# Limiting Allowed Methods in HTTP Headers and Content

https://campus.barracuda.com/doc/4259882/

While GET and POST are the predominant methods used by web servers for information access,

HTTP allows several less known methods*:

- HEAD
- GET
- POST
- PUT
- DELETE
- TRACE
- OPTIONS
- CONNECT

*RFC 2616 describes the above HTTP methods in detail.

The OPTIONS command allows clients to determine which methods the web server supports. Some methods allow modification of stored files, stealing of user credentials, or bypassing environment level access control checks. URL protection allows an explicit way to specify allowed or disallowed methods in URL calls. Disallowing PUT, DELETE, and TRACE is recommended. The allowed request content-types also need to be carefully restricted to prevent similar security threats.