帆软

让数据成为生产力！

商业智能安全白皮书

WHITE BOOK OF BUSINESS INTELLIGENCE SECURITY

2.0

目录

01/ 概述

依据《中华人民共和国计算机信息系统安全保护条例》(国务院 147 号令)、《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发 [2003]27 号)、《关于信息安全等级保护工作的实施意见》(公通字 [2004]66 号) 和《信息安全等级保护管理办法》(公通字 [2007]43 号)、《信息系统安全等级保护基本要求》(GB/T 22239-2008), 制定本白皮书。

本白皮书是中国商业智能产品 (以下简称 BI 产品) 的安全标准参考指南, 也是帆软商业智能系列产品 (FineBI、FineReport) 的安全框架和标准。

本白皮书在现行通用的国内外安全技术类标准的基础上, 主要参考《信息系统安全等级保护基本要求》, 并根据国内外主流商业智能产品的技术标准和产品情况, 提出了 BI 软件整体安全的保护要求规范, 即安全管理策略和隐私、设备及网络通信安全、应用及数据安全、移动端安全, 同时对帆软产品的安全特性及场景做了详细的说明。

本白皮书适用于企业评估选型商业智能产品, 也适用于指导和规范帆软商业智能产品的规划、设计、交付和相关解决方案在安全领域的程序和标准。

02/ 信息安全现状

信息安全是指为数据处理系统而采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。这里面既包含了层面的概念，其中计算机硬件可以看作是物理层面，软件可以看做是运行层面，再就是数据层面；又包含了属性的概念，其中破坏涉及的是可用性，更改涉及的是完整性，显露涉及的是机密性。

根据 Gartner 数据分析显示，2/3 的 Web 应用都或多或少存在着安全问题，其中很大一部分甚至是相当严重的问题。而对商业智能领域而言，绝大多数（主流）的商业智能软件均为 Web 应用，不能轻视安全性问题。

大环境而言，近年来，网络安全威胁事件频发，给个人和企业造成经济损失的情况快速增多。信息安全事件也已上升到国家战略，国家及企业对于信息安全的投入日益增加，很多企业也将信息安全作为企业信息化中不可或缺的一环。但安全意识并不是一朝一夕能够形成的，较多的企业由于安全意识落后，安全措施和安全教育宣传的力度不够，对于安全的认知只是停留在通过某次检测或者说购买一些软硬件的被动状态。安全机构每天都会公布新的漏洞信息，如果响应不及时，那么就很有可能会暴露在风险之中，企业需要对于信息安全持续关注投入，并且做好企业相关人员的安全管理教育。

对商业智能厂商而言，大部分厂商对于安全的问题关注度也缺乏，从开发过程中对安全风险的审核，发布前软件的安全测试、持续关注所用第三技术的漏洞再到内部的关键安全岗位人员安全教育，每一步的缺失都会变成最终企业用户的信息安全风险。在市场对安全要求提高倒逼商业智能厂商重视的同时，厂商更应该做好企业内部的安全建设，让整个商业智能领域向着更安全的方向发展。

最后，传统的操作系统由于逐渐成熟，系统漏洞越来越难以利用，攻击者的目标也从系统漏洞渐渐转移到应用漏洞。同时由于大多企业对 Web 应用安全的不重视，当前存在漏洞的 Web 应用程序是很容易被攻击者所利用,最终导致用户的重要数据被篡改、泄露或破坏。OWASP 组织（开放式 web 应用程序安全项目）在”TOP10 2017” 中公布了 2017 年的 “十大安全隐患列表”，其中列为第一的就是注入。在使用有 SQL 注入漏洞的应用的情况下，如果缺少专业安全厂商技术的有效识别保护，那么通过简单的 SQL 注入语句，就能实现轻易攻陷 Web 应用，访问他们本没有权限的敏感数据。

在外部信息安全越来越被重视的形势下，越来越多的企业开始重视自身信息系统的安全建设，这也是必然趋势。除了基本的安全宣传，内外网隔离和安装相关安全防护软硬件等措施，企业也必将对采购的相关信息系统（OA、ERP、CRM 等）提出了更高的安全要求，例如必须修复已知的安全漏洞，提供第三方权威机构的安全扫描检测报告，在账户安全，数据安全，运营安全等方面提供完备的解决方案等，这也是一个成熟的商业智能厂商需要能够提供的标准服务。

03/ 商业智能的安全策略

针对不同安全防护等级,BI 系统应该具有基本安全防护能力,这是对系统安全的基本要求.根据实现方式,对安全的基本要求可以分为两类：技术类和管理类。对应于基本要求，企业 BI 系统安全整体策略也可以分为技术安全策略和安全管理策略两类，如图 3-1 所示，下面将逐一展开介绍。

图 3-1 企业 BI 系统安全整体策略

3.1 技术安全策略

技术安全策略与 BI 系统提供的技术安全机制有关，主要通过在 BI 系统中部署软硬件并正确地配置其安全功能来实现，这也是 BI 系统所必备的安全能力。为了便于理解，我们从设备及网络通信安全、应用及数据安全、移动端安全三个方面解读和阐述技术安全策略。

3.1.1 设备及通信安全

1）设备安全

入侵防范

a. 应对 BI 应用服务器进行安全加固，能够检测到对其的入侵行为，记录入侵 IP、攻击类型、攻击目的、攻击时间等关键信息，并在发生严重入侵事件时提供报警；

b. 应对 BI 应用服务器安装防恶意代码软件，并及时更新防恶意代码软件和恶意代码库。

c. 使用安全扫描软件定期对 BI 应用服务器进行漏洞扫描，及时发现并修补操作系统、中间件相关漏洞。

身份鉴别

a. 应对登录 BI 应用服务器操作系统的用户进行身份鉴别;

b. 应对登录失败进行必要的限制, 如结束会话、限制非法登录次数和自动退出等;

c. 应对服务器远程管理采取必要措施, 防止鉴别信息在网络传输过程中被监听;

d. 应对登录 BI 应用服务器操作系统的不同用户分配不同的用户名, 同时采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

访问控制

a. 应对访问 BI 应用服务器的用户进行访问控制, 控制其对资源的访问;

b. 应及时删除多余、过期的账户, 避免出现共享账户;

c. 应对允许登录服务器的终端进行条件限制。

安全审计

a. 审计范围应覆盖到协同管理软件服务器和重要客户端上的每个操作系统用户和数据库用户;

b. 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件

c. 应保护审计记录, 避免受到未预期的删除、修改或覆盖等。

2) 网络通信安全

网络设备防护

a. 应对登录网络设备的用户进行身份鉴别, 且用户的标识应唯一, 具有不易被冒用的特点;

b. 主要网络设备应有两种及以上的鉴别技术来进行身份鉴别;

c. 应具有登录防暴力破解功能, 如登陆失败结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施;

d. 应对网络设备的管理员登录地址进行限制。

网络边界安全

a. 应在网络边界部署访问控制设备, 启用访问控制功能;

b. 应在网络边界处监视以下攻击行为: 端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等;

c. 应能够对边界进行完整性检查, 对内网用户私自访问外网和非授权用户私自访问内网进行有效阻断。

安全审计

a. 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录;

b. 审计记录应包括: 事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;

c. 应能够根据记录数据进行分析, 并生成审计报表;

d. 应对审计记录进行保护, 避免受到未预期的删除、修改或覆盖等。

HTTPS 通信

a. 经由 HTTPS 进行通信, 利用 SSL/TLS 加密数据包, 防止获取网站账户及隐私信息;

b. HTTPS 服务端证书可提供网站服务器的身份认证, 用于验证站点所有者身份, 保护交换数据的隐私及完整性;

c. HTTPS 客户端证书可提供客户端身份标识的认证, 用于识别客户端或用户的身份, 向服务器验证, 精准确定访问者身份;

d. 服务端、客户端双向认证, 避免匿名通信, 确保通信双方身份一致, 彼此信任。

3.1.2应用及数据安全

1) 账户安全

商业智能软件应当提供身份安全、访问控制和日志审计的安全机制来帮助客户保护账户安全以防止未授权的用户进行操作。

身份安全

身份安全用于鉴别登录用户的真实身份, 如表 3-1 所示, 可以使用 “用户名 + 静态密码” 的方式。在认证方式上, BI 系统需要支持使用 LDAP/AD 或 HTTP 认证, 同时支持通过二次开发接口编写其他认证方式, 如 ADFS (活动目录联合服务)。有的 BI 产品如 FineBI, 在提供以上具体安全策略外, 还能在用户登录时提示上次登录地, 而且支持单一登录, 开启登录验证码后, 将在用户名和密码之外再增加一层安全保护。

表 3-1 身份安全策略

身份认证方式	具体安全策略
用户名+静态密码	密码加密存储、加密传输; 登录防暴力破解：短信、邮箱验证码、静态验证码，失败次数限定; 密码安全策略：密码强度限制、密码定期更新
LDAP/AD	支持通过LDAP或AD进行身份认证
HTTP	支持通过HTTP进行身份认证
自定义扩展	提供登录认证的二次开发接口，可根据自身需求开发使用ADFS等认证方法

帆软数据分析平台在满足以上具体安全策略外，还支持登录时提示上次登录地功能，且支持单一登录，开启登录验证码后，系统将在用户名和密码之外再增加额外一层安全保护。

访问控制

为了保证信息和资源访问的安全，防止对任何资源进行未授权的访问，使系统在合法的范围内使用，访问控制是一项必不可少的技术，它也是保护网络信息安全的最核心策略之一。商业智能产品可采用基于对象的访问控制技术（OBAC Model: Object-based Access Control Model），如图 3-2 所示。

OBAC 的核心是控制策略和控制规则，在基于受控对象的访问控制模型中，将访问控制列表与受控对象或受控对象的属性相关联，并将访问控制选项设计成为用户、组或角色及其对应权限的集合；同时允许对策略和规则进行重用、继承和派生操作。从信息系统的数据差异变化和用户需求出发，有效地解决了用户数量多、数据种类繁多、资源更新变化频繁带来的系统安全管理难以维护的问题。

图 3-2 OBAC 模型结构图

帆软数据分析平台（决策系统）对系统权限采用 OBAC 基于对象的访问控制，同时基于 OBAC 实现自主访问控制和强制访问控制。通过对角色、部门、用户授权，确定用户的访问权限，支持临时禁用账户，同时对所有资源访问都做权限验证，避免了水平越权及垂直越权的问题。

2）应用安全

应用服务器安全

Web 应用程序往往需要部署在应用服务器上，此时应用服务器是否安全正确的进行配置，也会严重影响应用安全。

a. 应选用安全版本的应用服务器

b. 应对应用服务器进行安全配置，包括：屏蔽应用服务器版本信息、禁用不安全的请求方法、清除默认的样例工程、隐藏响应堆栈信息等

c. 应定期收集应用服务器相关安全漏洞，并及时进行修复或更新

常见安全问题防护

XSS 跨站脚本攻击、木马上传、SQL 注入、cc 攻击等都是 Web 应用常见的安全问题，如服务器端没有进行适当的过滤处理，极易引起用户敏感数据泄露、系统瘫痪此类的问题。

对于这些常见的 OWASP 攻击，商业智能软件应进行充分的防范。结合帆软积累的方法经验，有表 3-2 中的安全防护策略可以应对。

表 3-2 常见应用安全防护策略

应用安全防护策略	详细说明/意义
访问频率限制	通过对同一IP在一定时间内的访问次数进行限制，可以有效降低爬虫爬取数据及恶意访问cc攻击的风险
给请求头附加Security Heasders系列属性	可有效防护XSS跨站脚本、点击劫持、内容嗅探等攻击方式，保障应用的安全与可用性
对上传的文件进行二进制头校验	防止风险文件通过更改后缀等方式伪装上传
使用Token验证替代Cookie验证	对于CSRF（Cross-Site Request Forgery）跨站脚本伪造，系统使用Token验证替代了Cookie，如果请求中没有token或token内容不对则无法访问
禁用特殊关键字及字符转义	防止SQL注入
后台日志输出控制	防止系统运行异常导致堆栈泄露有关代码，避免向前台输出异常堆栈，输出敏感信息。如对401、404和500错误进行处理，避免泄漏中间件类型和版本信息。

安全测试

同时商业智能厂商需要在研发流程中，有明确的安全测试要求和测试策略，定期采用软件工具进行 web 扫描或联系可靠的第三方机构进行渗透测试，以确保 web 应用的安全性。

第三方软件安全

商业智能厂商在开发过程中往往会引入第三方软件，如果第三方软件出现安全漏洞，那么也会给应用带来安全风险。

商业智能厂商应建立第三方软件清单，建立第三方开源软件的管理机制，包括引入、退出和漏洞的收集，并定期进行安全检测，确保不包含存在安全问题的第三方框架版本。

3）数据安全

不管是病毒、黑客还是其他安全威胁，都是人为因素，而人为因素本身，以企业内部人员及商业间谍的信息安全威胁最大。对人为因素的识别存在较大难度，因此对数据本身的防护就显得尤为重要，目的是阻断人为因素或减小人为因素带来的不利影响。表 3-3 列出了主要的数据安全防护策略。

表 3-3 数据安全防护策略

分类	数据安全防护策略	详细说明/意义
底层防护	支持HTTPS	支持用户自行配置HTTPS访问，以大大增加第三方监听、拦截和信息破解的难度。
	密码存储加密	所有的用户密码，都是采用SHA256哈希算法，管理员也无法获取到用户密码，连接其他系统的密码采用RSA（2048位）非对称加密，每个系统可以自行设置加密秘钥，保障密码安全。
	数据权限分配	通过数据连接的权限分配，确保用户只能看到及使用自己有权限的数据连接。
	配置信息安全	配置信息不以文件形式存储，而是存储到数据库中，支持外置到指定的数据库，确保配置信息不被泄露。
	SQL日志	对所有的数据操作提供监控，资源执行的SQL将都记录在日志中，数据改动有迹可循
前端防护	禁止URL直接访问	对非登录用户的资源访问也进行了严控，开启限制后，非登录用户无法对后台的资源进行访问，解决了用户担忧外网开启后会被非授权用户通过url进行访问的问题。
	资源权限	支持对报表模板、分析、系统设置进行访问或编辑的权限，比如不同用户访问统一报表显示不同数据。
	操作权限	支持对报表或分析的打印、导出或数据录入的权限，比如只有特定角色才可以导出excel。
	安全水印	在访问报表等页面时，通过顶层显示水印，以达到震慑及溯源的目的，提高泄密成本，降低泄密风险。水印可设置为访问IP、访问人、访问时间等组合。

4) 运维安全

审计日志

审计日志可以帮助审计人员对风险或违规操作进行审计，也可以帮助更好的理解和诊断安全状况。帆软使用自主研发的 swift 引擎进行日志存储，在保证性能的同时确保管理员无法对日志进行删除和修改。日志审计策略如表 3-4 所示。

表 3-4 日志审计策略

面向角色	日志审计策略
管理员	记录管理员修改系统设置、对用户进行增删改、对资源目录进行增删改和对权限进行增删改等行为进行记录，记录的信息包括操作时间、操作IP、操作模块、设置项、被访问资源和操作类型等。
用户	对普通用户登录日志以及在系统中的行为日志进行记录，包括访问记录，资源导出打印记录，记录的信息包括操作时间、操作IP、被访问资源、操作类型和详情等。

密码审计

提供密码强度限制，可以自行配置对于密码强度的限制，设置后将不允许使用弱口令作为缺省密码。管理员可通过设置强制用户进行定期密码修改。帆软 BI 产品也支持密码防暴力破解，当某 IP 或用户出现多次登录密码错误时，将对用户或 IP 进行锁定，并提供给管理员查看及解锁的地方，保证用户登录信息的安全。

备份还原

商业智能产品应当具备备份还原的功能，确保系统发生故障或被恶意更改后可进行恢复。如帆软 BI 产品自带备份工具，会定期自动对应用系统进行备份，也可自行修改备份频率。

3.1.3 移动端安全

当前是移动互联网时代，移动端安全也是商业智能产品安全防护的重中之重。在保障移动端安全上，一般通过身份安全、数据安全、代码安全、网络通信安全、客户端运行安全、安全审计等多方面来实现安全保障。

1) 身份安全

帆软 BI 移动端（FineMobile）应对登录用户进行身份唯一性标识和鉴别，对终端常见的攻击手段提供相应的安全保护策略，如表 3-5 所示。

表 3-5 常见身份安全防护策略

身份安全保护策略	详细说明/意义
手势密码登陆	除常规帐号密码登录外，可以设置手势密码来加强身份鉴别。
登录验证	登录时除了需要用户名和密码外，还需要与用户相匹配的动态验证码，才能进行登录，保障账户信息的安全性，有效防止暴力破解。
设备绑定	通过设备绑定功能，对帐号登录的设备进行授权绑定后，账号只能在指定设备上登录,设备更换或遗失时，管理员也可以及时解除原有绑定避免安全隐患。

2) 数据安全

通过授权体系和客户端本地数据安全的方式，保障数据安全。

帆软 BI 移动端的资源及数据授权体系继承于 PC 端，其能力和安全防护标准均一致。此外，帆软可以在平台目录级的控制上，对移动端和 PC 端分别授权。

在保障客户端本地数据安全上，主要有表 3-6 中的两点策略。

表 3-6 本地数据安全策略

数据安全保护策略	详细说明/意义
本地文件内容安全	对敏感数据如用户名密码等进行加密存储。
本地日志内容安全	限制本地日志输出级别，确保本地日志中不存在敏感信息如应用网络请求调试信息。

3) 客户端运行安全

保障客户端运行安全，核心是对 Activity 的劫持保护。移动端需要对于重要页面有提示功能。如发现登录页 Activity 被劫持，会弹出提示，防止被恶意攻击者替换上仿冒的恶意 Activity 界面进行攻击和非法用途。

4) 网络通信安全

移动端网络通信安全防护策略如表 3-7 所示。

表 3-7 移动端网络通信安全防护策略

网络通信安全保护策略	详细说明/意义
HTTPS 数据安全传输	支持 HTTPS 协议，经由 HTTPS 进行通信，利用 SSL/TLS 加密数据包，防止获取网站账户及隐私信息。
支持 VPN	通过 VPN 建立与企业内网的可信安全连接，解决用户远程接入过程中终端、接入、链路等环节的安全问题。帆软 BI 移动平台内嵌了深信服 VPN，也支持与其他厂商客户端集成。
内外网隔离	通过代理配置实现移动端外网访问,实现内外网隔离场景。

5) 安全审计

用户行为会进行日志记录，内容包括（用户行为的日期和时间、用户、事件类型等），日志信息可以区分行为终端是移动端还是 PC 端，并能根据记录数据进行分析，生成审计报表。

3.2 安全管理策略及隐私

相比于技术上的漏洞，人们往往更容易忽略安全管理问题所带来的风险，这部分风险可能造成的危害并不亚于前者。因此，要在企业内加强信息安全教育，培养安全意识，完善安全管理策略，从源头保障 BI 应用安全。安全管理策略与 BI 系统中各种角色参与的活动有关，主要通过在政策、制度、规范、流程以及记录等方面制定规定,控制各种角色的活动。下面介绍一些具体的安全管理措施。当然,很多措施不只对 BI 系统有用,对于企业的整体信息安全都是非常有必要的。

3.2.1 安全管理

1) 安全管理部门

a. 应设立信息安全管理工作的职能部门，设立安全主管、系统管理员、安全管理员和网络管理员等各个方面的负责人，并制定文件，明确安全管理部门及各负责人的职责，岗位管理制度应包括保密管理；

b 应配备专职安全管理员，不可兼任，且关键事务岗位应配备多人共同管理；

c. 应根据各个部门和职位的职责进行授权或分级授权，并定期审查授权情况；

d. 应加强各管理人员、内部组织机构及安全职能部门的合作和沟通，共同写作处理信息安全问题；

e. 应加强与供应商、专业的安全公司、安全组织的合作和沟通；

f. 安全管理员应定期进行安全检查，包括日常运行，系统漏洞和数据备份等，并形成安全检查报告。

2) 人员安全管理

a. 应对关键岗位人员任用前进行背景核查，包括：1、个人身份核查；2、个人履历的核查；

b. 应与关键岗位人员签订保密协议；

c. 应建立安全培训制度，定期对所有工作人员进行信息安全培训，提高全员的信息安全意识；

d. 应严格规范人员离岗过程，及时终止离岗员工权限，关键岗位人员须承诺调离后的保密义务方可离开；

e. 应确保外部人员访问事先提出书面申请，批准后由专人陪同或监督，并登记备案。

3) 访问控制管理

a. 应建立包括物理和逻辑的系统访问权限管理制度；

b. 根据人员职责分配不同的权限，权限为满足工作需要的最小权限，且未经明确允许的一律禁止；

c. 应定期对权限进行检查，如发现不恰当的权限设置应及时调整。

4) 设施安全管理

a. 应由专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；

b. 应对信息系统相关设备、线路等指定专门的部门或人员定期进行维护管理；

c. 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动 / 停止、加电 / 断电等操作；

d. 应根据安全等级和涉密范围，对人员出入采取必要的技术与行政措施进行控制，对人员进入和退出的时间及进入理由进行登记等；

e. 应确保信息处理设备必须经过审批才能带离机房或办公地点。

5) 网络和系统安全管理

a. 应定期对网络和系统进行安全扫描和渗透测试，并对发现的安全漏洞进行及时修补；

b. 应进行计算机病毒等恶意代码的预防、检测及系统被破坏后的恢复措施；

c. 应保证与所有外部设备的连接均得到允许授权；

d. 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作，并定期对运行日志和审计数据进行分析，以便及时发现异常行为。

6）备份与恢复管理

a. 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b. 应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；

c. 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

d. 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；

e. 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

7）漏洞预警

a. 应由专门的部门或人员负责漏洞收集、漏洞测试、漏洞分析、漏洞修复及漏洞预警等

b. 应在发现安全漏洞后，尽快在企业内部发送漏洞预警，指导并监督相关系统的漏洞修复

8）应急预案管理

a. 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；

b. 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；

c. 应定期根据实际情况更新并开展应急演练。

3.2.2 隐私保护

商业智能产品应当注重对用户的隐私保护，遵守相关法律法规。

帆软严格遵守国家相关的法律法规，不会侵犯客户的隐私，仅为了提高产品对用户的服务质量和效率而收集相关信息，并将这些信息用于努力改善产品使用体验。且帆软不会主动上传服务器的功能使用情况，仅生成行为数据文件保存在客户自己的服务器上，客户可以主动提供，帮助帆软改进产品。

04/ 常见漏洞（OWASP TOP10 2017）解决措施

开放网页应用安全计划 (OWASP) 定期会发布十大最关键 Web 应用安全风险，是一个面向开发人员和 Web 应用程序安全性的标准意识文档。目前最新版本为 2017（见表 4-1），同时官方已经发起了 OWASP Top10 2020 数据分析计划。

虽然 2017 版本可能已经不代表当下最流行的前十个 Web 漏洞，但依旧对于应用的安全具有参考意义，商业智能则必须提供相应的解决措施，才能保护自己的应用。

表 4-1 2017 OWASP TOP10 及解决措施

2017 OWASP TOP10	帆软 BI 产品的解决措施
A1:2017– 注入	提供 SQL 防注入功能，对特殊字符在后台进行禁用或转义。
A2:2017– 失效的身份认证	支持多因子身份验证，同时提供密码强度限制并限制登录失败次数的功能。
A3:2017– 敏感信息泄漏	支持 HTTPS，对敏感信息进行加密，且使用高强度的加密算法存储用户密码等
A4:2017–XML 外部实体（XXE）	系统全局控制 XML 解析，对于所有的解析禁用外部实体和 DTD。
A5:2017– 失效的访问控制	系统严格限制对于资源的访问，通过角色权限的验证，确保未登录无法访问资源并杜绝水平及垂直越权。
A6:2017– 安全配置错误	去除 tomcat 容器的 manager 等管理组件，增加 security headers 设置。
A7:2017– 跨站脚本（XSS）	进行转义，不允许直接输出，同时使用 CSP 内容安全策略，进一步缓解潜在 XSS 漏洞。
A8:2017– 不安全的反序列化	无相关代码，不涉及此风险
A9:2017– 使用含有已知漏洞的组件	持续关注所用框架的 CVE 漏洞，并及时修复和升级
A10:2017– 不足的日志记录和监控	全面的日志记录，对于访问资源、设置更改和权限配置等都进行日志记录，便于审计

05/ 安全检测及评估指标

为方便评估商业智能产品的安全性，特给出以下安全监测指标建议。商业智能产品应当完成各项安全指标的达标验证。

为确保系统完备的安全体系，参照以下安全标准，商业智能领域产品应完成各项安全指标的达标验证。

5.1 PC 端平台安全检测指标

表 5-1 PC 端平台安全检测指标

序号	类别	测试点
1	产品开发、发布和安装安全	禁止绕过系统安全机制的功能
		禁止存在未文档化的命令 / 参数、端口等
		软件完整性
		安全编码
		安全补丁发布
		开源软件安全
2	协议与接口	通信矩阵
		协议安全
		端口接入认证
		协议健壮性
3	敏感数据与加密	加密算法清单
		私有密码算法
		不安全密码算法
		敏感数据存储安全
		敏感数据传输安全
		密钥安全
4	隐私保护	个人数据转移
		个人数据采集 / 处理
		精准位置信息
5	口令安全	口令复杂度检查
		用户锁定机制
		口令加密存储
		口令修改
		账号口令清单
6	日志审计	管理面的用户活动、操作指令必须记录日志
		日志内容要能支撑事后的审计
		日志要有访问控制，防篡改
7	防止非法监听	防止非法监听
8	安装和配置管理	软件安装
		不安全密码算法
9	用户管理	软件用户的隔离
10	Web 系统安全	SQL 注入
		跨站脚本攻击（XSS）
		XML 外部实体（XXE）注入
		跨站点伪造请求（CSRF）
		服务器端请求伪造（SSRF）
		任意文件上传
		任意文件下载或读取
		任意目录遍历
		.svn/.git 源代码泄露
		信息泄露
		CRLF 注入
		命令执行注入
		URL 重定向
		Json 劫持
		第三方组件安全
		本地 / 远程文件包含
		任意代码执行
		Struts2 远程命令执行
		Spring 远程命令执行
		缺少 “X-XSS-Protection” 头
		flash 跨域

10	Web 系统安全	HTML 表单无 CSRF 保护
		HTTP 明文传输
		使用 GET 方式进行用户名密码传输
		X-Frame-Options Header 未配置
		任意文件删除
		绝对路径泄露
		未设置 HTTPONLY
		X-Forwarded-For 伪造
		明文传输
		不安全的 HTTP Methods
		任意文件探测
		加密方式不安全
		使用不安全的 telnet 协议
		验证码缺陷
		反序列化命令执行
		用户名枚举
		用户密码枚举
		用户弱口令
		会话标志固定攻击
		平行越权访问
		垂直越权访问
		未授权访问
		业务逻辑漏洞
		短信炸弹

5.2 移动端安全检测指标

表 5-2 移动端安全检测指标

类别	测试点	测试内容
客户端静态安全	反编译保护	代码进行了混淆； 检测逆向工程、二次打包、代码注入等攻击风险
	安装包签名	可防止篡改及重签
客户端数据安全	本地文件内容安全	对用户敏感信息如帐号密码等进行加密存储
	本地日志内容安全	严格控制日志级别，仅输出error级别日志，一般调试信息尤其包含网络请求调试信息不允许输出
客户端运行时安全	输入记录保护	对用户敏感信息如密码输入时采用自定义软键盘替代系统键盘，防止恶意程序对敏感信息输入进行监听
	屏幕录像保护	对系统截屏进行监控提示
	Activity劫持保护	对重要页面如登录页进行Activity劫持防护，防止被恶意攻击者替换上仿冒的恶意Activity界面进行攻击和非法用途
身份安全	防暴力破解、弱密码	增强密码复杂度策略，设置密码定期修改； 对登录登录增加动态验证码校验
	登录设备限制	同一个帐号限制登录的设备
	会话超时策略	应包含登录超时及会话超时机制，超时后需重新验证方可使用
通信安全	数据加密传输	经由HTTPS进行通信，利用SSL/TLS加密数据包，防止获取网站账户及隐私信息； 通过VPN建立与企业内网的可信安全连接
应用组件安全	Activity/Service/BroadcastReceiver组件暴露	严格控制组件属性，防止恶意数据针对导出组件实施越权攻击

06/ 典型的安全防护场景

6.1 恶意访问防护

随着“大数据”一词大热，“爬虫”也渐渐为大家所熟知，对于企业而言，被爬数据危害巨大。有资料显示，多家航空公司的低价机票数据被爬,然后被加价出售,对相关企业造成了非常大的干扰,同时也扰乱了市场秩序。同时，和 cc 攻击一样，由于对服务器进行大量的请求，会导致服务器压力过大，影响业务人员的正常使用，甚至导致服务器宕机。

常规“反爬虫”技术包括访问频率控制、使用代理 IP 池、抓包、验证码的 OCR 处理等。其中，访问频率控制是非常有效的一种手段，通过限制单 IP 一段时间内访问数据的次数，可以有效遏制爬虫爬取数据。

比如，帆软 FineReport 10.0 提供访问频率控制功能，开启后，可以对一定时间内的访问次数进行限制，超出则拉入黑名单，无法再进行资源访问，可有效缓解异常访问，爬虫爬取和 cc 攻击的情况。

6.2 账户安全设置

账户安全问题正成为威胁企业信息安全的重要因素，很多用户在设置账户密码时会设置简单的密码或者多个平台使用同一个密码，并且没有定期改密码的习惯，这就给很多不法分子以可乘之机，只要通过简单的遍历或者通过其他平台的账户密码就可以破解企业账户，然后盗取大量重要信息，给企业带来不可挽回的巨大损失。

在一些安全保密等级强的企业，例如制造型外企，有很强的账户安全意识，但是目前只能通过下达文件要求和管理层督促的手段来推动账户安全策略的实施，这种传统的方式不仅损耗大量人力，效果也常常大打折扣，最终不了了之。

比如，帆软 FineBI 5.0 提供完善的强密码策略，包括：

1）增加五项密码强度限制选项，管理员可设定密码复杂度限制，密码强度不满足要求时登录会强制修改密码；

2）提供定期修改密码选项，到规定时间时提示用户修改密码，且新旧密码不允许相同；

3）开启修改密码校验，需要通过短信 / 邮箱验证才能修改密码。

同时为了防止账户被盗用或被暴力破解，提供了防暴力破解策略，包括：

1）登陆失败次数限定，限定登录失败次数上限，超过则锁定账户或 IP 一段时间，可由管理员进行解锁；

2）提供滑块 / 短信 / 邮箱三种登录验证方式，确保账户不被盗用。

6.3 数据防泄露

随着企业的发展，产生了大量的线上数据，防止数据泄露成为企业信息安全的重点。调查机构资料显示，企业面临的数据泄露威胁，不光来自外部的入侵，还要防止来自内部员工有意无意的泄露，堡垒都是从内部攻破的。

水印是一种数据防泄漏的有效方式，在内部员工截图或者导出时，既可以提醒该员工，这是绝密资料，禁止外传,也可以起到震慑的作用。同时万一有员工将带有水印的资料泄露出去,也方便企业追查责任人和泄漏源。

比如，帆软 FineBI 5.0 就提供了水印功能，报表可添加水印，始终显示在数据上层，可降低数据泄露的风险。在报表和决策报表中可以根据企业的场景，添加访问人姓名，访问时间，访问 IP 和文字等水印内容，还可根据需要调整水印的字号和颜色。

6.4 日志审计

当系统被攻击或存在可疑操作时，通常需要通过查询日志，回溯使用记录以定位到问题根源。因此需要系统能够完整记录下所有的访问或操作记录，便于进行日志审计，找到可疑用户或操作。

比如，帆软 FineReport 10.0 提供了完整的用户访问、管理操作记录，包括了访问用户、被访问资源、IP、

07/ 附录

7.1 国家信息中心软件评测中心委托评测报告

FineBI V5.0 委托评测报告

结 论 描 述

国家信息中心软件评测中心于 2018 年 06 月 06 日至 2018 年 08 月 03 日，受达孜帆软软件有限公司的委托，对“帆软商业智能软件[简称:FineBI] V5.0”进行委托评测。

针对本次测试，国家信息中心软件评测中心遵循测试标准和需求依据开展测试工作。测试过程中共设计测试用例 6 项，测试需求覆盖率 100%，用例执行比例 100%。

测试过程中依据测试用例，对“帆软商业智能软件[简称:FineBI] V5.0”进行信息安全性测试。系统具体表现如下：

信息安全性方面，被测系统具有身份鉴别、访问控制的安全机制；并且通过采用 IBM Security AppScan Standard9.0.3.6（安全规则库版本：10344）进行安全漏洞扫描的方式，针对“HTTP 响应分割”、“LDAP 注入”、“SOAP 数组滥用”、“SQL 注入”等扫描项，于 2018 年 07 月 20 日对“帆软商业智能软件[简称:FineBI] V5.0”进行安全漏洞扫描，未发现高、中、低级别安全风险。

具体测试结果参见本报告“1.1 信息安全性测试结果”。

通过本次测试及分析，“帆软商业智能软件[简称:FineBI] V5.0”满足附件列表中所规定的需求（需求列表见附件一）。

国家信息中心软件评测中心

2018 年 08 月 03 日

FineReport V10.0 委托评测报告

结 论 描 述

国家信息中心软件评测中心于 2018 年 07 月 20 日至 2018 年 09 月 11 日，受达孜帆软软件有限公司的委托，对“帆软报表软件[简称:FineReport] V10.0”进行委托评测。

针对本次测试，国家信息中心软件评测中心遵循测试标准和需求依据开展测试工作。测试过程中共设计测试用例 41 项，测试需求覆盖率 100%，用例执行比例 100%。

测试过程中依据测试用例，对“帆软报表软件[简称:FineReport] V10.0”进行信息安全性测试。通过严格执行测试。系统具体表现如下：

被测系统具有身份鉴别、访问控制的安全机制；并且通过采用 IBM Security AppScan Standard 9.0.3.6（安全规则库版本：10344）进行安全漏洞扫描的方式，针对“HTTP 响应分割”、“LDAP 注入”、“SOAP 数组滥用”、“SQL 注入”等扫描项，于 2018 年 09 月 05 日对“帆软报表软件[简称:FineReport] V10.0”进行安全漏洞扫描，未发现高、中、低级别安全风险。

具体测试结果参见本报告“1.1 信息安全性测试结果”。

通过本次测试及分析，“帆软报表软件[简称:FineReport] V10.0”满足附件列表中所规定的需求（需求列表见附件一）。

国家信息中心软件评测中心

2018 年 09 月 11 日

7.2 奇安信渗透测试报告

奇安信
新一代网络安全领军者

帆软报表系统 10.0.1 渗透测试报告

奇安信
新一代网络安全

网神信息技术（北京）股份有限公司

2019-08-23

新一代网络安全

奇安信 新一代网络安全领军者

一. 摘要

经南京帆软软件有限公司授权，网神信息技术（北京）股份有限公司于 2019-07-22 至 2019-07-26 对帆软报表系统进行了安全渗透测试。

本次渗透测试未发现安全漏洞，因此我们认为帆软报表系统总体安全状态为“良好状态”。

渗透测试结果及风险分布图如下：

严重问题：0 个

中等问题：0 个

轻度问题：0 个

安全风险汇总如下：

威胁级别	数量	安全问题名称

漏洞类型测试结果如下：

测试分类	测试项	测试结果
Web 安全	SQL 注入	通过
	跨站脚本攻击（XSS）	通过
	XML 外部实体（XXE）注入	通过
	跨站点伪造请求（CSRF）	通过
	服务器端请求伪造（SSRF）	通过
	任意文件上传	通过
	任意文件下载或读取	通过
	任意目录遍历	通过
	.svn/.git 源代码泄露	通过
	信息泄露	通过
	CRLF 注入	通过
	命令执行注入	通过
	URL 重定向	通过
	Json 劫持	通过
	第三方组件安全	通过

新一代网络安全

7.3 知安天下安全测试报告

KNOWSAFE

帆软 FineBI V5.1

安全测试报告

2019 年 7 月

KNOWSAFE

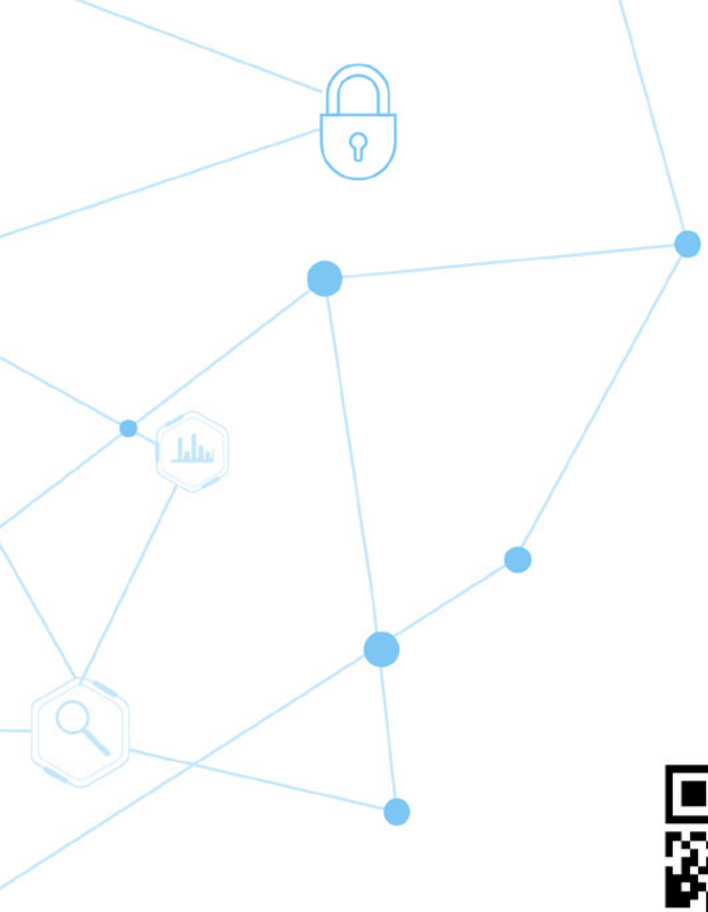
三、测试结论

帆软软件于 2019-06-25 通过了知安安全检测中心 589 位安全专家检测，聘用并授权知安安全检测中心全体安全专家成为其平台安全顾问，且帆软软件（FineBI V5.1）在服务时间内对已发现漏洞已完成修复，暂未发现安全风险。

四、安全建议

知安作为安全服务提供商建议帆软软件有限公司进行以下安全建设，以长期保证帆软 FineBI V5.1 的安全：

- 针对渗透测试结果协调开发团队或厂商进行有效的安全整改和修复。
- 配备专业的 WEB 应用安全防护设备，应对来自互联网的主流 WEB 应用安全攻击。
- 定期进行专业的安全评估，及时掌握信息系统的安全状况。
- 完善安全管理制度体系，对信息系统的日常维护和使用进行规范。
- 建立一套完善有效的应急响应预案和流程，并定期进行应急演练，一旦发现发生任何异常状况可及时进行处理和恢复，有效避免系统业务中断带来的损失。
- 定期对相关管理人员和技术人员进行安全培训，提高安全技术能力和实际操作能力。
- 对于 0day 等未被发现的问题，可采用 APT 高级可持续性攻击预警平台和网络安全保险等控制措施；对于不可预知的变化，可采取持续性态势感知监测技术，动态风险评估以及安全可信众测等措施加以防范。



扫码获取更多资料

与安全专家一对一交流

帆软数据应用研究院 发布