基于 Web 的信息平台数据安全风险及对策研究

Research on Data Security Risks and Countermeasures of Information Platform Based on Web

王利强

Liqiang Wang

中国煤炭地质总局一二九勘探队　中国·河北 邯郸 056004

No. 129 Exploration Team, CNACG, Handan, Hebei, 056004, China

摘　要：论文针对基于 Web 的信息平台数据安全问题，对数据安全现状进行了阐述。论文在此基础上，分析了基于 Web 信息系统中常见的数据安全风险和隐患，并对各类风险隐患的防范和对策进行了研究和总结。最后，就下一步的研究和拓展提出了新的方向。

Abstract: This paper focuses on the data security of information platform based on Web, elaborated the status quo of data security. On this basis, this paper analyzes the common data security risks and hidden dangers in Web based information systems, in addition, the prevention and countermeasures against various potential risks were studied and summarized. Finally, new directions are proposed for further research and expansion.

关键词：Web；信息平台；数据安全

Keywords: Web; information platform; data security

DOI: 10.12346/csai.v1i2.7126

1 引言

随着信息技术的飞速发展，数据管理也完成了由传统模式向数字化方式的转变。通过开发管理信息系统实现对数据的高效管理。

随着数据的信息化管理，数据的安全问题随之而来。信息系统的安全机制是否健全，对其所管理的数据安全起到了至关重要的作用。如何打造健壮的管理信息系统，确保数据安全，成了数据管理者面临的重要任务 [1]。

2 研究背景

初期的管理信息系统多以单机或局域网形式存在，其数据安全更多依赖于局部安全环境的好与坏。随着 Internet 技术的快速发展，管理信息系统开始向互联网延伸，系统架构也向 B/S 转变，称之为 Web 信息系统。

发展初期，服务器端是功能的提供者和数据的发布者，客户端只能查询无法进行更多的交互。称之为 Web 1.0 时代，数据安全问题尚不是特别突出。

随着技术的发展和带宽的快速增长，进入 Web 2.0 时代，客户端可与服务器端进行更多的功能交互；该阶段下基于 Web 的信息平台数据安全问题变得突出，对如何确保数据安全提出了挑战。论文聚焦该情形下的网络信息平台数据安全风险及对策展开研究 [2]。

3 研究意义

随着互联网发展，越来越多的管理信息系统开始部署在互联网上，以 Web 形式提供服务，短短几年时间各行各业开发建设了大量 Web 信息平台。在 Web 信息平台架构的演变过程中，不断暴露出新的漏洞和隐患，一方面使新建的系统不断自我完善，另一方面也导致已有系统不断出现新的风险点，对其管理的数据形成安全隐患。

随着《关于构建更加完善的要素市场化配置体制机制的意见》首次将数据作为一种新型生产要素，数据对于企业的

【作者简介】王利强（1979-），男，中国河北邢台人，硕士，高级工程师，从事信息技术与地质、测绘技术相结合研究。

地位和作用上升到了一个新层次；《数据安全法》《个人信息保护法》等相继施行，数据安全迈入有法可依的时代。因此，对 Web 信息系统的安全风险和对策进行研究，对于保障信息系统数据安全有重要意义 [3]。

4 数据安全现状

在调查中发现，Web 信息平台数据安全现状不容乐观，一部分存在轻微安全隐患，一部分存在明显安全漏洞，更有的几乎无任何安全防范，数据暴露对数据安全形成严重风险。

据美国威瑞森通信公司发布的《2021 年数据泄露调查报告》，Web 应用攻击导致了全年 39% 的数据泄露事件，而其中 85% 的数据泄露涉及人为因素。据国内某专业数据安全公司发布的《2020 上半年中国互联网安全报告》显示，仅上半年针对 Web 应用的恶意攻击和数据泄露同比激增超过 800%。

5 主要风险分类及对策

基于 Web 的信息系统影响其数据安全主要有以下几个方面，按风险所处的层级由外及内进行分类并给出防范对策（见表 1）。

表 1 主要风险层级

风险层级	防线	主要后果
网络层	第 1 道	网络漏洞被攻击者侵入网络，丢失网络控制权
系统层	第 2 道	服务器操作系统被攻击者侵入，丢失系统控制权限
应用层	第 3 道	业务系统被攻击者侵入，导致数据暴露
管理层	最后防线	日常管理缺位，数据无备份，无法挽回损失

5.1 网络层的安全风险

基于 Web 的信息系统其特点就是基于网络提供数据服务，系统所处的网络层是否安全，是整个系统数据安全的基础，通常采用以下方式部署：

5.1.1 自建服务器部署

该方式下首先要确保机房网络物理安全，包括防火、用电、防雷击安全，也要考虑地震等不可抗力对网络的冲击。其次要保障网络设备的运行安全，对设备参数进行正确配置，包括修改默认管理账号及密码，正确配置路由、端口封闭等，防止网络非法侵入；配备防火墙系统，采用高可用性、高稳定性的硬件设备；进行双机多冗余的设计模式，对关键网络设备采取同型号备件等。

5.1.2 云服务器部署

随着云计算技术的日趋成熟，云服务器凭借稳定性好、维护简单等特点，成为越来越多 Web 信息系统部署方式。

该方式下省去了对机房、网络等管理工作，可更多关注系统和业务应用。但这并非可以完全忽略安全工作。除了要选择稳定性好的云主机外，要把重心放在云主机所处网络的稳定性上，及时排查是否遭受 Ddos 攻击，第一时间屏蔽非法 IP 等，确保系统的稳健运行和存活。

5.2 系统层的安全风险

基于 Web 的信息系统由一台或多台服务器组成，服务器操作系统的安全对于信息系统的数据安全有至关重要作用，成为网络层安全屏障后的第二防线。服务器操作系统多为 Linux 或 Windows 系统，都是面向大众开放的操作系统，其架构功能已被大家所熟知、存在的漏洞也是公开信息，这为防范好系统层安全风险提出了严峻的考验。要做到以下几个方面：

5.2.1 对服务器操作系统进行正确安装和配置

服务器端操作系统首先要选用正规安装包，确保系统功能完整的同时避免不合法程序和后门，造成系统安全风险。其次要进行参数配置，包括修改管理员账号及具有复杂度的密码，删除或者禁用不必要的账号，关闭一切不必要的系统服务，设置正确的系统安全策略等，使系统处于最小限度的对外开放，提升操作系统的安全度。

5.2.2 对服务器操作系统进行及时更新

在系统的日常管理中，当操作系统出现更新包时要及时进行更新。尤其是官方发布的安全补丁要第一时间更新处理，防止由于公开漏洞未及时封堵，造成的操作系统级暴露。在实践中此类情况造成的安全隐患和数据泄露占了很大的比例，应引起足够重视。

5.2.3 对系统采用的中间件及时更新

对系统中涉及的中间件要及时版本更新，特别是有安全漏洞时要第一时间堵塞，必要时对中间件进行禁用。

5.2.4 对服务器防火墙进行有效配置

对操作系统进行配置中，开启防火墙并进行有效配置是确保服务器操作系统安全的一项重要工作。封闭一切不必要端口，修改敏感端口默认值，设置出入站访问规则等，从入口上确保访问合法。

5.3 应用层的安全风险

在网络层和系统层之后，应用层的安全防范机制成为第三道防线；应用层是信息系统直接对数据进行操作的层级，对数据的操作是否安全是最为关键的一道防线。依据 Web 信息系统采用的技术路线和依赖开发框架的成熟度不同，导致不同系统都有不同的风险点。具有共性的风险点主要有：

5.3.1 SQL 注入攻击

SQL 注入是 Web 信息系统中最常见的一种安全隐患，也是攻击者最先测试的安全漏洞点。其原理是在表单中输入

特殊的 SQL 字符串欺骗服务器，成为在服务器端能够执行的恶意 SQL 命令，对数据造成危害。为防止该风险，首先在后台程序尽可能减少直接 SQL 语句操作，同时对前端提交参数的类型、格式进行严格检查，对特殊字符进行过滤，确保参数是安全、可靠的。

5.3.2 文件上传漏洞攻击

在 Web 信息系统中，一项常见的功能是允许用户将本地文件上传到服务器。当攻击者将恶意文件上传至服务器后，形成一个提供内应的“特洛伊木马”，为进一步获取系统更大权限提供了可能性和便利性。该类风险是最常见的 Web 信息系统风险漏洞之一，也是攻击者最常用的手段。

为防止该风险，首先要对上传文件的类型进行控制，除对 exe/com/bat 等可执行文件拒绝上传外，还要对 asp/php/js 等脚论文件进行格式深度校验，防止伪文件后缀方式漏洞，从源头控制非法文件入侵；其次要在服务器端对 Web 信息系统的目录权限进行合理配置，按照“有运行权限的目录不允许上传、有上传权限的目录不允许运行”标准，对系统文件和上传文件进行隔离，这样即便恶意文件上传到了服务器也不能被执行。

5.3.3 数据明文传输风险

多数 Web 信息系统采用了 http 模式传输，该模式下所有的数据传输均是以明码方式进行传递。因此导致了数据在传输过程中可能被截获、分析、窃取的风险。为防止该风险，可将系统升级采用 https 模式，该模式下前台和后端所有的数据均是加密传输，可有效防范数据在传输过程中被窃取的风险。

5.3.4 Cookies 伪造

由于 http 请求是无状态化的协议，在 Web 信息系统中通常采用 Cookie 方式进行状态管理。如攻击者恶意截取或修改浏览器端 Cookie 值，将会对后台产生欺骗，从而导致信息系统的风险和漏洞。

为防止该风险，在后台生成 Cookie 值时除了实际数值外，要融合私钥和变量参数进行加密处理，并附带校验码共同组成 Cookie 值；在接收 Cookie 值后首先进行反向校验，当反向校验失败时则表明该 Cookie 系伪造。

5.3.5 API 接口无认证措施

根据系统模块化的思想，越来越多的 Web 信息系统采用 API 接口方式为前端提供服务，具有模块化高、耦合度低、便于分布式应用等优点。但开放的 API 接口也为数据安全带来了风险隐患。当 API 接口无安全认证措施时，将会出现任何人都可以调用接口获取数据的风险，因此必须对 API 接口的调用者进行身份鉴别，确保为合法调用。

在实现中，可通过公钥、私钥、身份 ID 共同生成调用接口的 token 令牌，调用者持有该 token 在一定时间内合法调用接口的机制；对于非面向公共开放的 API 接口，可对调用者的来源 IP 进行黑白名单控制，确保 API 接口的合法调用。

5.3.6 XSS 跨站脚本攻击

XSS 跨站脚本攻击是指在 Web 信息系统页面中插入并运行非法脚本进行攻击的一种方法，达到获取用户信息和数据的非法目的。

为防止该风险，首先是启用 Cookie 的 HttpOnly 属性，避免 cookie 被客户端的 js 非法获取；其次是对输入内容进行非法字符过滤、关键字转义存储；最后是通过设置 Header 中的 CSP 属性限制允许加载的资源种类和来源，使恶意脚本即便插入页面，也无法正确运行。

5.3.7 关键数据明码存储导致泄露风险

Web 信息系统数据常通过数据库存储，当攻击者越过网络防线、系统防线并成功获取数据库权限后，如果关键数据进行明码存储则数据将完全暴露在攻击者面前，可随意查看、篡改、删除数据，所谓数据安全将不复存在。

为避免该风险应对关键数据在数据库中进行加密存储，这样即便攻击者成功获取了数据库权限，看到的也是经过加密后的数据，可在一定程度上防止数据泄密和损失扩大。

5.3.8 用户身份认证防范形同虚设

Web 信息系统登录是对来访问者身份确认的入口，也成为攻击者的第一攻击目标。一些信息系统中身份认证机制形同虚设，攻击者可轻松绕过或者虚假认证，常见的如允许弱密码给攻击者密码猜测留下机会等，给系统安全造成隐患。

为避免该风险，信息系统应强化身份认证机制，包括对密码强度、复杂度、定期修改密码要求等；要强化验证码作用，可辅助手机短信验证，防止密码暴力破解；对于信息安全度要求高的可采用 U-Key 身份认证，确保来访者的身份合法。

除上述常见 Web 信息系统安全漏洞外，还有许多其他常见漏洞，比如 CSRF 跨站请求伪造、Host 头攻击、反序列化漏洞等，鉴于篇幅不再赘述。

总之，Web 信息系统在建设过程中，对于安全风险的重视是系统和数据安全至关重要的一环。须通过开发质量控制、上线安全验收、上线运营跟踪等多维度入手，全面强化 Web 信息系统自身应对风险能力和数据安全保护能力。

5.4 管理层的安全风险

在风险源中管理层的风险往往是最容易被忽视的，而该风险恰恰是贯穿于信息系统全生命周期影响最长的。常见的

风险点有以下几种：

5.4.1 管理机制不健全

未明确系统管理部门和责任人，形成了信息系统“重建设、轻管理”的局面。要明确责任人，不仅要对系统建设好、更要在系统上线后做好日常监测、安全风险评估工作。

5.4.2 应急预案不健全

多数信息系统未制订当出现系统故障、数据破坏或泄露时的应急预案，导致紧急情况下不能第一时间将损失降至最低。在系统上线之初要进行安保等级评估并制订出应急预案。

5.4.3 系统数据备份措施不到位

信息技术在不断发展，没有绝对安全的系统，也没有绝对安全的数据。要保障信息系统的数据安全，数据的备份就至关重要，也成为当系统故障、数据损失后进行补救的最后一道防线。除做好数据的日常备份外，根据数据敏感程度要进行异地灾备或实时双机热备，以便在系统出现故障和数据损失后进行快速恢复。

综上所述，Web 信息系统数据安全，是一个全方位的概念，需要从不同层面、不同角度全面加强风险防范和管理，才能确保 Web 信息系统的数据安全。

6 结语

论文分析了基于 Web 信息系统中常见的数据安全风险并提出了应对策略，主要是基于已知风险和漏洞隐患的基础上展开的。系统开发和安全攻击技术都在不断发展，面对层出不穷的操作系统安全漏洞和不断翻新的攻击手段，在可扩展性、预防性上存在一定的不足。通过对系统数据的智能化分析，结合数据算法对系统安全风险的态势感知、数据安全的主动防御开展进一步研究，对于保障 Web 信息系统数据安全将具有更深远的意义。

参考文献

[1] 李铀.基于WEB信息系统的安全架构研究[J].计算机光盘软件与应用,2014,17(5):2.

[2] 林世鑫.基于SQL注入的Web数据安全防范与优化[J].电脑知识与技术:学术版,2014(4):4.

[3] 武宝珠,李小玲.探讨云计算环境的web应用数据安全[J].电脑知识与技术:学术版,2018,14(5):3.