Do/Don't with passwords

- On the client side, do send passwords either:
  - ✓ in the headers (automatic with basic authentication) or
  - ✓ in the body (POST request with session authentication)
  - ◉ never in the URL
- On the server, do store passwords as
  - ✓ salted hash passwords only
  - ◉ never in clear or non-salted hash

Token-based Authentication