ICS 35.020
V 07

MH

中华人民共和国民用航空行业标准

MH/T 0067—2018

民航 Web 应用系统安全检查指南

Security testing guide for Web application system of civil aviation

2018－12－14 发布　　2019－04－01 实施

中国民用航空局　发布

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国民用航空局人事科教司提出。

本标准由中国民航科学技术研究院归口。

本标准起草单位：中国民航大学。

本标准主要起草人：马勇、顾兆军、刘春波、周景贤、王双、张礼哲、钟友兵。

民航 Web 应用系统安全检查指南

1 范围

本标准规定了针对民航Web应用系统检测的基本原则、工作方式。

本标准适用于指导对Web应用系统进行安全检测。

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 28448 信息安全技术 信息系统安全等级保护测评要求

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 31509 信息安全技术 信息安全风险评估实施指南

GB/T 25058 信息安全技术 信息系统安全等级保护实施指南术语和定义

3 术语和定义

下列术语和定义适用于本文件。

3.1

软件容错 software fault-tolerance

软件在一定程度上能从错误状态自动恢复到正常状态的功能。

4 民航 Web 应用系统安全检测基本原则和方式

4.1 检测的基本原则

4.1.1 标准性原则

民航Web应用系统安全检测应符合GB/T 31509和GB/T 25058中的检测流程的相关要求。

4.1.2 可控性原则

在安全检测项目实施过程中，应严格按照标准的项目管理方法对服务过程、人员和工具等进行控制，以保证检测实施过程的可控和安全，具体措施如下：

a) 人员与信息可控性：参与检测的人员应该签署保密协议，以保证检测项目信息的安全；对测试过程中产生的数据应严格管理，防止数据泄露；

b) 过程可控性：应按照项目管理要求，成立项目实施团队，项目组长负责制，以便使项目过程可控；进行安全测试前，测试人员应与被测试方进行充分的沟通，并且在测试前告知被测试方测试时间和测试策略；
c) 工具可控性： 检测过程中应使用经过国家或民航部门检测认可的相关工具。

4.1.3 最小影响原则

对于正在运行的民航Web应用系统，测试前应与被测试方确定合适的测试时间窗口，避开业务高峰期，同时做好业务系统的应急预案。

4.2 检测的工作方式

4.2.1 人工访谈

专业的信息安全人员与Web应用系统管理、运维和使用人员进行沟通、交流，全面地掌握Web应用系统的业务流程、数据流程、网络架构、主机系统、运维情况、管理机构以及管理制度等各个方面的信息，对Web应用系统的安全现状进行全面的了解。

4.2.2 人工检查

利用专业人员的技术和经验对民航Web应用系统进行安全测试。

4.2.3 工具测试

采用自动化Web扫描工具对检测目标进行安全测试，可以充分了解Web系统当前的安全现状、具有的脆弱性、面临的潜在威胁、可能的影响和风险等信息。

4.2.4 渗透测试

模拟黑客的攻击手段对民航Web应用系统进行安全测试。

5 民航 Web 应用系统安全检测阶段性工作

5.1 检测流程

民航Web应用系统安全检测应分为四个阶段：
——检测准备阶段；
——检测方案编制阶段；
——检测具体实施阶段；
——检测报告编写阶段。

5.2 检测准备阶段

5.2.1 检测准备阶段工作

检测准备阶段的主要任务是确定检测的目标、范围，成立检测团队以及掌握被检测的民航Web应用系统的相关信息。

5.2.2 确定检测目的

对民航Web应用系统检测的目标是了解Web应用系统存在的安全风险，并对发现的安全风险提出相应的安全加固建议。

5.2.3 确定检测范围

对民航Web应用系统进行检测，应掌握系统运行的业务特点，并根据其特点确定其业务逻辑边界。

5.2.4 组建检测团队

应针对检测项目组建检测团队，由检测方和被检测方共同组成项目组，并明确项目组成员的职责。

5.2.5 系统调研

应对要检测的民航Web应用系统进行调研，掌握被检测目标采用的编写语言、中间件、调用的第三方库文件等信息。

5.2.6 确定检测依据

检测依据为：

a) GB/T 28448
b) GB/T 20984

5.2.7 确定检测工具原则

检测工具的选择和使用应遵循以下原则：

a) 检测工具应尽可能具备比较全面的漏洞检测能力；
b) 检测工具使用的检测策略和检测方式不应对 Web 应用系统造成不正常的影响；
c) 应尽可能对工具检测的结果进行人工验证，尽可能少的出现误报现象；
d) 检测工具的选择和使用应符合国家有关规定。

5.3 检测方案编制阶段

应根据检测准备阶段获取的信息，制订检测方案。主要内容包括：

a) 检测的目标、评估范围和评估依据；
b) 检测团队成员及职责；
c) 检测工作计划：项目实施进度安排以及各阶段的工作内容、形式和工作成果；
d) 风险规避措施：包括保密协议、评估工作环境要求、评估方法、工具选择以及应急预案等；
e) 项目验收方式：包括验收方式、依据和结论定义。

5.4 检测具体实施阶段

5.4.1 通则

检测具体实施阶段的任务是按照检测方案对被检测目标，应按照附录A中的内容进行检测，并详细记录检测过程数据。

5.4.2 检测实施

5.4.2.1 身份鉴别

5.4.2.1.1 应访谈 Web 应用系统管理员，询问 Web 应用系统是否采取身份标识和鉴别措施，具体措施的内容；以及防止身份鉴别信息被冒用的措施种类。

5.4.2.1.2　应访谈Web应用系统管理员，询问Web应用系统是否具有登录失败处理功能。

5.4.2.1.3　应检查设计或验收文档，查看其是否有系统采用了保证唯一标识的措施的描述。

5.4.2.1.4　应检查操作规程和操作记录，查看其是否有添加、删除用户和修改用户权限的操作规程、操作记录和审批记录。

5.4.2.1.5　应检查主要Web应用系统，查看其是否采用了两个及两个以上身份鉴别技术的组合来进行身份鉴别。

5.4.2.1.6　应检查主要Web应用系统，查看其是否提供身份标识和鉴别功能；查看其身份鉴别信息是否具有不易被冒用的特点；其鉴别信息复杂度检查功能是否能保证系统中不存在弱口令等。

5.4.2.1.7　应检查主要Web应用系统，查看其提供的登录失败处理功能，是否根据安全策略配置了相关参数。

5.4.2.1.8　应测试主要Web应用系统，可通过试图以合法和非法用户分别登录系统，查看是否成功，验证其身份标识和鉴别功能是否有效。

5.4.2.1.9　应测试主要Web应用系统，验证其登录失败处理功能是否有效。

5.4.2.1.10　应渗透测试主要Web应用系统，验证Web应用系统身份标识和鉴别功能是否不存在明显的弱点。

5.4.2.2　访问控制

5.4.2.2.1　应访谈Web应用系统管理员，询问Web应用系统是否提供访问控制措施，以及具体措施和访问控制策略，访问控制的粒度。

5.4.2.2.2　应检查主要Web应用系统，查看系统是否提供访问控制机制；是否依据安全策略控制用户对客体的访问。

5.4.2.2.3　应检查主要Web应用系统，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作；访问控制的粒度是否达到主体为用户级，客体为文件、数据库表级。

5.4.2.2.4　应检查主要Web应用系统，查看其是否有由授权用户设置其它用户访问系统功能和用户数据的权限的功能，是否限制默认用户的访问权限。

5.4.2.2.5　应检查主要Web应用系统，查看系统是否授予不同帐户为完成各自承担任务所需的最小权限，特权用户的权限是否分离，权限之间是否相互制约。

5.4.2.2.6　应检查主要Web应用系统，查看是否依据安全策略严格控制用户对限制类型资源的操作。

5.4.2.2.7　应测试主要Web应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证Web应用系统访问控制功能是否有效。

5.4.2.2.8　应测试主要Web应用系统，可通过默认用户登录系统，并进行一些合法和非法操作，用来验证系统是否严格限制了默认账户的访问权限。

5.4.2.2.9　应渗透测试主要Web应用系统，验证Web应用系统的访问控制功能是否有效。

5.4.2.3　安全审计

5.4.2.3.1　应访谈安全审计员，询问Web应用系统是否有安全审计功能，对事件进行审计的策略，以及审计日志的保护措施。

5.4.2.3.2　应检查主要Web应用系统，查看是否开启了日志功能。

5.4.2.3.3　应检查主要Web应用系统，查看其当前审计范围是否覆盖到每个用户。

5.4.2.3.4 应检查主要 Web 应用系统，查看其审计策略是否覆盖系统内重要的安全相关事件，包括但不限于用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等。

5.4.2.3.5 应检查主要 Web 应用系统，查看其审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等内容。

5.4.2.3.6 应检查主要 Web 应用系统，查看其是否为授权用户浏览和分析审计数据提供专门的审计分析功能，并能根据需要生成审计报表。

5.4.2.3.7 应检查主要 Web 应用系统，查看其日志保存期是否少于 6 个月。

5.4.2.3.8 应测试主要 Web 应用系统，在 Web 应用系统上试图产生一些重要的安全相关事件，查看 Web 应用系统是否对其进行了审计，验证 Web 应用系统安全审计的覆盖情况是否覆盖到每个用户；如果进行了审计则查看审计记录内容是否包含事件的日期、时间、发起者信息、类型、描述和结果等。

5.4.2.3.9 应测试主要 Web 应用系统，试图非授权删除、修改或覆盖审计记录，验证安全审计的保护情况是否无法非授权删除、修改或覆盖审计记录。

5.4.2.4 系统敏感信息保护（顺序调整）

5.4.2.4.1 应访谈 Web 应用系统管理员，询问 Web 应用系统是否对敏感信息的存储和使用采取的安全措施。

5.4.2.4.2 应检查主要 Web 应用系统，查看其是否在发布文件中包含备份、系统配置等敏感文件。

5.4.2.4.3 应检查主要 Web 应用系统，查看其是否对部署文件进行必要的修改，防止敏感信息泄露。

5.4.2.4.4 应检查主要 Web 应用系统，查看其是否在停止使用后将所有信息进行清除。

5.4.2.4.5 应检查主要 Web 应用系统，查看其数据库中的敏感字段是否进行加密存储。

5.4.2.4.6 应测试主要 Web 应用系统，是否限制系统配置等敏感文件的下载。

5.4.2.4.7 应测试主要 Web 应用系统，是否有开源组件等信息暴露。

5.4.2.5 通信安全性

5.4.2.5.1 应访谈安全管理员，询问 Web 应用系统是否具有在数据传输过程中的保护措施，以及具体措施的内容。

5.4.2.5.2 应检查设计或验收文档，查看其是否有关于保护通信安全性的说明。

5.4.2.5.3 应测试主要 Web 应用系统，通过查看通信双方数据包的内容，查看系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证；查看系统在通信过程中，对整个报文或会话过程进行加密的功能是否有效。

5.4.2.6 软件容错

5.4.2.6.1 应访谈 Web 应用系统管理员，询问 Web 应用系统是否具有保证软件容错能力的措施，以及具体措施的内容。

5.4.2.6.2 应检查主要 Web 应用系统，查看 Web 应用系统是否对人机接口输入或通信接口输入的数据进行有效性和安全性校验。

5.4.2.6.3 应渗透测试主要 Web 应用系统，验证 Web 应用系统对用户输入的各类数据进行了有效性和安全性校验。

5.4.2.6.4 应采用代码审计手段对主要 Web 应用系统代码进行安全审计。

5.4.2.7 资源控制

5.4.2.7.1 应访谈 Web 应用系统管理员，询问 Web 应用系统是否有资源控制的措施，以及具体措施的内容。

5.4.2.7.2 应检查主要 Web 应用系统，查看是否限制单个账户的多重并发会话； 是否对一个时间段内可能的并发会话连接数进行限制；是否对最短连接时间进行限制。

5.4.2.7.3 应检查主要 Web 应用系统，查看是否有服务水平最小值的设定，当系统的服务水平降低到预先设定的最小值时，系统报警。

5.4.2.7.4 应测试主要 Web 应用系统，可通过对系统进行超过规定的单个账户的多重并发会话数进行连接，验证系统是否能够正确地限制单个账户的多重并发会话数。

5.4.2.7.5 应测试主要 Web 应用系统，可试图使服务水平降低到预先规定的最小值，验证系统是否能够正确检测并报警。

5.4.2.7.6 应测试重要 Web 应用系统，当 Web 应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。

5.4.2.8 数据的备份和恢复

5.4.2.8.1 应访谈 Web 应用系统管理员，询问应有程序是否有备份功能及备份策略。

5.4.2.8.2 应检查设计或验收文档，查看 Web 应用系统是否有备份功能。

5.4.2.8.3 应测试 Web 应用系统，查看 Web 应用系统数据备份功能策略以及有效性。

5.4.2.9 业务逻辑安全

5.4.2.9.1 应访谈业务主管人员，询问 Web 应用系统的业务处理流程，分析业务流程是否合理，并对系统代码进行验证。

5.4.2.9.2 应访谈系统开发人员，询问 Web 应用系统身份认证机制以及控制逻辑，并对系统代码进行验证。

5.4.2.10 管理制度

5.4.2.10.1 应按照信息系统等级保护三级基本要求对 Web 应用系统开展管理制度检测。

5.4.2.10.2 应访谈系统管理员、安全审计员和用户，询问 Web 应用系统是否有管理制度和使用说明文件等。

5.4.2.10.3 应检查设计或验收文档，是否按照信息系统等级保护三级基本要求进行设计和建设。

5.4.3 文档管理

确保检测文档资料的完整性、准确性和安全性，应遵循以下原则：

a) 应指派专人负责文档的整理和保存；
b) 文档应注明项目相关信息：项目名称、文档名称、版本号、审批人、分发范围等；
c) 未经允许不应将项目信息泄露给无关人员和组织。

5.5 检测报告编写阶段

应对检测过程和检测结果进行分析整理，并对被检测目标的安全状况进行评价，给出相应的安全加固建议，形成最终报告。

MH

附 录 A
（规范性附录）
Web 应用系统安全基本要求

A.1 身份鉴别

A.1.1 应在系统管理和普通用户管理等模块提供登录认证功能，对登录用户进行身份标识和鉴别。
A.1.2 对于重要的系统模块应采取两种及以上的鉴别技术对用户进行身份鉴别。
A.1.3 应对用户录入的帐户及口令进行唯一性和复杂度的验证，确保不被冒用。
A.1.4 应提供验证码、限制非法次数、自动退出、结束会话等措施，防止暴力破解等。

A.2 访问控制

A.2.1 应在配置文件中限定用户访问及下载的文件类型。（测试中要有具体的方式）
A.2.2 应在配置文件中限定用户对各个目录及文件的操作权限。
A.2.3 应对不同的账户设定不同的权限：一方面根据职能划分，另一方面根据管理权限划分，并在它们之间形成制约关系。
A.2.4 应在代码中限定上传的文件类型或访问的文件路径及类型。
A.2.5 应在后台登陆的模块代码中对用户的权限进行限制，防止纵向越权和横向越权访问。
A.2.6 访问控制还要参考等级保护基本要求中主机安全访问控制等要求。

A.3 安全审计（放在备份之后）

A.3.1 应在Web应用系统中设计操作日志审计模块。
A.3.2 操作日志的内容应覆盖到每个用户。
A.3.3 操作日志内容应包括操作类型、时间、账户、操作结果等。
A.3.4 应具有操作日志进行统计、查询、分析及生成报表的功能。
A.3.5 日志保存期不少于6个月。

A.4 系统信息保护

A.4.1 应对报错文件进行配置，防止暴露敏感信息。
A.4.2 不应在系统中存放敏感信息，如系统备份文件、系统配置信息等。
A.4.3 应对配置文件进行设置，尽量不暴露系统的信息，如操作系统，web容器等。
A.4.4 如采用开源组件应进行必要的修改，防止相关信息暴露。
A.4.5 系统在停止使用后，应将所有信息进行完全清除。
A.4.6 数据库中的敏感信息加密存储。

A.5 通信的安全性

A.5.1 对于重要模块，建议采用加密方式进行信息交互。

A.5.2　应对数据的原发者和接收者提供数据接收和发送的抗抵赖功能。

A.6　软件容错

应对用户输入的数据进行有效的校验，包括内容的有效性和攻击代码的检测。

A.7　资源控制

A.7.1　应在Web容器中限定最大连接时间。
A.7.2　应在Web容器中限定系统的最大并发连接数。
A.7.3　应在系统代码设计时对单个用户的多重会话进行限制。
A.7.4　对重要的Web应用系统，应部署运行状况监测系统对系统资源的状态进行检测和报警。

A.8　数据的备份恢复

A.8.1　系统应提供数据备份功能，可以手工或自动对数据进行备份。
A.8.2　对于重要Web应用系统应采取冗余的方式。
A.8.3　特别重要Web应用系统数据备份应采用异地备份方式。

A.9　业务逻辑安全

A.9.1　应对民航Web应用系统的业务处理流程进行审计，防止业务流程漏洞。
A.9.2　应对民航Web应用系统的身份认证流程进行安全审计，防止非授权进入系统。

A.10　管理制度

A.10.1　应用户操作管理制度，防止人为原因造成安全隐患。
A.10.2　应根据 GB/T 22239对系统进行设计、建设和运维。