高等职业教育专科、本科计算机类专业新形态一体化教材
高等职业教育信息安全专业系列教材

Web 基础渗透与防护（第 2 版）

王德鹏　谭方勇　张月红　主　编
刘　刚　张洪璇　副主编

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书介绍了 Web 中高危漏洞的形成原理、利用方法、加固和防御方法。全书共 11 个项目，项目一和项目二为 Web 信息安全基础知识与法律法规，主要论述了当前的信息安全状况、存在的问题。项目三～项目十主要介绍了命令注入、文件上传、SQL 注入、SQL 盲注、暴力破解、文件包含、XSS、CSRF 攻击与防御等漏洞原理、利用方法与针对性加固方法。项目十一为代码审计，主要分析了代码审计的必要性、代码审计的方法，以及代码审计的案例。

本书既可以作为高等职业院校计算机网络与信息安全等相关专业的教材，也可以作为信息安全从业人员的学习指导用书。

图书在版编目（CIP）数据

Web 基础渗透与防护 / 王德鹏, 谭方勇, 张月红主编. 2 版. -- 北京 : 电子工业出版社, 2025. 4. -- ISBN 978-7-121-50185-2

Ⅰ. TP393.08

中国国家版本馆 CIP 数据核字第 2025C32Z90 号

责任编辑：李　静
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　　印张：18.5　字数：474 千字
版　　次：2019 年 8 月第 1 版
　　2025 年 4 月第 2 版
印　　次：2025 年 4 月第 1 次印刷
定　　价：55.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254604，lijing@phei.com.cn。

前　言

党的二十大报告中指出，推动战略性新兴产业融合集群发展，构建新一代信息技术、人工智能、生物技术、新能源、新材料、高端装备、绿色环保等一批新的增长引擎。

为贯彻落实党的二十大精神，以培养高素质技能人才助推产业和技术发展，建设现代化产业体系，编者依据新一代信息技术领域的岗位需求和院校专业人才目标编写了本书。

“没有网络安全就没有国家安全，没有信息化就没有现代化。”我国在过去的十年间见证了信息化领域的迅猛发展，这一进程深刻影响并改变了民众生活的方方面面。然而，随着信息化的全面发展，网络安全问题也日益成为不容忽视的重大挑战。其中，Web 信息安全领域作为网络安全——乃至国家网络空间安全战略的核心构成之一，不仅成了网络防御的前沿阵地，还是与广大用户日常互动最为频繁的安全领域。

为了有效提升公众的网络安全意识，普及网络安全知识教育显得尤为迫切。网络安全是一个复杂而庞大的生态系统，它涵盖了通信设备、安全设备、服务器设施以及各类应用软件等多个维度的技术与知识。对于普通民众而言，Web 信息安全因其直接关联网络应用层面，因而与每个人的日常生活紧密相连，影响深远。

对于 Web 渗透测试工程师，深入掌握 Web 安全漏洞的原理、攻击手段以及相应的安全加固措施，是其专业技能体系中不可或缺的一环。在这个信息化高速发展的时代，Web 应用作为互联网服务的核心载体，其安全性直接关系到国家安全、企业利益乃至个人隐私的保护。因此，深入理解 Web 安全的每一个细节，不仅是职业发展的硬性要求，更是守护数字世界安宁的重要使命。

本书采用最容易让学习者理解的方式，通过场景化的项目案例将理论与技术应用密切结合，让技术应用更具画面感，通过标准化业务实施流程熟悉工作过程，通过项目拓展（实训任务）进一步巩固业务能力，促进学习者养成规范的职业行为。全书通过 8 个精心设计的项目案例，让学习者逐步地掌握 Web 漏洞原理、测试方法、加固方法，成为一名准 Web 渗透测试工程师。

本书鲜明的职业导向特色体现在以下几个方面。

一、课证岗深度融通，校企合作

本书携手深信服、天创等多家知名企业，深度融合其 Web 渗透测试工程师的课题体系与实战案例。通过校企合作开发，不仅确保了教学内容的前沿性和实用性，还实现了课程与职业资格认证、实际工作岗位需求的无缝对接，本书为学习者铺设了一条从理论到实践的快速通道。

二、项目驱动学习，课产深度融合实践

本书采用项目贯穿始终的教学方式，每个章节或模块均围绕 Web 渗透测试工程师岗位的实际工作场景设计。通过模拟真实项目，将理论知识与产业实践紧密结合，使学习者在解决实际问题的过程中，逐步掌握 Web 渗透测试的核心技能，实现学习与工作的无缝对接。

三、实训项目具有复合性和延续性

考虑企业真实工作项目的复合性，编者精心设计了实训项目。实训项目不仅考核与本项目相关的知识、技能和业务流程，还涉及前序知识与技能，强化了各阶段知识点、技能点之间的关联，让学生熟悉知识与技能在实际场景中的应用。

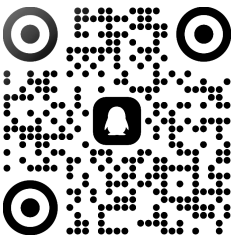
编者根据多年从事网络安全专业教学的经验，以及多年参与高等职业院校技能大赛信息安全管理与评估赛项的技术积累，采纳一线信息安全专家的建议，完成了本书的编写工作。本书在编写过程中得到了江苏天创科技有限公司的大力支持，该公司主要从事网络安全方面的工作，与苏州市政府具有广泛的合作。编者以该公司丰富的实战案例为依据，编写了本书。

本书由苏州市职业大学的王德鹏、谭方勇、张月红任主编，苏州市职业大学刘刚、江苏天创科技有限公司张洪璇任副主编。

由于水平有限，书中难免存在疏漏和不妥之处，敬请读者批评指正。

编　　者

2025 年 2 月



教材资源服务交流 QQ 群

（QQ 群号：684198104）

目　录

项目一　认识 Web 安全基础

1.1　当前 Web 安全形势

Web 安全的概念与内涵是随着时间推移而有所不同的。在早期互联网中，Web 并非互联网的主流应用，网络安全主要作用于网络、操作系统及软件等领域，Web 安全领域的攻击与防御技术均处于非常原始的阶段。但随着互联网技术的不断发展，Web 应用逐渐成为主流，Web 安全也日益受到重视。具体来说，Web 安全的发展历程可以分为以下几个阶段。

1. 初始阶段

在早期互联网中，Web 安全并未受到足够的重视。此时，黑客们主要关注系统软件的安全漏洞，通过攻击系统软件来获取系统权限。当时涌现出了许多经典漏洞以及漏洞利用代码（exploit），例如，著名的黑客组织 TESO 曾编写过一个攻击 SSH 的 exploit，并宣称利用该 exploit 入侵过美国中央情报局（cia.gov）。此时的 Web 安全还处于非常原始的阶段，攻击与防御技术都相对简单。

2. 防火墙与 ACL 技术兴起

随着 Web 技术的成熟和 Web 应用功能的增强，Web 应用逐渐成为互联网的主流。黑客们的目光也渐渐转移到了 Web 上，Web 安全问题开始成为焦点。Web 安全最早可追溯到互联网诞生，彼时还是一个黑客备受尊敬和崇拜的时代。但由于 Web 业务所蕴含的信息量越来越大，价值越来越高，架设在 Web 平台上的 Web 业务不仅成了黑客们练手的训练场馆，也因为巨大的现实利益而沦为“黑产”中的“庄稼地”，网络不法分子利用各种漏洞获得控制权，轻则留下“到此一游”的记号，重则一茬一茬地进行“收割”，将 Web 供应商保存的机密敏感信息、数据层层洗劫。而且最恐怖的是大规模的恶意攻击，比如发生在 2003 年的冲击波蠕虫事件，这个针对 Windows 操作系统 RPC 服务的蠕虫在短时间内席卷了全球，造成了巨大的损失。此次事件后，网络运营商们开始在骨干网络上屏蔽相关端口的连接请求，整个互联网对于安全的重视达到了一个空前的高度。

Web 应用防火墙（WAF）的诞生在一定程度上缓解了 Web 安全防护岌岌可危的堡垒，但这种从一开始就建立在规则匹配的亡羊补牢式防护，在很多情况下只是无济于事。所以，初代 Web 防护形象地说就是建了一道形同马其诺防线的“墙”，“墙”是死的而黑客是活的，很容易被绕过，这也意味着“墙”时代的传统 WAF 产品已经无法满足当前复杂的 Web 环境。

3. Web 安全“智”时代破釜沉舟的选择

在 Web 1.0 时代，人们更多关注服务器端动态脚本的安全问题，如将可执行脚本（俗称 webshell）上传到服务器上获取权限。SQL 注入的出现是 Web 安全史上的一个里程碑，它使得黑客可以通过注入 SQL 语句来获取敏感数据或系统权限。随着 Ajax、XML、RSS 等技术的普及，以及 jQuery、Bootstrap、React 等前端框架和库的出现，Web 攻击技术也变得更加多样化，常规的安全设备已经无法满足复杂的安全要求。

业内对 NGWAF 的呼唤由来已久，业内公认的研究方向集中在语义分析技术、机器学习技术和自学习技术上。机器学习技术和自学习技术是浅层面上的识别和基于概率控制的，相对而言较为容易实现。而语义分析技术相较于机器学习技术、自学习技术而言是一个深度挖掘的过程，类似于人类认知、思考、判断的行为，自然也最难实现，毕竟在人工智能的终极问题没有解决之前，这一领域的最高成就依旧停留在大数据层面。

但长亭科技这家初创公司从开发 WAF 产品之始就是冲着 NGWAF 中最难落地的语义分析技术而去的，显然抱着“不成功便成仁”的心态和“破釜沉舟”的勇气，当然最重要的还是这群年轻人的群体智慧。经过潜心研究后，人工智能语义分析引擎 Demo 诞生。该引擎在 2015 年被带入世界安全峰会 Black Hat USA 的舞台，其研究成果“新型 SQL 注入检测与防御引擎 SQLChop”被纳入军械库展示，这个针对黑客攻击实现智能识别和拦截的创新点与实际效果得到全球安全专家的一致认可。2016 年 7 月，长亭科技基于该技术的 NGWAF 产品——雷池（SafeLine）正式推出，相当于在平静多年的 Web 安全领域投下了一颗石子，自然一石激起千层浪，以实力获得全球顶级安全赛事、峰会、评审的青睐和赞誉。雷池多次被 Gartner《Web 应用防火墙魔力象限》提名，并入围 Gartner 2018 年《Web 应用防火墙魔力象限报告亚太版》、Forrester *Now Tech: Web Application Firewalls, Q4 2019* 等报告，获得众多行业及客户的认可。

4. Web 安全“云”时代创新能力的对决

这依然不是 Web 安全防护的最终形态，与其说 2018 年之前的长亭雷池是智能动态防御技术的顶尖代表，那么 2018 年 RSA 上宣布升级的雷池则将“云”时代的“智能”落地到了更深的层次。

在企业对“云服务”接受程度不断提升的今天，如何从根本上避免云 WAF 存在轻易被绕过的风险，解决其可靠性低和保密性低的弊端，是业界长期以来的难题。长亭科技在雷池（SafeLine）智能语义分析技术的基础之上升级云端部署解决方案，不改变原有网络结构，实现了软件层面的灵活拓展。

雷池相比其他云 WAF 的优势在于：一方面，雷池的 WAF 服务器部署在企业私有云，与 WebServer 处于相同 VPC 中不需要通过将用户的流量解析到云节点来实现防护，不存在强制解析域名问题；另一方面，处理过程只需一个环节，不需要过多的环节协同工作，最大限度地避免了问题。并且，雷池云端部署非第三方云服务，数据处理转发完全在企业私

有云内部，保密性自然毋庸置疑。此外，雷池围绕不同类型用户业务类型而匹配的动态化、个性化、定制化模块和衍生服务始终遵循一种“化繁为简”的科技理念。

显然，在 Web 安全“云”时代，这种技术创新能力的对决也纵深化到了事无巨细的层面。以金融行业为例，目前主要面临数据泄露、APT 攻击、DDos 攻击、Web 攻击等多种网络威胁，其中绝大部分攻击均指向关键服务器，以试图获取包括客户信息、机密交易数据在内的重要商业信息。还有很大一部分则是僵尸网络、“羊毛党”们的“薅羊毛”行为（当然“薅羊毛”是目前绝大多数流量网站每时每刻都会遇到的难题），单一的 WAF 产品显然与客户的业务模式很难实现产业交互，甚至传统 WAF 还会直接影响客户业务的正常运维，毕竟传统 WAF 产品的规则匹配和多环节协同加载是老大难问题。

长亭科技显然在这方面做足了功课，长亭雷池能一炮而红不仅得益于其独一无二的技术创新。越来越多的重量级客户不仅仅看重技术优势，看上的还是整个长亭科技安全团队持续性、纵深化的服务能力，譬如雷池此次升级后成为业内首个支持私有云 WAF 部署的 NGWAF 产品，譬如长亭科技基于多年的顶级国际黑客赛事的经验而推出的洞鉴（X-Ray）安全评估系统，未来预估还会有相应的安全人才培养计划，这一切结合起来其实就像哈利波特这部魔幻巨著里的魔法学校霍格沃兹一样。长亭科技将不仅仅是一家初创型信息安全企业，还是肩负重担且正努力在信息安全领域，通过技术创新实现对全球网络安全行业巨头弯道超车的企业，在网络安全上升为国家安全战略的当下，中国各行业乃至整个社会，都乐见并希望更多这样的企业相继涌现。

现在人们使用互联网时，个人的安全意识已经提高很多。大多的互联网应用为了保障客户安全，投入也越来越多，但现今 Web 安全还存在下面几个问题。

1）网络钓鱼事件激增

Webroot 调查研究发现，网络钓鱼已经取代了其他新型恶意软件，成为近年来企业最容易遭受的攻击。虽然网络钓鱼已存在多年，但曾经不在网络钓鱼攻击者目标范围内的中小企业如今已不再免疫，他们往往会被当成进入大型企业的跳板而加以攻击。

2）勒索软件问题深化

Webroot 研究发现，后 WannaCry（勒索病毒）时代，在中小企业心中的威胁排行榜上，勒索软件从第五位爬升到了第三位，而英国的中小企业更是将勒索软件列在了最易遭受的攻击类型 No.1 的位置。

对很多小公司而言，被勒索软件攻击已成了他们的“恐慌时刻”，很多情况下他们会选择支付赎金。然而，即便支付了赎金，黑客们也可能只还给他们 50%的文件，有时候甚至一份文件都不恢复。

3）内部人威胁问题依然存在

Webroot 调查显示，全球仅 25%的公司称内部人威胁依然成为问题。过去几年中大部分公司都开展了积极的教育项目，企业更小心谨慎地对待权限授予问题，让员工也更加了解来自内部的威胁。

4）新型恶意软件担忧持续

Webroot 对 3 个国家安全人员的调查表明，新型恶意软件感染仍然是安全人员比较关心的重点。在美国，担忧新型恶意软件的企业占比 37%，澳大利亚占比 34%，英国占比 32%。攻击者持续推出新型恶意软件，让安全公司忙于跟进。现在的情况显然与 5 年或 10 年前大不相同。过去，安全人员添加一个病毒特征码就能挡住一个已知恶意软件。今天，很多新型恶意软件动态改变特征码，当前威胁环境变得极为棘手。

5）培训项目并不持续

太多公司企业的培训项目没有保持连贯性。比如说，接受信用卡的公司就没跟进年度 PCI（支付卡行业数据安全标准）培训。企业要么做一遍培训就完事，要么只对 CEO 或董事团队进行培训，而将负责具体事务的员工排除在外。

Webroot 进行安全培训的方法是在每次事件发生时插入培训内容。例如，当某员工点击了恶意链接，系统就会弹出一段 2 分钟的可疑链接点击后果教育视频。在事件发生时进行培训，员工更容易记住教训，公司也避免了浪费大量工作时间搞培训。而最糟糕的培训方式，就是所谓的“照单划勾”式培训——每年搞一两次形式化的培训，没人认真对待，根本没有效果。

6）安全事件损失巨大

Webroot 和卡巴斯基的研究在安全事件的损失额度上出现了分歧。Webroot 报告称安全事件平均损失为 52.7 万美元，下降了 9%，而卡巴斯基将这个数字定在了 12 万美元。不过，卡巴斯基称，企业规模不同，安全事件所致损失数额也有较大差异，员工数在 500 人以下的中小企业遭遇安全事件的平均损失在 20 万美元，500～999 人规模的中小企业遭遇安全事件的平均损失约为 100 万美元。企业计算安全事件损失时，还必须考虑罚款、律师费、缓解工作开支和信誉损失所致的业务损失。

7）安全预算增长

卡巴斯基称，小公司往往负担不起聘请年薪 15～20 万美元的 CISO（首席信息安全官），但越来越多的小公司开始诉诸业内流行的“CISO 租赁”概念。企业可以租借 CISO 来搞培训，或者请 CISO 花费一段时间来评估他们的整体安全准备程度，然后请 CISO 定期回访查看公司安全的进展。

8）代价最高昂的安全事件发生在云提供商身上

卡巴斯基的报告显示，影响第三方托管 IT 基础设施的攻击，是中小企业面临的代价最高昂的威胁之一。中小企业平均要花费 11.8 万美元才能从此类攻击中恢复，AWS 和微软 Azure 之类的大型公有云提供商兵强马壮，而很多终端解决方案云提供商并没有把安全当成头等大事来看待。

9）技术复杂性驱动安全投资

卡巴斯基报告称，超过 1/3 的企业将 IT 基础设施复杂度的增加和提升专业安全知识的需求作为投资网络安全的动机。在边界上搭建防火墙来保护“护城河”的时代一去不复返，

今天，移动性驱动业务发展，而业务的方方面面几乎都依赖 IT。有太多的基础设施需要保护，太多的设备和应用需要锁定。于是，专精某方面安全技能的安全人员投入也就更大了，DDoS 攻击、网络钓鱼、云、IoT 等，各方面都需要相应的安全人才。

1.2　Web 安全防御技术

针对 Web 安全常见的攻击方式有 SQL 注入攻击、文件上传攻击、XSS 跨站脚本攻击、CSRF（Cross-site Request Forgery，跨站请求伪造）、程序逻辑漏洞、DDoS、暴力破解等。黑客在成功渗透到服务器后还可以进行内网攻击，某台服务器被攻陷后通过内网进行 ARP、DNS 等内网攻击。

针对 Web 安全问题的防御方法为强化口令、代码加固、网页防篡改、WAF、身份鉴别访问控制等。另外，对 Web 信息采用 Web 安全审计系统（WAS）进行安全审计，采用 Web 应用防护系统（HWAF）进行安全监控与恢复。最基本的防御原则就是永远不要相信用户提交的数据（包括 header\cookie\sessionid 文件）。

下面以几种典型的 Web 安全攻击方式进行原理解析与防御方法分析。

1. SQL 注入攻击

SQL 注入攻击见表 1-1。

表 1-1　SQL 注入攻击

	内容
漏洞原理	SQL 注入通过构建特殊的输入作为参数传入 Web 应用程序，而这些输入大都是 SQL 语法里的一些组合，通过执行 SQL 语句进而执行攻击者所要的操作，其主要原因是程序没有细致地过滤用户输入的数据，致使非法数据入侵系统
漏洞分类	（1）平台层 SQL 注入：由不安全的数据库配置或数据库平台的漏洞所致。 （2）代码层 SQL 注入：程序员对输入数据未进行细致的过滤从而执行了非法的数据查询
产生原因	（1）不妥当的类型处理。 （2）不安全的数据库。 （3）不合理的查询集处理。 （4）不妥当的错误处理。 （5）转义字符处理不合适。 （6）多个提交处理不当
防御方法	（1）对用户的输入进行校验，可以通过正则表达式，或者限制长度；对单引号和双“-”进行转换等。 （2）不要使用动态拼装 SQL，可以使用参数化的 SQL。 （3）不要使用管理员权限进行数据库连接，为每个应用使用单独的、权限有限的账号进行连接。 （4）不要把机密信息直接存放，加密或用 hash 过滤密码和敏感信息。 （5）应用的异常信息应该给出尽可能少的提示，最好使用自定义的错误信息对原始错误信息进行包装
流程建议	（1）在部署应用系统前，始终要进行安全评审。建立一个正式的安全过程，并且每次做更新时，要对所有的编码进行评审。 （2）开发队伍在正式上线前会进行很详细的安全评审，然后在几周或几个月之后他们进行一些很小的更新时，可能会跳过安全评审这关，例如，“就是一个小小的更新，我们以后再做编码评审好了”。请始终坚持进行安全评审

（续表）

	内容
编码规范	（1）Java：不允许直接根据用户输入的参数拼接 SQL 的情况出现，直接使用 PreparedStatement 进行 SQL 的查询，并且需要对输入的参数进行特殊字符的过滤。使用 Hibernate 等框架的，可以使用参数绑定等方式操作 SQL 语句。但是同样不允许直接使用拼接 SQL 语句。 （2）PHP：数据库操作，如使用框架进行处理，必须使用框架中提供的 sqlTemplate 或 paramBind、mysqli::preparesatement 等方式进行 SQL 语句的参数值注入（绑定），不要直接使用参数拼接原始 SQL 语句。不使用数据库操作类直接操作原始 SQL 语句，必须使用 Intval 对整型参数过滤，使用 mysql_real_escape_string 对字符串型进行过滤，并要配合 mysql_set_charset 设置当前字符集
测试方法	基于编码规范部分进行 CODE REVIEW，小的项目边缘业务使用自动化代码审查与安全扫描工具（如 GitHub Copilot、OpenVAS 等）进行扫描，核心业务在扫雷平台的基础上使用 sqlmap 进行安全测试扫描

2. CSRF 攻击

CSRF 攻击见表 1-2。

表 1-2　CSRF 攻击

	内容
攻击对象	应用程序的其他用户，属于客户端漏洞
漏洞原理	通过伪装成受信任用户来利用受信任的网站，伪造客户端请求的一种攻击，攻击者通过一定技巧设计网页，强迫受害者的浏览器向一个易受攻击的 Web 应用程序发送请求，最后达到攻击者指定的操作行为
漏洞危害	在受害者毫不知情的情况下以受害者名义伪造请求发送给受攻击站点，从而在并未授权的情况下执行在权限保护之下的操作，危害受害者资金信息安全
防御方法	验证 HTTP Referer 字段，存在问题：验证 Referer 值的方法，就是将安全性都依赖于第三方（浏览器）来保障，从理论上来讲，这样并不安全，因为浏览器也有漏洞，即 Referer 被篡改的情况下不可靠。对于提交的 form 表单服务器生成 CSRF TOKEN，不能使用 GET 请求更新资源，使用$_POST 请求获取 post 资源
测试方法	CODE REVIEW（代码审查），根据 Java 语言开发编码规范：对于改写数据类的提交请求，需要对请求的来源真实性进行验证。如果使用 struts 框架，可以使用框架提供的 TOKEN 机制。如未使用，可以参考其机制自行实现

3. URL 跳转

URL 跳转见表 1-3。

表 1-3　URL 跳转

	内容
攻击对象	客户端，该网站的其他用户
漏洞原理	服务器未对传入的跳转 URL 变量进行检查和控制，可能导致意外构造任意一个恶意地址，诱导用户跳转到恶意网站
漏洞危害	由于 URL 是从可信的站点跳转出去的，用户会比较信任，所以跳转漏洞一般用于钓鱼攻击，通过转到恶意网站欺骗用户输入用户名和密码盗取用户信息，或者欺骗用户进行金钱交易；也可能引发 XSS 漏洞（主要是跳转常常使用 302 跳转，即设置 http 响应头，Location:url，如果 URL 包含了 CRLF，则可能隔断了 http 响应头，使得后面部分落到了 http body 部位，从而导致 XSS 漏洞）
防御方法	（1）如果需要跳转的 URL 可以确定，可在后台配置，从客户端传入 URL 索引，服务器根据索引找到具体的 URL 再跳转。

（续表）

	内容

防御方法	（2）如果服务器生成 URL，链接生成的 URL 之后再进行签名，签名验证通过再跳转。
	（3）如果只能传入前端参数，是否符合授权白名单规则
	百度网站上的建议修复方案:
	`function checkurl($url) {`
	`if ($url != '') {`
	`$urlParse = parse_url($url);`
	`$urlHost = strval($urlParse['host']);`
	`if (!preg match("/\.baidu\.com$|\.baidu\.com\:|\.baidu\.com\.cn$|\.baidu\.com\.cn\:|\.baidu\.cn$|\.baidu\.cn\:/i", $ urlHost)) {`
	`return false;`
	`} else {`
	`return true;`
	`}`
	`} else {`
	`return false;`
	`}`
	`}`

测试方法	使用工具进行黑盒扫描

4. 路径遍历

路径遍历见表 1-4。

表 1-4　路径遍历

攻击对象	服务器
漏洞原理	Web 应用程序一般会对服务器的文件进行读取查看，大多会用到提交的参数来指明文件名，如 http://www.nuan***.com/getfile=image.jpg，当服务器处理传送过来的 image.jpg 文件名后，Web 应用程序会自动添加完整路径，如 d://site/images/image.jpg，将读取的内容返回给访问者。由于文件名可以任意更改而服务器支持“~/”“/..”等特殊符号的目录回溯，从而使攻击者越权访问或覆盖敏感数据，如网站的配置文件、系统的核心文件，这样的缺陷被命名为路径遍历漏洞，例如，恶意攻击者会利用对文件的读取权限进行跨越目录访问，访问一些受控制的文件，如“.../etc/passwd”或“.../boot.ini”，如果对用户的下载路径不进行控制，将导致路径遍历攻击，造成系统重要信息泄露，并可能对系统造成危害
防御方法	（1）数据净化，对网站用户提交的文件名进行硬编码或统一编码，对文件后缀进行白名单控制，对恶意符号（反斜线或斜线）或空字节进行拒绝。 （2）Web 应用程序可以使用 chrooted 环境进入包含访问文件的目录，或者使用“绝对路径+参数”方式来控制访问目录，即使越权跨越目录也要在指定的目录下
测试方法	路径遍历漏洞会导致恶意攻击者突破 Web 应用程序的安全控制，直接访问攻击者想要的敏感数据，包括配置文件、日志、源代码等，配合其他漏洞的综合利用，攻击者可以轻易地获取更高的权限，并且这样的漏洞也是很容易发现的，只要对 Web 应用程序的读/写功能块直接手工检测，通过返回的页面内容来判断，这是很直观的，操作起来也相对简单

5. 文件上传漏洞

文件上传漏洞见表 1-5。

表 1-5　文件上传漏洞

攻击对象	服务器
漏洞原理	由于服务器没有对用户上传的文件进行正确的处理，导致攻击者可以向某个可通过访问的目录上传恶意文件，并且该文件可以被服务器解析执行。

（续表）

攻击对象	服务器
漏洞原理	利用该漏洞产生攻击的条件：具体来说就是存放上传文件的目录要有执行脚本的权限，用户能够通过 Web 访问这个文件
漏洞危害	文件上传攻击是指攻击者利用 Web 应用对上传文件过滤不严，导致可以上传应用程序定义类型范围之外的文件到服务器上。如可以上传一个网页木马，如果存放上传文件的目录刚好有执行脚本的权限，那么攻击者就可以直接得到一个 webshell。 webshell 解释：以 asp、php、jsp 或 cgi 等网页文件形式存在的一种命令执行环境，取得对服务器某种程度上的操作权限，黑客在入侵了一个网站后，常常将这些 asp 或 php 木马后门文件放置在服务器的 Web 目录中，与正常的网页文件混在一起；然后黑客就可以用 Web 的方式，通过 asp 或 php 木马后门控制服务器，包括上传下载文件、查看数据库、执行任意程序命令等；再通过 DOS 命令或植入木马后门，通过服务器漏洞达到获取权限的目的
防御方法	（1）客户端检测：在上传页面里含有专门检测文件上传的 javascrIPt 代码，在文件被上传之前进行检测，最常见的就是检测上传文件的文件类型和规格是否合法。该方法仅仅作为辅助手段，不完全可靠。 （2）服务器检测：这类检测方法通过检查 http 包的 Content-Type 字段中的值来判断上传文件是否合法。 （3）服务器文件扩展名检测：这类检测方法通过在服务器端检测上传文件的扩展名来判断文件是否合法。 （4）服务器目录路径检测：这类检测一般通过检测路径是否合法来判断。 （5）服务器文件内容检测：这类检测方法相对于上面 4 种检测方法来说是最为严格的一种。它通过检测文件内容来判断上传文件是否合法。这里，对文件内容的检测主要有两种方法。其一，通过检测上传文件的文件头来判断。通常情况下，通过判断前 10 字节，基本就能判断出一个文件的真实类型。其二，文件加载检测，一般调用 API 或函数对文件进行加载测试。常见的是图像渲染测试，再严格点的是进行二次渲染

1.3 Web 安全发展趋势

Web 安全的发展趋势主要受到技术进步、网络攻击手段演变以及法规更新等多方面因素的影响。随着互联网应用的普及和复杂度的提高，Web 安全面临的挑战日益严峻，以下是 Web 安全未来发展的几个主要趋势。

1. 人工智能和机器学习在 Web 安全中的应用

人工智能（AI）和机器学习（ML）技术正在被广泛应用于 Web 安全领域，AI 的高级数据分析功能正在被越来越多地应用于识别和预测网络威胁，以增强早期检测系统的功能。机器学习算法不断发展，逐渐改进防御措施，预计 AI 算法将在 2025 年提供实时威胁分析，从而更快、更精准地应对网络事件，提升了自动化检测、应急响应和安全防护的能力。

（1）攻击检测与防护：AI 和 ML 可以通过分析网络流量、行为模式和系统日志来识别潜在的攻击行为，如 DDoS 攻击、SQL 注入和恶意软件等。与传统的基于规则的防御系统不同，AI 系统能够不断自我学习和优化，提升对新型攻击的应对能力。

（2）入侵检测与响应：机器学习可以帮助自动化入侵检测系统（IDS）更准确地识别异常行为，同时缩短响应时间，及时阻止攻击。

（3）自动化漏洞扫描与修复：AI 技术可以快速扫描 Web 应用中的安全漏洞，并在发现漏洞时提供修复建议或自动修复，提高修复效率。

随着 AI 技术的应用，攻击者也可能利用 AI 技术来进行更加精准的攻击，例如，通过机器学习生成更加难以检测的恶意代码和攻击行为。数据隐私和安全问题成为 AI 应用中的重要考虑方面，尤其是在需要大量数据来训练模型时，如何确保数据安全和防止数据泄露是一个亟待解决的难题。

2. 零信任架构（Zero Trust Architecture, ZTA）的普及

零信任架构是指在任何情况下都不信任任何用户或设备，始终对其身份和权限进行验证，只有验证通过后才能访问资源，这种架构特别适用于分布式和云计算环境中的 Web 安全。

（1）强身份认证：在零信任架构中，用户和设备的身份验证更加严格，除了传统的用户名和密码外，还包括多因素认证（MFA）和生物识别等技术。

（2）最小权限原则：只有授权的用户和设备才能访问特定的资源，且访问权限严格控制在最小范围内，减少攻击面。

（3）网络微分段：通过将网络划分为多个安全区域，限制攻击者的横向移动，降低攻击的蔓延风险。

零信任架构能有效提升安全性，尤其是在远程办公和云环境中。然而，实施零信任架构需要较大的技术投入和复杂的管理工作，需要企业在架构设计和运维方面做出较大调整。随着零信任架构的普及，用户体验可能会受到一定影响，特别是在身份验证和权限管理方面的复杂性增加。

3. Web 应用防火墙（WAF）与 API 安全的重要性增加

随着 Web 应用程序和 API 的广泛应用，WAF 和 API 安全管理将成为 Web 安全的重要组成部分。

（1）WAF 防护能力提升：传统的 WAF 主要基于规则的方式过滤恶意请求，但随着 Web 应用攻击技术的不断演进，现代 WAF 将结合 AI 和机器学习来增强自适应能力，动态防御越来越复杂的攻击（如 webshell、OWASP Top 10 漏洞等）。

（2）API 安全管理：随着 RESTful API 和 GraphQL 等 API 的普及，API 的安全问题也逐渐成为焦点。攻击者可能通过 API 注入攻击等。API 安全管理技术将越来越重要，涉及认证、访问控制、数据加密、速率限制等方面。

对 WAF 和 API 的持续投入至关重要，尤其是为了防范不断变化的 Web 攻击模式。随着 API 数量和复杂度的增加，如何高效地管理和保护大量 API 成为一个挑战。

4. 云安全与 Web 安全的融合

云计算的广泛应用使得 Web 安全不再局限于传统的物理设备和网络环境，云安全成为 Web 安全的重要组成部分。

（1）云平台安全：越来越多的企业将数据存储和应用部署到云端，云服务提供商（如 AWS、Azure、Google Cloud 等）为客户提供了 Web 安全解决方案，但企业仍需强化云环境中的安全控制，确保数据、应用和基础设施的安全。

（2）Serverless 安全：Serverless 架构的流行使得 Web 应用的部署更加灵活和高效，但也带来了新的安全挑战。例如，如何保护无服务器计算环境中的函数、事件和数据传输等。

（3）混合云与多云安全：企业正在采用混合云和多云架构，如何确保不同云平台之间的数据安全和统一管理是一个重要问题。

云环境中的多租户架构和资源共享，可能会导致数据隔离和隐私泄露的风险。企业需要具备一定的云安全管理能力，同时确保安全策略与云服务商的安全措施有效配合。

5. 数据隐私与合规性要求的加强

随着《中华人民共和国个人信息保护法》和《中华人民共和国数据安全法》的实施，Web 应用和互联网企业需要更加重视数据隐私保护与合规性要求。

（1）数据加密与隐私保护：Web 安全不仅要防止黑客入侵，还需要保护用户的个人信息不被非法使用。加密技术（如 TLS/SSL、端到端加密）将成为 Web 应用的标准配置。

（2）合规性要求：Web 应用开发和运营将必须遵循日益严格的法律法规要求，特别是在数据处理、存储和传输方面。企业需要满足信息安全法律法规的合规要求，确保个人数据的合法、安全和透明处理。

企业将面临更加严格的监管和处罚，合规性成本和运营负担增加。用户隐私保护成为 Web 应用设计的重要考虑，要求企业在产品开发和运营中优先考虑数据保护问题。

6. 量子计算对 Web 安全的影响

量子计算技术的不断发展将给现有的加密算法带来威胁，尤其是 RSA、ECC 等公钥加密算法。

（1）量子计算威胁：量子计算能够在短时间内破解传统的公钥加密算法，因此，Web 安全领域需要提前规划和适应量子计算的威胁。

（2）量子加密：量子加密技术（如量子密钥分发、量子数字签名等）被认为是解决量子计算威胁的一种方法。随着量子计算技术的发展，Web 安全领域将逐步引入量子级别的安全防护措施。

量子计算的普及可能使现有的加密技术失效，因此必须加快量子安全技术的研发与应用。企业需要关注量子计算对加密算法的影响，提前进行加密技术的更新和迭代。

人工智能、零信任架构、云安全、API 保护、数据隐私保护等将成为未来 Web 安全的关键组成部分。同时，量子计算等新兴技术对现有安全体系的影响也需要关注。企业和开发者在面对新的安全挑战时，必须不断更新技术手段，强化合规性，并加大对安全防护的投资。