HZ BOOKS
华章IT

永信至诚® | 带给世界安全感

· 网络空间安全技术丛书 ·

Web安全防护指南

基础篇

蔡晶晶 张兆心 林天翔 编著

- 系统梳理各类 Web 安全漏洞，从 Web 应用的业务逻辑层面寻找防护方法，总结攻防视角下的 Web 安全防护体系建设方法。
- 从 Web 安全问题的表现形式、实现原理到防护原则、动手实践，层层深入，使读者理解问题的成因、危害、关联，进而实现有效防御。

机械工业出版社
China Machine Press

· 网络空间安全技术丛书 ·

Web安全防护指南

基础篇

FUNDAMENTAL OF WEB SECURITY

蔡晶晶 张兆心 林天翔 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Web 安全防护指南：基础篇 / 蔡晶晶，张兆心，林天翔编著 . —北京：机械工业出版社，2018.3
（网络空间安全技术丛书）

ISBN 978-7-111-58776-7

I. W…　II. ①蔡…　②张…　③林…　III. 互联网络 - 安全技术 - 指南　IV. TP393.408-62

中国版本图书馆 CIP 数据核字（2017）第 320073 号

Web 安全防护指南：基础篇

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：朱　劼　　责任校对：李秋荣
印　　刷：中国电影出版社印刷厂　　版　　次：2018 年 4 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：23.5
书　　号：ISBN 978-7-111-58776-7　　定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

推 荐 序

网络安全如今似乎进入到了一个非常混乱的状态：层出不穷的安全漏洞、不间断的安全事件，似乎所有东西都能入侵控制的攻击演示。这些让人们变得十分麻木，同时网络安全工作者也十分困惑：究竟怎样才能改善网络安全状况呢？

尽量跳出具体的漏洞或者事件，从更全面的视角来看问题；尽量越过令人眼花缭乱的表象，把握事物更深层次的本质，从更基础的角度来设法解决问题——这应该是让我们摆脱被动的一个方向。而这本书就是试图从这样的角度给读者提供一些帮助。

然而，Web 似乎是一个被说烂了的话题，并且 Web 安全的门槛貌似也很低，很多中学生都可以轻易找到很多 Web 站点的问题。同时，Web 安全的书籍也不少，为什么还要读这本关于 Web 安全的书呢？

安全攻防是一个体系的对抗。再高深、再尖端的技术，也经常在最简单的地方被彻底击败，因此，并不能根据感官上难度的大小来评价一件事情的意义。另外，Web 攻防不但不是想象中那么简单（无论是什么原因，有问题的 Web 站点始终还是多如牛毛），而且还是攻防体系中的一个兵家必争之地：从 Web 出现以来，在短短的时间之内，它就一统江湖，结束了之前众多的应用入口，变成了各种互联网应用的统一门户。Web 自然也成为攻防重地。

这本书的内容是作者和一个有十年经验的安全研究团队一起在实践中磨合出来的。相较于纯粹产业圈朋友的著作来说，这本书更加强调学术和教育圈关注的话题：如何让读者学到更加全面的东西？如何形成体系化的能力？毕竟授人以渔要比授人以鱼重要得多。而相较于纯粹学术圈朋友的著作来说，这本书又具有大量的一线工程实践方面的内容。

因此，如同作者所说，如果你是安全运维人员、开发人员、服务人员，甚至是互联网应用体系的设计人员，认真读一读这本书，都会有很大收益。

杜跃进

前　言

一、为什么要写这本书

随着网络的普及，人们的工作、生活已经与网络深度融合。Web 系统由于其高度可定制的特点，非常适合承载现有的互联网应用。目前，大量在线应用网站的出现和使用也印证了这一点。我们每个人每天都会打开各种网站搜索自己感兴趣的内容或使用某一个应用，其中每个站点的功能各不相同，业务流程也各自独立，并且站点功能及版本的迭代、更新速度非常快。同时，由于大量 Web 应用功能及版本的快速更新，也导致各类新型 Web 安全问题不断出现。尽管 Web 安全问题的表现形式各异，但深入分析各类安全问题的成因会发现，这些安全问题有一定的共性并能通过相关的网络安全技术来加以防御和解决。

反观 Web 安全的学习过程，由于 Web 安全攻防涉及的技术、工具繁多，安全问题也表现出各种复杂的形式，学习者很容易被这些表象混淆，进入“只见树木不见森林”的误区，无法快速成长。因此，本书作者基于多年的安全研究、教学、工程实践经验，以帮助读者建立知识体系为目标，通过原理、方法、代码、实践的层层深入，使读者充分理解 Web 安全问题的成因、危害、关联，进而有效地保护 Web 系统，抵御攻击。

二、本书的主要内容

本书试图整理出 Web 安全防护知识的体系，因此对每一类 Web 安全问题，都对从原理到攻防技术的演进过程加以详细的讲解。在针对安全问题的分析方面，本书从基础的漏洞环境入手，可排除不同业务环境的干扰，更聚焦于安全问题本身。这种方式有利于帮助读者在掌握每种 Web 安全问题的解决方案的同时，对整个 Web 安全防护体系建立清晰的认知。

本书主要内容共分为 5 部分，各部分内容如下。

第一部分（包括第 1 章）：Web 应用概念庞大、涉及的协议广泛，因此，此部分没有系统地介绍所有的基础内容，而是抽取了与 Web 安全关系密切的协议等方面的基础知识。这些知识对后续理解 Web 攻防技术极为关键。

第二部分（包括第 2 ～ 8 章）：重点讲解 Web 应用中的基础漏洞，从用户端到服务器端依次开展分析。首先从主要攻击用户的跨站请求攻击入手，之后了解 Web 应用中的请求伪造攻击、针对 Web 应用于数据库交互产生的 SQL 注入攻击。再针对可直接上传各类危险文件的上传漏洞进行分析，并说明上传漏洞中常用的木马的基本原理。最后对服务器端的危险

应用功能（文件包含、命令执行漏洞）进行分析。此部分重点讲解上述基本漏洞的原理及攻防技术对抗方法，并针对每个漏洞的测试及防护方法的技术演进思路进行整理。

第三部分（包括第 9 ～ 15 章）：重点讲解 Web 应用的业务逻辑层面的基础安全问题。Web 应用基于用户管理机制来提供个性化的服务，用户的身份认证则成为安全开展 Web 应用的基础功能。此部分从用户的未登录状态入手，讲解用户注册行为中潜在的安全隐患。然后对用户登录过程中的安全问题进行整理，并对常见的用户身份识别技术进行原理说明。最后对用户登录后的基本功能及用户权限处理方式进行讲解。

第四部分（包括第 16 ～ 19 章）：主要讲解在实际 Web 站点上线之后的基础防护方式，并从 Web 整体应用的视角展示攻防对抗过程中的技术细节。重点针对 Web 服务潜在的基础信息泄漏方及对应处理方法进行总结。最后提供可解决大部分问题的简单防护方案，这对安全运维有较大的用途。

第五部分（包括第 20 ～ 23 章）：在前几部分的基础上总结 Web 安全防护体系建设的基本方法。本部分先从 Web 安全中常见的防护类设备入手，分析各类安全防护设备的特点及适用范围。之后，对目前业界权威的安全开发体系进行基本介绍，并对安全服务中的渗透测试的主要流程进行说明。最后以实例的形式展示如何进行快速的代码审计。

以上每个部分的知识均为递进关系。第一部分和第二部分帮助读者了解 Web 应用中各类漏洞的原理及测试方式、防护手段等。第三部分和第四部分让读者了解业务层面和整体安全的防护方法。第五部分则从整体层间构建有效防护体系的思路。最后可综合掌握 Web 安全防护的整体内容，这也是本书希望读者获得的阅读效果。

三、本书的读者对象

本书适合所有对 Web 安全感兴趣的初学者以及从事安全行业的相关人员，主要包括以下几类读者：

- **信息安全及相关专业本科生**

  本书以基本的漏洞为例，循序渐进地梳理攻防对抗方式及各类漏洞的危害。信息安全及相关专业学生可根据这些内容快速入门，并以此作为基础来探索信息安全更前沿的领域。

- **安全运维人员**

  本书提供了大量漏洞利用特征及有效的安全运维方式，可供安全运维人员在实际工作中快速发现系统安全状况，并对安全漏洞进行基本的处理。

- **安全开发人员**

  本书列举了各种漏洞的原理分析及防护方式，可帮助开发人员在 Web 系统的开发过程中对漏洞进行规避，进而从根源上避免 Web 漏洞的出现。

- **安全服务人员**

  安全服务人员重点关注如何快速发现目标 Web 系统的安全隐患并针对问题提出处理

建议。此类读者建议重点阅读本书前三部分以及最后一部分的最后两章，可为安全服务的工作开展提供更全面的技术支持。

- **攻防技术爱好者**

  对于攻防技术爱好者来说，本书提供了体系化的 Web 安全基础原理，可有效丰富个人的知识储备体系。

四、如何阅读这本书

本书虽然篇幅不大，但涉及的内容繁多，加之 Web 安全是一个实践性极强的领域，因此，我们对学习本书给出如下建议。

1. 需要具备的基础知识

Web 系统一般需要服务器、中间件、Web 语言、数据库等多方面的支持，相应地，在 Web 安全防护中也会应用到上述知识。安全从业者不一定要像开发人员那样对以上内容非常熟悉，但应对以上内容有初步了解并理解基本用法。这方面的教程很多，读者可以自行选择。另外，本书的所有案例均基于 PHP 环境编写，因此读者如有基本的 PHP 知识，则能更好地理解本书的内容。

2. 具有一定编程经验

在了解攻防技术方向之前，最好具有一定的编程经验。这些经验可帮助读者快速阅读漏洞源码及相应的语句，并可显著提升 Web 安全的学习效率。这里的编程经验以可独立阅读各种语言的基础示例代码为基准，并不需要有十分专业的开发能力。

3. 善用搜索引擎

在学习 Web 安全的过程中会遇到非常多的基础内容或者特点，且每个人的基础并不相同。针对个人不理解的问题，建议善用各类搜索引擎来获取帮助。关于如何高效使用搜索引擎，可参考本书第四部分的讲解。

4. 动手实践

Web 安全是一个实践性很强的领域，需要通过大量的直接攻防技术练习来建立对漏洞的直观认识，并积累解决问题的经验。本书给出了大量的案例，读者可以利用这些案例进行练习，或者登录“i 春秋在线培训平台”（www.ichunqiu.com）进行专项练习。

在本书的学习阅读顺序上，建议读者顺序学习本书的各章，以便对 Web 安全防护建立系统认识。不同基础的读者也可根据自身情况以及关注内容进行选择性的阅读。

五、致谢

本书的编写工作历时两年，在整个过程中得到了永信至诚科技股份有限公司与哈尔滨工业大学（威海）网络与信息安全研究中心的同事的支持和帮助，在本书即将付梓之际，谨向

他们表示最诚挚的感谢！

感谢哈尔滨工业大学（威海）计算机科学与技术学院的迟乐军教授、谷松林老师在本书编写的各个环节中提供的支持；感谢殷亚静为本书绘制插图；感谢倪远东、王续武、刘深荣、孟晨、彭衍豪、刘骁睿、余超、卢鑫、李思锐、张鹏、雷朋荃、刘家豪、李彦哲、张瑞淇、付尧、黄欣、靳祯等对本书中案例的持续调整和完善；感谢机械工业出版社华章分社的编辑对本书的出版付出的劳动。

限于作者水平，加之 Web 安全防护技术的进展迅速，本书难免存在不当和疏漏之处，恳请各位读者提出、指正！我们期待与读者的交流！

作者

2018 年 1 月

目　录

第三部分 业务逻辑安全

第一部分

基础知识

Web安全有着非常明显的“入门简单精通难”的特点。“简单”表现在Web漏洞的原理通常较为清晰，利用方式及案例非常多，学习过程中的阻力较小。“难”则表现在Web应用在构建过程中涉及的技术非常多，且范围非常广。

针对上述特点，建议读者在开始接触Web安全时，要充分理解Web应用的构成环境及协议基础、运行原理等，这些内容会为理解Web基础漏洞及业务逻辑缺陷提供有效的支持。当具备一定Web安全技术基础后，再根据不同研究方向或安全需求开展进一步的安全研究。

本部分将重点针对Web应用中基础的协议及技术涉及的安全内容进行初步分析。当然在Web安全中这仅仅是很小的一部分，建议在后续学习过程中，根据个人理解及知识储备情况补充相关的知识，实现整体攻防技术实力的提升。

第 1 章

Web 安全基础

Web 是万维网（World Wide Web，WWW）的简称，它利用 HTTP（HyperText Transfer Protocol，超文本传输协议）来建立用户与服务器之间的标准交互方式。常用的 Web 应用都是基于网页形式开展的，即用户输入域名，利用 HTTP 协议发起访问请求。服务器接收到用户请求后，根据 HTTP 协议向用户返回响应页面。在这个过程中，HTTP 协议规定了在当前请求中需要的参数，从而实现标准化的传输效果，如图 1-1 所示。

提供各种类型服务的 Web 网站非常多，网站是由多个页面组成的。用户可通过浏览不同的页面来开展不同的业务。HTML（Hyper Text Markup Language，超文本标记语言）规定了 Web 应用的页面格式。使用 HTML 的好处在于规定了页面的基本格式后，用户端只要利用可以解析 HTML 格式的浏览器即可实现访问。如图 1-2 所示。

Web 网站从早期只有浏览功能，逐渐发展到能支持用户进行自定义查询、支持用户登录并互动、在线交易等复杂业务。在这个过程中，需要添加额外的组件来实现上述功能。因此，目前的 Web 站点都会附带数据库及其他服务，从而实现对当前站点及用户信息的存储及复杂功能的支持。

下面来分析一个常见的 Web 应用：访问一个网站并做一次信息查询。这个过程中涉及的服务及功能流程如图 1-3 所示。

图中所示的流程与真实的大型网站应用流程并不完全一致，只用于说明基本原理。因为大型网站要同时为数以千万的用户请求提供服务，仅通过一台服务器根本无法支持海量的用户访问请求，所以会利用负载均衡、CDN、云技术、分布式数据库等技术来应对大量用户的并发访问。值得说明的是，以上所有环节均可能存在安全隐患，其中一项服务产生问题都可能影响用户的正常使用或者危害 Web 服务器的安全。

1.1 Web 安全的核心问题

日益丰富的各类 Web 网站被 Web 用户使用，而且 Web 也不仅仅是利用浏览器访问站点。因此，在了解 Web 各类漏洞之前，我们先了解一下常见的 Web 应用表现形式。

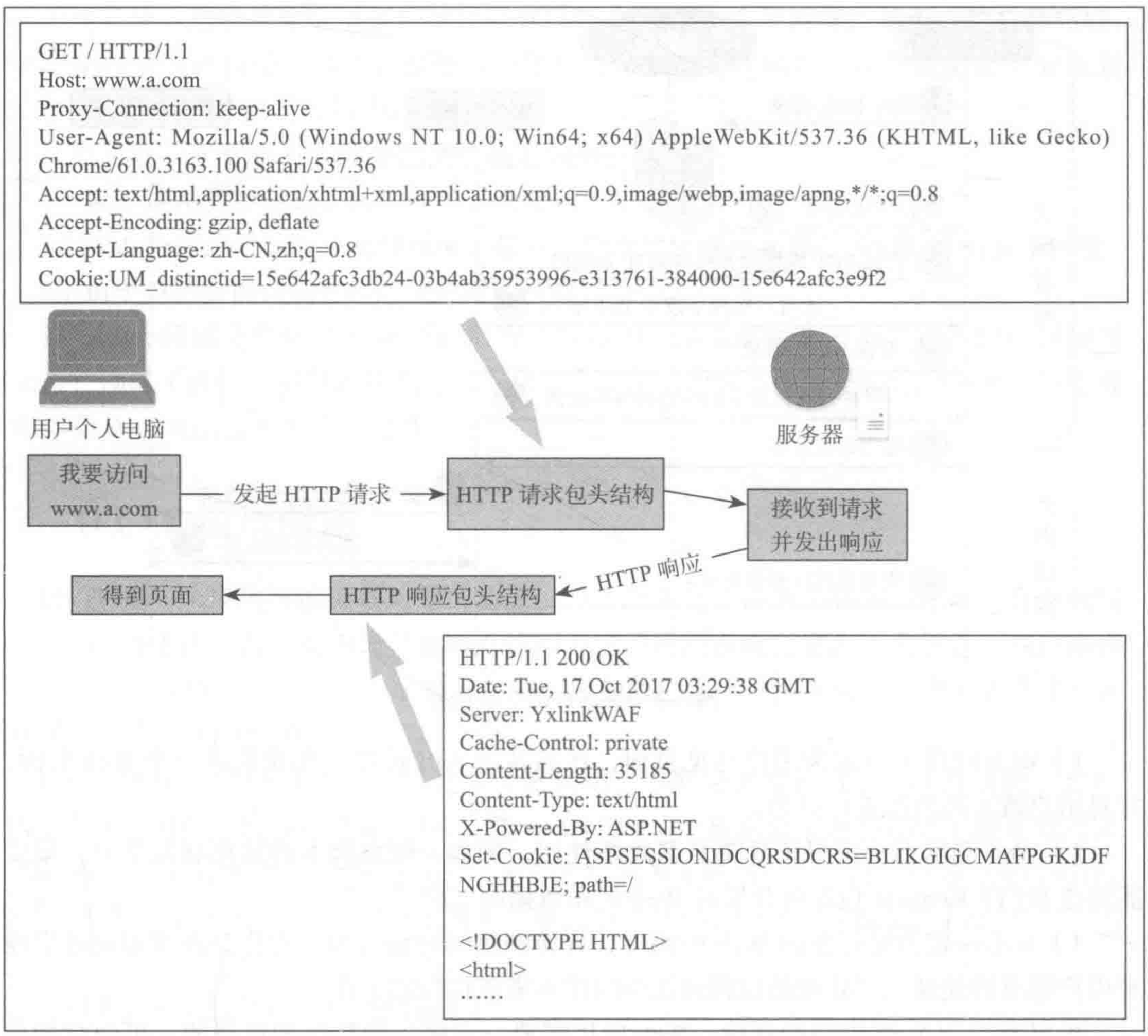

图 1-1　HTTP 请求包头与响应包头结构

图 1-2　利用 Chrome 浏览器访问站点

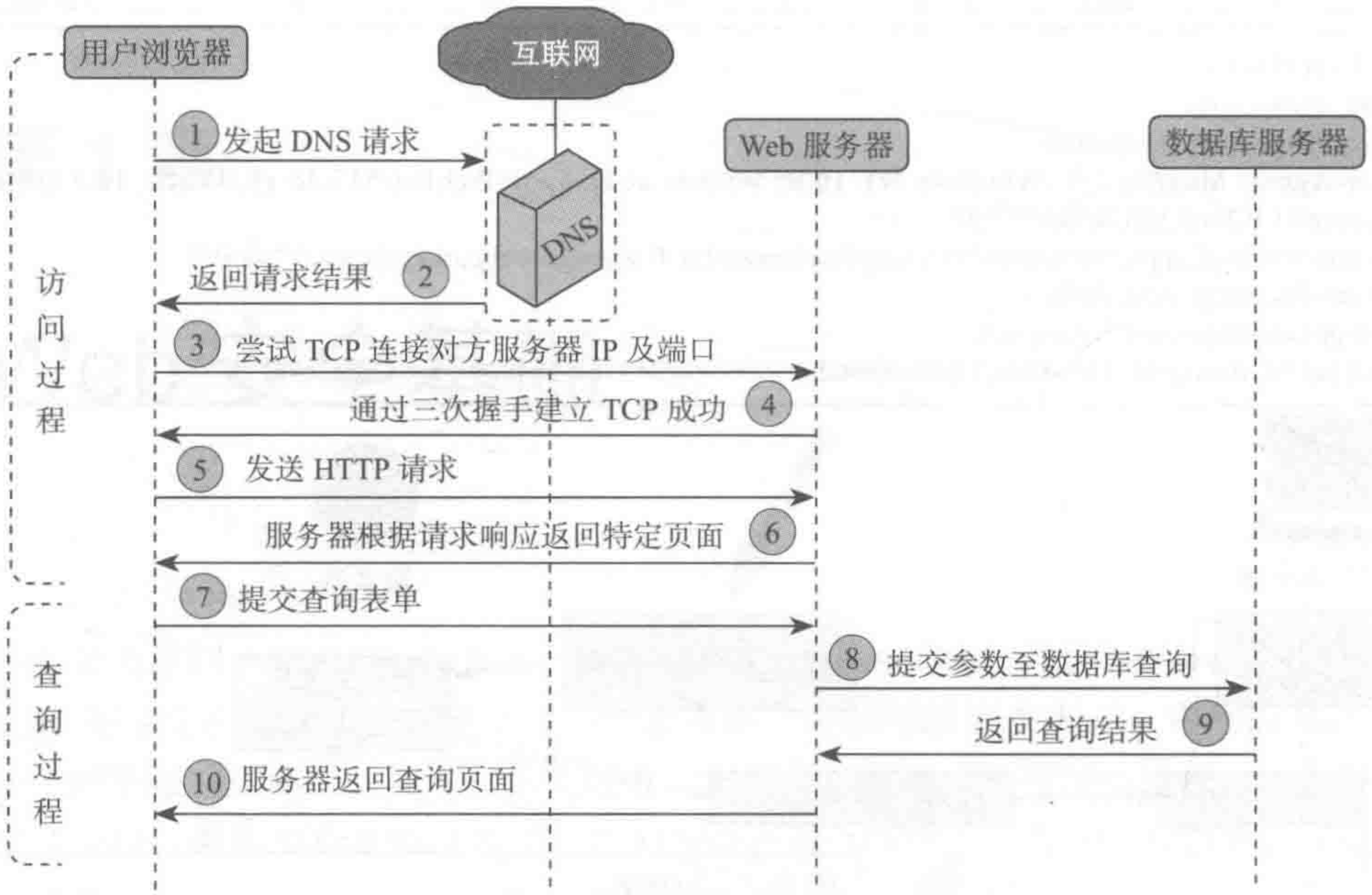

图 1-3　信息查询功能流程

1）Web 应用不一定为用户可见页面，比如各类 API 接口，其原理是一个 Web 页面，并对用户请求的内容进行处理。

2）Web 应用不一定要依托浏览器才能使用，例如，爬虫脚本的数据获取部分，只要能构造 HTTP Request 包即可开展对 Web 应用数据的获取。

3）并不一定需要标准的 Web 中间件，直接利用编程语言编写对应处理规则也可实现对用户请求的处理，但处理的过程就是中间件本来该执行的工作。

再思考一下 Web 应用的环境。Web 应用需要一台服务器提供基础资源，可运行操作系统，并配合中间件来为用户提供服务。如果站点功能较为复杂，那么还需要用数据库提供基础的数据存储支持，用文件服务器进行备份，用 SAN 系统提供高性能的文件存储等。在这个过程中，任何一个环节出现问题，都可能导致 Web 安全问题出现。

可以把 Web 应用环境类比为一个球队。球队中有负责打比赛的队员，有指导教练、领队、队医、后勤人员，它们共同为球队的运转服务，任何一个环节或岗位出现问题，都会影响球队的成绩。类似地，在 Web 系统中，无论有多少硬件设备、提供支持的组件有哪些，只要它们为 Web 提供支持，那么都要纳入防护体系。从安全角度考虑，Web 应用中的中间件、数据库、操作系统等均会影响 Web 系统的安全，因此关注点并不能仅放在网页层面。

最后从交互角度来思考。HTTP 协议作为 Web 应用的基础协议，其特点就是用户请求 – 服务器响应。在这个过程中，服务器一直处于被动响应状态，无法主动获取用户的信息。再看一下 HTML 结构，服务器在完成用户响应后，当前的 HTML 页面会被发送到用