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！