ICS XX.XXX.XX

CCS X XX

DB 21

辽 宁 省 地 方 标 准

DB 21/T XXXX—XXXX

信息安全技术 自防护系统（RASP）技术规范

Information Security Technology - Runtime Application Self-Protection (RASP) Technical Specification

（征求意见稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

辽宁省市场监督管理局　　发 布

目　　次

前　言

本标准按照 GB/T1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规则起草。

本文件由中共辽宁省委网络安全和信息化委员会办公室提出并归口。

本文件起草单位：赛特科技服务（沈阳）有限公司、国家计算机网络应急技术处理协调中心辽宁分中心、安百科技（北京）有限公司

本文件主要起草人：

本文件实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函的方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

归口管理部门通讯地址：中共辽宁省委网络安全和信息化委员会办公室，沈阳市和平区光荣街 26 甲。

文件起草单位通讯地址：赛特科技服务（沈阳）有限公司，沈阳市铁西区北二东路 33-2 号。

信息安全技术 自防护系统（RASP）技术规范

1 范围

本标准规定了应用软件安全自防护技术要求，主要包括应用软件安全自防护功能要求，安全管理中心功能要求以及用于接受外部安全管理策略或指令的安全管理接口技术规范等内容。

本标准适用于开发具有网络安全自防护功能的应用软件，或采购部署应用软件自防护功能产品，或用于实施信息系统应用层安全加固。

2 规范性引用文件

下列文件对本文件的应用是必不可少的。凡注日期的引用文件，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 31506－2015 信息安全技术 政府门户网站系统安全技术指南

GB/T 32917－2016 信息安全技术 应用防火墙安全技术要求与测试评价方法

GB/T GB/T 38249-2019 信息安全技术　政府网站云计算服务安全指南

GB/T GB/T 37956-2019 信息安全技术 网站安全云防护平台技术要求

GB/T 7408-2005 数据元和交换格式 信息交换 日期和时间表示法

ISO/IEC 9075-1:2011 Information technology--Database languages--SQL RFC2616 超文本传输协议（HTTP）1.1（Hypertext Transfer Protocol HTTP/1.1） ECMA-262 ECMAScript Language Specification

RFC8259 The JavaScript Object Notation (JSON) Data Interchange Format RFC 3548 The Base16, Base32, and Base64 Data Encodings

RFC6229 Test Vectors for the Stream Cipher RC4

3 术语和定义

GB/T 25069-2010、GB/T 32917－2016和GB/T 31506－2015界定的以及下列术语和定义适用于本文件。

3.1 应用软件 application

一种可以通过访问的应用程序，由完成特定任务的各种组件构成，并通过将服务提供给用户。

3.2 运行时应用自我安全防护 Runtime app lication se lf-protection （RASP）

一种新型应用安全保护技术，它将安全保护功能直接嵌入到应用程序中，与应用程序融为一体，能在不修改应用程序源代码的情况下实时进行安全检测，并阻断安全攻击，使应用程序具备应用层的自我安全保护能力。

3.3 智能安全管理中心 Intelligent security protection center

可以为一个或多个自免疫安全模块远程提供安全防护策略制定、下发以及安全事件收集、智能综合分析的安全管理平台。

3.4 安全防护策略 security protection pol icy

一种专门用于应用安全的安全策略，实现安全防护功能模块的开关以及对各安全功能模块操作的配置管理。

3.5 安全事件 security event

真实和可疑的网络攻击或异常事件。

3.6 安全连接密钥 secure connect key

一种用来实现智能安全管理中心安全地连接和管理具有自我安全防护功能的应用软件的随机字符串，该字符串由智能安全管理中心分配，通过一种安全的方式分发到所管理的应用软件，并由应用软件安全保存，应用软件在接收到来自智能安全管理中心的安全管理命令后，通过核对智能安全管理中心出示的安全连接密钥来验证智能安全管理中心是否具有远程安全管理权限。

3.7 虚拟补丁 virtual l patch

一种由智能安全管理中心制定和下发的安全防护规则，由具有运行时应用自我安全防护功能的应用软件动态执行，实现对应用软件安全漏洞的临时修补。

3.8 检测白名单 Detect white list

用来定义某个特殊处理的系统页面，要求安全防护模块不要对该页面或该页面的某个输入参数进行安全监测或防御。

4 缩略语

下列缩略语适用于本文件。

XSS：跨站脚本攻击(Cross Site Script)

HTTP：超文本传输协议(Hypertext Transfer Protocol)

CSRF: 跨站请求伪造（Cross-Site Request Forgery）

SSRF: 服务端请求伪造（Server-Side Request Forgery）

XML：可扩展标记语言（eXtend Mark Language）

XXE：XML外部实体（eXtent XML Entity）

RASP：运行时应用自我防护 (Runtime Application Self-Protection)

JSON：JavaScript对象表示法 (JavaScript Object Notation)

LDAP：轻量级目录访问协议(Light Directory Access Protocol)

XPATH：XML路径操作语言（XML Path Language）

OS：操作系统（Operating System）

MVC：模式视图控制器编程模式（Model View Controler）

API：应用编程接口（Application Programming Interface）

URI：统一资源指示器（Universal Resource Indicator）

SQL：结构查询语言（Structure Query Language）

5 总体架构

5.1 应用系统自防护系统（RASP）技术概述

应用自防护（RASP）是一种新型应用安全保护技术，它常应用于B/S架构应用软件，通过将安全保护功能模块注入到应用软件中，实时检测和阻断安全攻击。由于采用RASP技术实现的安全防护模块可以识别用户行为和程序上下文等安全运行状态，通过实时地对系统访问行为与攻击特征进行匹配、分析和研判，从而对攻击行为进行有效的处理和响应。RASP技术作用于系统应用层，但对应用程序的代码设计没有任何影响，不需要修改任何代码。同时可作为现有软硬件安全防护体系的有力补充，成为应用系统安全的最后一道防线。

5.2 应用安全自防护技术框架

应用安全自防护技术框架主要由Agent客户端和系统一管控中心两部分组成：

1）Agent内含扫描监测、攻击验证、日志分析、智能加固、策略管理等模块，其部署在Java Web 应用服务器/容器中，作为防护引擎为应用系统提供攻击实时防护能力。

2）统一管控中心作为 Agent 的集中管理工具，与Agent之间通过加密通讯进行指令下达和数据上传，支持私有云和公有云模式部署。管理中心内置知识库（安全事件库、安全规则库、漏洞后门库、分析挖掘库）和风险分析引擎，利用历史安全事件和安全信息进行预测分析，并通过收集、计算各节点 Agent 信息实现应用安全、攻击态势、安全事件、攻击回溯等维度的可视化展现。

如图1所示，一个具备运行时应用自我安全防护（RASP）功能的应用软件的整体安全防护框架包括两部分：第一部分为嵌入了安全防护功能模块的应用软件，它一般部署在企业应用域中；第二部分为智能安全管理中心，它一般部署在安全管理域或云计算数据中心（以下称为管理中心）。由内嵌在应用软件中的安全防护模块和智能安全管理中心共同组成应用软件安全防护整体框架，形成一个包括多个安全防护客户端和一个智能安全管理中心的客户机/服务器模式框架，从而实现 对来自互联网域的安全攻击的实时、智能安全检测和自动防御。

内嵌在应用软件中的自我安全防护模块基于运行时应用自我安全防护技术（RASP）实现，它深入结合应用程序的上下文和运行时环境，通过截获用户HTTP输入请求和敏感函数执行，可更为精确的 分析出来自互联网域恶意用户的安全攻击和正常用户的普通请求，从而实现对恶意用户发起的安全攻击的实时检测和精确阻断。

智能安全管理中心负责为所管理的应用软件安全防护模块定制和下发安全防护策略和规则，以及收集应用软件中自我安全防护模块上报的安全事件，并进行综合智能分析、态势感知和可视化展示等。

同时，应用软件运行时应用自我安全防护整体框架还需要明确定义运行时应用自我安全防护模 块与智能安全管理中心之间的安全管理接口，实现智能安全管理中心的安全防护策略和规则的安全下发，以及运行时应用自我安全防护功能模块的安全事件安全上报等操作。

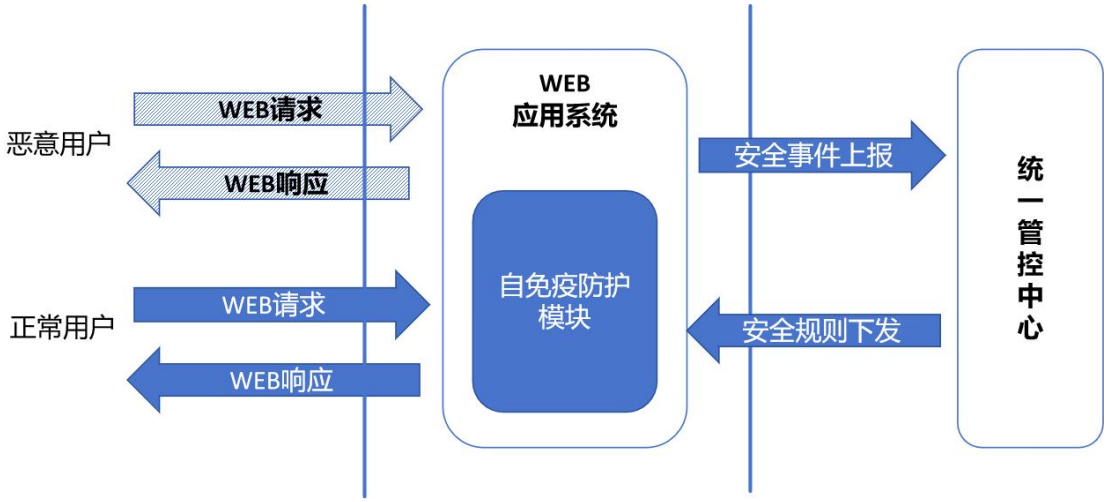

图1 应用软件运行时自我安全防护框架

本标准第六章规范了应用软件自防护安全技术的应用域功能要求，用户可依此开发具有自防护功能的应用软件，或采购部署应用软件自防护功能模块；

本标准第七，八章规范了应用软件自防护安全技术的智能安全管理中心功能要求及安全管理接口通用要求，用户或信息安全主管部门依此设计建设完整的应用软件安全防护体系。（安全管理接口技术规范见附录 A）

6 安全防护技术要求

6.1 安全防护工作模式要求

具有运行时应用自我安全防护（RASP）功能的应用软件应：

a)支持以下安全防护工作模式：

1)失效模式：当处于失效模式时，应用软件的自我安全防护功能关闭，即应用软件不受RASP保护；

2)监控模式：当处于监控模式时，应用软件的RASP安全防护功能模块开启，并依据智能安全 管理中心下发的安全防护策略检测和记录所识别出的安全攻击，但并不阻断安全攻击；

3)防护模式：当处于防护模式时，应用软件的RASP安全防护功能模块开启，并依据智能安全管理中心下发的安全防护策略检测、记录和阻断所识别出的安全攻击。

b)接收来自智能安全管理中心的指令，可以在失效模式、监控模式和防护模式之间切换。

6.2 安全防护功能要求

6.2.1 跨站脚本攻击防护能力

具有运行时应用自我安全防护功能的应用软件应具备检测和防护跨站脚本攻击的能力，包括：

a)存储式跨站脚本攻击；

b)反射式跨站脚本攻击。

6.2.2 XML实体注入攻击防护能力

具有运行时应用自我安全防护功能的应用软件应具备检测和防护XML实体注入攻击（XXE）的能力。

6.2.3 跨站请求伪造防护能力

具有运行时应用自我安全防护功能的应用软件宜具备检测和防护跨站请求伪造（CSRF）攻击的能力。

6.2.4 SQL注入攻击防护能力

具有运行时应用自我安全防护功能的应用软件应具备对支持ISO/IEC 9075-1中定义的ANSI-SQL的常见关系数据库管理系统软件的SQL注入检测和防护能力。

注：常见的支持ANSI-SQL的关系数据库管理软件包括MSSQL、Oracle、mysql、db2、postgreSQL等。

6.2.5 命令注入防护能力

具有运行时应用自我安全防护功能的应用软件应具备以下命令注入攻击的检测和防护能力：

a)LDAP命令注入；

b)XPath命令注入；

c)OS命令注入。

6.2.6 shell后门防护能力

具有运行时应用自我安全防护功能的应用软件应具备识别shell后门的能力，并在攻击者调 用shell后门时进行拦截并记录攻击细节。

6.2.7 扫描器防护能力

具有运行时应用自我安全防护功能的应用软件应具备对常见的脆弱性扫描器的识别和阻断能力，包括：

a)应具备根据扫描器发出的HTTP请求中包含的固定标识符来识别和阻断常见扫描器能力；

b)宜具备对未知扫描器（即HTTP请求中不包含固定标识符）的识别和阻断能力。

注：常见的脆弱性扫描器包括Nikto、Paros proxy、Scarab、Inspect、Whisker、libwhisker、 Burpsuite、Wikto、Pangolin、Watchfire AppScan 、N-Stealth、AWVS等。

6.2.8 开发框架漏洞防护能力

具有运行时应用自我安全防护功能的应用软件应具备对以下开发框架漏洞的远程命令执行 和表达式攻击防护能力，从开发框架底层拦截各类已知或未知的黑客攻击：

a) Apache Struts2;

b) Spring.

6.2.9 敏感文件泄露防护能力

具有运行时应用自我安全防护功能的应用软件应具备对以下敏感文件的防泄漏能力：

a)程序源代码文件；

b)网站或数据库备份文件；

c)日志文件。

6.2.10 IP 黑名单防护能力

具有运行时应用自我安全防护功能的应用软件应：

a)具备从智能安全管理中心接收IP黑名单的能力；

b)根据IP黑名单中的IP地址列表和拦截时间拦截攻击者访问应用软件的能力。

6.2.11 SSRF攻击防护能力

具有运行时应用自我安全防护功能的应用软件应具备检测和防御SSRF攻击的能力。

6.2.12 恶意文件上传防护能力

具有运行时应用自我安全防护功能的应用软件应具备对客户端上传的文件进行以下安全检测的能力：

a） 恶意病毒或木马的检测能力；

b） 格式不正确图片文件的检测能力。

6.2.13 文件系统访问控制能力

具有运行时应用自我安全防护功能的应用软件应具备对底层文件系统的文件操作进行智能判断并 阻断具有风险的文件操作的能力：

a)增加文件；

b)重命名文件；

c)文件读取；

d)文件上传；

e)文件修改。

6.2.14 反序列化攻击防御能力

具有运行时应用自我安全防护功能的应用软件应具备对JAVA反序列化攻击的检测和防御能力。

6.2.15 详细日志记录能力

具有运行时应用自我安全防护功能的应用软件应具备对应用软件中由各用户触发的行为日志记录能力。

6.2.16 虚拟补丁能力

具有运行时应用自我安全防护功能的应用软件应具备虚拟补丁能力：

a）允许智能安全管理中心通过安全管理接口下发针对具体页面或指定输入参数的安全补丁；

b)应用软件安装虚拟补丁，实现对指定页面的安全漏洞的临时修复；

c)允许智能安全管理中心通过安全管理接口删除已安装的虚拟补丁。

6.2.17 Java反射式攻击防护能力

具有运行时应用自我安全防护功能的应用软件均具备以下Java反射式攻击防护能力：

a)在Java进行反射调用之前智能判断该反射方法是否存在风险，如果存在风险则阻断其执行。

6.3 安全管理接口要求

具有运行时应用自我安全防护功能的应用软件应提供安全管理接口，供智能安全管理中心调用，并满足以下要求：

a)实现的安全管理接口可以对调用者进行身份认证，只有通过身份认证的智能安全管理中心才允 许通过该安全管理接口实现对应用软件的安全管理；

b)智能安全管理中心和应用软件安全防护模块之间通过安全管理接口传输安全防护策略或回传安全日志时，需要确保通信安全和数据安全，防止重放、窃听和篡改攻击。

6.4 开发语言环境要求

具有运行时应用自我安全防护功能的应用软件，其内嵌的安全防护功能模块应支持以下开发语言环境：

1)JAVA

2)ASP.net

3)PHP。

7 智能安全管理中心管理功能要求

7.1 安全策略管理功能

安全管理中心应支持定制安全管理策略，并通过端提供的远程安全管理接口下发，以实现 对RASP技术实现的安全防护功能模块的开关，以及实现对各安全功能模块的攻击检测和安全防 御功能的配置管理。

7.2 日志收集功能

安全管理中心应支持从RASP端处获取错误日志管理接口和获取端日志，以实现日志的汇聚和集中管理分析。

7.3 RASP 管理功能

安全管理中心应支持对所控制的RASP端进行各种管理操作，包括启动、暂停和终止RASP保护功能。

7.4 安全审计功能

安全管理中心应具备对RASP端和云端管理中心的安全审计功能，实现对所控制的RASP端管理操作 的安全审计（包括启动、暂停和终止RASP保护功能），以及对安全管理中心的各种重要操作的安全审计。

8 安全管理接口通用要求

8.1 安全管理接口协议要求

智能安全管理中心与应用软件之间的安全管理接口应满足如下协议要求：

a) 智能安全管理中心和应用软件之间的安全管理命令请求和响应消息格式应满足JSON格式要求（ECMA-262）；

b) 智能安全管理中心和应用软件之间的安全管理命令请求和响应消息应分别封装在HTTP协议（RFC2616）请求消息和响应消息中进行传输；

c)在将JSON格式的安全管理命令请求和响应消息封装到HTTP协议前，应对其进行加密和编码处理，以确保安全管理命令请求和响应消息的安全性。

8.2 安全连接密钥管理要求

应用软件应允许来自智能安全管理中心的安全管理连接请求，并采用安全连接密钥来验证安全连接的有效性，具体应满足如下要求：

a）应在安全防护模块安装前或安装过程中，由智能安全管理中心为某应用软件生成一个安全连接密钥，并通过安全方式（如邮件、短信或人工方式）传输到应用软件，并由双方安全保存，用来验证双方安全连接的有效性；

b）应用软件应基于本地安全保存的安全连接密钥对智能安全管理中心发送的JSON格式安全管理命令请求消息进行验证，只有安全连接密钥匹配成功，才能真正执行智能安全管理中心下发的JSON格式安全管理命令。

8.3 安全会话密钥管理要求

智能安全管理中心和应用软件在将JSON格式的安全管理命名请求和响应消息封装到HTTP请求和响应消息之前，应采用安全会话密钥对安全管理命令请求和响应消息进行数据加密和解密，并满足以下要求：

a)用来解密数据的安全会话密钥由智能安全管理中心通过一种安全的方式生成，并通过安全方式下发到应用软件，并由应用软件安全存储；

b)对从智能安全管理中心接收到的加密的安全管理命令请求消息，应用软件应能够使用先前获取和存储的安全会话密钥进行数据解密和解码处理；并在条件允许的情况下判定数据的完整性；

c)对需要返回到智能安全管理中心的安全管理命令响应消息，应用软件应能够对安全管理命令响应消息采用安全会话密钥进行加密和编码处理，确保数据的保密性和完整性。

8.4 安全连接数据解封和封装规范

应用软件应支持对智能安全管理中心发送的安全管理命令请求消息进行安全解封，以及对将要发送到智能安全管理中心的安全管理请求响应消息进行安全封装，具体要求如下：

a)对于接收到的安全管理命令请求消息，应用软件首先采用base64(RFC3548)解码，然后获取本 地存储的安全会话密钥，采用双方协商的加密算法对消息进行解密，得到json格式的安全管理命令请求 消息，然后从消息中抽取安全连接密钥，并和本地的安全连接密钥进行比较，只有比对成功才能执行安 全管理命令，否则拒绝执行；

b)对于应用软件需要发送的安全管理命令响应消息，首先采用存储于本地的安全会话密钥对消息进行加密，然后对加密后的安全管理命令响应消息进行base64编码，然后封装在HTTP响应消息中，通过HTTP协议发送该消息。

附录 A

（规范性附录）

智能安全管理中心和应用系统之间的安全管理接口技术规范

A.1 安全管理接口通用组件定义

A.1.1 HTTP请求消息公共扩展头定义

智能安全管理中心在将安全管理命令请求消息封装到HTTP请求消息后，在通过安全管理接口发送 给应用软件之前， 可能会在HTTP请求消息中包括HTTP请求消息扩展头，以向对方说明本次安全管理 接口通信所采用的协议版本，所采用的加密算法等信息。具体可以使用的HTTP消息扩展头如表1所示。

表1 HTTP请求消息公共扩展头定义表

英文名称	中文名称	值类型	描述	选择状态
x_iswaf_api	客户端请求地址	字符串	当HTTP请求消息中包含该扩展头 时，表示该消息属于智能安全管 理中心专门发送给 应用软件 安全防护模块的安全管理命令消息， 以区别于应用软件中的 业务功能页面。	可选。如果缺失，则通过其他方式 （如约定URI固定字符串）来识别 当前HTTP请求是否为智能安全管理 中心专门发送给 应用软件安全 防护模块的安全管理命令消息；当 包含该HTTP扩展头时，其值可以为 任意值。
x-Version	API 协议 版本	字符串	安全管理接口的协议版本号，本标 准规定的安全管理接口版本号为 1.1。设置协议版本主要是考虑多 版本的兼容问题。	可选。如果缺失，则默认安全管理接 口协议版本为1.0。如果存在，则可 以取值为1.0或1.1。
x-Crypt	密码参数	字符串	密码参数包括两部分， 前半部分标 识所采用的加密算法；后半部分标 识所采用的签名算法。两部分之间 采用分号隔开。如“RC4；HMACMD5”。 本标准要求必须支持RC4加密算法 (RFC6229)。	可选。当缺失该扩展头时，表示仅采 用了RC4算法对消息进行了加密，而 没有进行签名；当包含该HTTP扩展 头时，加密算法部分必选，签名算法 部分为可选。

A.1.2 安全管理命令请求消息公共JSON参数定义

表2定义了智能安全管理中心发送给应用软件的JSON消息格式的安全管理命令请求消息中的公共JSON参数。

表2 安全管理命令请求消息中的公共JSON参数定义表

参数名	必要性	参数值	说明
controller	必须	string	采用MVC开发框架时，用来标识该安全管理命令所对应的 API由哪个控制器所管理。
Connectkey	必须	string	安全连接密钥，用来实现智能安全管理中心和应用软件 之间安全连接的字符串。
Action	必须	String	标识当前安全管理命令请求消息的命令类型
timestamp	可选	“YYYY/MM/DD HH/MM/SS”。	用来抑制重放攻击的时间戳。精度精确到秒。

A.1.3 虚拟补丁JSON定义

本标准所定义的虚拟补丁是一种针对某个安全漏洞的安全防护规则，它由智能安全管理中心定制和下发，由具有运行时应用自我安全防护功能的应用软件安装，从而实现在不修改应用软件源代码的情况下对应用软件安全漏洞的临时修补。

智能安全管理中心通过安装虚拟补丁命令（setpatch）来下发和安装虚拟补丁，通过删除虚拟补丁命令（delpatch）来删除已安装的虚拟补丁。表3定义了一个规范 的虚拟补丁应该包含的JSON参数（其所对应的JSON对象称为WVP），表4定义了虚拟补丁触发条件 （Trigger）应该包含的JSON参数。

表3 虚拟补丁JSON定义

参数名	必要性	参数值	说明
hotfixId	必须	string	虚拟补丁编号
userid	必须	Number	管理员用户编号。
siteId	必须	Number	所属站点编号。
isSystem	必须	Number	是否属于系统层面补丁。
harmLevel	必须	Number	虚拟补丁对应用软件的可能影 响程度。

title	必须	string	虚拟补丁的名称。
Des	必须	String	虚拟补丁的描述。
scriptName	必须	String	虚拟补丁所对应页面的URI值。
Trigger	必须	List of WVPTrigger（定义见表4）	虚拟补丁触发条件列表。
content	必须	List of WVPContent（定义见表5）	虚拟补丁防护规则内容列表。
createTime	必须	Time	虚拟补丁创建时间。

表4 虚拟补丁触发器（WVPTrigger）JSON定义参数表

参数名	必要性	参数值	说明
triggerIndex	必须	Number	触发器编号
key	必须	String	触发器键名称。
keyValMethod	必须	String	触发器名称比较方法
val	必须	Number	触发器比较方法所对应的值。

表5 虚拟补丁防护规则内容（WVPContent）JSON定义参数表

参数名	必要性	参数值	说明
content_funArgs	必须	string	防护规则函数参数
contentIndex	必须	Number	防护规则内容编号。
param	必须	Number	防护规则所指定的参数名。
functionName	必须	Number	防护规则函数名称。

A.1.4 检测白名单JSON定义

在某些特定的业务场景下，如压力测试、特殊的API接口、应用程序逻辑等情况，需要对特定页面和请求参数进行检测白名单放行处理，以适应各种业务场景的需求。检测白名单和某个指定的页面关联，通过对检测白名单中定义页面或指定请求参数进行免检测处理，目的是减少误报。检测白名单通常由用户自定义。一个检测白名单一般包括如下JSON参数（如表6所示）。

表6 检测白名单JSON参数定义

参数名	必要性	参数值	说明
port	必须	Number	端口
Whitelist_id	必须	Number	白名单编号
domain	必须	String	应用系统域名。
Service	必须	String	服务类型，*代表全部服务
parameters	必须	List of String	请求参数。
Request_uri	必须	URI地址。	请求的URI地址。

A.1.5 Ip黑名单JSON定义

IP黑名单应该包括IP地址和时间段。需要和研发团队讨论后才能确定。

表7 IP黑名单JSON参数定义

参数名	必要性	参数值	说明
ID	必须	String	IP黑名单标识符。
IP	必须	String	客户端IP地址。
starttime	必须	Timestamp	拦截起始时间。
endtime	必须	TimeStamp	拦截结束时间。

A.1.6 安全管理命令请求消息命令标识符

表7定义了本标准中应用软件支持的所有安全管理命令请求消息的命令标识符，主要用于设置 安全管理命令请求消息（JSON格式消息）中的动作（action）参数。

表8 安全管理命令请求消息相关的命令标识符定义表

序号	安全管理命令中文名称	安全管理命令英文标识符
1	更新安全密钥	Mdfcryptkey
2	开启安全功能模块	setmodule
3	应用软件系统配置	System_config
4	功能模块开关	Service_set

5	设置客户端工作模式	setmode
6	设置回传日志开关	PostLogFlag
7	设置检测白名单	setwhitelist
8	删除检测白名单	delwhitelist
9	获取站点文件信息	getfileinfo
10	获取站点目录文件信息	getDirFile
11	检查站点通信状态	ConnectStatus
12	获取应用软件错误日志	err_log
13	获取客户端日志	fetch
14	安装虚拟补丁	setpatch
15	删除虚拟补丁	delpatch
16	设置IP黑名单	setIPblacklist
17	删除IP黑名单	delIPBlacklist

注：安全管理命令英文标识符不区分大小写。

A.2 安全管理接口通信信息数据安全保护规范

智能安全管理中心和应用软件之间的安全管理通信接口必须满足如下安全要求：

a) 要求智能安全管理中心和应用软件之间传输的所有JSON格式的安全管理命令请求和响应消息必须经过加密和编码处理，并满足以下要求：

1) 应用软件必须为智能安全管理中心提供一个可用的安全管理接口URL地址，安全管理接口URL地址可以是特定的URL地址（如通过固定后缀字符串标识），或者是普通的URL地址（但通过HTTP请求头部中的x_iswaf_api扩展头来明确标识），接口地址一旦设定将不再允许修改；

注：如果采用固定后缀字符串来标识安全管理接口URL地址，则默认为iswaf.api。

2) 支持对待传输的JSON格式的安全管理命令请求和响应消息进行数据加密，加密算法至少支 持RC4(RFC6229)，如果不通过x-crypt指明加密算法，则默认加密算法为RC4；

3) 对加密后的数据进行Base64编码（RFC 3548），并采用HTTP请求消息格式进行封装；

4)在采取HTTP请求消息格式进行封装时，将加密和编码后的数据放置在AdmCommandData的值域中， 然后置于HTTP请求消息主体（Body）位置，并在HTTP请求消息头部采用扩展头 X-Crypt标识所采用的加密算法和编码算法。

b)要求智能安全管理中心在加密和编码安全管理命令请求消息前，在JSON格式的安全管理命令请求消息中包含以下数据，以保证安全管理接口的通信和数据安全：

1)应包含安全连接密钥（Connectkey），应用软件在接收到JSON格式的安全管理命令请 求消息后，待Base64解码和解密之后，从请求消息中抽取出安全连接密钥，并与本地存储的安全连接密钥进行比对，只有比对成功后，才去执行安全管理命名请求消息中的包含的安全管理指令；

2) 应包含一个时间戳（timestamp），应用软件在接收到JSON格式消息后，抽取出时间戳信息，确保该消息是刚刚发送的，以防止重放攻击。

c)智能安全管理中心宜在HTTP请求消息头部采用扩展头x-Version指明本次通信所采用的安全管理 接口协议版本为1.1，应用软件在接收到HTTP请求消息后，先要检查是否存在协议版本信息，如果没有，则默认协议版本为1.0。