第12章

基本认证机制

有数百万的人在用 Web 进行私人事务处理，访问私有的数据。通过 Web 可以很方便地访问这些信息，但仅仅是方便访问还是不够的。我们要保证只有特定的人能看到我们的敏感信息并且能够执行我们的特权事务。并不是所有的信息都能够公开发布的。

未授权用户无法查看我们的在线旅游档案，也不能在未经许可的情况下向 Web 站点发布文档，这会让我们感觉舒服一些。我们还要确保，组织中未经授权或不怀好意的成员无法获取那些最敏感的公司计划文档。我们与孩子、配偶以及暗恋对象的私人 Web 通信都是在带有些许隐私保护的情况下进行的，这样我们才能放心。

服务器需要通过某种方式来了解用户身份。一旦服务器知道了用户身份，就可以判定用户可以访问的事务和资源了。认证就意味着要证明你是谁。通常是通过提供用户名和密码来进行认证的。HTTP 为认证提供了一种原生工具。尽管我们可以在 HTTP 的认证形式和 cookie 基础之上“运行自己的”认证工具，但在很多情况下，HTTP 的原生认证功能就可以很好地满足要求。

本章阐述了 HTTP 的认证机制，深入介绍了最常见的 HTTP 认证形式，*基本认证*（basic authentication）。下一章将介绍一种称为*摘要认证*（digest authentication）的功能更强的认证技术。

12.1 认证

认证就是要给出一些身份证明。当出示像护照或驾照那样有照片的身份证件时，就给出了一些证据，说明你就是你所声称的那个人。在自动取款机上输入 PIN 码，或
277 在计算机系统的对话框中输入了密码时，也是在证明你就是你所声称的那个人。

现在，这些策略都不是绝对有效的。密码可以被猜出来或被人偶然听到，身份证件可能被偷去或被伪造，但每种证据都有助于构建合理的信任，说明你就是你所声称的那个人。

12.1.1 HTTP的质询/响应认证框架

HTTP 提供了一个原生的*质询 / 响应*（challenge/response）框架，简化了对用户的认证过程。HTTP 的认证模型如图 12-1 中所示。

Web 应用程序收到一条 HTTP 请求报文时，服务器没有按照请求执行动作，而是以一个“认证质询”进行响应，要求用户提供一些保密信息来说明他是谁，从而对其进行质询。

用户再次发起请求时，要附上保密证书（用户名和密码）。如果证书不匹配，服务器可以再次质询客户端，或产生一条错误信息。如果证书匹配，就可以正常完成请求了。

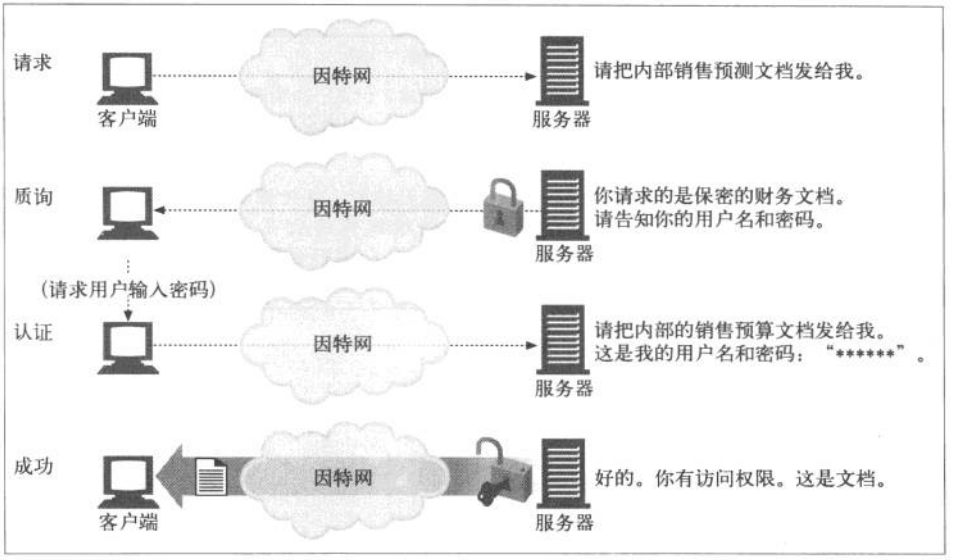

图 12-1　简化的质询 / 响应认证框架

12.1.2　认证协议与首部

HTTP 通过一组可定制的控制首部，为不同的认证协议提供了一个可扩展框架。表 12-1 列出的首部格式和内容会随认证协议的不同而发生变化。认证协议也是在 HTTP 认证首部中指定的。

278

HTTP 定义了两个官方的认证协议：基本认证和摘要认证。今后人们可以随意设计一些使用 HTTP 质询 / 响应框架的新协议。本章的其余部分将解释基本认证机制。摘要认证的细节请参见第 13 章。

表12-1　认证的4个步骤

步骤	首　部	描　述	方法/状态
请求		第一条请求没有认证信息	GET
质询	WWW-Authenticate	服务器用 401 状态拒绝了请求，说明需要用户提供用户名和密码。 服务器上可能会分为不同的区域，每个区域都有自己的密码，所以服务器会在 WWW-Authenticate 首部对保护区域进行描述。 同样，认证算法也是在 WWW-Authenticate 首部中指定的	401 Unauthorized

（续）

步骤	首　部	描　述	方法/状态
授权	Authorization	客户端重新发出请求，但这一次会附加一个 Authorization 首部，用来说明认证算法、用户名和密码	GET
成功	Authentication-Info	如果授权证书是正确的，服务器就会将文档返回。有些授权算法会在可选的 Authentication-Info 首部返回一些与授权会话相关的附加信息	200 OK

为了具体地说明这个问题，我们来看看图 12-2。

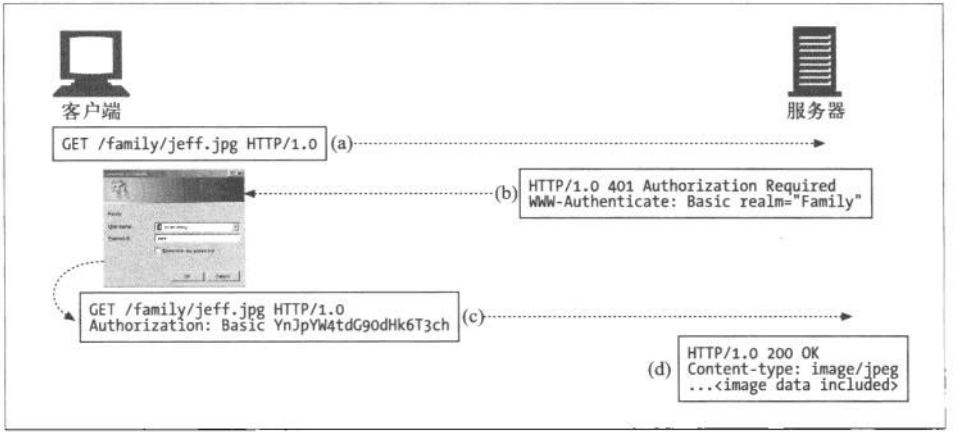

图 12-2　基本认证实例

服务器对用户进行质询时，会返回一条 401 Unauthorized 响应，并在 WWW-Authenticate 首部说明如何以及在哪里进行认证（参见图 12-2b）。

279

当客户端授权服务器继续处理时，会重新发送请求，但会在 Authorization 首部附上加密的密码和其他一些认证参数（参见图 12-2c）。

授权请求成功完成时，服务器会返回一个正常的状态码（比如，200 OK）；对高级认证算法来说，可能还会在 Authentication-Info 首部附加一些额外的信息（参见图 12-2d）。

12.1.3　安全域

在对基本认证的细节进行讨论之前，需要解释一下 HTTP 是怎样允许服务器为

不同的资源使用不同的访问权限的。你可能已经注意到了，图 12-2b 的 WWW-Authenticate 质询中包含了一个 realm 指令。Web 服务器会将受保护的文档组织成一个安全域（security realm）。每个安全域都可以有不同的授权用户集。

比如，假设 Web 服务器建立了两个安全域：一个用于公司的财务信息，另一个用于个人家庭文档（参见图 12-3）。不同的用户对各个安全域的访问权限是不同的。公司的 CEO 应该能够访问销售额预测资料，但不应该允许他访问员工和其家人度假的照片！

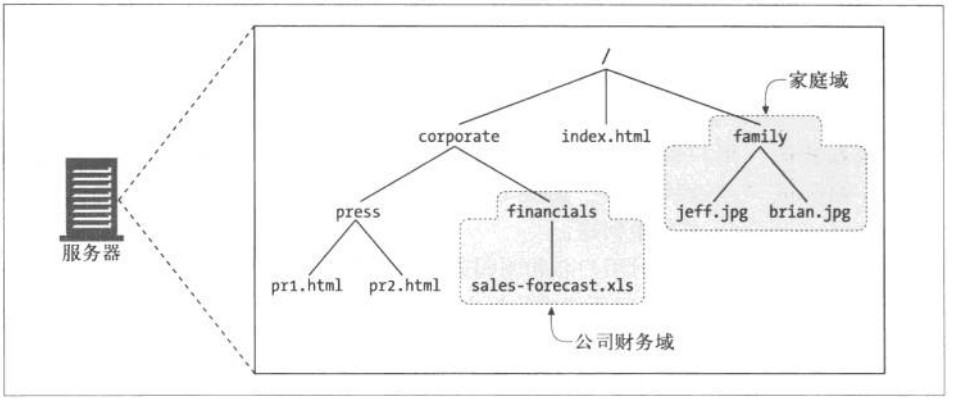

图 12-3 Web 服务器上的安全域

下面是一个假想的基本认证质询，它指定了一个域：

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="Corporate Financials"
```

域应该有一个描述性的字符名，比如 Corporate Financials（公司财务资料），以帮助用户了解应该使用哪个用户名和密码。在安全域的名称中列出服务器主机名也是很有帮助的——比如，executive-committee@bigcompany.com。 280

12.2 基本认证

基本认证是最流行的 HTTP 认证协议。几乎每个主要的客户端和服务器都实现了基本认证机制。基本认证最初是在 HTTP/1.0 规范中提出的，但此后被移到了 RFC 2617 中，它详细介绍了 HTTP 的认证机制。

在基本认证中，Web 服务器可以拒绝一个事务，质询客户端，请用户提供有效的用户名和密码。服务器会返回 401 状态码，而不是 200 状态码来初始化认证质询，并

用 WWW-Authenticate 响应首部指定要访问的安全域。浏览器收到质询时，会打开一个对话框，请求用户输入这个域的用户名和密码。然后将用户名和密码稍加扰码，再用 Authorization 请求首部回送给服务器。

12.2.1 基本认证实例

图 12-2 是一个详细的基本认证实例。

- 在图 12-2a 中，用户请求了私人家庭相片 /family/jeff.jpg。
- 在图 12-2b 中，服务器回送一条 401 Authorization Required，对私人家庭相片进行密码质询，同时回送的还有 WWW-Authenticate 首部。这个首部请求对 Family 域进行基本认证。
- 在图 12-2c 中，浏览器收到了 401 质询，弹出对话框，询问 Family 域的用户名和密码。用户输入用户名和密码时，浏览器会用一个冒号将其连接起来，编码成“经过扰码的”Base-64 表示形式（下节介绍），然后将其放在 Authorization 首部中回送。
- 在图 12-2d 中，服务器对用户名和密码进行解码，验证它们的正确性，然后用一条 HTTP 200 OK 报文返回所请求的报文。

表 12-2 总结了 HTTP 基本认证的 WWW-Authenticate 和 Authorization 首部。

表12-2 基本认证首部

质询/响应	首部语法及描述
质询（服务器发往客户端）	网站的不同部分可能有不同的密码。域就是一个引用字符串，用来命名所请求的文档集，这样用户就知道该使用哪个密码了： WWW-Authenticate: Basic realm=quoted-realm
响应（客户端发往服务器）	用冒号（:）将用户名和密码连接起来，然后转换成 Base-64 编码，这样在用户名和密码中包含国际字符会稍微容易一些，也能尽量避免通过观察网络流量并只进行一些粗略的检查就可以获取用户名和密码情况的发生： Authorization: Basic base64-username-and-password

281

注意，基本认证协议并没有使用表 12-1 所示的 Authentication-Info 首部。

12.2.2 Base-64 用户名/密码编码

HTTP 基本认证将（由冒号分隔的）用户名和密码打包在一起，并用 Base-64 编码方式对其进行编码。如果不知道 Base-64 编码是什么意思，也不用担心。你并不需要对它有太多的了解，如果对此感兴趣，可以在附录 E 中读到所有与之有关的内容。简单来说，Base-64 编码会将一个 8 位字节序列划分为一些 6 位的块。用每个 6

位的块在一个特殊的由 64 个字符组成的字母表中选择一个字符，这个字母表中包含了大部分字母和数字。

图 12-4 显示了使用 Base-64 编码的基本认证实例。在这个例子中，用户名为 brian-totty，密码为 Ow!。浏览器用冒号将用户名和密码连接起来，生成一个打包字符串 brian-totty:Ow!。然后对这个字符串进行 Base-64 编码，变成一串乱码：YnJpYW4tdG90dHk6T3ch。

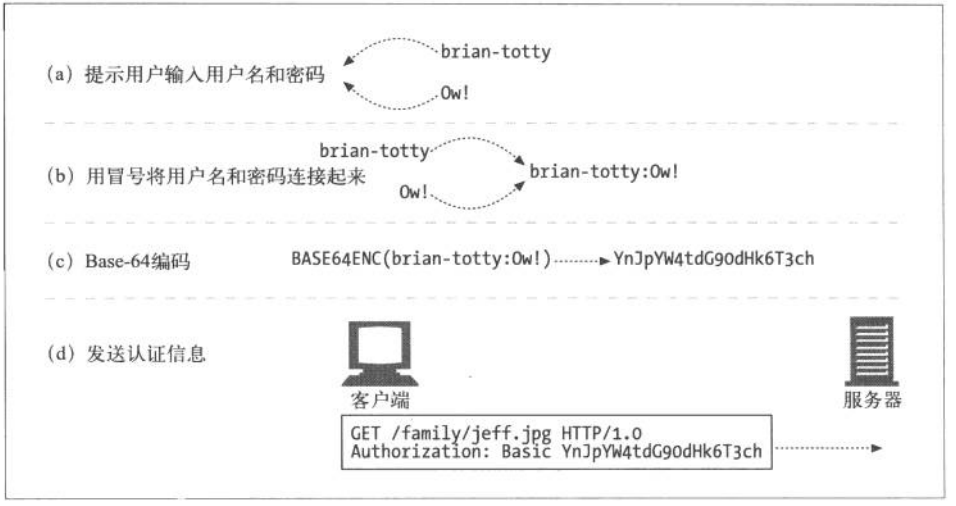

图 12-4　从用户名和密码中生成一个基本认证首部

Base-64 编码可以接受二进制字符串、文本、国际字符表示的数据（在某些系统中会引发一些问题），将其暂时转换成一个易移植的字母表以便传输。然后，在远端就可以解码出原始字符串，而无需担心传输错误了。

有些用户名和密码中会包含国际字符或其他在 HTTP 首部中非法的字符（比如引号、冒号和回车换行符），对这些用户名和密码来说，Base-64 编码是非常有用的。而且，Base-64 编码扰乱了用户名和密码，这样也可以防止管理员在管理服务器和网络时，不小心看到用户名和密码。 282

12.2.3　代理认证

中间的代理服务器也可以实现认证功能。有些组织会在用户访问服务器、LAN 或无线网络之前，用代理服务器对其进行认证。可以在代理服务器上对访问策略进行集中管理，因此，通过代理服务器提供对某组织内部资源的统一访问控制是一种很便捷的

方式。这个过程的第一步就是通过代理认证（proxy authentication）来识别身份。

代理认证的步骤与 Web 服务器身份验证的步骤相同。但首部和状态码都有所不同。表 12-3 列出了 Web 服务器和代理在认证中使用的状态码和首部的差异。

表12-3 Web服务器与代理认证

Web服务器	代理服务器
Unauthorized status code: 401	Unauthorized status code: 407
WWW-Authenticate	Proxy-Authenticate
Authorization	Proxy-Authorization
Authentication-Info	Proxy-Authentication-Info

12.3 基本认证的安全缺陷

基本认证简单便捷，但并不安全。只能用它来防止非恶意用户无意间进行的访问，或将其与 SSL 这样的加密技术配合使用。

基本认证存在下列安全缺陷。

(1) 基本认证会通过网络发送用户名和密码，这些用户名和密码都是以一种很容易解码的形式表示的。实际上，密码是以明文形式传输的，任何人都可以读取并将其捕获。虽然 Base-64 编码通过隐藏用户名和密码，致使友好的用户不太可能在进行网络观测时无意中看到密码，但 Base-64 编码的用户名和密码可以很轻易地通过反向编码过程进行解码，甚至可以用纸笔在几秒钟内手工对其进行解码！所以经过 Base-64 编码的密码实际上就是“明文”传送的。如果有动机的第三方用户有可能会去拦截基本认证发送的用户名和密码，就要通过 SSL 加密信道发送所有的 HTTP 事务，或者使用更安全的认证协议，比如摘要认证。

283

(2) 即使密码是以更难解码的方式加密的，第三方用户仍然可以捕获被修改过的用户名和密码，并将修改过的用户名和密码一次一次地重放给原始服务器，以获得对服务器的访问权。没有什么措施可用来防止这些重放攻击。

(3) 即使将基本认证用于一些不太重要的应用程序，比如公司内部网络的访问控制或个性化内容的访问，一些不良习惯也会让它变得很危险。很多用户由于受不了大量密码保护的服务，会在这些服务间使用相同的用户名和密码。比如说，某个狡猾的恶徒会从免费的因特网邮件网站捕获明文形式的用户名和密码，然后会发现用同样的用户名和密码还可以访问重要的在线银行网站！

(4) 基本认证没有提供任何针对代理和作为中间人的中间节点的防护措施，它们没有修改认证首部，但却修改了报文的其余部分，这样就严重地改变了事务的本质。

(5) 假冒服务器很容易骗过基本认证。如果在用户实际连接到一台恶意服务器或网关的时候，能够让用户相信他连接的是一个受基本认证保护的合法主机，攻击者就可以请求用户输入密码，将其存储起来以备未来使用，然后捏造一条错误信息传送给用户。

这一切说明，在友好的环境，或者说是希望有隐私保护但隐私保护并不十分必要的环境中，可以通过基本认证来提供便捷的文档个性化服务或访问控制保护。通过这种方式，可以用基本认证来防止一些好奇的用户无意中或不小心对文档进行访问。[1]

比如，在一个公司内部，产品管理可能要对未来的产品计划进行密码保护，以防止信息的过早发布。对一般用户而言，基本认证就足以让他们感到不便而不会再去访问这些数据了。[2] 同样，你可能会用密码来保护那些并非高度机密的，或者没什么信息价值的私人照片或私有站点，这些信息确实和其他人也没什么关系。

将基本认证与加密数据传输（比如 SSL）配合使用，向恶意用户隐藏用户名和密码，会使基本认证变得更加安全。这是一种常用的技巧。

我们会在第 14 章讨论安全加密技术。下一章将介绍更复杂的 HTTP 认证协议——摘要认证，摘要认证具有比基本认证更强的安全特性。 284

12.4 更多信息

更多与基本认证和 LDAP 有关的信息，请参见以下资源。

- http://www.ietf.org/rfc/rfc2617.txt
  RFC 2617，“HTTP Authentication：Basic and Digest Access Authentication.”（“HTTP 认证：基本和摘要访问认证”）

- http://www.ietf.org/rfc/rfc2616.txt 285
  RFC 2616，“Hypertext Transfer Protocol-HTTP/1.1.”（“超文本传输协议——HTTP/1.1”。）

注 1：小心，基本认证中使用的用户名和密码要有别于你在更安全的系统中所使用的密码，否则恶意用户就可以用它们来攻破你的安全账户了！

注 2：尽管不是非常安全，但公司内部的员工通常也没有太大的动力去恶意捕获这些密码。这也说明，公司确实会有间谍，也确实会有不满，想要报复的员工，所以，明智的做法是对一旦被恶意获取就会造成很大损害的数据应用更安全的策略。