

java代码审计 深度解析



第三课 如何验证及修复struts2漏洞

审查第三方框架安全-Struts2利用

The screenshot shows a web security tool interface with the following details:

- 设置 (Settings):**
 - 目标 (Target): `http://localhost:8080/omnnefujian/login/login.action`
 - 漏洞编号 (Vulnerability ID): 选择全部 (Select All)
 - 数据提交方式 (Data Submission Method): POST
 - Cookie: (Empty)
 - 超时时间 (Timeout): 20
 - 验证漏洞 (Verify Vulnerability) and 环境信息 (Environment Info) buttons.
- 基本信息 (Basic Information):** 命令执行 (Command Execution), 文件上传 (File Upload), 批量验证 (Batch Verification)
- 漏洞描述 (Vulnerability Description):**
 - 2018-08-24: 增加SS-05: Struts 2.3 到 2.3.34, Struts 2.5 到 2.5.16. 此漏洞影响范围非常小, 要求配置条件比较苛刻, 同时, 一些特定版本没有看到有少数绕过, 所以, 目前exp只是基于SS-046改写的, 所以exp并不是所有版本都能用, 正常情况下Struts 2.3.6-2.3.31, Struts 2.5-2.5.10版本可以使用此exp.
 - 2017-07-07: 增加SS-048 Struts 2.3.X 支持检查官方示例struts2-showcase应用的代码执行漏洞, 参考地址: <http://127.0.0.1:8080/struts2-showcase/integration/save@angster.action>
 - 2017-03-21: 增加SS-046, 官方发布SS-046和SS-045漏洞引发原因一样, 只是利用漏洞的位置发生了变化, SS-046方式可能绕过部分WAF防护, 存在SS-045就存在SS-046: <http://struts.apache.org/docs/ss-046.html>
 - 2017-03-07: 增加安恒信息研究员nike_zheng发现的SS-045, jabatar处理复杂数据类型时, 异常处理不当, 导致OGNL代码执行, 通过在请求的Content-Type头中构造OGNL表达式来执行Java代码: <http://struts.apache.org/docs/ss-045.html>
 - 2016-04-28: 增加最新的SS-032远程代码执行漏洞, 和SS-019很相似。参考: <http://seclab.dappssecurity.com/en/?p=924>
 - 2015-12-01: 不用scanner读取概念, 再也不用担心s16不能执行net user/ipconfig/netstat -s等命令了。
 - 增加复杂数据包包 (multipart/form-data) 提交方式进行漏洞利用, 可绕过部分防护, 可执行命令, 暂时无法上传文件。
 - 2014-11-12: 最近遇到s19这个debug模式开启导致代码执行, 这个有点小, 但还是有一些, 为了方便大家把13版本修改了一下, 可以利用这个漏洞执行命令、上传shell。
- 警告 (Warning):** 本工具为漏洞自查工具, 请勿非法攻击他人网站!
- 漏洞编号 (Vulnerability ID):** SS-057 CVE-2010-11776 Struts 2.3 到 2.3.34, Struts 2.5 到 2.5.16 <https://wiki.apache.org/confluence/display/WW/SS-057> 影响
- 漏洞影响 (Vulnerability Impact):** 官方公告 <https://wiki.apache.org/confluence/display/WW/SS-057> 影响
- 漏洞利用 (Vulnerability Exploit):** 2019/5/5 15:13:29 - `http://localhost:8080/omnnefujian/login/login.action` - 不存在Struts2 SS-046远程代码执行漏洞!
- 漏洞利用 (Vulnerability Exploit):** 2019/5/5 15:13:29 - `http://localhost:8080/omnnefujian/login/login.action` - 不存在Struts2 SS-045远程代码执行漏洞!
- 漏洞利用 (Vulnerability Exploit):** 2019/5/5 15:13:29 - 警告: 存在Struts2远程代码执行漏洞-编号SS-016
- 漏洞利用 (Vulnerability Exploit):** 2019/5/5 15:13:29 - 返回验证标志: struts2_security_check
- 漏洞利用 (Vulnerability Exploit):** 2019/5/5 15:13:29 - `http://localhost:8080/omnnefujian/login/login.action` - 不存在Struts2 SS-019远程代码执行漏洞!
- 漏洞利用 (Vulnerability Exploit):** 2019/5/5 15:13:29 - `http://localhost:8080/omnnefujian/login/login.action` - 不存在Struts2 SS-037远程代码执行漏洞!
- 漏洞利用 (Vulnerability Exploit):** 2019/5/5 15:13:29 - `http://localhost:8080/omnnefujian/login/login.action` - 不存在Struts2 SS-032远程代码执行漏洞!
- 漏洞利用 (Vulnerability Exploit):** 2019/5/5 15:13:29 - 验证完毕.....



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, a network of interconnected nodes and lines, and several padlock icons scattered across the scene, suggesting themes of cybersecurity, digital privacy, or global connectivity. The overall aesthetic is futuristic and high-tech.

谢谢观赏