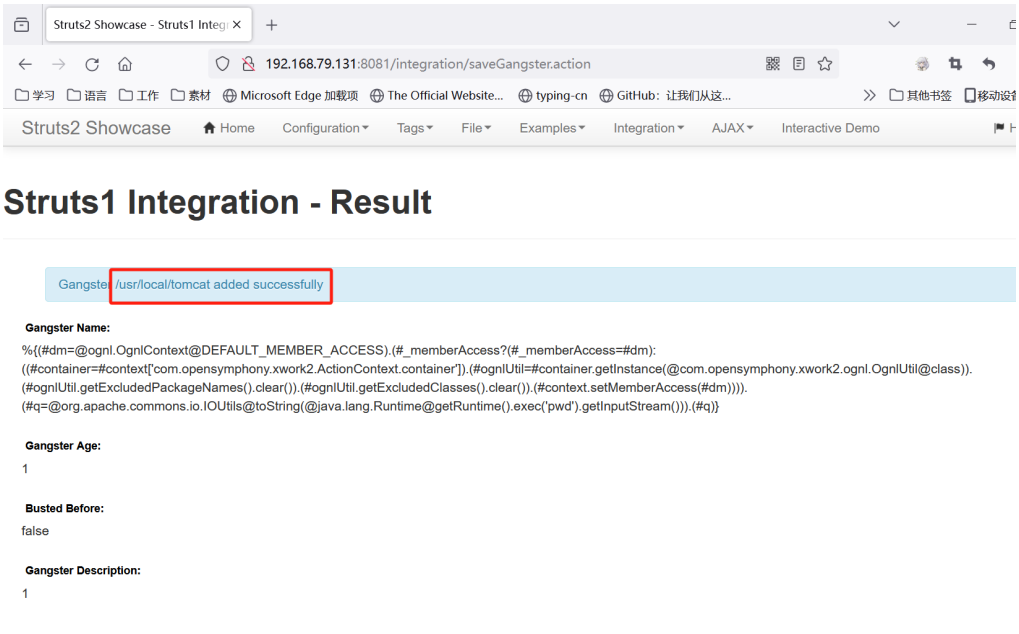
2. 练习 Tomcat PUT 方法任意写文件漏洞（CVE-2017-12615），提供命令执行截图。



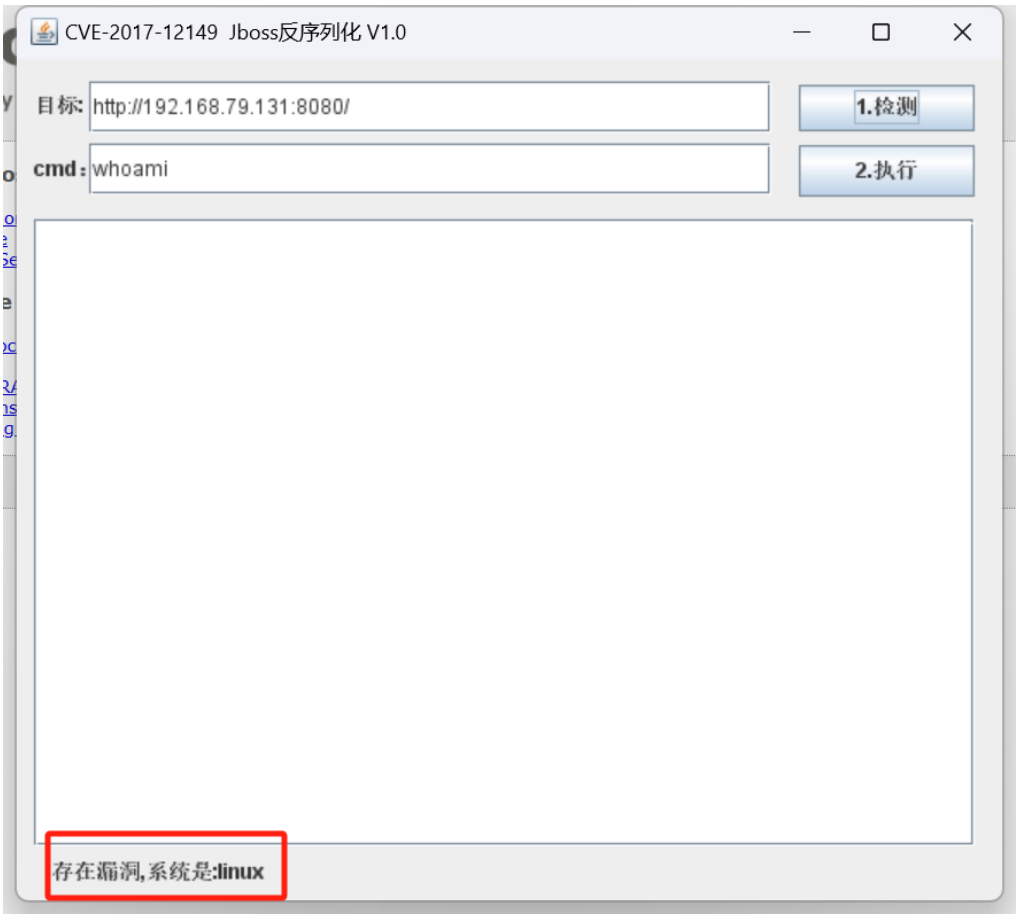


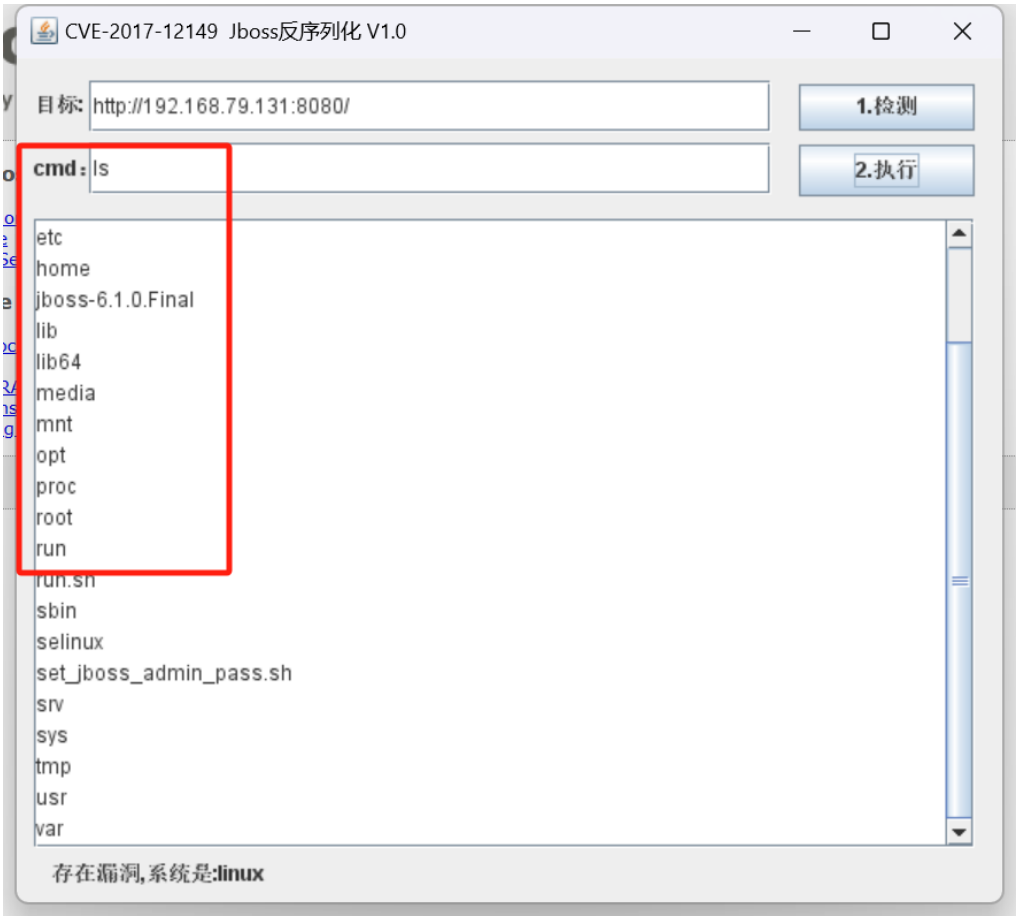
3. 练习 S2-048 远程代码执行漏洞（CVE-2017-9791），提供命令执行截图。



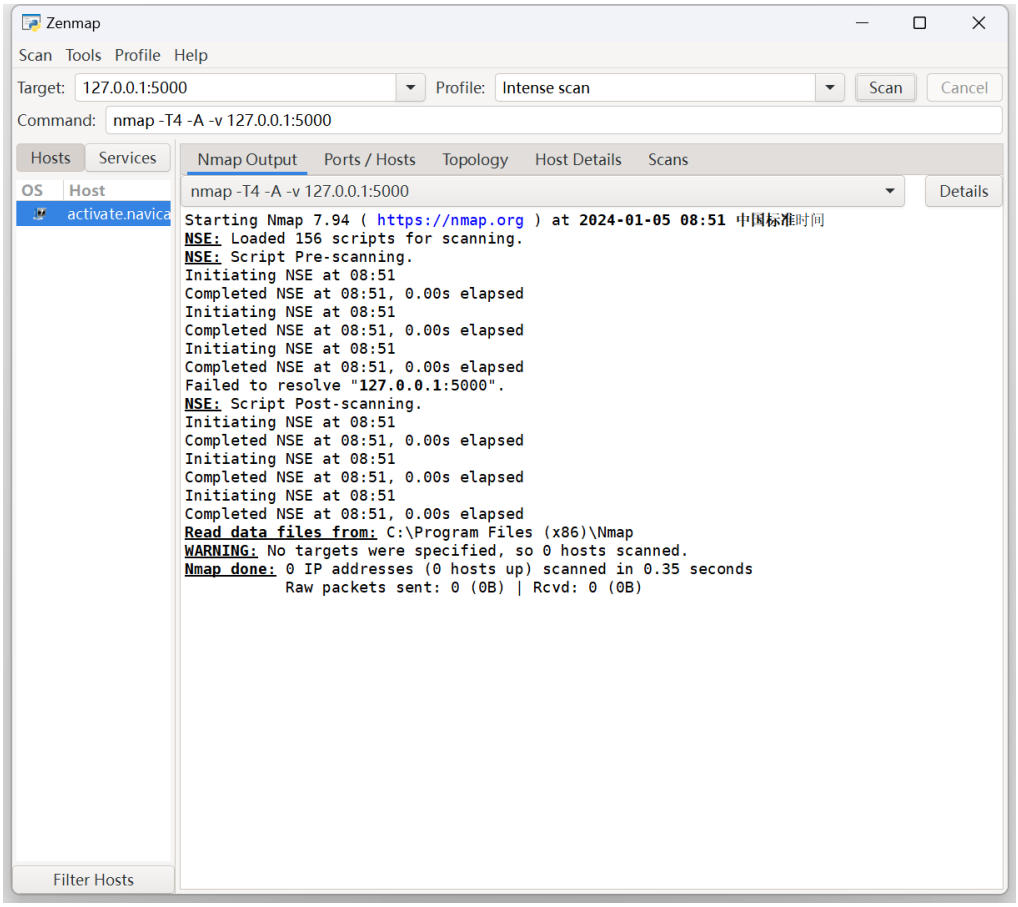


4. 练习 JBoss 5.x/6.x 反序列化漏洞（CVE-2017-12149），提供命令执行截图。


CVE-2017-12149 Jboss反序列化 V1.0
目标: http://192.168.79.131:8080/
1.检测
cmd: whoami
2.执行
存在漏洞,系统是:linux


CVE-2017-12149 Jboss反序列化 V1.0
目标: http://192.168.79.131:8080/
1.检测
cmd: ls
2.执行
etc
home
jboss-6.1.0.Final
lib
lib64
media
mnt
opt
proc
root
run
run.sh
sbin
selinux
set_jboss_admin_pass.sh
srv
sys
tmp
usr
var
存在漏洞,系统是:linux

5. 安装并使用 Nmap 扫描一个地址（本机、VPS、虚拟机环境都可以），提供扫描结果截图。



6. 以任一企业为关键词进行信息收集练习并汇总形成报告，禁止进行违规操作。

报告

Wappalyzer：

1. JavaScript 框架：Vue.js
2. Web 服务器：Apache HTTP Server
3. 安全：HSTS
4. 编程语言：PHP
5. 杂项：SWFObject Babel LottieFiles
6. JavaScript 库： jQuery Underscorejs core-js

nmap

发现其80和443端口是开放的在110.242.68.4IP上，使用的是Apache，公钥类型RSA算法，公钥位2048

Discovered open port 80/tcp on 110.242.68.4 Discovered open port 443/tcp on 110.242.68.4

80/tcp open http Apache httpd

443/tcp open ssl/http Apache httpd

Public Key type: rsa Public Key bits: 2048

天眼查

whois信息、真实IP

结果为：违禁域名

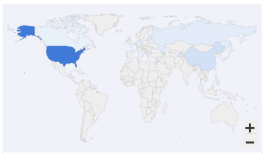
zoomzy

搜索结果 统计报告 全球视角 相关漏洞

订阅 收藏 下载 分词

相关漏洞数据由 Seebug 支持提供，仅供参考

漏洞搜索



mysql

97295	2018-05-17	高危	Multi-Master Replication Manager for MySQL mmm_agentd Rem...
92976	2017-04-19	高危	Pre-Auth MySQL remote DOS (Integer Overflow)（CVE-2017-359...
92513	2016-11-02	高危	MySQL / MariaDB / PerconaDB 权限提升漏洞（CVE-2016-6664）
92510	2016-11-02	高危	MySQL / MariaDB / PerconaDB 提权/条件竞争漏洞（CVE-2016-6663）
92405	2016-09-13	高危	MySQL <= 5.7.15 远程 Root 权限代码执行漏洞

apache httpd

99689	2023-05-23	高危	Apache HTTP Server 请求走私漏洞(CVE-2023-25690)
99364	2021-10-08	高危	Apache HTTPd 多个路径穿越与命令执行漏洞（CVE-2021-41773 CVE-2021-42013）...
97900	2019-04-10	高危	CVE-2019-0211 Apache Root Privilege Escalation

搜索类型

设备	259
ipv4设备	257
ipv6设备	2
网站	1

年份

2024	3
2023	78
2022	17

更多

国家