Helmet automatically sets a collection of HTTP security headers that harden your app. Some key ones:

- **X-Content-Type-Options: nosniff**
  Prevents browsers from MIME-sniffing responses away from declared types.

  Stops attacks like interpreting a .txt file as JavaScript.
- **X-DNS-Prefetch-Control**
  Controls DNS prefetching (reduces metadata leaks).
- **Strict-Transport-Security (HSTS)**
  Enforces HTTPS connections (only when serving over HTTPS).
- **X-Frame-Options / frame-ancestors (Clickjacking defense)**
  Prevents your site from being embedded in an iframe unless you allow it.
- **Referrer-Policy**
  Controls how much referrer info browsers send to other sites.
- **Cross-Origin-Embedder/Opener/Resource-Policy**
  Mitigates certain cross-origin leaks and side-channel attacks.

Benefit: These are widely recognized as "secure defaults." They reduce your exposure to common browser attack vectors without breaking normal app functionality.