Usage: curl [options...] <url>

Options: (H) means HTTP/HTTPS only, (F) means FTP only

--anyauth 选择“所有”认证方法（h）

-a, --append 追加到目标文件时，上传（F / SFTP）

--basic 使用HTTP基本认证（H）

--cacert FILE CA证书验证点对（SSL）

--capath DIR CA目录验证点对（SSL）

-E, --cert CERT[:PASSWD] 客户端证书文件和密码（SSL）

--cert-status 验证服务器证书的状态（SSL）

--cert-type TYPE 证书文件类型（德/ PEM /英文）（SSL）

--ciphers LIST 使用SSL加密（SSL）

--compressed 请求响应（使用deflate压缩或压缩）

-K, --config FILE 从文件读取配置

--connect-timeout SECONDS 允许连接的最大时间

--connect-to HOST1:PORT1:HOST2:PORT2 连接到主机（网络级）

-C, --continue-at OFFSET 恢复传送偏移

-b, --cookie STRING/FILE 从字符串/文件（h）读取饼干

-c, --cookie-jar FILE 操作后将cookie写入文件（h）

--create-dirs 创建必要的本地目录层次

--crlf 如果在上传时转换

--crlfile FILE 从给定的文件获得PEM格式CRL列表

-d, --data DATA HTTP POST data (H)

--data-raw DATA HTTP POST data, '@' allowed (H)

--data-ascii DATA HTTP POST ASCII数据（H）

--data-binary DATA HTTP POST binary data (H)

--data-urlencode DATA HTTP POST data url encoded (H)

--delegation STRING GSS-API delegation permission

--digest Use HTTP Digest Authentication (H)

--disable-eprt 禁止使用EPRT或LPRT（F）

--disable-epsv Inhibit using EPSV (F)

--dns-servers DNS server addrs to use: 1.1.1.1;2.2.2.2

--dns-interface 接口使用DNS请求

--dns-ipv4-addr IPv4地址使用的DNS请求，点符号

--dns-ipv6-addr IPv6地址使用的DNS请求，点符号

-D, --dump-header FILE Write the headers to FILE

--egd-file FILE EGD socket path for random data (SSL)

--engine ENGINE Crypto engine (use "--engine list" for list) (SSL)

--expect100-timeout SECONDS How long to wait for 100-continue (H)

-f, --fail Fail silently (no output at all) on HTTP errors (H)

--false-start Enable TLS False Start.

-F, --form CONTENT Specify HTTP multipart POST data (H)

--form-string STRING Specify HTTP multipart POST data (H)

--ftp-account DATA Account data string (F)

--ftp-alternative-to-user COMMAND String to replace "USER [name]" (F)

--ftp-create-dirs 创建远程目录不存在(F)

--ftp-method [MULTICWD/NOCWD/SINGLECWD] Control CWD usage (F)

--ftp-pasv 使用 PASV/EPSV 而不是 PORT (F)

-P, --ftp-port ADR 用口代替PASV地址（F）

--ftp-skip-pasv-ip Skip the IP address for PASV (F)

--ftp-pret 发送预前PASV（为drftpd）（F）

--ftp-ssl-ccc 验证后发送CCC（F）

--ftp-ssl-ccc-mode ACTIVE/PASSIVE Set CCC mode (F)

--ftp-ssl-control Require SSL/TLS for FTP login, clear for transfer (F)

-G, --get Send the -d data with a HTTP GET (H)

-g, --globoff Disable URL sequences and ranges using {} and []

-H, --header LINE 将自定义头文件传递给服务器（h）

-I, --head Show document info only

-h, --help 这帮助文本

--hostpubmd5 MD5 十六进制编码的MD5字符串主机公钥。（SSH）

-0, --http1.0 Use HTTP 1.0 (H)

--http1.1 Use HTTP 1.1 (H)

--http2 Use HTTP 2 (H)

--http2-prior-knowledge 2不使用HTTP HTTP / 1.1升级（H）

--ignore-content-length 忽略HTTP内容长度标头

-i, --include 包括在输出（H / F）的协议头

-k, --insecure Allow connections to SSL sites without certs (H)

--interface INTERFACE Use network INTERFACE (or address)

-4, --ipv4 Resolve name to IPv4 address

-6, --ipv6 Resolve name to IPv6 address

-j, --junk-session-cookies 忽略会话cookie从文件中读取（h）

--keepalive-time SECONDS 等待几秒钟之间发生了

--key KEY Private key file name (SSL/SSH)

--key-type TYPE Private key file type (DER/PEM/ENG) (SSL)

--krb LEVEL Enable Kerberos with security LEVEL (F)

--libcurl FILE 把这条命令的libcurl等价代码

--limit-rate RATE 极限传输速率

-l, --list-only List only mode (F/POP3)

--local-port RANGE 强制使用本地端口号的范围

-L, --location Follow redirects (H)

--location-trusted Like '--location', and send auth to other hosts (H)

--login-options OPTIONS 服务器登录选项 (IMAP, POP3, SMTP)

-M, --manual 显示完整的手册

--mail-from FROM 从这个地址的邮件（SMTP）

--mail-rcpt TO 对这些地址的电子邮件（SMTP）

--mail-auth AUTH 原来的电子邮件地址（SMTP）创始人

--max-filesize BYTES 最大文件大小（h / F）

--max-redirs NUM 重定向允许的最大数量（H）

-m, --max-time SECONDS 允许传输的最大时间

--metalink 给定的URL上的XML文件的过程

--negotiate 使用HTTP进行谈判（SPNEGO）认证（H）

-n, --netrc 必须阅读。用户名和密码的Netrc

--netrc-optional 使用.netrc文件或URL重写N；

--netrc-file FILE Specify FILE for netrc

-:, --next 允许以下URL使用单独的选项集

--no-alpn 禁用alpn TLS扩展（H）

-N, --no-buffer 禁用输出流的缓冲区

--no-keepalive 禁用它使用的连接

--no-npn Disable the NPN TLS extension (H)

--no-sessionid Disable SSL session-ID reusing (SSL)

--noproxy List of hosts which do not use proxy

--ntlm Use HTTP NTLM authentication (H)

--ntlm-wb Use HTTP NTLM authentication with winbind (H)

--oauth2-bearer TOKEN OAuth 2 Bearer Token (IMAP, POP3, SMTP)

-o, --output FILE Write to FILE instead of stdout

--pass PASS Pass phrase for the private key (SSL/SSH)

--path-as-is Do not squash .. sequences in URL path

--pinnedpubkey FILE/HASHES Public key to verify peer against (SSL)

--post301 不要切换后得到一个301重定向（H）

--post302 不要切换后得到一个302重定向（H）

--post303 不要切换后得到一个303重定向（H）

-#, --progress-bar Display transfer progress as a progress bar

--proto PROTOCOLS Enable/disable PROTOCOLS

--proto-default PROTOCOL Use PROTOCOL for any URL missing a scheme

--proto-redir PROTOCOLS Enable/disable PROTOCOLS on redirect

-x, --proxy [PROTOCOL://]HOST[:PORT] Use proxy on given port

--proxy-anyauth Pick "any" proxy authentication method (H)

--proxy-basic Use Basic authentication on the proxy (H)

--proxy-digest Use Digest authentication on the proxy (H)

--proxy-negotiate 使用HTTP进行谈判（SPNEGO）在代理认证（H）

--proxy-ntlm Use NTLM authentication on the proxy (H)

--proxy-header LINE Pass custom header LINE to proxy (H)

--proxy-service-name NAME SPNEGO proxy service name

--service-name NAME SPNEGO服务名称

-U, --proxy-user USER[:PASSWORD] Proxy user and password

--proxy1.0 HOST[:PORT] Use HTTP/1.0 proxy on given port

-p, --proxytunnel 通过一个HTTP代理隧道操作（使用连接）

--pubkey KEY Public key file name (SSH)

-Q, --quote CMD 传输前将命令发送到服务器 (F/SFTP)

--random-file FILE 读取随机数据的文件 (SSL)

-r, --range RANGE 只检索字节数 RANGE

--raw Do HTTP "raw"; no transfer decoding (H)

-e, --referer Referer URL (H)

-J, --remote-header-name Use the header-provided filename (H)

-O, --remote-name Write output to a file named as the remote file

--remote-name-all Use the remote file name for all URLs

-R, --remote-time Set the remote file's time on the local output

-X, --request COMMAND Specify request command to use

--resolve HOST:PORT:ADDRESS Force resolve of HOST:PORT to ADDRESS

--retry NUM 重试请求Num次如果瞬态问题的发生

--retry-delay SECONDS Wait SECONDS between retries

--retry-max-time SECONDS Retry only within this period

--sasl-ir 使SASL认证的初始响应

-S, --show-error Show error. With -s, make curl show errors when they occur

-s, --silent Silent mode (don't output anything)

--socks4 HOST[:PORT] SOCKS4 proxy on given host + port

--socks4a HOST[:PORT] SOCKS4a proxy on given host + port

--socks5 HOST[:PORT] SOCKS5 proxy on given host + port

--socks5-hostname HOST[:PORT] SOCKS5代理，通过代理主机名

--socks5-gssapi-service NAME SOCKS5 proxy service name for GSS-API

--socks5-gssapi-nec 与NEC Socks5服务器兼容性

-Y, --speed-limit RATE 停止以下速度时间秒率传输

-y, --speed-time SECONDS Trigger 'speed-limit' abort after SECONDS (default: 30)

--ssl Try SSL/TLS (FTP, IMAP, POP3, SMTP)

--ssl-reqd Require SSL/TLS (FTP, IMAP, POP3, SMTP)

-2, --sslv2 Use SSLv2 (SSL)

-3, --sslv3 Use SSLv3 (SSL)

--ssl-allow-beast 允许的安全漏洞，提高互操作 (SSL)

--ssl-no-revoke 证书吊销检查可 (WinSSL)

--stderr FILE Where to redirect stderr (use "-" for stdout)

--tcp-nodelay Use the TCP\_NODELAY option

--tcp-fastopen Use TCP Fast Open

-t, --telnet-option OPT=VAL Set telnet option

--tftp-blksize VALUE Set TFTP BLKSIZE option (must be >512)

--tftp-no-options 不要发送TFTP OPTIONS请求

-z, --time-cond TIME Transfer based on a time condition

-1, --tlsv1 Use >= TLSv1 (SSL)

--tlsv1.0 Use TLSv1.0 (SSL)

--tlsv1.1 Use TLSv1.1 (SSL)

--tlsv1.2 Use TLSv1.2 (SSL)

--trace FILE 编写一个调试跟踪到文件

--trace-ascii FILE Like --trace, but without hex output

--trace-time 添加时间戳迹/详细输出

--tr-encoding 请求压缩传输编码（h）

-T, --upload-file FILE 传输文件到目的地

--url URL URL to work with

-B, --use-ascii Use ASCII/text transfer

-u, --user USER[:PASSWORD] Server user and password

--tlsuser USER TLS username

--tlspassword STRING TLS password

--tlsauthtype STRING TLS authentication type (default: SRP)

--unix-socket FILE 通过这个Unix域套接字连接

-A, --user-agent STRING 将用户代理字符串发送到服务器（h）

-v, --verbose Make the operation more talkative

-V, --version 显示版本号并退出

-w, --write-out FORMAT 完成后使用输出格式

--xattr 在扩展文件属性中存储元数据

-q, --disable 禁用。curlrc（必须是第一个参数）