基于 Web 渗透测试的信息泄露防御方法研究

文◆大庆油田有限责任公司勘探开发研究院应用软件研究室　王垠楠

引言

在信息安全越来越受到重视的情况下，各单位信息安全管理日趋完善，网络攻击逐渐转向隐蔽化。为提高 Web 信息系统的安全性，依据在实战化攻防演练中的经验，归纳常见信息泄露问题，如明文流量、应用指纹泄露、系统不当反馈信息等，基于案例分析简述信息利用的方法步骤及其所带来的安全隐患危害，提出对信息进行加密、混淆、过滤等相应的解决思路，设计应用安全架构并加以验证，再从软件设计、编码开发、项目运维等方面，总结 Web 软件项目全生命周期的信息泄露防御方法。

1 研究背景

信息安全是信息化建设的基础，数据一旦丢失、损坏或泄露，会对企业造成巨大损失。经过多次网络攻防演习，企业已有了相对完善的安全管理制度。在技术手段方面，着重边界防护。边界防护手段是以网络为中心的建设方式和理念，在边界部署多个设备（如全流量设备、防火墙、WAF 等），具备应对大部分主动式攻击的能力，然而对更加隐蔽或者被动监听式的攻击难以防范 [1]。由于安全设备多数是基于已知攻击特征进行防护，存在大量误报以及加密信息，对于此类异常信息需要专业人员进行分析研判 [2]，难度较高。如果攻击者利用“零日（0day）”漏洞攻击，将更加难以发现。基于“零日（0day）”漏洞攻击具有较高的有效性，以最大程度检验防守方防护体系的完善性以及防守能力 [3]。据谷歌 Project Zero 团队统计，2021 年未受控而被利用的“零日（0day）”漏洞有 58 个，此前最大值为 2015 年的 28 个。依据 PTES 渗透测试执行标准以及实战经验，在确定目标范围后，在进行此类相对隐蔽攻击时首先进行信息情报的收集工作。同时，信息的泄露情况无法通过扫描设备掌握，信息泄露的问题亟须重视处理。

2 渗透分析

在已授权环境下，总结信息泄露方面的渗透攻击。攻击过程中发现信息泄露问题普遍存在，通过收集到的情报信息进行威胁建模、漏洞分析，随后开始攻击达成渗透目的，其中 20% 的泄露信息可以利用，可造成严重危害的高危漏洞占 2%。危害性取决于泄露的具体信息，高危漏洞造成危害如下。（1）网页内容篡改，发布违规内容或者挂马。（2）数据库内容泄露，包含企业内部资料和大量个人信息。同时，删除数据造成各系统瘫痪、数据丢失。（3）控制服务器，渗透至内网，攻击单位内部其他计算机或服务器，进行更大规模横向渗透。

2.1 调试信息泄露

经多角度渗透测试，主站防御性较好，对于一般的网络攻击有着良好的防护能力。然而，根据信息安全木桶原理，应寻找其他薄弱环节，以旁站子系统作为入侵起点，通过 SQL 注入漏洞越过 DMZ 区服务器的防护，深入控制企业一台云中心数据库，进而以此为跳板在企业云中心以及办公网内部进行大规模横向渗透。因此，企业在加强主站防御的同时，还应重视对旁站子系统等薄弱环节的安全管理。对于系统管理员和开发者来说，确保不泄露敏感信息、及时修复已知漏洞是保障系统安全的重要一环。

2.2 应用指纹分析

通过 Wappalyzer、爬虫类分析工具、默认图标、错误页等获取平台

【作者简介】王垠楠（1989—），男，黑龙江哈尔滨人，本科，中级工程师，研究方向：网络安全、软件开发。

开发商、软件名称、版本、服务类型等信息，有助于了解目标平台的技术架构和特性。例如，某次渗透测试通过错误页获取一信息系统的框架为 V5.0.23 版本的 ThinkPHP，针对性利用版本漏洞，编写木马程序，并使用免杀处理，获取服务器控制权。

2.3 网络流量分析

攻击者采取隐秘的手段获取目标系统的流量信息，包括但不限于中间人攻击或其他高级技术手段。在不被目标系统防火墙规则检测到的情况下，被动地监听网络通信，窃取传输中的敏感数据。在监测过程中，攻击者发现一些系统漏洞，例如，某系统中存在的明文弱口令问题，为攻击者提供了直接登录并利用系统的机会。

2.4 代码信息泄露

在网络安全领域，代码审计是一项重要任务。通过对代码进行细致分析，可以获取许多有用信息，有助于更好地了解系统的运作方式和潜在的安全风险。例如，在某次渗透测试过程中，查看前台 JavaScript 代码时，发现一些隐藏的注册接口，这些接口未被官方文档提及，或者是通过某些特殊手段实现访问目的。一旦攻击者找到了这些接口，就等于找到了一个潜在的突破口，最终在取得未授权的情况下，攻击者能够在该网址获得任意用户注册权限，从而进行非法登录。

3 防控措施

由于信息泄露危害之严重、影响之广大，在程序开发和使用方面应该越来越谨慎。在程序安全加固方面，根据以上渗透测试完成的报告，应做到以下针对性的修复，总体归纳为以下 4 个方面。

3.1 开发规范化

（1）简化输出信息。编写程序时将错误反馈信息最小化，避免服务器泄露信息。（2）过滤非法字符。在不影响业务情况下，对高危字符采取转义过滤等手段。（3）删除冗余代码。编写程序时删除冗余代码，避免 JavaScript 信息泄露。（4）合理使用加密手段，兼顾业务的性能与安全，如在关键数据中使用国密、RSA 算法。（5）合理设计软件。包括权限控制、内部通信等，防止内部 IP 地址、Email 等信息泄露，遵循安全设计原则指导开发工作。

3.2 运维规范化

首先，对最小化信息系统的攻击面，关闭非必要服务、协议，根据业务需求配置黑、白名单，保证访问来源安全，同时规避网络空间测绘系统扫描。其次，合理优化配置，包含容器、组件、平台等，如 IIS、Tomcat、Druid、PhpMyAdmin，选择隐藏或者伪装类型、版本，审查并修改默认配置，防止目录遍历、后台路径信息泄露等情况发生。最后，完善管理制度，并严格执行，注意删除隐藏的临时文件，防止 GIT 信息、.bak 文件泄露下载等情况发生。

3.3 服务持久化

为了全面提升企业的信息安全防护能力，必须持续加强对信息安全的审查与台帐管理。时刻保持警惕，确保每一项服务、系统、设备都处于受控状态，杜绝任何未受控元素的出现。在信息安全审查与台帐管理的基础上，还要及时修补组件、平台等存在的漏洞，如 Flash 漏洞、泛微漏洞、Fastjson 漏洞、ThinkPHP 漏洞等。漏洞是信息安全的隐患，一旦被恶意利用，将给企业带来不可估量的损失。因此，要密切关注最新的安全动态，定期扫描和评估系统的安全性，发现漏洞后及时制定修补方案并实施。

3.4 安全架构部署

对应用软件进行安全功能研发、升级，安全架构探讨的网络环境情况主要包含 DMZ 区和内网办公区 [4]。在 DMZ 区设计使用数据传输控制服务，基于 Gateway 进行二次开发，主要功能包含身份认证、权限控制、企业微信集成、业务数据分类请求、日志统计等，基于安全引擎设置了多重服务器安全策略，建立应用防护系统进一步控制访问接口，具体如下。

（1）设置服务器黑白名单。限制 DMZ 区内部其他无业务往来的服务器访问，防止横向渗透，严格限制服务器开放的端口，仅供有需求的业务使用。（2）用户管理。严格控制用户授权，通过集成 SSO 认证方式等访问业务流程，从多维度限制用户使用系统功能、资源访问权限。（3）安全管理。系统管理员通过内网管理，仅可利用特定端口、特定 IP 才能远程操作设备。（4）防护引擎。1）限制 DMZ 服务对内网访问的对象，仅能访问负载入口 API 服务端口。2）限制访问频率上限，目前设置为 500 次 / 分钟，防御 DDOS 攻击、扫描行为等。3）限制接口访问白名单，仅允许有外部访问权限的办公流程接口，详情如 /api/**、/

blog/js/**、/css/**、/docs/** 等。4）扩展软 WAF 应用防火墙，限制关键字黑名单，包含 SQL 注入、目录穿越、历史版本 CVE 漏洞路径等，用以防范零日漏洞，如 ./、../、%27、' 等。

4 应用效果

4.1 调试信息防护

当遇到某些特定情况时，服务会返回错误信息，暴露系统的潜在漏洞，为攻击者提供了可乘之机。经过优化和改进，服务已经不再返回错误信息，而是改为返回无查询结果的 Json 格式数据。不仅提升了用户体验，还增强了系统的安全性。避免直接暴露错误信息，有效减少了攻击者获取系统敏感信息的可能性。同时，为了进一步提升系统的安全防护能力，加入了过滤非法字符的 WAF（Web 应用防火墙）。WAF 作为一道重要的安全屏障，能够实时检测和拦截恶意请求，过滤其中的非法字符和攻击代码，有效防止 SQL 注入、跨站脚本攻击等常见安全威胁。需要指出的是，仅仅采取最小化错误信息这一措施远远不够，如果不使用 WAF，那么系统仍然面临着布尔盲注和时间盲注等攻击的可能性。攻击方式虽然隐蔽，但同样能够对系统造成严重危害。因此，必须综合运用多种安全手段，构建多层次的安全防护体系，才能确保系统的安全稳定运行。

4.2 应用指纹防护

为了确保系统的安全性，修改容器配置文件成为一项至关重要的任务。调整配置文件不仅能够优化容器的性能，还能够增加防御能力，有效抵御潜在的网络攻击。在这个过程中，加入混淆的错误信息，以迷惑入侵的恶意用户。核心思想在于故意制造误导性的错误信息，使入侵者在分析系统时产生误判；修改容器的响应机制，使入侵者在接受请求时，返回伪造的错误信息。这些错误信息看起来如同是来自另一种完全不同的服务或软件，实际上却是为攻击者设计的陷阱。例如，将 IIS 容器伪装成 Apache 容器，当入侵者尝试探测或攻击 IIS 容器时，入侵者接收到的错误信息会让他们误以为正在面对的是一个 Apache 服务器[5]。这种伪装不仅让入侵者难以判断容器的真实身份，还会导致他们使用错误的攻击策略，有利于降低攻击的成功率，提高容器的安全性，为系统构筑一道坚固的防线。

4.3 流量监听防护

加密流量在当今数字化时代显得尤为重要，不仅是保护数据安全的关键手段，还是维护企业或个人隐私的重要防线。在考虑密钥安全性问题的背景下，数据上传过程中采用 RSA 非对称加密技术，确保信息的机密性和完整性。RSA 非对称加密技术是一种广泛应用的加密方法，其特点在于使用一对密钥进行加密和解密操作。即使监听者截获了密文，由于没有相应的私钥，监听者也无法解密出原始数据，从而保证了数据的机密性。此外，同属的非对称加密还有国密 SM2 算法等，有较高的安全性，能够有效抵御各种攻击手段，确保数据的完整性和真实性。

结语

信息安全是信息系统运作的重要组成部分，在网络攻击逐渐趋于隐蔽化的时代，做好信息安全的防护愈发重要。因此，分析在攻防演练中取得的成果，完成了企业安全防护等级的提升。以信息泄露问题为出发点，在应用技术上的加固之外，得出以下 3 点认识。首先，完善信息安全制度，建立开发与运维的安全管理规范，以及信息安全审查、软件安全测试机制。相比传统测试方法，模糊测试（Fuzz）、渗透测试能够在有限测试点内有效发掘高危风险。其次，注重信息安全培训，软件开发与运维过程中需要注重信息安全，了解相关风险。最后，信息安全需要持久化，并非一次性投入，其贯穿整个软件的生命周期，从确定需求、设计、编码、测试、供应链交付、部署、运维直至销毁下线，都需要信息安全的保障，需要持续关注并加以完善。

引用

[1] 刘璐.央企移动应用安全防护研究[D].北京:北京邮电大学,2021.

[2] 李东,蔡良飞.攻防演练中网络安全监测研究[J].信息安全研究,2021,7(7):669-673.

[3] 李沁蕾,樊旭东,闫海林,等.银行系统0day漏洞挖掘与分析方法研究[J].中国金融电脑,2020(10):67-72.

[4] 王春伟.油田工控系统信息安全体系构建分析[J].办公自动化,2023,28(9):7-9.

[5] 何源,邢长友,张国敏,等.面向网络侦察欺骗的差分隐私指纹混淆机制[J].计算机科学,2022,49(11):351-359.