









TRACE

客户端发起一个请求时，这个请求可能要穿过防火墙、代理、网关或其他一些应用程序，每个中间节点都可能会修改原始的 HTTP 请求，TRACE 方法允许客户端在最终请求发送给服务器时，看看它变成了什么样子。该命令主要用于 HTTP 通信的诊断和调试。

TRACE 请求会在目标服务器端发起一个「环回」诊断，行程最后一站的服务器会返回一条 TRACE 响应，并在响应主体中携带它收到的原始请求报文，这样，客户端就可以查看在所有中间 HTTP 应用程序组成的请求/响应链上，原始报文是否以及如何被修改过。

发送 TRACE 请求时，可以在 Max-Forwards 首部字段中填入数值，每经过一个服务器/中间节点该数值就会减1，当数值刚好减到0时，就停止继续传输，最后接收到请求的服务器/节点则返回状态码 200 OK 的响应（不管是否到达最终目标服务器都会返回，不会再继续传递请求）。

但是，TRACE 方法并不怎么常用，再加上容易引发 XST（Cross-Site Tracing，跨站追踪）攻击，就更不会用到了。

