ICS 35.240
L 60

团　　体　　标　　准

T/ISC XXXX—XXXX

组装式应用开发平台 第2部分：安全要求和测试方法

Security Requirements and Testing Methods for Development Platform of Composable Applications

（征求意见稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

中 国 互 联 网 协 会　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分 标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中国互联网协会提出并归口。

本文件起草单位：中国信息通信研究院、浪潮通用软件有限公司、金蝶软件（中国）有限公司、用友网络科技股份有限公司、北京致远互联软件股份有限公司、北京仁科互动网络技术有限公司、北京火山引擎科技有限公司、腾讯云计算（北京）有限责任公司、北京百度网讯科技有限公司、深圳市蓝凌软件股份有限公司、上海泛微网络科技股份有限公司、广东云徙智能科技有限公司、北京数势云创科技有限公司、南京数睿数据科技有限公司、金现代信息产业股份有限公司、云智慧（北京）科技有限公司、北京朗新天霁软件技术有限公司、北京微金时代科技有限公司、体坛传媒集团股份有限公司、上海易校信息科技有限公司、北京炎黄盈动科技发展有限责任公司、中国农业银行研发中心、中国工商银行软件开发中心。

本文件主要起草人：李玮、王景尧、吴荻、曹海啸、郑伟波、孙立新、宫保金、李帆、彭璐、陈张伟、刘然、刘岩、王文友、魏俊华、刘志强、马戈、黄通、董洪辰、王星、王倩、潘征、张社丽、李楠、孙圭光、李晓明、谢玉鑫、王海虎、张飞禄、何裕涛、李玖伟、严琦东、赵娟、赖强、王飞。

组装式应用开发平台　第 2 部分：安全要求和测试方法

1　范围

本文件规定了组装式应用开发平台的安全要求和测试方法。

本文件适用于组装式应用开发平台的开发者、提供商及专业测评机构开展安全测试工作，为提升组装式应用开发平台安全能力水平、强化测试能力、健全技术手段提供指引和依据。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 信息安全技术 术语

3　术语、定义和缩略语 TBD

3.1　术语定义

GB/T 25069-2010和GB/T 29246-2017中界定的以及下列术语和定义适用于本文件。

3.1.1　应用程序接口 Application Programming Interface

一组预先定义好的功能，开发者可通过该功能（或功能的组合）便捷地访问相关服务，而无需关注服务的设计与实现。

3.2　缩略语

下列缩略语适用于本文件。

API	应用程序接口	Application Programming Interface

4 安全技术要求

4.1 供应链安全

应确保平台所依赖的供应链组件安全性,确保内部开源中间件引用安全，包括不限于开发工具、数据库、引用的第三方Jar、Kafka、rabbitmq、Elasticsearch、容器镜像等高危CVE漏洞。

4.2 代码安全

平台应保证代码安全性，通过完整的SDL流程，保证在人员培训、需求分析、代码开发、应用测试、项目发布、应急响应等安全开发生命周期中的应用代码安全。

4.3 认证安全

4.3.1 身份鉴别

1、 平台应对需要授权访问的请求核实用户的身份是否合法，是否有权执行操作。
2、 会话Cookie应正确设置Secure、Domain和Path属性，并设置HttpOnly。
3、 会话的生成具有随机性、唯一性、不可预测。
4、 系统会话超时时间设置合理，超时后应销毁会话。用户认证通过后，应更换会话标识。用户退出登录后，应注销服务器会话数据。
5、 系统应保障会话信息不泄漏，如不应在GET请求中URL携带会话、不应在日志中打印Session和Token等信息。
6、 用户登录认证失败时，应采取模糊提示，如不区分用户名还是密码错误，防止恶意猜测系统用户（可选）。
7、 应支持与企业现有身份认证系统的集成认证，如AD、企微等（可选）。
8、 应支持常见的单点登录协议来与企业的统一账号系统进行集成认证，如SAML、OIDC、OpenID（可选）。

4.3.2 登录策略

1、 平台应提供多因素认证，如静态密码、图形验证码、短信验证码、生物认证等两种或两种以上组合验证方式。
2、 平台在验证码设计上应保证验证码生成的随机性、不可预测、验证码复杂度、时效性、一次性（使用过立即失效），在使用过程中应由后端服务器进行验证。
3、 应提供用户登出功能，注销服务器会话数据
4、 对第三方系统访问，平台应提供登录认证机制，如Token认证、签名认证等。
5、 支持第三方统一认证中心接入，根据登录认证结果进行系统登录状态管理（可选）。

4.3.3 数据审计

1、 平台日志应包括但不限于操作人、操作时间、操作名称、被访问资源名称、访问发起客户端地址和名称、操作结果等，支持数据安全审计。

4.3.4 认证权限

1、 用户认证与权限鉴别应在服务端进行，禁止客户端篡改请求参数绕过认证。
2、 平台支持基于角色的账户权限管理。
3、 平台中管理员用户建议采用基于角色的账户权限管理，对安全性要求较高的场景下宜遵循“三权分立”原则。

4、 平台应对每个需要授权访问的请求核实用户是否被授权执行该操作。

4.3.5 错误锁定

1、 平台应提供账户锁定策略配置功能，密码多次输入错误时，提供图片验证码、短信验证码处理方式，达到错误次数时，进行账户锁定。
2、 平台应对提供给第三方系统获取Token进行登录访问的方式，当密钥/密码连续输入错误时，需具备账户/第三方应用ID锁定机制。

4.3.6 账号口令

1、 平台应对口令复杂度进行控制，包括口令长度、字符组成、密码有效期、密码历史等；避免使用含有账号信息的口令及常见口令。
2、 平台生成的密码和认证过程应加盐处理，防止用户密码被撞库破译。
3、 管理员新增/重置用户账户，应由管理员设置初始口令或系统自动产生随机口令（口令应满足口令复杂度要求），用户首次登陆或链接宜建议修改。
4、 系统中各账户的权限需满足“权限最小化”原则；新建账户默认不授予任何权限或者默认只指派最小权限的角色。
5、 平台应提供密码变更与找回密码功能。
6、 平台的密码重置与更改应严格校验输入参数进行身份验证，如验证旧密码、手机短信验证码等机制（可选）。

4.4 应用安全

4.4.1 授权管理

1、 平台应支持用户功能权限设置，应核实用户是否被授权执行相应操作。
2、 平台应支持数据规则权限设置，对数据的使用进行权限控制。
3、 平台应支持字段权限设置，控制用户对字段查看、编辑等权限。
4、 用户权限变更应及时生效，且平台应记录权限日志变更信息。

4.4.2 数据安全

1、 平台应支持敏感数据保护机制，提供敏感数据脱敏规则、加密规则配置功能。
2、 平台应禁止敏感数据在日志、数据库、配置文件、提示语、告警信息、堆栈信息、源代码等处明文显示。
3、 平台应支持对敏感数据的访问认证和鉴权机制。
4、 平台应支持敏感数据的传输加密或者采用加密通道。
5、 敏感数据的加密存储需采用安全的加密算法。
6、 平台应支持页面启用数字水印功能（可选）。
7、 提供数据备份管理能力（可选）。

4.4.3 输入输出

1、 平台应具备输入数据有效性检验功能,例如防护sql注入、xss注入、csv注入、xml注入等注入风险防御机制。
2、 平台应具备防止CSRF（跨站请求伪造）的功能。
3、 平台应具备异常处理机制，当程序发生异常时应在日志中详细记录错误消息；应向外部调用程序发送通用的提示信息或重定向特定网页，严禁泄露内部出错信息。
4、 平台应支持多种输入数据验证方式，比如：类型、长度、数值范围、特殊字符等。
5、 平台服务端和客户端都应进行输入验证，路径遍历漏洞检查（可选）。

4.4.4 密码安全

1、 平台应具备多种密码算法的选择和加密方式的选择。
2、 提供秘钥设置及安全保护（可选）。
3、 支持可信第三方密钥存储及分发（可选）。

4.5 通信安全

4.5.1 通信加密

1、 客户端与服务端通信应使用SSL，并使用SSL3.0/TLS1.0以上版本。
2、 客户端与服务器端传输数据应使用安全的证书，证书的格式、签名算法、密钥长度、过期时间满足安全要求。

4.5.2 访问控制

1、 除特定的公开内容，对其它功能和数据访问要求应进行身份认证
2、 未经授权访问平台功能和数据，平台应提示用户进行登录或者拒绝访问。
3、 支持配置用户或组织在固定的IP段访问登录平台。
4、 支持对web端和移动端能否同时登录进行限制（可选）。
5、 支持基于移动设备指纹对移动端登录进行限制（可选）。
6、 支持仅限于API访问的认证，避免高权限账号泄露后被用于登录web管理后台执行恶意操作（可选）。

4.6 安全策略

1、 平台出厂应提供安全配置指南
2、 管理配置应支持安全配置项。
3、 平台应具备安全应急响应团队，对外部漏洞、客户安全问题可及时处理。
4、 平台应具备灰度发布策略定制能力（可选）。
5、 平台应具备运行态监控基础能力，提供基础限流、负载均衡等基础能力（可选）。
6、 支持定期漏洞扫描及分析（可选）。

5 测试方法

5.1 供应链安全

编号	4.1
预置条件	已梳理平台所引用的供应链组件，以及组件所使用的版本。
测试方法	**1、** 采用开源安全工具或自研安全工具对组件进行安全版本检测，如开源工具 Dependency check 检测平台引用的第三方 jar 是否存在 CVE 漏洞。 **2、** 手工检测，在组件官方网站或第三方软件风险管理网站查找对应组件及版本是否存在 CVE 漏洞。如 https://nvd.nist.gov/vuln/search/results 网站查询。
预期结果	引用的供应链组件版本是安全版本，无 CVE 漏洞。

5.2 代码安全

编号	4.2
预置条件	平台运行正常

测试方法	了解和整理整个产品研发流程，咨询产品设计、研发、测试、质量管理、安全运维等人员，确定是否遵循安全开发流程（SDL）。
预期结果	在产品设计、开发、测试、配置管理、交付等关键环节，有安全开发流程检查点和对应输出件。

5.3 认证安全

5.3.1 身份鉴别

编号	4.3.1
预置条件	平台运行正常
测试方法	**1、** 梳理平台提供的所有登录页面 **2、** 根据用户登录交互流程，逐一检查流程各节点对账户、会话 Cookie、身份鉴别、认证提示语等处理逻辑是否满足身份鉴别安全技术要求。
预期结果	满足身份鉴别安全技术要求。

5.3.2 登录策略

编号	4.3.2
预置条件	平台运行正常
测试方法	**1、** 打开平台登录策略配置页面。 **2、** 对登录策略进行配置和登录操作，检查是否满足登录策略安全技术要求。
预期结果	满足登录策略安全技术要求。

根据登录认证结果进行系统登录状态管理

编号	4.3.2
预置条件	平台运行正常
测试方法	**1、** 打开平台登录策略配置页面。 **2、** 根据登录认证结果进行系统登录状态管理
预期结果	满足登录策略安全技术要求。

5.3.3 数据审计

编号	4.3.3
预置条件	平台运行正常
测试方法	**3、** 打开平台日志页面。 **4、** 检查平台日志是否包括操作人、操作时间、操作名称、被访问资源名称、访问发起客户端地址和名称、操作结果等，是否满足数据审计安全技术要求。
预期结果	满足数据审计安全技术要求。

5.3.4 账号口令

编号	4.3.4
预置条件	平台运行正常
测试方法	**1、** 梳理平台所有提供账户口令的功能页面。 **2、** 检查账户与口令在生成、传输、存储、使用过程中是否满足账户口令安全技术要求。
预期结果	满足账户口令安全技术要求。

5.4 应用安全

5.4.1 授权管理

编号	4.4.1
预置条件	平台运行正常
测试方法	**1、** 对平台提供用户功能的菜单项、按钮、超链接、API 展开测试验证，包括不限于基于 URL、用户身份、资源 ID 等的横向纵向越权测试。 **2、** 对平台提供的预置数据和用户数据展开测试验证，检查当前用户是否有数据的增、删、改、查权限。 **3、** 对平台提供的表单字段，检查当前用户是否有字段值的编辑、查看等权限。
预期结果	满足授权管理安全技术要求，并且控权准确。

5.4.2 数据安全

编号	4.4.2
预置条件	平台运行正常
测试方法	确定平台敏感数据范围，检查敏感数据在生成、传输、存储、处理、使用过程中是否满足安全技术要求。
预期结果	满足数据安全安全技术要求。

编号	4.4.2
预置条件	平台运行正常
测试方法	**1、** 为敏感数据使用安全的加密算法加密存储。 **2、** 为敏感数据使用数字水印以及备份管理功能。
预期结果	平台能够提供数字水印功能以及备份管理能力。

5.4.3 输入输出

编号	4.4.3

预置条件	平台运行正常
测试方法	**1、** 梳理平台数据录入的功能界面和 API 接口，确定业务功能处理逻辑。 **2、** 对外界输入的数据进行篡改或重放，组合各种正常/异常请求数据，观察平台是否存在安全防御机制，对请求进行拦截提示、禁止访问等。
预期结果	平台对外界输入能有效过滤或拦截，对输出合理响应；满足安全技术要求。

5.4.4 密码安全

编号	4.4.4
预置条件	平台运行正常
测试方法	**1、** 检查平台具备的密码算法和加密方式以及对应的选择模式。 **2、** 检查是否提供密钥保护，密钥在生成、传输、存储、使用过程中是否满足安全保护要求。 **3、** 检查第三方密钥的存储分发方式。
预期结果	平台对能够提供多种密码算法的选择和加密方式的选择；满足安全技术要求。

5.5 通信安全

5.5.1 通信加密

编号	4.5.1
预置条件	平台运行正常
测试方法	检查客户端与服务端通信是否采用 HTTPS 协议，并使用安全的 SSL 协议和证书。
预期结果	**1、** 采用 SSL3.0/TLS1.0 以上版本。 **2、** 使用安全证书。

5.5.2 访问控制

编号	4.5.2
预置条件	平台运行正常
测试方法	**1、** 梳理平台公开、未公开的功能和数据。 **2、** 分别对公开、未公开的功能和数据进行访问控制测试，包括不限于认证、鉴权、访问 IP 限制等。
预期结果	满足访问控制安全技术要求。

编号	4.5.2（可选）
预置条件	平台运行正常

测试方法	**1、** 检查平台是否支持对 web 端和移动端同时登录进行限制。
预期结果	满足访问控制安全技术要求。

编号	4.5.2（可选）
预置条件	平台运行正常
测试方法	**1、** 检查平台是否支持基于移动设备指纹对移动端登录进行限制。
预期结果	满足访问控制安全技术要求。

编号	4.5.2（可选）
预置条件	平台运行正常
测试方法	**1、** 检查平台是否支持仅限于 API 访问的认证。
预期结果	满足访问控制安全技术要求。

5.6 安全策略

编号	4.6
预置条件	平台运行正常
测试方法	**1、** 检查平台是否提供安全配置指南。 **2、** 检查平台提供的安全配置项是否可配置。 **3、** 检查平台是否存在安全应急团队，对平台的安全漏洞是否有效及时处理。
预期结果	满足安全策略安全技术要求。

编号	4.6
预置条件	平台运行正常
测试方法	**1、** 检查平台是否具备灰度发布策略定制能力。 **2、** 检查平台是否具备运行态监控基础能力（基础限流、负载均衡能力）。 **3、** 检查平台是否支持定期漏洞扫描及分析。
预期结果	满足安全策略安全技术要求。