13.4.1 多重质询

服务器可以对某个资源发起多重质询。比如，如果服务器不了解客户端的能力，就可以既提供基本认证质询，又提供摘要认证质询。客户端面对多重质询时，必须以它所支持的最强的质询机制来应答。

质询自身可能会包含由逗号分隔的认证参数列表。如果 WWW-Authenticate 或 Proxy-Authenticate 首部包含了多个质询，或者提供了多个 WWW-Authenticate 首部，用户 Agent 代理在解析 WWW-Authenticate 或 Proxy-Authenticate 首部字段值时就要特别小心。注意，很多浏览器只支持基本认证，要求这是提交给它的第一种认证机制。

在提供了认证选项范围的情况下，安全问题上就会存在明显的“最薄弱环节”。只有当基本认证是最低可接受认证方式时，服务器才应该包含它，而且管理员还应该警告用户，即使运行了不同层次安全措施，系统间使用相同密码也存在一定危险性。

13.4.2 差错处理

在摘要认证中，如果某个指令或其值使用不当，或者缺少某个必要指令，就应该使用响应 400 Bad Request。

如果请求的摘要不匹配，就应该记录一次登录失败。某客户端连续多次失败可能说明有攻击者正在猜测密码。

认证服务器一定要确保 URI 指令指定的资源与请求行中指定的资源相同。如果不同，服务器就应该返回 400 Bad Request 错误。（这可能是一种攻击的迹象，因此服务器设计者可能会考虑将此类错误记录下来。）这个字段包含的内容与请求 URL 中的内容是重复的，用来应对中间代理可能对客户端请求进行的修改。这个经过修改（但估计语义是等价的）的请求计算后得到的摘要可能会与客户端计算出的摘要有所不同。

13.4.3 保护空间

域值，与被访问服务器的标准根 URL 结合在一起，定义了保护空间。

通过域可以将服务器上的受保护资源划分为一组保护空间，每个空间都有自己的认
301 证机制和 / 或授权数据库。域值是一个字符串，通常由原始服务器分配，可能会有认证方案特有的附加语义。注意，可能会有多个授权方案相同，而域不同的质询。

保护空间确定了可以自动应用证书的区域。如果前面的某条请求已被授权，在一段