

13.3.2 摘要认证首部

基本认证和摘要认证协议都包含了 WWW-Authenticate 首部承载的授权质询、Authorization 首部承载的授权响应。摘要认证还添加了可选的 Authorization-Info 首部, 这个首部是在成功认证之后发送的, 用于实现三步握手机制, 并传送下一个随机数。表 13-8 给出了基本认证和摘要认证的首部。

表13-8 HTTP认证首部

阶段	基 本	摘 要
质询	WWW-Authenticate: Basic realm="<realm-value>"	WWW-Authenticate: Digest realm="<realm-value>" nonce="<nonce-value>" [domain="<list-of-URIs>"] [opaque="<opaque-token-value>"] [stale="<true-or-false>"] [algorithm="<digest-algorithm>"] [qop="<list-of-qop-values>"] [<extension-directive>]
响应	Authorization: Basic <base64 (user:pass)>	Authorization: Digest username="<username>" realm="<realm-value>" nonce="<nonce-value>" uri="<request-uri>" response="<32-hex-digit-digest>" [algorithm="<digest-algorithm>"] [opaque="<opaque-token-value>"] [cnonce="<nonce-value>"] [qop="<qop-value>"] [nc="<8-hex-digit-nonce-count>"] [<extension-directive>]
Info	n/a	Authentication-Info: nextnonce="<nonce-value>" [qop="<list-of-qop-values>"] [rspauth="<hex-digest>"] [cnonce="<nonce-value>"] [nc="<8-hex-digit-nonce-count>"]

摘要认证首部要复杂得多。详细介绍参见附录 F。

13.4 应该考虑的实际问题

使用摘要认证时需要考虑几件事情。本节讨论了其中一些问题。

300