中国石化资金集中管理信息系统
Web 应用安全测试报告

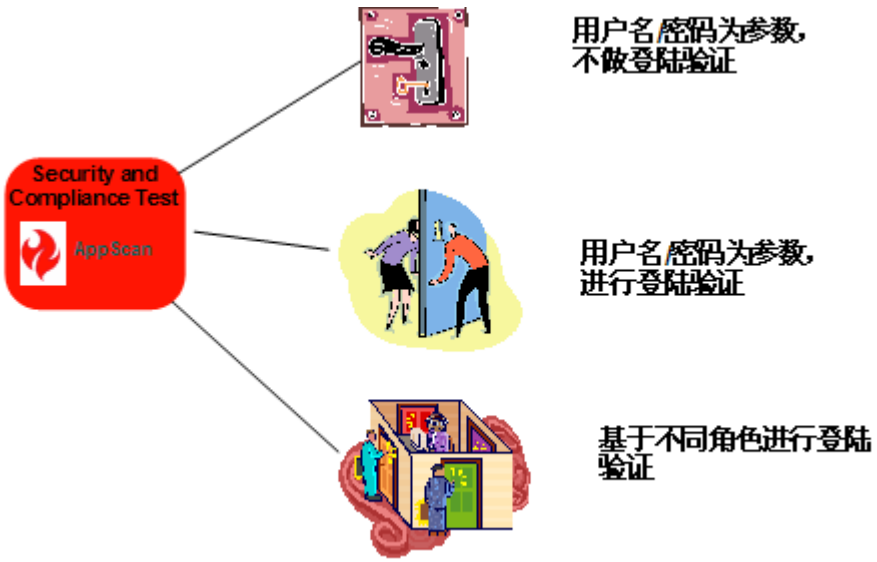
1.简介

本文针对中国石化资金集中管理信息系统，采用 IBM Rational 的安全测试产品 AppScan 进行安全测试，并基于此次测试的结果进行分析。

1.1 中国石化资金集中管理信息系统应用特点

中国石化资金集中管理信息系统应用采用 Jboss4.2.4 作为应用服务器，系统使用基于 Spring 的 Acegi 进行安全认证和授权；其中还大量采用了 Javascript 技术，所有其对于 url 的解析处理，需要动态进行处理。

1.2 针对中国石化资金集中管理信息系统应用特点的安全测试设置



针对于中国石化资金集中管理信息系统应用的以上特点，并结合实际使用情况分为三种场景进行测试，测试内容选择了系统的功能 1 和功能 2：

1）使用用户名/密码，但不进行登陆验证：此场景如同一般用户登陆系统，但不进行登陆验证，即不判断针对特殊应用安全的登陆，是否存在安全问题。

2）使用用户名/密码，进行登陆验证：此场景选择正常用户登陆系统，进行

登陆验证，即判断针对特殊应用安全的登陆，是否存在安全问题。

3）基于不同角色登陆处理：结合权限较高的 admin 用户和权限较低的 cqusr1 用户进行登陆，除了常规的安全的检测，特别还要针对跨权限的安全访问进行判断。

通过以上的配置，结合 AppScan 的登陆设置就可以了。

2.测试结果简析

结合以上的三个场景，针对部分功能进行安全测试后，初步获得以下测试结果。

2.1 整体内容分析

场景内容	安全问题总计	问题分类及数量
场景 1：用户名/密码登陆，无登陆验证	访问 192url，发现 60 问题	严重：2 类/16 个 中等：2 类/3 个 低等：3 类/6 个 泄漏：4 类/35 个
场景 2：用户名/密码登陆，进行登陆验证	访问 243url，发现 104 问题	严重：3 类/22 个 中等：2 类/3 个 低等：3 类/36 个 泄漏：4 类/43 个
场景 3：分角色用户登陆	访问 192url，发现 69 问题	严重：3 类/23 个 中等：2 类/3 个 低等：3 类/6 个 泄漏：4 类/37 个

3.严重安全问题分析及修改建议

3.1 XSS 跨站点脚本攻击漏洞

问题概述：黑客可以应用此漏洞，获取最终用户信息，并基于此进行伪装，进行攻击。

url:

http://10.1.19.92:40001/wfProject/jsp/app/sinopec/wf/loan/commissionedLoanApply.jsp

http://10.1.19.92:40001/wfProject/jsp/app/sinopec/wf/loan/loanApply.jsp

http://10.1.19.92:40001/wfProject/jsp/app/sinopec/wf/tongye/RMBOverdraftApply.jsp

http://10.1.19.92:40001/wfProject/jsp/app/sinopec/wf/tongye/RMBchaijieApply.jsp

测试方式：在参数中增加 javascript:alert(134108)处理，可执行 url

修改方法：修改对于参数的处理，将无效值进行排除。

3.2 注入漏洞

问题概述：黑客可以应用此漏洞，获取交易信息。

url：

http://10.1.19.92:40001/wfProject/jsp/app/netbank/common/customDropDownDict.jsp

测试方式：在 http request 中填写 foobar=foobar 之类内容进行攻击

修改方法：修改 http parameter 处理，将无效内容过滤

3.3 JBoss 管理控制台打开

问题概述：对于 jboss 控制台没有进行控制。

url：

http://10.1.19.92:40001/

测试方式：直接进行访问即可

修改方法：如果上线，此控制台建议关闭或者设置安全。

3.4 跨权限设置访问

问题概述：登陆用户，即可不受权限限制，通过 url 直接访问用户管理。

url：

http://10.1.19.92:40001/wfProject/jsp/app/acountmanager/interestBill.jsp

http://10.1.19.92:40001/wfProject/jsp/app/acountmanager/outlayBill.jsp

http://10.1.19.92:40001/wfProject/jsp/app/acountmanager/paymentBill.jsp

http://10.1.19.92:40001/wfProject/jsp/app/acountmanager/reciveBill.jsp

http://10.1.19.92:40001/wfProject/jsp/app/netbank/common/bankInfo.jsp

http://10.1.19.92:40001/wfProject/servlet/dataengine

测试方式：采用权限较低用户，可以访问用户管理内容。

修改方法：一定要配置用户授权内容。

4.总结

详细内容请详见通过 AppScan 生成的测试结果，并针对其进行修改。针对此次扫描的情况建议：

1）将应用的授权进行设置，保障不同角色能够针对的不同功能的角色权限。

2）防止 XSS 以及 SQL 注入攻击，对于 http parameter 进行过滤和控制。

3）设置登陆处理逻辑，比如对用户登陆账户设置访问三次后冻结/Session 不可重用等登陆处理逻辑。

本次安全测试工作，只是选择了部分功能，针对 jboss 的测试部署环境进行的，本应用一定还包括大量其他问题，等待进行验证和处理。