浙江电力信息安全实验室

测试报告

浙电信安试字2019第102号

**系统名称** 智慧物资供应链管理平台-仓储模块V1.0.0

**测试类别** 信息安全性

**委托单位** 国网浙江省电力有限公司信息通信分公司

（信息通信工程中心）

报告日期： 2019 年 12 月 13 日

地 址：浙江省杭州市朝晖八区华电弄 邮政编码：310014

查询电话：0571-51211026 投诉电话：0571-88393888

**有效性声明**

1. 本测试报告无授权签字人批准签字无效；
2. 本测试报告不准许以电子文档形式传递；
3. 本测试报告未经测试机构书面批准，不得部分复制；
4. 本测试报告仅对该软件版本有效；
5. 测试报告版权归委托方和测试机构共有，其他任何单位和个人未经许可均无权使用本测试报告，否则将保留对其追究法律责任的权利。

地 址:浙江省杭州市朝晖八区华电弄 邮政编码:310014

查询电话:0571-51211026 投诉电话:0571-88393888

**测试结论**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 系统名称 | 智慧物资供应链管理平台-仓储模块 | | 版本号 | | V1.0.0 |
| 委托单位 | 国网浙江省电力有限公司信息通信分公司(信息通信工程中心) | | 研发单位 | | 浙江华云信息科技有限公司 |
| 样品接收日期 | 2019 年 11 月 20 日 | | 样品编号 | | 2019110401-YP02 |
| 测试日期 | 2019 年 11 月 21 日至2019 年 12 月 13 日 | | | | |
| 测试地点 | 杭州市下城区华电弄1号综合楼14楼 | | | | |
| 服务类型 | 验收□ 上线□ 单项■ | | | | |
| 测试特性 | 安全功能-基本型 ■ 安全功能-增强型□ 安全漏洞□  其它 | | | | |
| 依据标准 | GB/T 25000.51-2016 系统与软件工程 系统与软件质量要求与评价（SQuaRE）第51部分：就绪可用软件产品(RUSP)的质量要求和测试细则  GB/T 25000.10-2016 系统与软件工程 系统与软件质量要求与评价（SQuaRE）第10部分：系统与软件质量模型  GB/T 28452-2012 应用软件系统通用安全技术要求  Q/GDW 1597-2015 国家电网公司应用软件通用安全要求  《应用软件安全作业指导书》（实验室内部测试规范）  《渗透测试工具作业指导书》（实验室内部测试规范）  《软件测试文档编写指导书》（实验室内部测试规范） | | | | |
| 结论 | 本次测试主要针对智慧物资供应链管理平台-仓储模块V1.0.0，在测试委托方已确认的环境下进行应用软件安全测试。  经检测，所检项目（26项）中26项通过，0项部分通过，0项不通过。共进行了2轮，共发现0个高危，1个中危，1个低危，最后一轮测试中上述漏洞均修复。  测试结论：■通过 □基本通过 □不通过  具体情况详见测试结果和总结。 | | | | |
| 测试人 |  | 时间 | |  | |
| 审核人 |  | 时间 | |  | |
| 批准人 |  | 时间 | |  | |

**目录**

[1 概述 7](#_Toc25855296)

[2 测试环境 10](#_Toc25855302)

[3 测试结果 11](#_Toc25855306)

[4 总结 14](#_Toc25855310)

[1 测试结果 16](#_Toc25855311)

[2 附录 18](#_Toc25855313)

**测试报告**

1. **概述**
   1. **标识**

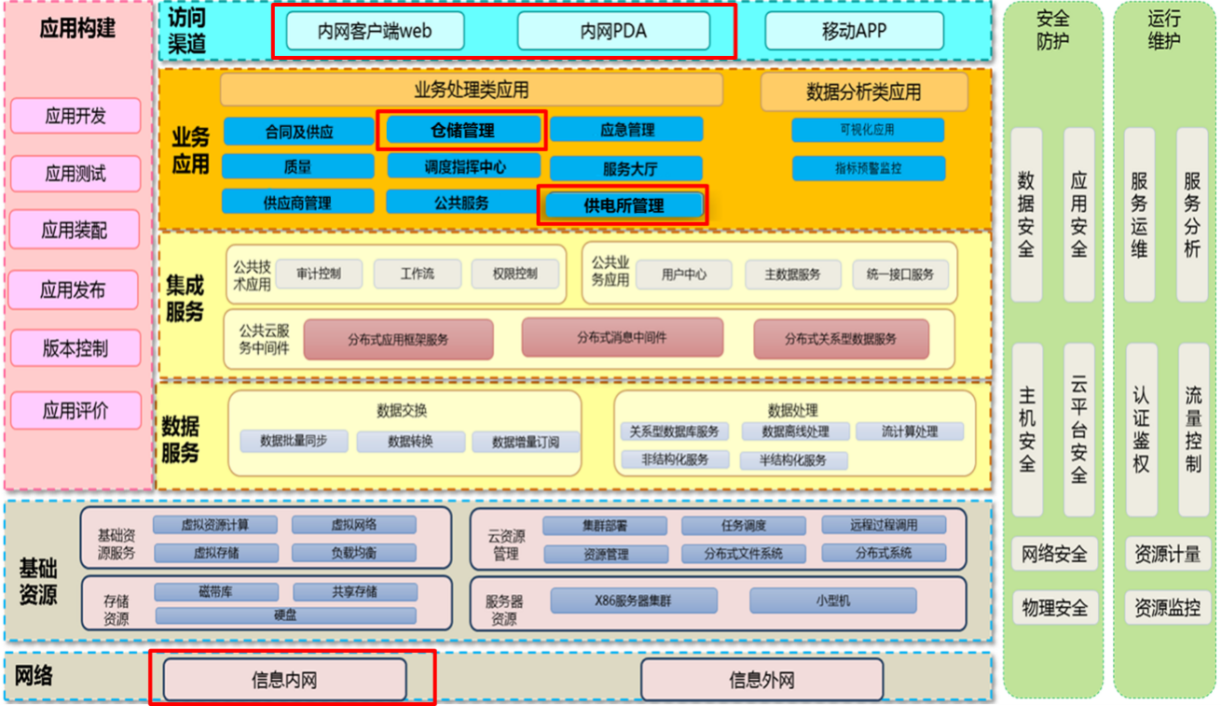
系统全称：智慧物资供应链管理平台-仓储模块

版本号：V1.0.0

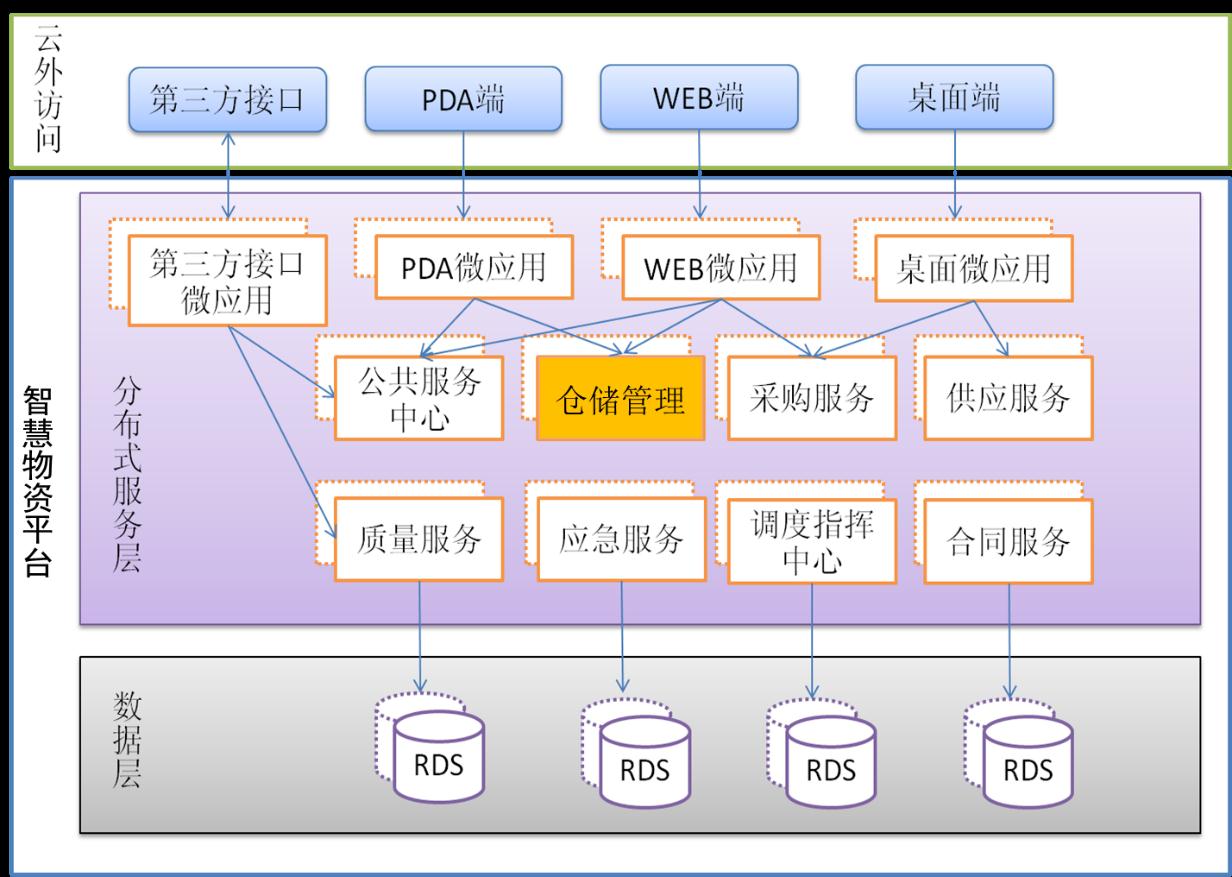
* 1. **被测系统概述**

智慧物资供应管理平台-仓储模块涵盖基础管理、入库管理、出库管理、拣选管理、空容器管理、在库管理等；仓库管家涵盖设备信息管理。其中仓库管家模块为新增功能。

智慧物资供应管理平台-仓储模块主要用途为大数据开发运维人员提供了稳定，高效，灵活的大数据分布式系统开发、运维和管理支撑系统，实现大数据资源的集中管理，实时监测和可视化管理，有效提升大数据平台服务支撑能力。平台从功能上主要分为应用开发、应用测试、应用发布、版本控制和应用评价。一体化云平台架构如图所示：



平台内网技术架构是分布式服务架构，包括分布式服务层与数据层。分布式服务层支撑不同业务类型服务，分为端处理服务与非端处理服务。端处理服务应对一体化云平台外访问，不同访问方式对应不同端处理服务，比如浏览器端访问对应WEB端处理服务、桌面端访问对应桌面端处理服务。端处理服务可以调用任意非端处理服务。非端处理服务可相互调用，同时也可调用对应RDS。数据层包含多个RDS实例，这里简化一体化云平台其他组件（如ODPS、HBASE、ADS等），具体数据层调用查看平台数据架构内容。



* 1. **测试充分性评价**

1.对智慧物资供应链管理平台-仓储模块V1.0.0测试需求经全面分析，并经委托单位确认，整理出26项测试用例，实现软件可测需求的100%覆盖。

2.测试环境经相关单位确认，符合要求。

3.所有测试用例均进行充分性测试，并针对缺陷进行充分回归。

* 1. **测试范围**

本次测试范围为智慧物资供应链管理平台-仓储模块V1.0.0安全测试特性，不包含与该系统相关的其他系统的接口和通信。安全测试主要针对应用系统本身的安全状况，不包括其操作系统、数据库系统的安全配置。

* 1. **测试工具**

|  |  |  |
| --- | --- | --- |
| **类别** | **工具名称** | **用途** |
| 安全渗透测试工具 | Burp suite 1.6 | 执行软件安全渗透测试 |
| 安全渗透测试工具 | Nmap7.70 | 端口扫描 |
| 安全渗透测试工具 | Sqlmap1.2.8.15 | sql注入测试 |

1. **测试环境**
   1. **硬件环境**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备** | **CPU** | **内存** | **硬盘** | **IP地址** |
| 应用服务器 | Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz | 8G | 125G | http://wztppt-db.test.cloud.zj.sgcc.com.cn/wztppt-db/treesoft/login |
| 数据库服务器 | Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz | 2400M | 500G | 172.31.35.123 |
| 测试终端 | Intel(R) Core(R) i5-2400 CPU @ 3.10Ghz 3.09Ghz | 4G | 500G | 10.136.26.205 |

* 1. **软件环境**

|  |  |  |
| --- | --- | --- |
| **设备** | **操作系统** | **应用软件** |
| 应用服务器 | Red hat 4.8.5-28 | Tomcat 7 |
| 数据库服务器 | Red hat 4.8.5-28 | MySQL5.6 |
| 测试终端 | Microsoft Windows XP Professional 版本2002 | Google Chrome版本 49.0.2623.112 |

* 1. **网络环境**

本次测试通过远程访问对该系统（地址：http://wztppt.test.cloud.zj.sgcc.com.cn/wztppt-web/）进行测试，测试环境由开发单位提供和部署。

网络拓扑图如下：



1. **测试结果**
   1. **问题情况**

本章节描述了测试手段和过程，列出各个测试用例及其执行结果，结果分析和建议请参考本报告第四部分测试记录与分析。测试结果中，“通过”是指该测试项的功能正常运行，或未发现相关的安全漏洞和安全问题；“部分通过”是指测试项结果只满足部分预期结果；“不通过”是指功能运行不正常，或发现安全漏洞和安全问题；“N/A”是指测试用例不适用，不进行测试。

表 1 问题缺陷统计表

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 测试特性 | 问题数 | | | | 缺陷比例 | 修复 | | | | 现存 | | | |
| 紧急 | 高危 | 中危 | 低危 | 紧急 | 高危 | 中危 | 低危 | 紧急 | 高危 | 中危 | 低危 |
| 安全漏洞 | 0 | 0 | 1 | 1 | 7.69% | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |

有关问题级别的判定准则如下：

表 2 问题级别判定准则表

|  |  |
| --- | --- |
| 危险等级 | 说明 |
| 紧急 | 可以直接被利用的漏洞，且利用难度较低。被攻击之后可能对网站或服务器的正常运行造成严重影响，或对用户财产及个人信息造成重大损失。 |
| 高危 | 被利用之后，造成的影响较大，但直接利用难度较高的漏洞。或本身无法直接攻击，但能为进一步攻击造成极大便利的漏洞。 |
| 中危 | 利用难度极高，或满足严格条件才能实现攻击的漏洞。或漏洞本身无法被直接攻击，但能为进一步攻击起较大帮助作用的漏洞。 |
| 低危 | 无法直接实现攻击或对网站安全没有直接影响，提供的信息可能让攻击者更容易找到其他安全漏洞或提供少量帮助或用于社工攻击。 |

* 1. **测试执行结果**

本项测试依据《GB/T 25000.51-2016 系统与软件工程 系统与软件质量要求与评价（SQuaRE）第51部分：就绪可用软件产品(RUSP)的质量要求和测试细则》和《应用软件安全作业指导书》等信息安全组织提供的安全测试向导和常见应用系统安全漏洞列表，对应用系统进行了全面的安全性测试，测试结果如下。

表 3 测试结果

|  |  |  |  |
| --- | --- | --- | --- |
| **测试特性** | **用例编号** | **用例名称** | **测试结果** |
| **安全漏洞** | APPSEC\_SS\_001 | 测试WEB服务器是否开启了不必要的HTTP高危方法 | 通过 |
| APPSEC\_SS\_002 | 测试WEB服务是否开启目录浏览 | 通过 |
| APPSEC\_SS\_003 | 测试Web服务器管理工具是否存在默认弱口令 | 通过 |
| APPSEC\_SS\_004 | 测试Web服务器是否存在默认Demo程序 | 通过 |
| APPSEC\_SS\_005 | 测试系统所使用的服务是否存在高危漏洞 | 通过 |
| APPSEC\_SM\_001 | 测试应用程序是否使用了易被破解的会话维护方式 | 通过 |
| APPSEC\_SM\_002 | 测试会话ID是否通过URL存储和传输 | 通过 |
| APPSEC\_SM\_003 | 测试系统是否提供了完善的用户注销登录功能 | 通过 |
| APPSEC\_SM\_004 | 测试系统是否提供了会话超时退出功能 | 通过 |
| APPSEC\_SM\_005 | 测试系统是否在关键操作上没有进行验证导致跨站请求伪造漏洞 | 通过 |
| APPSEC\_IL\_001 | 测试系统是否存在可被访问的备份文件、临时文件、日志文件、配置文件，造成敏感信息泄露 | 通过 |
| APPSEC\_IL\_002 | 测试客户端和HTML源代码里是否包含开发者留下的敏感信息 | 通过 |
| APPSEC\_IL\_003 | 测试应用程序发生异常时抛出的错误页面中是否存在敏感信息 | 通过 |
| APPSEC\_PM\_001 | 测试系统同等级别权限用户是否可越权操作 | 通过 |
| APPSEC\_PM\_002 | 测试系统低级别权限用户能否向高级别权限越权操作 | 通过 |
| APPSEC\_PM\_003 | 测试系统在业务逻辑方面是否存在缺陷导致业务逻辑限制失效 | 通过 |
| APPSEC\_IA\_001 | 测试系统身份认证功能是否可被绕过 | 通过 |
| APPSEC\_IA\_002 | 测试修改密码功能是否允许修改其他用户的密码 | 通过 |
| APPSEC\_DV\_001 | 测试应用系统是否存在SQL注入漏洞 | 通过 |
| APPSEC\_DV\_002 | 测试系统是否存在脚本注入漏洞 | 通过 |
| APPSEC\_DV\_003 | 测试系统是否存在命令执行漏洞 | 通过 |
| APPSEC\_DV\_004 | 测试系统是否存在XPath注入漏洞 | 通过 |
| APPSEC\_DV\_005 | 测试系统是否存在跨站脚本漏洞 | 通过 |
| APPSEC\_DV\_006 | 测试系统是否可上传有害的文件 | 通过 |
| APPSEC\_DV\_007 | 测试系统是否存在目录遍历漏洞 | 通过 |

* 1. **缺陷问题清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **缺陷编号** | **缺陷内容** | **缺陷类型** | **问题级别** | **是否消缺** |
| **D\_001** | 应用系统会话失效时间过长。 | 会话处理失效 | 低 | 是 |
| **D\_002** | 修改信息处数据库语句信息泄露 | 信息泄露 | 中 | 是 |

1. **总结**

2019 年 11 月 21 日至 2019 年 12 月 13 日，对智慧物资供应链管理平台-仓储模块V1.0.0进行了应用系统安全漏洞测试。所检项目（26项）中26项通过，0项部分通过，0项不通过。测试共进行了2轮，共发现0个高危，1个中危，1个低危。测试发现系统在会话处理失效、信息泄露等方面存在一定安全问题，详情请见附录整改通知单。

测试结论为：**通过**

（以下无正文）

附录01

整改通知单

编号：2019110401-01

**系统名称** 智慧物资供应链管理平台-仓储模块V1.0.0

**测试类别** 信息安全性

**委托单位** 国网浙江省电力有限公司信息通信分公司

（信息通信工程中心）

日期： 2019年 11月 26 日

1. **测试结果**

2019年11月21日至2019年11月26日，对智慧物资供应链管理平台-仓储模块V1.0.0进行了安全测试。测试发现该系统存在会话处理失效、信息泄露的安全问题，具体情况如下：

* 1. **安全缺陷**

|  |  |  |  |
| --- | --- | --- | --- |
| **缺陷编号** | **D\_001** | | |
| 缺陷类型 | 会话处理失效 | | |
| 缺陷内容 | 未提供会话超时退出功能 | | |
| 缺陷详情 | 应用系统会话失效时间过长。 | | |
| 缺陷影响 | 可能导致使用已过期的认证进行操作，从而对系统的完整性和可用性造成破坏 | | |
| 消缺建议 | 对登录的会话进行失效管理 | | |
| 缺陷等级 | **低** | 对应的测试编号 | **APPSEC\_SM\_004** |

|  |  |  |  |
| --- | --- | --- | --- |
| **缺陷编号** | **D\_002** | | |
| 缺陷类型 | 信息泄露 | | |
| 缺陷内容 | 数据库语句信息泄露 | | |
| 缺陷详情 | 修改信息处数据库语句信息泄露（详见附录1） | | |
| 缺陷影响 | 攻击者可能获取敏感信息，为其进一步攻击创造有利条件 | | |
| 消缺建议 | 建议配置统一错误处理界面，并对一些敏感信息进行处理 | | |
| 缺陷等级 | **中** | 对应的测试编号 | **APPSEC\_IL\_003** |

测试人：

审核人：

审批人：

1. **附录**
   1. **附录1**

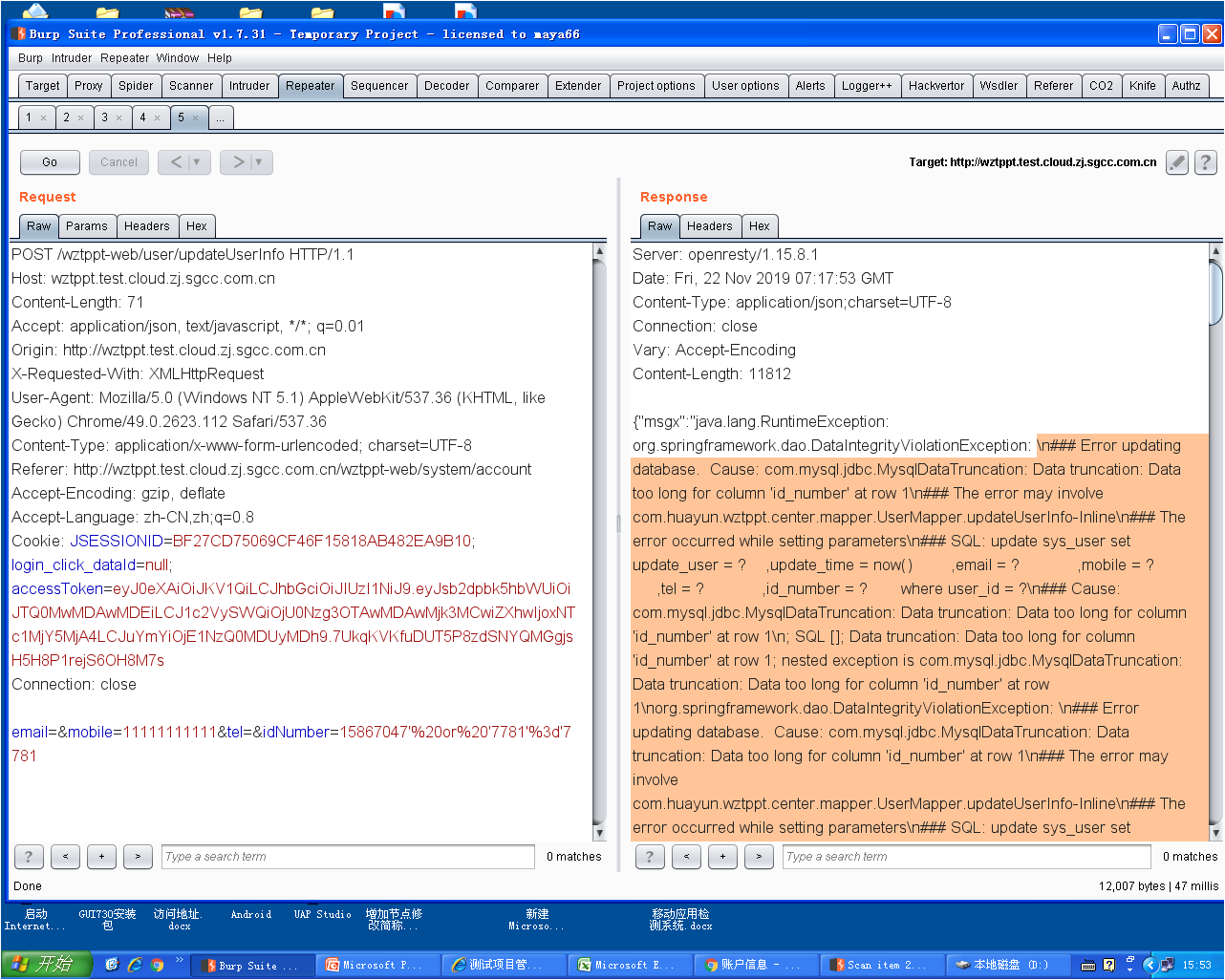


图 1 数据库语句信息泄露

（以下无内容）